WBASNY

The Women's Bar Association of the State of New York

presents

Convention 2026
Continuing Legal Education Series

Navigating the Aftermath: Liabilities for Law Firms After a Data Breach

May 30, 2026
9:45 am - 10:45 am

Presenter: Nicole E. Osborne, Esq.

RUSKIN MOSCOU FALTISCHEK P.C.
Smart Counsel. Straight Talk.

NICOLE E. OSBORNE / PARTNER

NOSBORNE@RMFPC.COM
O: 516.663.6687 F:516.663.6887

EDUCATION

- Hofstra Law School (J.D., magna cum laude, 2016)
- SUNY Albany (B.A., magna cum laude, 2013)

PRACTICE AREAS

- Health Law
- Blockchain Technology and Digital Asset
- Commercial Litigation
- Crisis Management
- Cybersecurity and Data Privacy
- Employment
- White Collar Crime & Investigations
- Insurance & Reinsurance Litigation, Dispute Resolution, Transactions, and Regulatory Problem Solving

Nicole E. Osborne is a Partner at Ruskin Moscou Faltischek, P.C., where she is a member of the firm's Commercial Litigation and Health Law Departments. Nicole also serves as Co-Chair of the firm's Cybersecurity and Data Privacy Practice Group and is a member of the Employment, White Collar Crime and Investigations, Insurance & Reinsurance Litigation, Dispute Resolution, Transactions, and Regulatory Problem Solving and Crisis Management Practice Groups.

Nicole has addressed numerous cybersecurity matters, navigating the complex intersection of law and technology. Nicole assists companies in managing and responding to data privacy and security incidents and breaches of all sizes, across various industries. These incidents include business email compromise, ransomware, as well as other network intrusions. During breach management, she works closely with a client's internal/external IT team and third parties such as forensic investigators, public relations consultants, and cybersecurity insurance companies. Nicole manages all parts of an incident, including identification and investigation of an incident, through reporting of an incident in accordance with state, federal, and international law, as well as industry specific guidelines and regulations. Nicole likewise assists in defending enforcement proceedings, government investigations and private party civil actions following a cybersecurity incident. In addition to her data breach incident response work, Nicole advises businesses based on their level of cyberpreparedness and conducts risk and threat assessments, incident response planning and privacy impact assessments. Nicole also assists companies in complying with the growing web of state, federal, and international data privacy laws and regulations.

Nicole also has experience in a variety of matters involving the employer-employee relationship, including wage and hour compliance and investigations, employment discrimination prevention, employee handbooks and trainings, administrative proceedings, disability accommodations and leave related issues. Nicole has defended claims in administrative and court proceedings relating to sexual harassment, age, race, and national origin discrimination, restrictive covenant violations, confidentiality violations, and trade secret theft for various clients, both large and small.

Nicole has experience as a commercial litigator, in federal and state courts, representing individuals and companies in a wide area of complex commercial litigation – including matters involving employer/employee disputes, trade secret misappropriation, business torts, breach of contract and shareholder disputes, professional liability (including claims related to Employment Practices Liability and Directors and Offices Insurance Policies), and Article 78 proceedings.

Nicole was named in Long Island Business News in its Ones to Watch in 2019, New York Metropolitan Area Super Lawyer Rising Star in 2021, 2022, 2023, 2024, and 2025, and is also included in the 2026 edition of the Best Lawyers: Ones to Watch™ in America for her work in Labor and Employment Law - Management.

Nicole is also an Adjunct Professor at Hofstra University's Maurice A. Deane School of Law, where she teaches courses on the Fundamentals of the Law of Cybersecurity. During law school Nicole was Notes Editor of the Hofstra Law Review, was an active competitive member in Hofstra's Moot Court Board and a member of the Hofstra Trial Advocacy Association.

Nicole is a member of the Nassau County Bar Association, where she serves as Chair of the Cyber Law Committee. Nicole is also a member of the American Bar Association, the Suffolk County Women's Bar Association, and Moxxie Network.

Presentations

- Ruskin Moscou Faltischek and Flushing Bank – Cybersecurity Fraud Seminar – 2023
- Suffolk County Women's Bar Association – Cybersecurity CLE – 2023
- Hofstra Law School – Cybersecurity Webinar – 2023
- Thomson Reuters, Long Island Emerging Tech Event – 2019
- CPD, Cyber Security Seminar – 2019
- Skytop Strategies, Cyber Risk Governance Conference – 2018
- Long Island Cybersecurity Conference – 2017
- LIBN Cybersecurity Roundtable – 2017
- Institute of Internal Auditors Fraud Conference – 2016

Publications

- Long Island Employers Face Rising Wage and Hour Risks in 2026 (Articles, Employment)
- New York Employment Law Changes: What Long Island Businesses Need to Know for 2026 (Alerts, Employment)
- New York City Expands Safe and Sick Time Leave (Alerts, Employments)
- Twenty-Six Ruskin Moscou Faltischek Attorneys Named As New York Metropolitan Area Super Lawyers For 2025 (Press Release)
- Ten RMF Attorneys Recognized in 2026 Edition of The Best Lawyers in America (Press Releases)
- From Catwalk to Contract: Navigating the New York Fashion Workers Act (Alerts, Employment)
- Ruskin Moscou Faltischek, P.C. Partner Nicole E. Osborne Named Co-Chair of Firm's Cybersecurity and Data Privacy Practice Group (Press Release)
- The End of an Era: New York Sunsets COVID-19 Paid Leave (Alerts, Employment)

- Ruskin Moscou Faltischek Partner Nicole E. Osborne Appointed Chair of Nassau County Bar Association's Cyber Law Committee (Press Release)
- RMF Attorney Nicole E. Osborne Presented Ruskin Moscou Faltischek, P.C. Award for Outstanding Appellate Advocacy at the Maurice A. Deane School of Law at Hofstra University (Press Release)
- 23andMyData: Data Privacy Concerns Amid Biotech Company's Bankruptcy (Alerts, Data Privacy & Bankruptcy Law)
- Smart Glasses, Smarter HR Policies: Navigating Recording Devices in Today's Workplace (Alerts, Employment)
- New Year – New Standard: New York Amends Data Breach Notification Law (Alerts, Cybersecurity and Data Privacy)
- Thirty-Three Ruskin Moscou Faltischek Attorneys Named As New York Metropolitan Area Super Lawyers For 2024 (Press Release)
- RMF Attorneys Recognized By Best Lawyers® For 2025 (Press Release)
- New York State 2024-2025 Budget: Updates to Employment Law (Alerts, Employment)
- RMF Attorney Nicole E. Osborne To Present Ruskin Moscou Faltischek, P.C. Award for Outstanding Appellate Advocacy At The Maurice A. Dean School of Law At Hofstra University (Press Release)
- FTC Final Rule: Nationwide Ban of Non-Compete Agreements (Alerts, Employment)
- RMF Attorney Nicole E. Osborne Honored at the Girls Inc. Champion for Girls Breakfast (Press Release)
- New Jersey Enacts Consumer Privacy Law (Alerts, Cybersecurity and Data Privacy)
- Governor Hochul Vetoes Non-Compete Ban (Alerts, Employment)
- PODCAST: A Discussion with Nicole E. Osborne on Data Breaches and her Role as a Cybersecurity Attorney (Media Coverage)
- New Law Demands Prompt Notice Of Unemployment Benefits Eligibility (Alerts, Employment)
- Thirty-One Ruskin Moscou Faltischek Attorneys Named As New York Metropolitan Area Super Lawyers For 2023 (Press Release)
- New York State's Pay Transparency Law Goes into Effect on September 17, 2023 (Alerts, Employment)
- New Form I-9 Requirements: Employers Must Comply by August 30th (Alerts, Employment)
- RMF Attorneys Steven J. Kuperschmid and Nicole E. Osborne Named Adjunct Professors of Maurice A. Deane School of Law at Hofstra University (Announcement)
- Four Days to Report: The SEC Tightens Cybersecurity Reporting Requirements for Public Companies (Alerts, Cybersecurity)
- Is It The Beginning of the End for Non-Compete Agreements in New York? (Alerts, Employment)
- THE PREGNANT WORKERS FAIRNESS ACT – TIME TO UPDATE YOUR EEOC POSTER (Alerts, Employment)
- NEW YORK STATE'S UPDATED SEXUAL HARASSMENT PREVENTION POLICY REQUIREMENTS (Alerts, Employment)
- Employer and Employee Rights Since the Passage of MRTA (Cannabiz New York Podcast, May 2023)
- 90.3 WHPC Law You Should Know – "Employment and Labor Laws" with RMF Attorneys Rachel Morgenstern and Nicole Osborne (Media Coverage)
- The SEC Proposes Enhancements To Regulation S-P (Alerts, Cybersecurity)
- Ruskin Moscou Faltischek Forms Blockchain Technology and Digital Asset Practice Group (Press Releases)
- Ruskin Moscou Faltischek and Flushing Bank To Present 2023 Cybersecurity Fraud Seminar (Press Releases)

- RMF Attorney Nicole Osborne to Present Suffolk County Women's Bar Association CLE Program (Announcement)
- Heightened Cybersecurity Standards and Risks: Transacting with the Federal Government (Alerts, Cybersecurity)
- RMF Attorney Nicole Osborne Co-Presenting Cybersecurity Webinar Titled "Best Practices for Professionals (Non-Lawyers) and Business Owners" (Announcement)
- Employment Law Update - October 2022 (Alerts, Employment)
- Thirty-One Ruskin Moscou Faltischek Attorneys Named As New York Metropolitan Area Super Lawyers For 2022 (Press Releases)
- Covid-19 Update (Alerts, Employment)
- RMF Attorney Nicole Osborne Named Adjunct Professor of Maurice A. Deane School of Law at Hofstra University (Press Releases)
- NYS HERO Act Extended Once Again (Alerts, Employment)
- New York Ends Indoor Mask Mandate For Businesses (Alerts, Employment)
- Supreme Court Blocks The Large Employer Vaccine Mandate (Alerts, Employment)
- New York Updates Quarantine and Isolation Guidance (Alerts, Employment)
- Stay in Enforcement Lifted: Large Employers Must Prepare for OSHA Vaccine Mandate (Alerts, Employment)
- New York City Issues Vaccine Mandate Guidance (Alerts, Employment)
- New COVID-19 Vaccine or Masking Requirements for New York Businesses (Alerts, Employment)
- NYC Employers Must Prepare For Vaccine Mandate (Alerts, Employment)
- OSHA Halts Implementation And Enforcement Of Vaccine Mandate For Large Employers (Alerts, Employment)
- Vaccine Mandate: Coming Soon To A Large Employer Near You (Alerts, Employment)
- Twenty-Five Ruskin Moscou Faltischek Attorneys Named As New York Metropolitan Area Super Lawyers For 2021 (Press Releases)
- HERO ACT: COVID-19 NOW REQUIRES HERO ACT PLANS TO BE ACTIVATED (Alerts, Employment)
- Important Upcoming Employment Deadlines: NYS HERO Act and COBRA Subsidy Final Notice (Alerts, Employment)
- RMF Attorney Nicole Osborne Named Adjunct Professor of Maurice A. Deane School of Law at Hofstra University (Announcements)
- HERO Act Guidance Published By NY Department of Labor (Alerts, Employment)
- New York Updates Restrictions For Office Spaces (Alerts, Employment)
- May 31 Notice Deadline Approaching For COBRA Subsidy (Alerts, Employment)
- New York Increases Capacity for Office Spaces (Alerts, Employment)
- Employees Are Entitled To Paid Leave Under NY Law To Receive COVID-19 Vaccine (Alerts, Employment)
- New York Provides New Guidance Regarding Use Of NYS COVID-19 Sick Leave (Alerts, Employment)
- Additional COVID-19 Relief Legislation (Alerts, Employment)
- Updates To New York's Travel Advisory For Out-Of-State Travel (Alerts, Employment)
- New York State Sick Leave Law Takes Effect (Alerts, Employment)
- New School Year, New Questions: Employee Leave Rights Under The FFCRA (Alerts, Employment)

- RMF Attorney Nicole Della Ragione To Present MCLE Webinar On Cybersecurity Ethics For The Trusts & Estates Practitioner (Announcements)
- COVID-19 Antibody Tests and Returning to Work (Alerts, Employment)
- Back to Work Planning and New Guidance from the Department of the Treasury Regarding PPP Loan Forgiveness (Alerts, Employment)
- Part II-Restructuring and Bankruptcy Options to Save your Company from the Brink: Large Company Solutions for Small and Mid-Market Enterprises (Alerts, Financial Services Banking and Bankruptcy)
- Small Businesses and the Families First Coronavirus Response Act (Alerts, Employment)
- COVID-19 and WORKPLACE IMPACT FAQS (Alerts, Employment)
- UPDATED: Coronavirus Legal Update- NYS WORKFORCE REDUCTION ORDER (Employment)
- Coronavirus Legal Update- NYS WORKFORCE REDUCTION ORDER (Employment)
- There are resources available to help plan for a crisis. (Cybersecurity)
- In Uniondale, A Law Firm Adds Practice Group (Insurance & Insurance Litigation, Insurance & Insurance Litigation, Press Releases)
- Ruskin Moscou Faltischek P.C. Establishes Insurance & Insurance Litigation Practice Group, With Michael D. Brown to Chair (Insurance & Insurance Litigation, Insurance & Insurance Litigation, Press Releases)
- Nicole Della Ragione to Speak at Nassau County Bar Association Labor and Employment Committee (Announcements)
- Opinion: Beware – SHIELD law to overhaul cyber security reporting (Cybersecurity)
- RMF Associate Nicole Della Ragione Speaks at Event Covering Cybersecurity and the Risks Business Owners Encounter. (Press Releases)
- RMF Attorney Nicole Della Ragione Speaks at Event Covering Cybersecurity and the Risks Business Owners Encounter (Press Releases)
- Ruskin Moscou Faltischek Associate Nicole Della Ragione Speaks at Event Covering the Cybersecurity Legal Needs for Today's Emerging Technologies (Cybersecurity, Press Releases)
- Ruskin Moscou Faltischek Attorney Nicole Della Ragione Named to Board of Girls Inc. of Long Island (Press Releases)
- New Year and New Obligations: What Employers Need to Know about 2019 (Employment)
- EU's data protection regulation could impact LI firms (International Practice Group)
- New Sexual Harassment Laws Affecting New York State Employers (Alerts, Employment)
- CYBER RISK- Next Steps for Evolving Security (Cybersecurity)
- Regulatory Gap: Cybersecurity at K-12 Schools (Cybersecurity)

- The C-Suite must become involved in cybersecurity (Cybersecurity)
- Lawyers Say More Regulation Is Likely to Follow Equifax Breach (Cybersecurity)
- Equifax Breach and Protecting Yourself in the Aftermath (Cybersecurity)
- Ransomware Mitigation Tips and Steps to Increase Security (Cybersecurity)
- Increased Enforcement of HIPAA Security Rules (Cybersecurity)
- Major Expansion of Cybersecurity and Data Privacy Practice Group at Ruskin Moscou Faltischek (Press Releases)
- Gone In 60 Milliseconds (Cybersecurity, Cybersecurity)
- Data Breaches and the Cost of Delay and Disorganization (Cybersecurity)
- Financial Services Industry in New York is About to be Pounded by Proposed New Cybersecurity Regulations (Cybersecurity, Cybersecurity)
- Ruskin Moscou Faltischek Presents Annual Award for Outstanding Appellate Advocacy at the Maurice A. Dean School of Law at Hofstra University (Press Releases)

Table of Contents

Letitia James
New York State Attorney General

Attorney General James Secures $200,000 from Law Firm for Failing to Protect New Yorkers' Personal Data

March 27, 2023

HPMB Law Firm Failed to Implement Data Security Measures to Protect New Yorkers' Health Information from Data Breaches

NEW YORK – New York Attorney General Letitia James secured $200,000 from the law firm, Heidell, Pittoni, Murphy & Bach LLP (HPMB) for failing to protect New Yorkers' personal and healthcare data. HPMB's poor data security measures made it vulnerable to a 2021 data breach that compromised the private information of approximately 114,000 patients, including more than 60,000 New Yorkers. The law firm represents New York City area hospitals and maintains sensitive private information from patients, including dates of birth, social security numbers, health insurance information, medical history, and/or health treatment information. HPMB's data security failures violated not only state law, but also HIPAA, which required HPMB to adhere to certain advanced data security practices. As a result of the agreement, HPMB must pay $200,000 in penalties to the state and strengthen its cybersecurity measures to protect consumers' personal and private health information.

"New Yorkers should not have to worry that their privacy is being violated and their sensitive information is being mishandled," said **Attorney General James**. "Confidential patient information should be treated with care and secured online to protect New Yorkers from identity theft and fraud. The institutions charged with protecting this information have a responsibility to get it right, and to keep authorities and New Yorkers informed about breaches. Companies can, and should, strengthen their data security measures to safeguard consumers' digital data, otherwise they can expect to hear from my office."

In November 2021, an attacker was able to exploit a vulnerability in HPMB's Microsoft Exchange email server to gain access to HPMB's systems. Patches for this vulnerability had been released by Microsoft several months earlier, but HPMB had not applied these patches in a timely manner, leaving this vulnerability exposed for potential exploitation. In December 2021, an attacker deployed malware on HPMB's systems which resulted in a disruption in HPMB's email system. In its subsequent investigation, HPMB found that tens of thousands of files had been potentially taken from HPMB's systems. An analysis of these files determined that electronic health information and/or private information — including names, dates of birth, social security numbers, and/or health data — of 114,979 individuals, including 61,438 New York residents, had likely been exposed as a result of the attack.

In May 2022, HPMB began notifying affected consumers whose personal information was compromised during the incident. The Office of the Attorney General determined that HPMB had failed to adopt reasonable practices to protect consumers' personal information in several areas. In particular, HPMB failed to adopt several measures required by HIPAA, which HPMB is covered by due to its business relationship with hospitals and hospital, including conducting regular risk assessments of its systems, encrypting the private information on its servers, and adopting appropriate data minimization practices.

As a result of today's agreement, HPMB must pay the state $200,000 in penalties. HPMB is also required to adopt measures to better protect the personal and private health information of its clients' patients going forward, including:

- Maintaining a comprehensive information security program that includes regular updates to keep pace with changes in technology and security threats and reporting security risks to the firm's leadership;

- Encrypting the private and health information it collects, uses, stores, and maintains;

- Implementing centralized logging and monitoring of network activity, including logs that are readily accessible for a period of at least 90 days and stored for at least one year from the date the activity was logged;

- Establishing a reasonable patch management program, including appropriate monitoring of required updates, supervision of the program, and training for

employees;

- Developing a penetration testing program that includes regular testing of HPMB's network security; and,

- Updating its data collection and retention practices, including only collecting data to the minimum extent necessary to perform legitimate business functions and permanently deleting all such data when there is no longer a reasonable business or legal purpose to retain such information.

This matter was handled by Assistant Attorney General Laura Mumm and Deputy Bureau Chief Clark Russell, with special assistance from Internet and Technology Analyst Nishaant Goswamy, of the Bureau of Internet and Technology, under the supervision of Bureau Chief Kim Berger. The Bureau of Internet and Technology is a part of the Division for Economic Justice, which is led by Chief Deputy Attorney General Chris D'Angelo and overseen by First Deputy Attorney General Jennifer Levy.

ATTORNEY GENERAL OF THE STATE OF NEW YORK
BUREAU OF INTERNET & TECHNOLOGY

In the Matter of

Assurance No. 23-011

Investigation by LETITIA JAMES,
Attorney General of the State of New York, of

Heidell, Pittoni, Murphy & Bach LLP,

Respondent.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York (the "OAG") commenced an investigation pursuant to Executive Law § 63(12) and General Business Law ("GBL") §§ 899-aa and 899-bb as well as the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226 ("HIPAA") into a data security incident at Heidell, Pittoni, Murphy & Bach LLP ("HPMB" or "Respondent") (together with the OAG, the "Parties"). This Assurance of Discontinuance ("Assurance") contains the findings of the OAG's investigation and the relief agreed to by the OAG and HPMB.

FINDINGS OF OAG

1. Respondent, HPMB, is a law firm based in New York, NY, that, among other things, represents hospitals and hospital networks in litigation. In connection with its role in representing hospitals and hospital networks in litigation, HPMB receives and maintains electronic protected health information ("ePHI") and other private information related to its clients' patients. As a result, HPMB was, at all relevant times, classified as a "Business Associate" under HIPAA and related regulations. *See* 45 C.F.R. §§ 160.103.

The 2021 Data Breach

2. On or about November 22, 2021, an attacker exploited vulnerabilities in HPMB's Hybrid Exchange Management Server to gain access to HPMB's systems. The vulnerabilities the attacker exploited had been identified by Microsoft several months earlier—in April and May 2021—and Microsoft had released patches for the software vulnerabilities around the same time. HPMB did not timely apply the patch for these vulnerabilities, rendering the server vulnerable to the attack.

3. On or around December 25, 2021, the attacker deployed the Lockbit ransomware variant on HPMB's systems using PSExec. HPMB personnel were alerted to this intrusion on December 25, when HPMB received an internal alert relating to syncing errors. HPMB subsequently identified encryption on its network consistent with a ransomware attack.

4. In response to the attack, HPMB disconnected its servers from the internet and hired a forensic cybersecurity firm to conduct a forensic investigation. The forensic firm engaged in discussions with the attackers, who provided the forensic firm a list of tens of thousands of files the attackers claimed to have exfiltrated from HPMB's systems. This list included legal pleadings, patient lists, and medical records that HPMB had in its possession in connection with litigation matters. The forensic firm identified evidence that the listed files had been staged and exfiltrated from HPMB's systems.

5. HPMB subsequently paid $100,000 in ransom in exchange for the return and promised deletion of the exfiltrated data but was not provided evidence the data was deleted.

6. With the aid of a contractor, HPMB engaged in an analysis of the files exfiltrated from its systems. As a result of this analysis, HPMB determined that the ePHI and/or private information—including names, dates of birth, social security numbers, and/or health data—of

114,979 individuals, including 61,438 New York residents, had likely been exposed as a result of the attack. Of this number, 846 New Yorkers had their social security numbers exposed, 23 New Yorkers had their driver's license numbers exposed, 13 New Yorkers had their other identification card details exposed, and 25 New Yorkers had their biometric data exposed.

7. On May 16, 2022, after HPMB's data-mining vendor had concluded its analysis of the exfiltrated files, Respondent began notifying affected individuals whose ePHI and private information had been exposed during the attack.

8. As a HIPAA Business Associate, HPMB must comply with the federal standards that govern the privacy and security of ePHI, as defined in 45 C.F.R. § 160.103—specifically, the HIPAA Privacy Rule and HIPAA Security Rule, 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A, C, and E.

9. In the course of its investigation of the 2021 Data Breach, the OAG determined that HPMB failed to comply with many of the standards and procedural specifications required by HIPAA's Privacy Rule and Security Rule including, *inter alia*, the following:

a. HPMB failed to ensure the confidentiality and integrity of all ePHI it creates, receives, maintains, or transmits, *see* 45 C.F.R. § 164.306(a)(1);

b. HPMB failed to protect against reasonably anticipated threats or hazards to the security or integrity of such information, *see* 45 C.F.R. § 164.306(a)(2);

c. HPMB failed to review and modify its data protection practices as needed to ensure reasonable and appropriate protection of ePHI, *see* 45 C.F.R. § 164.306(e);

d. HPMB failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI

it holds, *see* 45 C.F.R. § 164.308(a)(1)(ii)(A);

e. HPMB failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a), *see* 45 C.F.R. § 164.308(a)(1)(ii)(B);

f. HPMB failed to implement procedures to regularly review records of information system activity, *see* 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. HPMB failed to implement procedures sufficient to guard against, detect, and report malicious software, *see* 45 C.F.R. § 164.308(a)(5)(ii)(B);

h. HPMB failed to implement procedures sufficient for periodic testing and revision of contingency plans, *see* 45 C.F.R. § 164.308(a)(7)(ii)(D);

i. HPMB failed to perform a periodic technical and nontechnical evaluation, based upon the standards implemented under the Security Rule and in response to environmental or operational changes affecting the security of ePHI, that established the extent to which its security policies and procedures meet the requirements of 45 C.F.R. Part 164, Subpart C, *see* 45 C.F.R. § 164.308(a)(8);

j. HPMB failed to sufficiently implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4), *see* 45 C.F.R. § 164.312(a)(1);

k. HPMB failed to implement a sufficient mechanism to encrypt and decrypt ePHI, *see* 45 C.F.R. § 164.312(a)(2)(iv);

l. HPMB failed to implement a centralized logging system that would allow it to record and examine activity in information systems that contain ePHI, *see* 45

C.F.R. § 164.312(b);

m. HPMB failed to implement a system to identify whether PHI has been altered or destroyed in an unauthorized manner, *see* 45 C.F.R. § 164.312(c)(2);

n. HPMB failed to implement procedures sufficient to verify that a person or entity seeking access to ePHI is the one claimed, *see* 45 C.F.R. § 164.312(d);

o. HPMB failed to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, and other requirements of 45 C.F.R. Part 164, Subpart C, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv), *see* 45 C.F.R. § 164.316(a);

p. HPMB failed to prevent unauthorized access to the ePHI of individuals whose information was maintained on the HPMB Network, *see* 45 C.F.R. § 164.502(a); and,

q. HPMB failed to implement reasonable and appropriate policies and procedures to comply with the "minimum necessary" requirements for ePHI requests, use, and disclosure, *see* 45 C.F.R. § 164.502(b).

10. The OAG further finds that HPMB violated GBL § 899-aa by failing to provide affected New Yorkers with timely notice of the 2021 Data Breach and GBL § 899-bb(2) by failing to adopt reasonable data security practices to protect private information.

11. Respondent neither admits nor denies OAG's Findings, paragraphs 1-10 above.

12. The OAG finds the relief and agreements contained in this Assurance appropriate and in the public interest. THEREFORE, the OAG is willing to accept this Assurance pursuant to Executive Law § 63(15), in lieu of commencing a statutory proceeding for violations of HIPAA, *see* 42 U.S.C. § 1320d-5(d), or Executive Law § 63(12) and GBL §§ 899-aa & 899-bb.

IT IS HEREBY UNDERSTOOD AND AGREED, by and between the Parties:

RELIEF

13. For the purposes of this Assurance, the following definitions shall apply:

    a. "Affected Consumer" means any person who resided in New York at the time of the Security Event and whose Private Information or ePHI was potentially subject to the Security Event.

    b. "Effective Date" shall be the date of the last signature to this agreement.

    c. "ePHI" or "Electronic Protected Health Information" has the same meaning as the same term in 45 C.F.R. § 160.103.

    d. "Private Information" shall have the same meaning as the same term in New York General Business Law § 899-aa.

    e. "Security Event" means the ransomware attack that occurred in December 2021 and resulted in unauthorized access to and acquisition of Private Information and ePHI maintained by HPMB.

GENERAL COMPLIANCE

14. Respondent shall comply with Executive Law § 63(12) and GBL §§ 899-aa & 899-bb as well as HIPAA's Privacy Rule and Security Rule, 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A, C, and E, in connection with its collection, use, and maintenance of ePHI and Private Information.

INFORMATION SECURITY PROGRAM

15. Respondent shall maintain a comprehensive information security program ("Information Security Program") that is reasonably designed to protect the security, integrity, and confidentiality of the ePHI and Private Information that Respondent collects, stores, transmits,

and/or maintains. Respondent shall document in writing the content, implementation, and maintenance of the Information Security Program. The Information Security Program shall, at a minimum, include the following processes:

a. Assess and document, not less than annually, internal and external risks to the security, integrity and confidentiality of ePHI and Private Information;

b. Design, implement, and maintain reasonable administrative, technical, and physical safeguards to control the internal and external risks Respondent identified that are appropriate to: (i) the size and complexity of Respondent's operations; (ii) the nature and scope of Respondent's activities; and (iii) the volume and sensitivity of the ePHI and Private Information that Respondent collects, stores, transmits, and/or maintains;

c. Assess, not less than annually, the sufficiency of any safeguards in place to address the internal and external risks Respondent identified, and modify the Information Security Program based on the results to ensure that the safeguards comply with (b) above;

d. Test and monitor the effectiveness of the safeguards not less than annually, and modify the Information Security Program based on the results to ensure the safeguards comply with (b) above;

e. Select service providers capable of appropriately safeguarding ePHI and Private Information, contractually require service providers to implement and maintain appropriate safeguards to protect ePHI and Private Information, and take appropriate steps to verify service providers are complying with the contractual requirements;

f. Evaluate the Information Security Program not less than annually and adjust the Program in light of any changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have an impact on the effectiveness of the Program.

16. Respondent shall appoint a qualified employee to be responsible for implementing, maintaining, and monitoring the Information Security Program with the credentials, background, and expertise in information security appropriate to the level, size, and complexity of her/his role in implementing, maintaining, and monitoring the Information Security Program (the "Chef Information Security Officer"). The Chief Information Security Officer shall report at a minimum quarterly to the Chief Executive Officer (or the equivalent thereof) and senior management concerning Respondent's security posture, the security risks faced by Respondent, and the Information Security Program. The Chief Information Security Officer shall report at a minimum semi-annually to the Board of Directors (or the equivalent thereof) regarding the same.

17. Respondent shall provide notice of the requirements of this Assurance to its management-level employees responsible for implementing, maintaining, or monitoring the Information Security Program and shall implement appropriate training of such employees. The notice and training required under this paragraph shall be provided to the appropriate employees within sixty (60) days of the Effective Date of this Assurance, or within thirty (30) days of when an employee first assumes responsibility for implementing, maintaining, or monitoring the Information Security Program.

SPECIFIC INFORMATION SECURITY REQUIREMENTS

18. Encryption: Respondent shall encrypt ePHI and Private Information that it collects, uses, stores, transmits and/or maintains, whether stored within Respondent's network, or

transmitted electronically within or outside the Respondent's network, using a reasonable encryption algorithm where technically feasible.

19. Logging & Monitoring: Respondent shall, to the extent it has not already done so, establish, and, thereafter, maintain a system designed to programmatically collect and monitor network activity, such as through the use of security and event management tools, as well as policies and procedures designed to properly configure such tools to report anomalous activity. The system shall, at a minimum: (1) provide for centralized logging and monitoring that includes collection and aggregation of logging for Respondent's network, and (2) monitor for and alert security personnel to suspicious activity. Logs for network activity should be actively accessible for a period of at least 90 days and stored for at least one year from the date the activity was logged.

20. Patch Management: Respondent shall implement and maintain a reasonable policy to update and patch software on its computer network including the following:

a. Monitoring software and application security updates and security patch management, including but not limited to, receiving notifications from software manufacturers and ensuring the appropriate and timely application of all security updates and/or security patches;

b. Supervising, evaluating, and coordinating any system patch management tool(s); and,

c. Training requirements for individuals responsible for implementing and maintaining Respondent's patch management policies.

21. Penetration Testing: Respondent shall develop, implement, and maintain a penetration testing program designed to identify, assess, and remediate security vulnerabilities within Respondent's computer network. This program shall include regular penetration testing,

risk-based vulnerability ratings, and vulnerability remediation practices that are consistent with industry standards.

22. Data Collection: Respondent shall request, collect, use, or store ePHI and/or Private Information only to the minimum extent necessary to accomplish the intended legitimate business purpose for collection.

23. Data Deletion: Respondent shall permanently and securely delete or otherwise dispose of ePHI and/or Private Information when there is no reasonable business or legal purpose to retain it.

INFORMATION SECURITY PROGRAM ASSESSMENTS

24. Within one (1) year of the effective date, Respondent shall obtain a comprehensive assessment of the information security of the HPMB Network conducted by an independent third-party assessor who uses procedures and standards generally accepted in the profession (the "Third-Party Assessment") which shall be documented ("Third-Party Assessment Report") and provided to the OAG within two weeks of completion. Annually for five (5) years thereafter, Respondent shall obtain Third-Party Assessment Reports which shall be provided to the OAG upon request. The Third-Party Assessment Reports shall:

a. Identify the specific administrative, technical, and physical safeguards maintained by Respondent's Information Security Program;

b. Document the extent to which the identified administrative, technical and physical safeguards are appropriate based on the volume and sensitivity of the ePHI and Private Information that is at risk and the likelihood that the risk could be realized and result in the (1) unauthorized collection, maintenance, use, disclosure of, or provision of access to ePHI or Private Information, or the (2)

misuse, loss, theft, alteration, destruction, or other compromise of such information; and,

c. Assess the extent to which the administrative, technical, and physical safeguards that have been implemented by Respondent meet the requirements of the Information Security Program.

CREDIT MONITORING

25. Respondent shall offer two (2) years of credit monitoring and identify theft protection services to all Affected Consumers who were impacted by the 2021 Data Breach and were not previously offered identify theft protection services.

MONETARY RELIEF

26. Respondent shall pay to the State of New York two hundred thousand dollars ($200,000) in penalties (the "Monetary Relief Amount"). Payment of the Monetary Relief Amount shall be made in full within forty-five (45) days of the Effective Date of this Assurance. Any payment shall reference AOD No. 23-011.

MISCELLANEOUS

27. Respondent expressly agrees and acknowledges that the OAG may initiate a subsequent investigation, civil action, or proceeding to enforce this Assurance, for violations of the Assurance, or if the Assurance is voided pursuant to paragraph 34, and agrees and acknowledges that in such event:

a. any statute of limitations or other time-related defenses are tolled from and after the Effective Date of this Assurance;

b. the OAG may use statements, documents or other materials produced or provided by the Respondent prior to or after the effective date of this Assurance;

c. any civil action or proceeding must be adjudicated by the courts of the State of New York, and that Respondent irrevocably and unconditionally waives any objection based upon personal jurisdiction, inconvenient forum, or venue.

d. evidence of a violation of this Assurance shall constitute prima facie proof of a violation of the applicable law pursuant to Executive Law § 63(15).

28. If a court of competent jurisdiction determines that the Respondent has violated the Assurance, the Respondent shall pay to the OAG the reasonable cost, if any, of obtaining such determination and of enforcing this Assurance, including without limitation legal fees, expenses, and court costs.

29. This Assurance is not intended for use by any third party in any other proceeding.

30. Acceptance of this Assurance by the OAG is not an approval or endorsement by the OAG of any of Respondent's policies, practices, or procedures, and the Respondent shall make no representation to the contrary.

31. All terms and conditions of this Assurance shall continue in full force and effect on any successor, assignee, or transferee of the Respondent. Respondent shall include any such successor, assignment, or transfer agreement a provision that binds the successor, assignee, or transferee to the terms of the Assurance. No party may assign, delegate, or otherwise transfer any of its rights or obligations under this Assurance without the prior written consent of the OAG.

32. Any failure by the OAG to insist upon the strict performance by Respondent of any of the provisions of this Assurance shall not be deemed a waiver of any of the provisions hereof, and the OAG, notwithstanding that failure, shall have the right thereafter to insist upon the strict performance of any and all of the provisions of this Assurance to be performed by the Respondent.

33. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 23-011, and shall be in writing and shall, unless expressly provided otherwise herein, be given by hand delivery; express courier; or electronic mail at an address designated in writing by the recipient, followed by postage prepaid mail, and shall be addressed as follows:

If to the Respondent, to:

Adam M. Dlugacz, or in his absence, to the person holding the title of Managing Partner
Heidell, Pittoni, Murphy & Bach, LLP
99 Park Avenue
New York, NY 10016
adlugacz@hpmb.com

If to the OAG, to:

Laura Mumm, Assistant Attorney General, or in her absence, to the person holding the title of Bureau Chief Bureau of Internet & Technology
28 Liberty Street
New York, NY 10005
Laura.Mumm@ag.ny.gov

34. The OAG has agreed to the terms of this Assurance based on, among other things, the representations made to the OAG by the Respondent and its counsel and the OAG's own factual investigation as set forth in Findings, paragraphs (1)-(10) above. The Respondent represents and warrants that neither it nor its counsel has made any material representations to the OAG that are inaccurate or misleading. If any material representations by Respondent or its counsel are later found to be inaccurate or misleading, this Assurance is voidable by the OAG in its sole discretion.

35. No representation, inducement, promise, understanding, condition, or warranty not set forth in this Assurance has been made to or relied upon by the Respondent in agreeing to this Assurance.

36. The Respondent represents and warrants, through the signatures below, that the terms and conditions of this Assurance are duly approved. Respondent further represents and warrants that Heidell, Pittoni, Murphy & Bach, LLP, by Adam M. Dlugacz, as the signatory to this AOD, is a duly authorized officer and managing partner acting at the direction of the Executive Committee of Heidell, Pittoni, Murphy & Bach, LLP.

37. Unless a term limit for compliance is otherwise specified within this Assurance, the Respondent's obligations under this Assurance are enduring. Nothing in this Agreement shall relieve Respondent of other obligations imposed by any applicable state or federal law or regulation or other applicable law.

38. Respondent agrees not to take any action or to make or permit to be made any public statement denying, directly or indirectly, any finding in the Assurance or creating the impression that the Assurance is without legal or factual basis.

39. Nothing contained herein shall be construed to limit the remedies available to the OAG in the event that the Respondent violates the Assurance after its Effective Date.

40. This Assurance may not be amended except by an instrument in writing signed on behalf of the Parties to this Assurance.

41. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held by a court of competent jurisdiction to be invalid, illegal, or unenforceable in any respect, in the sole discretion of the OAG, such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

42. Respondent acknowledges that it has entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.

43. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

44. The Assurance and all its terms shall be construed as if mutually drafted with no presumption of any type against any party that may be found to have been the drafter.

45. This Assurance may be executed in multiple counterparts by the parties hereto. All counterparts so executed shall constitute one agreement binding upon all parties, notwithstanding that all parties are not signatories to the original or the same counterpart. Each counterpart shall be deemed an original to this Assurance, all of which shall constitute one agreement to be valid as of the effective date of this Assurance. For purposes of this Assurance, copies of signatures shall be treated the same as originals. Documents executed, scanned and transmitted electronically and electronic signatures shall be deemed original signatures for purposes of this Assurance and all matters related thereto, with such scanned and electronic signatures having the same legal effect as original signatures.

46. The Effective Date of this Assurance shall be March 10, 2023.

LETITIA JAMES
ATTORNEY GENERAL OF THE STATE OF NEW YORK

By: _____

Laura Mumm
Assistant Attorney General
Bureau of Internet & Technology
28 Liberty Street
New York, NY 10005
Laura.Mumm@ag.ny.gov
Phone: (212) 416-8276

Date: 3/9/2023

HEIDELL, PITTONI, MURPHY & BACH, LLP

By: _____

Adam M. Dlugacz
Heidell, Pittoni, Murphy & Bach, LLP
99 Park Avenue
New York, NY 10016
adlugacz@hpmb.com
Phone: (212) 286-8585

Title: Managing Partner

Date: 3/3/23

Office of the Maine Attorney General

Home > Consumer Information > Privacy, Identity Theft and Data Security Breaches > Data Breach Notifications

Data Breach Notifications

Entity Information

- Type of Organization: **Other Commercial**
- Entity Name: **Heidell, Pittoni, Murphy & Bach, LLP**
- Street Address: **99 Park Avenue**
- City: **New York**
- State, or Country if outside the US: **New York**
- Zip Code: **10016**

Submitted By

- Name: **Ross Molina**
- Title: **Counsel**
- Firm name (if different than entity): **Wilson Elser**
- Telephone Number: **5047021726**
- Email Address: **ross.molina@wilsonelser.com**
- Relationship to entity whose information was compromised: **Counsel**

Breach Information

- Total number of persons affected (including residents): **114,979**
- Total number of Maine residents affected: **9**
- If the number of Maine residents exceeds 1,000, have the consumer reporting agencies been notified: **Yes**
- Date(s) Breach Occured: **11/22/2021**
- Date Breach Discovered: **04/22/2022**
- Description of the Breach:
  - **External system breach (hacking)**
- Information Acquired - Name or other personal identifier in combination with: **Social Security Number**

Notification and Protection Services

- Type of Notification: **Written**
- Date(s) of consumer notification: **05/16/2022**
- Copy of notice to affected Maine residents: **HPMB Notification Proof.pdf**
- Date of any previous (within 12 months) breach notifications: **N/A**
- Were identity theft protection services offered: **Yes**
- If yes, please provide the duration, the provider of the service and a brief description of the service: **12 months of credit monitoring and identity theft protection services**

Credits

HPM&B
ATTORNEYS AT LAW

P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
(833) 940-2336
Or Visit:
https://response.idx.us/hpmb
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

Via First-Class Mail

May 16, 2022

Notice of Data Incident

Dear <<Full Name>>:

Heidell Pittoni Murphy & Bach LLP ("HPMB") serves as litigation counsel for New York Presbyterian Hospital in medical malpractice cases. In this role, HPMB receives medical records for some of New York Presbyterian Hospital's patients. We recently discovered that a data security incident resulted in the unintentional exposure of some of your personal information. This letter contains additional information about the incident, our response to this incident, and steps you can take to protect yourself. Please be assured that HPMB takes the protection and proper use of your personal information very seriously, and we sincerely apologize for any inconvenience this may cause.

What Happened

On December 25, 2021, HPMB detected suspicious activity within its network environment. Upon discovery, we worked with our information technology (IT) support team and immediately engaged a law firm specializing in cybersecurity and data privacy to investigate further. Additionally, HPMB engaged third-party forensic specialists to assist HPMB in its analysis of any unauthorized activity. The preliminary assessment showed that an unauthorized person or entity gained control over certain of the firm's information for a period of time until HPMB was able to negotiate its return.

Following the incident, HPMB's experts conducted an extensive investigation, which concluded on April 22, 2022. Based on the investigation, we have, determined that certain of your information, including your name, date of birth, social security number, and certain medical treatment information, was part of a tranche of data accessed and briefly held by the unauthorized party.

At this time, HPMB does not have any evidence to indicate that, since its return to us, any of your personal information has been or will be further misused as a result of this incident.

What We Are Doing

Upon detecting this suspicious activity, we moved quickly to initiate a response, which included conducting an investigation with the assistance of third-party forensic specialists and confirming the security of our network environment. We have ensured that no further unauthorized activity has continued. We have also reviewed and updated our policies and procedures relating to the security of our systems and servers, as well as our information life cycle management. We will also be reporting this incident to the appropriate authorities.

We value the safety of your personal information and are, therefore, offering credit monitoring and identity theft protection services through IDX. IDX's services include: <<12/24>> months of credit monitoring and fully managed id theft recovery services. With this protection, IDX will notify you and assist you to resolve issues if your identity is compromised.

What You Can Do:

We encourage you to enroll in free IDX services by going to https://response.idx.us/hpmb and using the Enrollment Code provided above. Please note the deadline to enroll is August 16, 2022.

Enclosed hereto you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information.

For More Information

We recognize that you may have questions not addressed in this letter. We encourage you to contact IDX with any questions and to enroll in free IDX services by calling (833) 940-2336, Monday through Friday, 9 am to 9 pm Eastern Time.

Sincerely,

Daniel S. Ratner

Additional Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 www.transunion.com/credit-freeze

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (https://www.transunion.com/fraud-alerts); or
- Experian (https://www.experian.com/fraud/center.html).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can

obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

For New York residents, the Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, and https://ag.ny.gov/.

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

Cost of a Data Breach Report 2025

The AI Oversight Gap

think report

IBM

Table of contents

Executive summary

Welcome to IBM's annual Cost of a Data Breach Report. With this edition, we mark 20 years of data breach research. This year, we set our sights on the most fundamental technological shift in a generation: the adoption of AI.

With the 2025 report, we begin chronicling and quantifying the risks associated with AI. What we've found is concerning: organizations are skipping over security and governance for AI in favor of do-it-now AI adoption. Those ungoverned systems are more likely to be breached—and more costly when they are. We're not surprised.

Since 2005, this report has tracked an ever expanding technology landscape and the threats that follow it. Our research partners at Ponemon Institute have not only documented the emergence of new threats and attack surfaces, but also quantified these threats in financial terms security and business leaders can understand and act on. All told, their researchers have studied more than 6,485 breaches and interviewed over 34,652 technology, security and business leaders involved in their organization's response to the breach.

20 Years of Data Breach Research

Obviously, security threats have changed through the years. Two decades ago, nearly half of all data breaches (45%) were caused by a lost or stolen computing device, such as a laptop or thumb drive, while only 10% of breaches were attributed to "hacked electronic systems." Today, most breaches are caused by a range of malicious activities, from phishing to insider threats.

Ten years ago, breaches due to cloud misconfiguration weren't even a categorized threat. Today, the cloud and the data in it are a prime target. And it was only during the COVID-19 lockdowns in 2020 that ransomware began to surge. A year later, those attacks accounted for an average USD 4.62 million in breach costs, a figure that hit USD 5.08 million in this year's report.

However, one constant has been the work of Ponemon. This year's research—conducted independently by Ponemon Institute and sponsored, analyzed and published by IBM—studied 600 organizations impacted by data breaches between March 2024 and February 2025. Together, we looked at organizations across 17 industries, in 16 countries and regions, and breaches that ranged from 2,960 to 113,620 compromised records. To gain on-the-ground insights, Ponemon researchers interviewed 3,470 security and C-suite business leaders with firsthand knowledge of the data breach incidents at their organizations. These leaders included CEOs, CISOs, heads of operations, controllers or heads of finance, IT practitioners, business unit leaders and general managers, and risk management and cybersecurity practitioners.

The result is a benchmark report that business, technology and security leaders can use to strengthen their defenses, inform resource allocation and drive innovation, particularly around securing and governing their AI initiatives.

This year's headline: global data breach costs have declined for the first time in five years, dropping to USD 4.44 million, due to faster breach containment that was driven by AI-powered defenses. But as defenders move smarter and faster, so do attackers—16% of breaches reportedly involved attackers using AI, often used in phishing and deepfake attacks. While this escalating AI arms race has benefitted organizations by pushing global breach costs lower, the US is bucking the trend. Breach costs there have surged past USD 10 million, driven by steeper regulatory penalties and rising detection costs.

We also found AI adoption is outpacing oversight. We found 97% of AI-related security breaches involved AI systems that lacked proper access controls. And most breached organizations reported they have no governance policies in place to manage AI or prevent shadow AI—the use of AI without employer approval or oversight. Both the covert use of shadow AI and the lack of governance are driving up breach costs.

What's new in the 2025 report

As always, the Cost of a Data Breach Report reflects new technologies, emerging tactics and recent events. For the first time, this year's research explores the:

- State of security and governance for AI
- Prevalence and risk profile of shadow AI
- Type of data targeted in security incidents involving AI
- Length of breach disruptions to organizations
- Cost savings from using quantum security tools
- Breach costs associated with AI-driven attacks
- Amount of breach costs passed on to customers

Key findings

The key findings described here are based on IBM analysis of research data independently compiled by Ponemon Institute.

USD 4.44M

The global average cost of a data breach

The global average breach cost dropped to USD 4.44 million from USD 4.88 million in 2024, a 9% decrease and a return to 2023 cost levels. Faster identification and containment of breaches—much of it from organizations' own security and security service teams, with help from AI and automation—drove this decline. The global average would have been lower were it not for the United States, where the average cost surged by 9% to USD 10.22 million, an all-time high for any region. Higher regulatory fines and higher detection and escalation costs in the United States contributed to this surge.

97%

Share of organizations that reported an AI-related breach and lacked proper AI access controls

Security incidents involving an organization's AI remain limited—for now. On average, 13% of organizations reported breaches that involved their AI models or applications. However, among those that did, almost all (97%) lacked proper AI access controls. The most common of these security incidents occurred in the AI supply chain, through compromised apps, APIs or plug-ins. These incidents had a ripple effect: they led to broad data compromise (60%) and operational disruption (31%). The findings suggest AI is emerging as a high-value target.

USD 4.92M

Average cost of malicious insider attacks

For the second year in a row, malicious insider attacks resulted in the highest average breach costs among initial threat vectors: USD 4.92 million. Third-party vendor and supply chain compromise followed closely at USD 4.91 million. Other expensive attack vectors included vulnerability exploitation and phishing. However, the most frequent type of attack vector on organizations was phishing, at 16%, which averaged USD 4.8 million.

USD 670K

Added breach cost for shadow AI

Among the organizations studied this year, 20% said they suffered a breach due to security incidents involving shadow AI. For organizations with high levels of shadow AI, those breaches added USD 670,000 to the average breach price tag compared to those that had low levels of shadow AI or none. These incidents also resulted in more personal identifiable information (65%) and intellectual property (40%) data being compromised. And that data was most often stored across multiple environments, revealing just one unmonitored AI system can lead to widespread exposure. The swift rise of shadow AI has displaced security skills shortages as one of the top three costly breach factors tracked by this report.

USD 1.9M

Cost savings from extensive use of AI in security

Security teams using AI and automation extensively shortened their breach times by 80 days and lowered their average breach costs by USD 1.9 million compared to organizations that didn't use these solutions. Nearly a third of organizations said they used these tools extensively across the security lifecycle—in prevention, detection, investigation and response. However, that figure is up only slightly from the previous year, suggesting AI adoption may have stalled. It also shows the majority are still not using AI and automation and, therefore, aren't seeing the cost benefits.

63%

Share of organizations that refused to pay ransomware attackers

More ransomware victims refused to pay a ransom in 2025 (63%) than 2024 (59%). However, the average cost of an extortion or ransomware incident remains high, particularly when disclosed by an attacker (USD 5.08 million). At the same time, fewer ransomware victims reported involving law enforcement—40% of organizations this year versus 53% last year.

49%

Share of organizations investing in security post breach

There was a significant reduction in the number of organizations that plan to invest in security following a breach, 49% this year compared to 63% last year. Less than half of those who plan to invest in a security plan to focus on AI-driven security solutions or services, such as threat detection and response, incident response (IR) planning and testing, and data security or protection tools.

63%

Share of organizations that lack AI governance policies

A majority of breached organizations (63%) either don't have an AI governance policy or are still developing one. Even when they have a policy, less than half have an approval process for AI deployments, and 61% lack AI governance technologies. Among organizations that have governance polices in place, only a minority (34%) perform regular audits for unsanctioned AI. It shows AI remains largely unchecked as adoption outpaces both security and governance.

1 in 6

Number of breaches involving AI-driven attacks

Attackers can use generative AI (gen AI) to both perfect and scale their phishing campaigns and other social engineering attacks. IBM previously found gen AI reduced the time needed to craft a convincing phishing email from 16 hours down to only five minutes. This year's report shows the impact: on average, 16% of data breaches involved attackers using AI, most often for AI-generated phishing (37%) and deepfake impersonation attacks (35%).

Complete findings

The complete findings from this year's survey address 16 themes, presented in the following order:

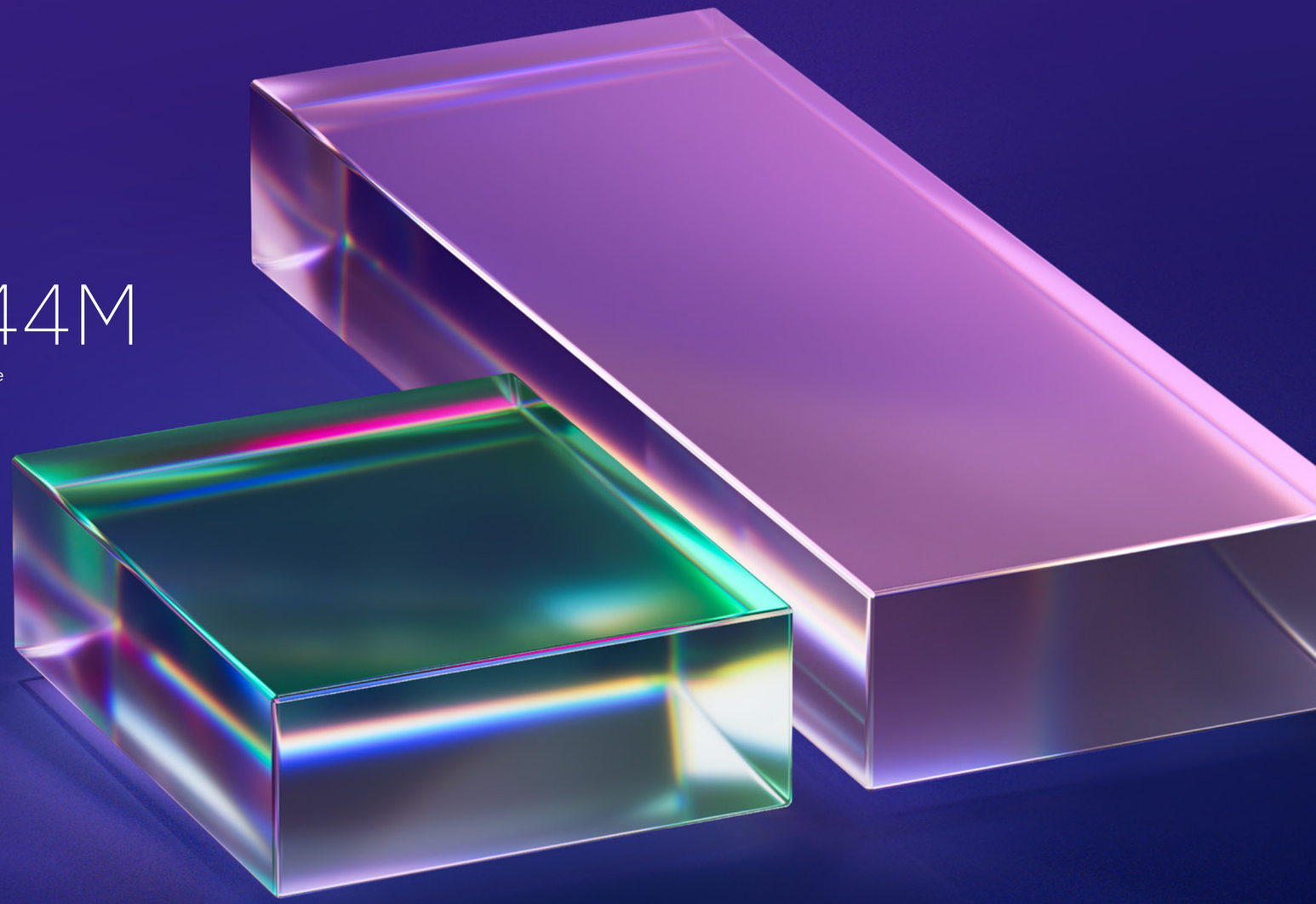
- Global highlights
- Data security
- Initial attack vectors and root causes
- Data breach lifecycle
- Identifying the breach
- Regulatory fines
- Recovery time
- Breaches involving AI
- AI governance
- AI-driven attacks
- Ransomware attacks
- Raising prices post-breach
- Business disruption
- Factors that increase or decrease breach costs
- Security AI and automation
- Security investments

10.22M

United States average

4.44M

Global average



Globally, the average cost of a data breach fell while it hit a record high in the US.

Measured in USD

Global highlights

While the cybersecurity skill shortage continues to grow, security teams are managing to identify and contain beaches faster, with the help of AI and automation. That approach is helping drive down data breach costs globally. These teams are doing so even as attackers use gen AI to create and scale realistic phishing and deepfake attacks. Despite the overall global decrease, the United States saw breach costs rise, driven by higher regulatory fines and increased detection and escalation costs. Healthcare continues to top the list of costliest industries for breaches. The following section provides a look at these and other issues across industries, countries and regions.

The global average cost of a data breach fell
For the first time in five years, the global average cost of a data breach dropped, reaching USD 4.44 million. Globally, shorter breach investigations are pushing down detection and escalation costs, which can include assessment and audits, crisis management, and communications to executive leadership and boards. See Figure 1.

Figure 1.
Measured in USD millions

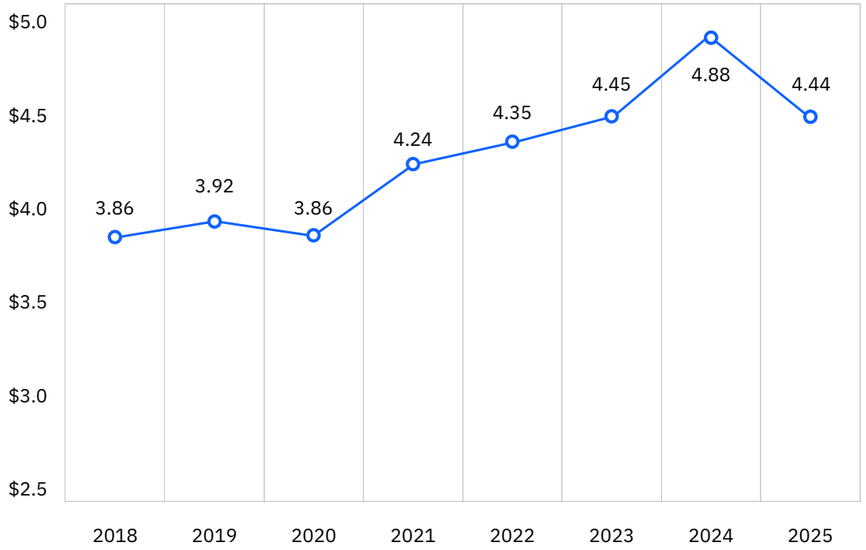


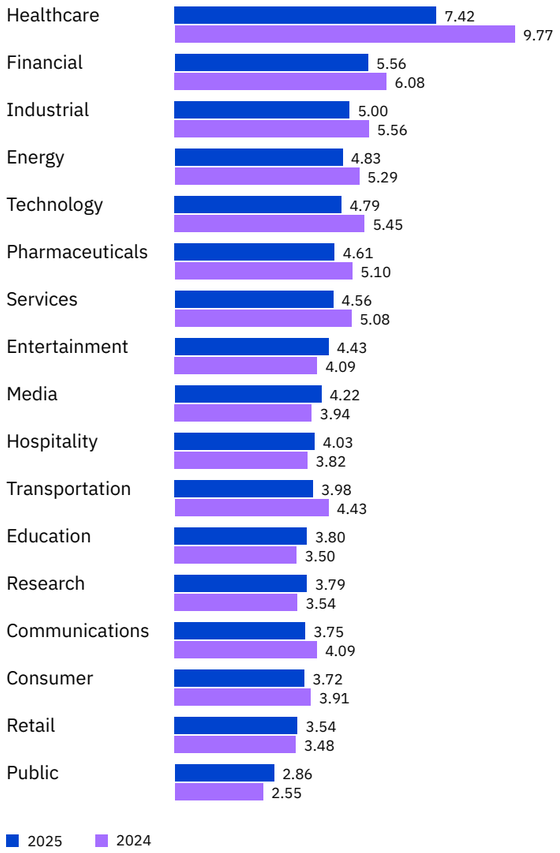
Figure 2.
Measured in USD millions

#	Country		2025	2024
1	United States	↑	$10.22	$9.36
2	Middle East	↓	$7.29	$8.75
3	Benelux	↑	$6.24	$5.90
4	Canada	↑	$4.84	$4.66
5	United Kingdom	↓	$4.14	$4.53
6	Germany	↓	$4.03	$5.31
7	Latin America	↓	$3.81	$4.16
8	France	↓	$3.73	$4.17
9	ASEAN	↑	$3.67	$3.23
10	Japan	↓	$3.65	$4.19
11	Italy	↓	$3.44	$4.73
12	South Korea	↓	$2.84	$3.62
13	Australia	↓	$2.55	$2.78
14	India	↑	$2.51	$2.35
15	South Africa	↓	$2.37	$2.78
16	Brazil	↓	$1.22	$1.36

The United States breaks a breach cost record
Average breach costs in the United States reached a record USD 10.22 million, a 9% increase over last year, driven in part by higher regulatory fines and detection and escalation costs. Most countries or regions recorded a decrease, due to lower detection and escalation costs. Some places, such as Saudi Arabia, were likely assisted by increased security spending and maturing security frameworks. Among the decliners were Italy (-27%), Germany (-24%) and South Korea (-21.5%). On the increase list were Canada, India, the Association of Southeast Asian Nations (ASEAN) and Benelux—the economic union of Belgium, the Netherlands and Luxembourg. Benelux made its debut in the 2024 study and witnessed a 6% increase in average breach cost. See Figure 2.

Healthcare remained the most expensive industry for breaches
At USD 7.42 million, healthcare recorded the highest average breach cost among industries for the 12th consecutive year—even as it saw a sharp reduction from last year (USD 9.77 million). Attackers continue to value and target the industry's patient personal identification information (PII), which can be used for identity theft, insurance fraud and other financial crimes. Healthcare breaches took the longest to identify and contain at 279 days. That's more than five weeks longer than the global average. See Figure 3.

Figure 3.
Measured in USD millions



Time to identify and contain a breach decreased
The mean time organizations took to identify and contain a breach fell to 241 days, reaching a nine-year low and continuing a downward trend that started after a 287-day peak in 2021. As noted in last year's report, security teams continue to improve their mean time to identify (MTTI) and mean time to contain (MTTC) with the help of AI-driven and automation-driven defenses. See Figure 4.

Figure 4.
Measured in days

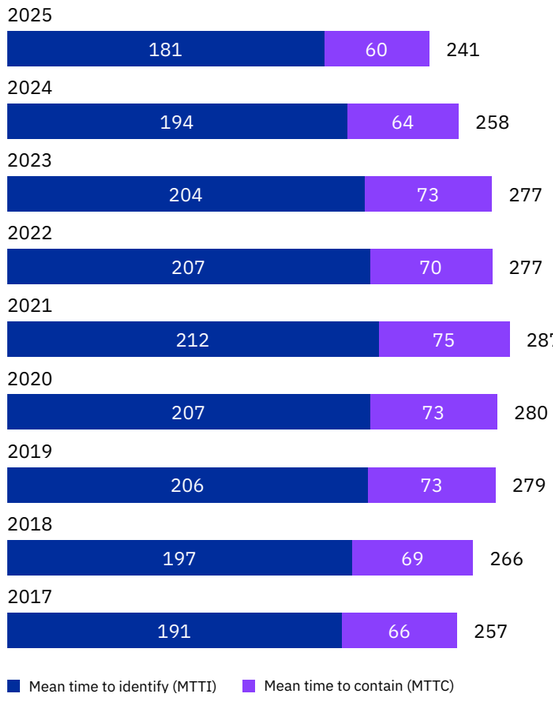
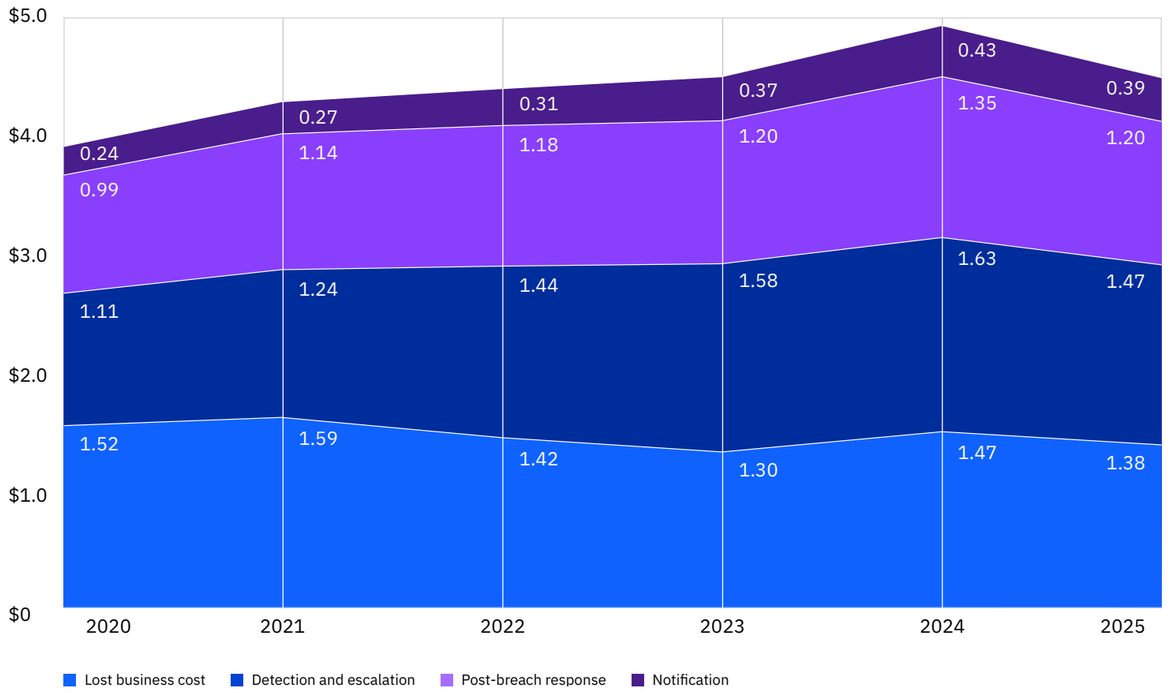
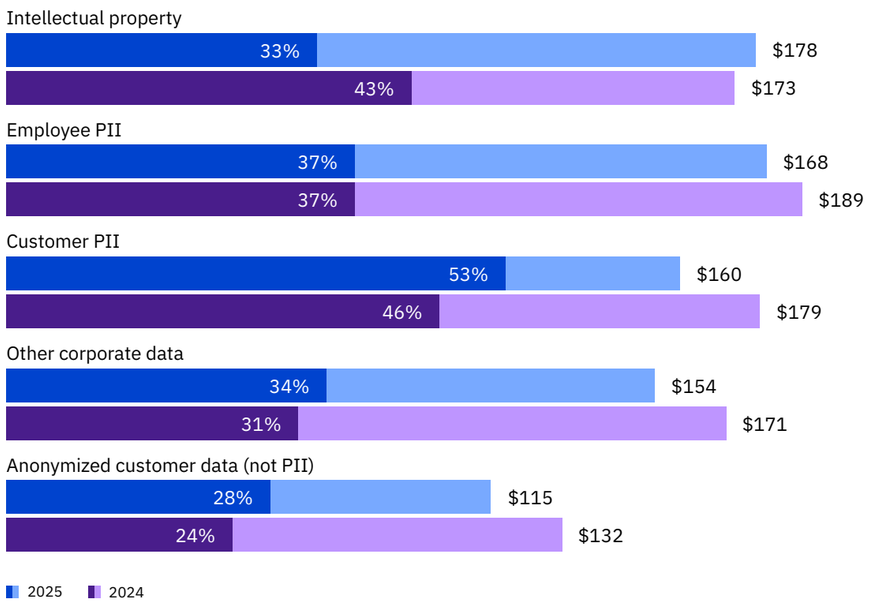


Figure 5.
Measured in USD millions



Detection and escalation costs plunged
Average costs for detection and escalation fell to USD 1.47 million, a nearly 10% drop from last year. These costs were the top decliners among four cost categories. Still, the other three categories—notification, ex-post response and lost business costs—also fell. Lost business, which includes revenue from system downtime, lost customers and reputation damage, dropped 6% after an 11% surge last year that helped drive total breach costs higher. See Figure 5.

Figure 6.
Measured in USD; more than one response permitted



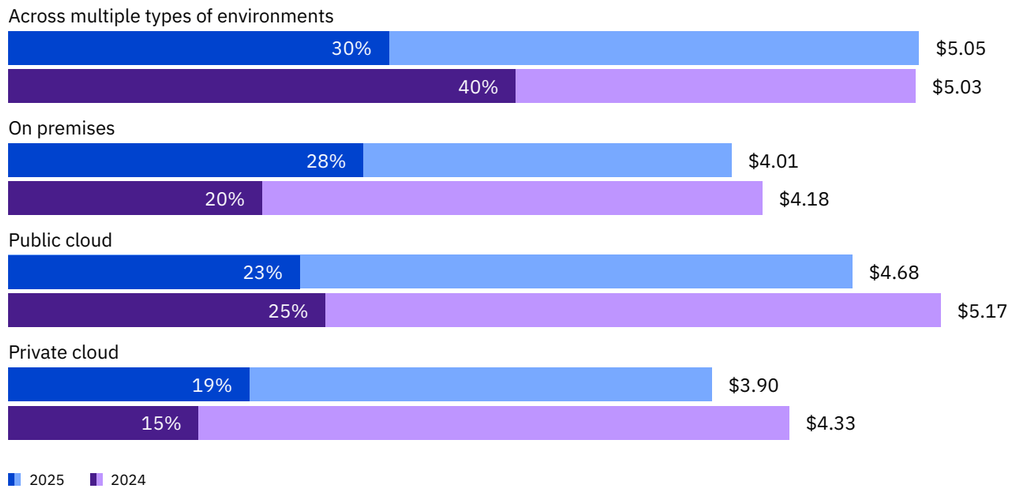
Most breaches targeted customer PII
Attackers targeted customer PII over other types of data by a wide margin. At 53%, it was the most stolen or compromised data type. Customer PII can include tax identity (ID) numbers, emails and home addresses, and can be used in identity theft and credit card fraud. On the other hand, company intellectual property (IP), while less commonly stolen or compromised, was the most costly (USD 178 per record). See Figure 6.

Data security

Data can be vulnerable wherever it's stored. Last year, most breaches involved data distributed across multiple environments, such as public clouds, private clouds and on premises. That finding remained true this year, but the share of those breaches fell, while the share of breaches involving data stored solely on premises grew. Meanwhile, the average costs associated with each location type was drastically different.

The effect of storage location on cost and frequency of a data breach
30% of all breaches involved data distributed across multiple environments, down from 40% last year. Meanwhile, breaches involving data stored on premises increased sharply to 28% from 20% last year. However, costs for each category differed. Data breaches involving multiple environments cost an average USD 5.05 million, while data breached on premises cost an average USD 4.01 million. See Figure 7.

Figure 7.
Measured in USD millions; more than one response permitted

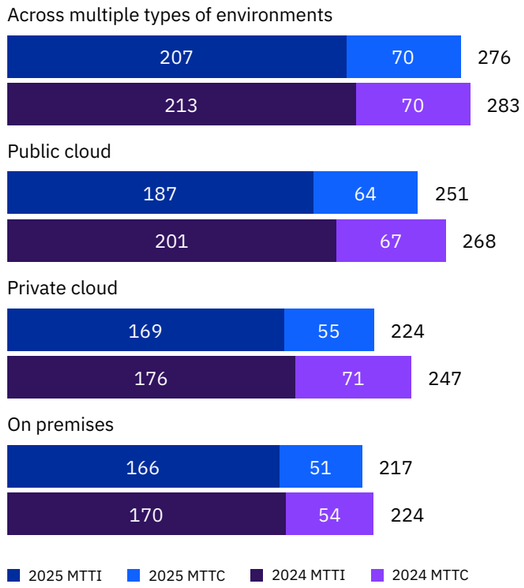


276

Days it took to identify and contain a data breach across various environments

Breaches of cross-environment data took longer to resolve
Breached data stored across multiple environments took the most time to identify and contain (276 days), the longest of the four storage locations. It reflects the increased complexity and uncertainty of such breaches. Compared to 2024, resolution times decreased for all categories. On-premises breaches were the quickest to resolve at 217 days. See Figure 8.

Figure 8.
Measured in days



Initial attack vectors and root causes

For the third year in a row, phishing was among the top attack vectors. Vendor and supply chain compromise followed closely behind, overtaking compromised credentials as the number two attack vector. All three vectors, which can be gained through malware, data breaches and credential stuffing, carried heavy costs for breached organizations. Our research also compared the average time to identify and contain those breaches, with supply chain compromise taking the longest to resolve.

Phishing topped initial attack vectors
Phishing replaced stolen credentials this year as the most common initial vector (16%) attackers used to gain access to systems. At an average USD 4.8 million per breach, it was also one of the costliest. Meanwhile, supply chain compromise surged to become the second most prevalent attack vector (15%), and second costliest (USD 4.91 million) after malicious insider threats (USD 4.91 million). See Figure 9.

Figure 9.
Measured in USD millions; percentage of all breaches

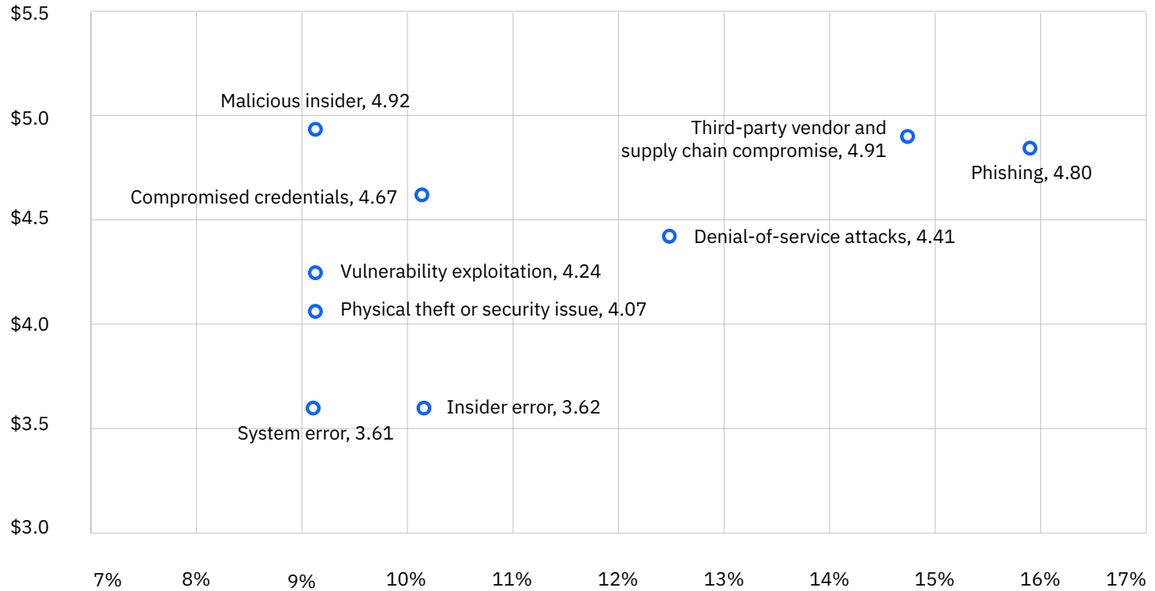


Figure 10.
Measured in days

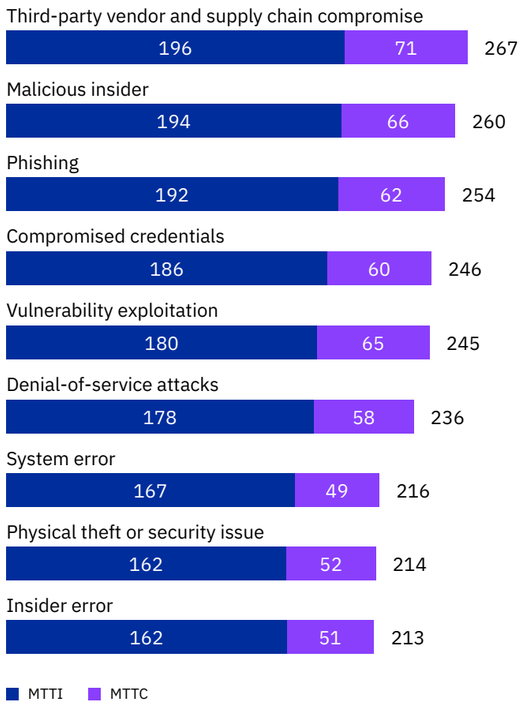
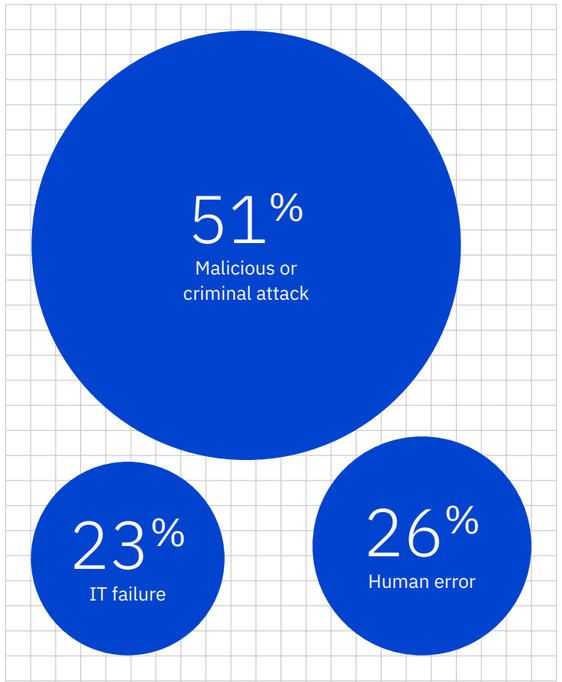


Figure 11.
Share of all breached organizations



Supply chain compromise took longest to resolve
Supply chain attacks are hard to detect because they exploit trust between vendor-and-customer and computer-to-computer communications. At a combined 267 days, they took the longest to detect and contain. Likewise, another trust-based attack, malicious insiders, took the second longest, with a combined 260 days to resolve. Compromised credentials, on the other hand, took the fourth longest to identify (186 days) but were less time-consuming to contain (60 days). See Figure 10.

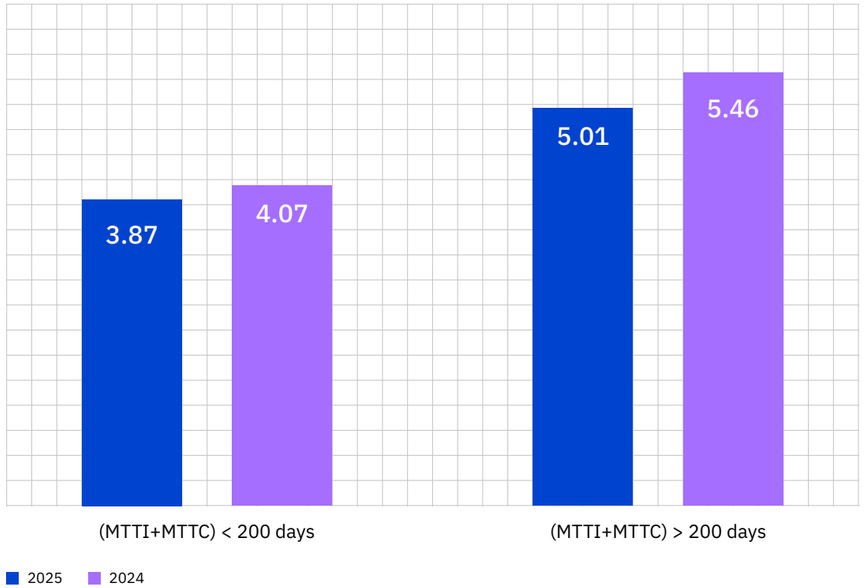
Malicious attacks dominate root cause of breaches
At 51%, malicious or criminal attacks, whether launched within or outside an organization, continue to dominate and occupy security teams. Human error and IT failure, which are preventable with robust employee training and proactive security measures, account for the rest, at 26% and 23% respectively. See Figure 11.

Data breach lifecycle

When an attacker breaches an organization, costs go up by the day. Each year, researchers analyze the average costs of the complete breach lifecycle—the total average number of days to identify and contain the breach—by breaking them into two categories: those that took less than 200 days and those that exceeded 200 days. While the costs for both categories rose in the previous two years, they declined this year. It was likely due to the lower costs of AI-driven and automation-driven detection and response.

Shorter breach lifecycles led to lower costs
Data breaches with a lifecycle under 200 days saw a drop in average costs, to USD 3.87 from USD 4.07 last year, a nearly 5% decline. Meanwhile, data breaches with a lifecycle exceeding 200 days had the highest average cost, at USD 5.01 million, compared to breaches with lifecycles under 200 days. It's nearly an 8% decrease from last year. See Figure 12.

Figure 12.
Measured in USD millions



Identifying the breach

Breach costs rise or fall depending on how they're identified: who detects them and when. This year, like last year, in-house security teams continued to increase the share of breaches they identified. Researchers looked at the prevalence of breach disclosures by outsiders, such as benign third parties, security researchers, law enforcement and consultants, and by the attackers themselves. They also examined the costs associated with each type of breach identification.

Security teams improved their breach identification
In the past two years, security teams and their tools have improved their performance in breach detection. This year, researchers found these teams and tools detected 50% of breaches, a vast leap over last year's tally of 42%, which was itself was a jump from 33% in 2023. Correspondingly, fewer breaches this year were identified by third parties and attackers. See Figure 13.

Figure 13.
Only one response permitted

Breaches identified by internal security teams cost less
By detecting a breach first—before third parties or attacker disclosure—security teams can move fast and limit potential damage. When security teams identified a breach, the average cost was USD 4.18 million, down from USD 4.55 million last year. By comparison, when the attacker disclosed the breach, and presumably had more time to do damage and steal or compromise data, the average cost was far greater (USD 5.08 million). However, that cost decreased from last year (USD 5.5 million). See Figure 14.

Figure 14.
Measured in USD millions

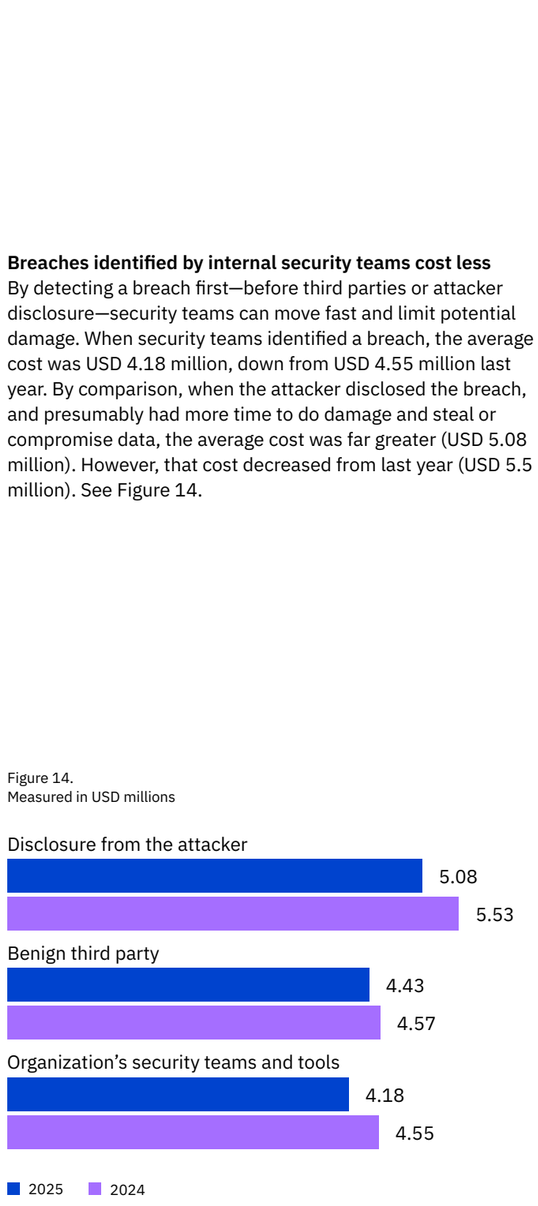
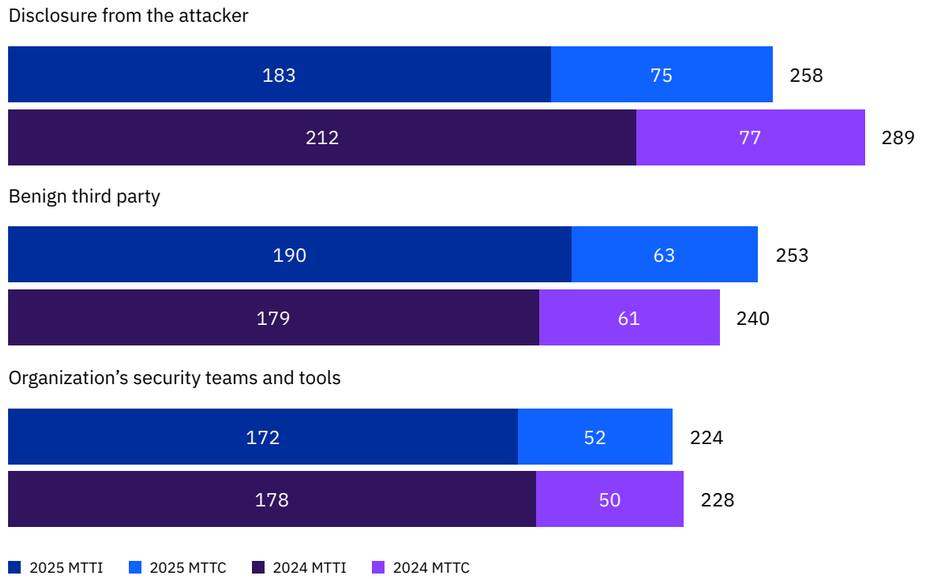


Figure 15.
Measured in days



Faster breach identification and containment
Not only did internal security teams identify more breaches, they did it in record time: 172 days, six days faster than last year. They also contained those breaches two days faster. The use of AI and automation is likely contributing to this acceleration, as the next section in the report shows. See Figure 15.

Recovery time

Recovery from a breach can continue after containment. In this study, recovery means:

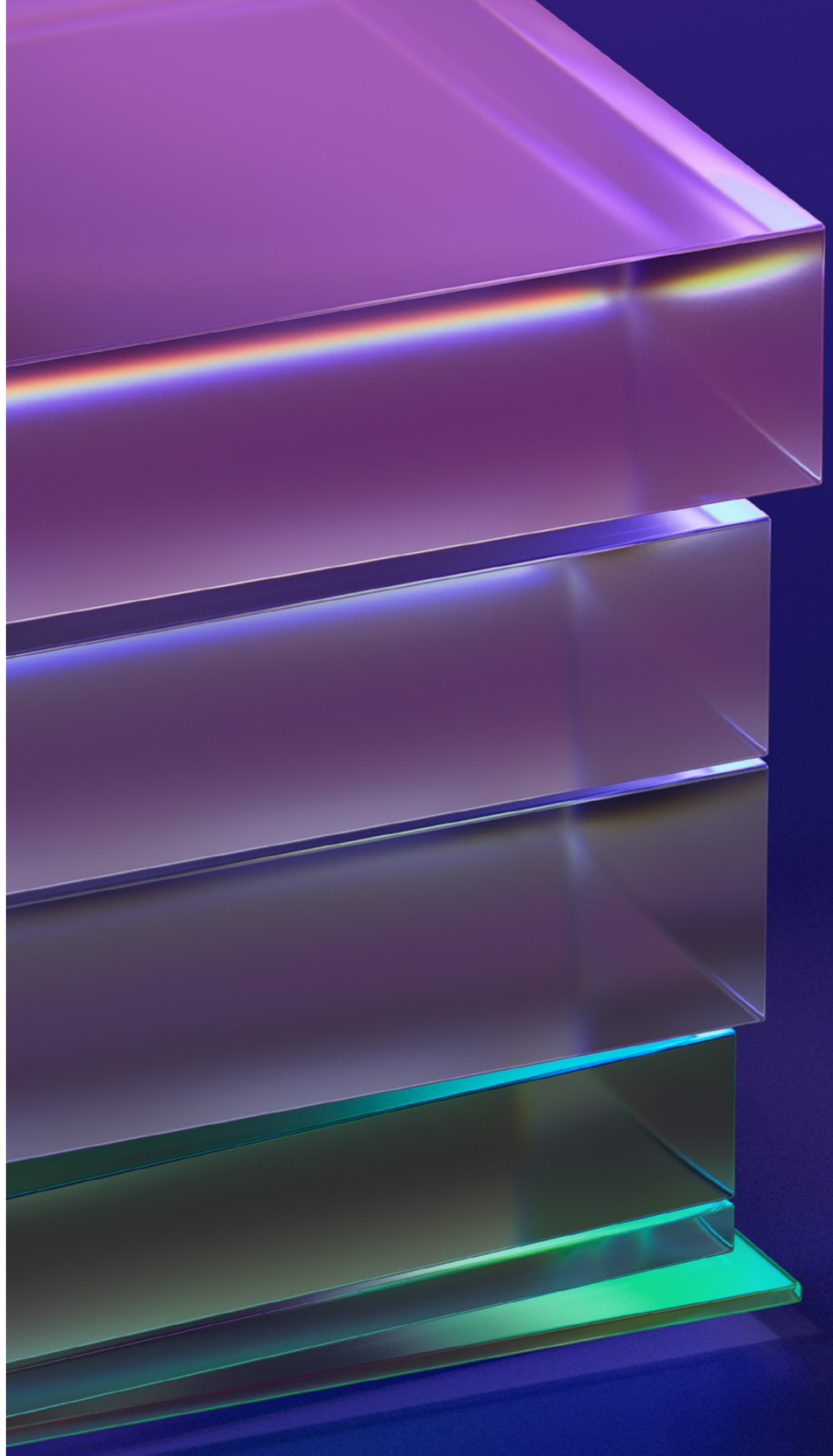
- Business operations are back to normal in areas affected by the breach.
- Organizations have met compliance obligations, such as paying fines.
- Customer confidence and employee trust have been restored.
- Organizations have put controls, technologies and expertise in place to avoid future data breaches.

Much of this work, such as re-establishing customer confidence, involves factors beyond technology. Despite progress compared to 2024, only a minority of organizations reported complete recovery. For most organizations, the hard work of recovery can take months or even years.

Breach recovery rates improved
Most organizations in this year's survey (65%) said they were still recovering from the data breach. However, 35% said they had fully recovered, nearly tripling the response from last year (12%). This improvement coincided with a nine-year low for faster identification and containment of breaches.

65%

Share of organizations that have not fully recovered from a data breach



Recovery typically took more than 100 days

Among the organizations that had fully recovered, 76% said the recovery took longer than 100 days. Roughly a quarter (26%) said recovery took more than 150 days. Only 2% said recovery was possible within as little as 50 days.
See Figure 16.

Figure 16.
From organizations that reported fully recovering from a data breach; measured in days

26%
>150 days

24%
126 – 150 days

26%
101 – 125 days

17%
76 – 100 days

5%
51 – 75 days

2%
< 50 days

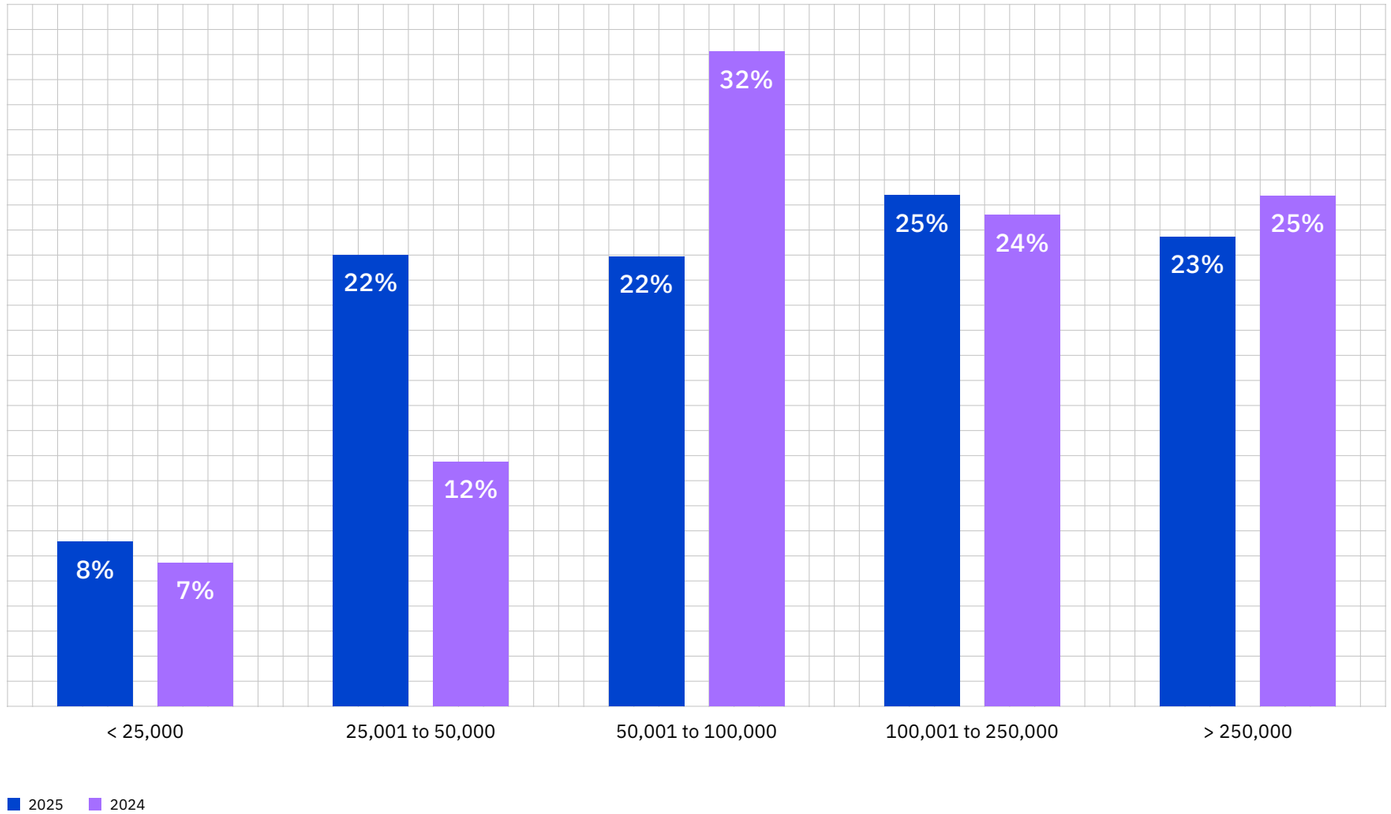
Regulatory fines

Reporting a breach to regulators and other government agencies has become a common part of post-breach responses. This year's report found a third of organizations paid a regulatory fine because of breaches. The study looked at the size of fines, which varied across countries and regions. Organizations in the United States paid the highest fines, which, in turn, drove up total United States breach costs.

32%

Share of data breaches that resulted in fines

Figure 17.
Among those organizations that experienced fines; measured in USD



Distribution of regulatory fine costs
The share of organizations that paid fines after a breach remained the same as last year, about one third. A total of 48% of those fines were above USD 100,000. However, the distribution of fine costs grew in some categories and shrank in others. For instance, the share that paid a fine of up to USD 50,000 grew by 45% while those that paid USD 50,001 to USD 100,000 decreased by 31%. Organizations that paid over USD 250,000 remained approximately the same.
See Figure 17.

Breaches involving AI

Security for AI is lacking. This year's report quantifies the extent to which attackers are taking advantage of this deficiency and successfully targeting AI models and applications. While the share of breaches involving AI security incidents are small, IBM researchers expect them to grow as AI vendors gain greater market share and penetration into enterprise systems. Shadow AI is of particular concern. As AI becomes integral to operations, AI security incidents have the potential to disrupt a range of business activities, including compromising sensitive data.

97%

Share of organizations that had an AI-related security incident to their models or applications and had lacked proper AI access controls

Security incidents involving AI

AI models and applications are emerging as an attack surface, especially in cases of shadow AI. This year, 13% of organizations reported a security incident on an AI model or application that resulted in a breach. But 97% of those breached organizations said they lacked proper AI access controls. An additional 8% of breached organizations were unsure if their breach involved an AI security incident.
See Figure 18.

Figure 18.
From organizations that reported a security incident on an AI model or application

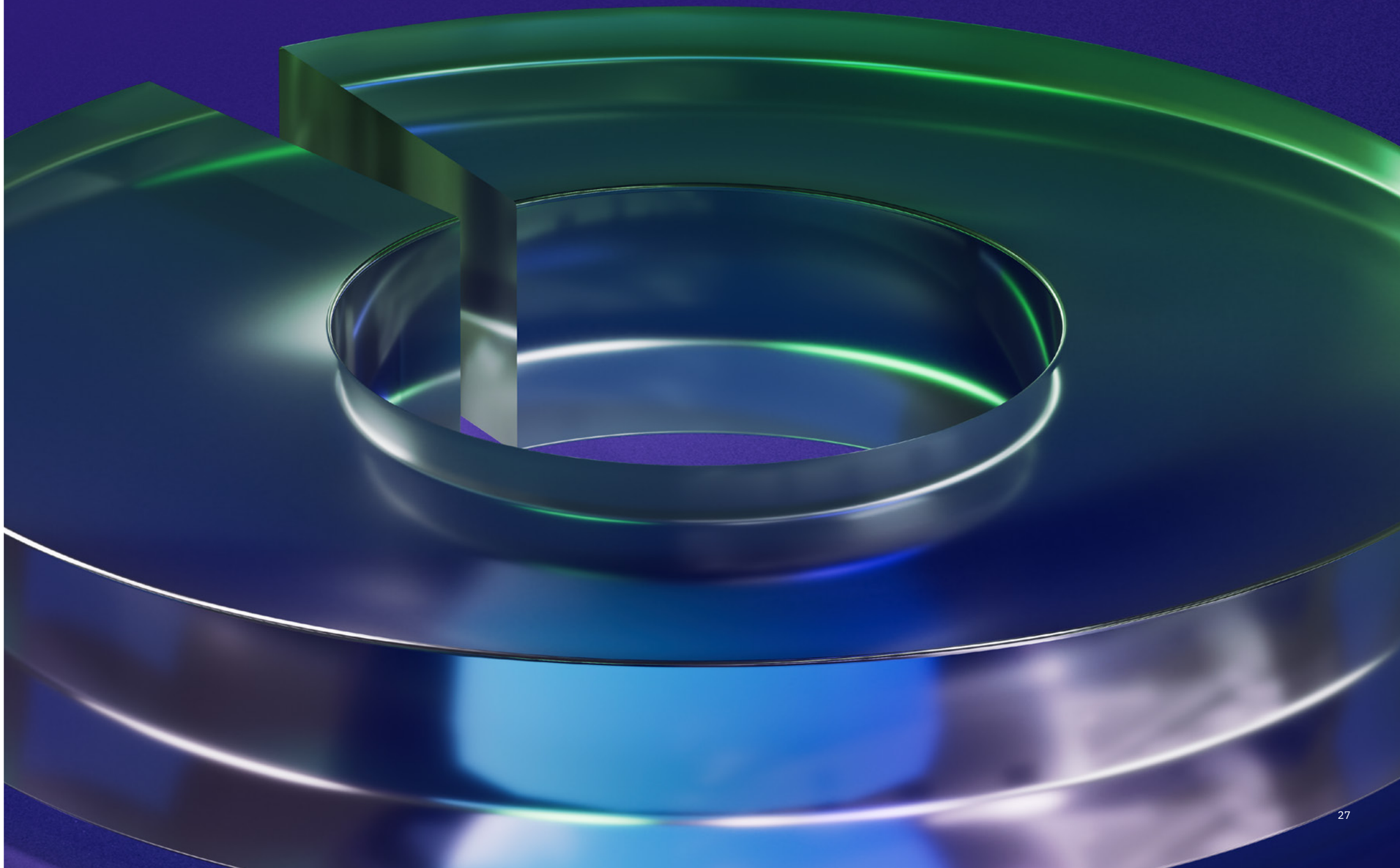
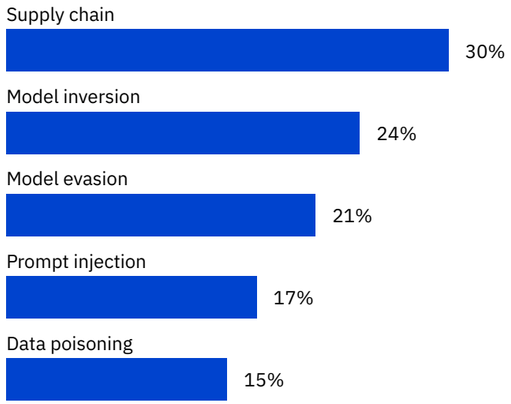
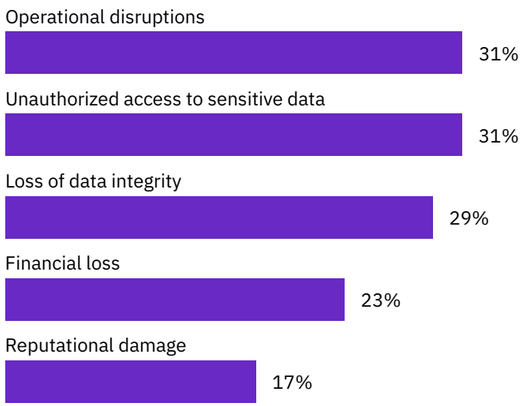


Figure 19.
From organizations that reported a security incident involving an AI model or application; more than one response permitted



Supply chain compromise was the most common cause of AI security incidents
Security incidents involving AI models and applications were varied, but one type clearly claimed the top ranking: supply chain compromise (30%), which includes compromised apps, APIs and plug-ins. Following supply chain compromise were model inversions (24%) and model evasions (21%). Incidents involving prompt injections and data poisonings made up 17% and 15% of cases respectively. See Figure 19.

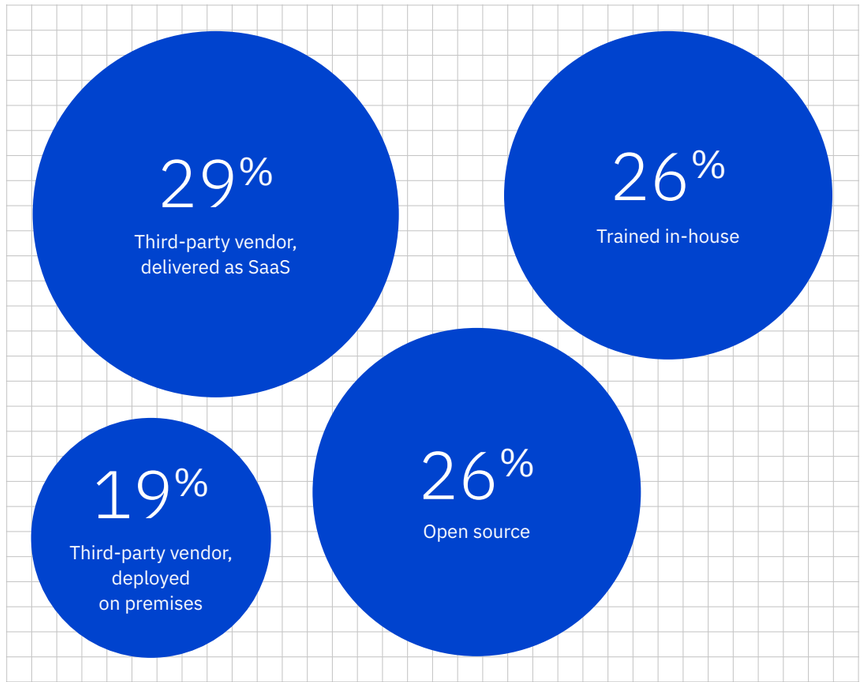
Figure 20.
From organizations that reported a security incident involving an AI model or application; more than one response permitted



Impacts of security incidents on authorized AI
Approximately one-third (31%) of organizations that experienced a security incident involving authorized AI suffered operational disruption and saw attackers gain unauthorized access to sensitive data. 29% of organizations reported a loss of data integrity. The impact of reputational damage (17%) underscores the potential long-tailed effects of these incidents.
See Figure 20.

Most AI security incidents came from AI delivered as software as a service (SaaS)
From a security and governance standpoint, where an AI model or application comes from matters. The majority of organizations that reported a security incident involving AI said the source was a third-party vendor and delivered as SaaS (29%). There were fewer incidents involving AI from third-party vendors that were deployed on premises (19%). However, the risks to in-house and open-source models—at 26%—were a close second to the AI delivered by SaaS. See Figure 21.

Figure 21.
From organizations that experienced a security incident involving an AI model or application



Unsanctioned AI security incidents were more common than sanctioned AI
Shadow AI may go undetected by an organization, and attackers can exploit its vulnerabilities when employees use it. Security incidents involving shadow AI accounted for 20% of breaches, which is 7 percentage points higher than those security incidents involving sanctioned AI. A further 11% of breached organizations were unsure if they experienced a shadow AI incident.
See Figure 22.

Figure 22.
Has your organization experienced a security incident involving shadow AI?

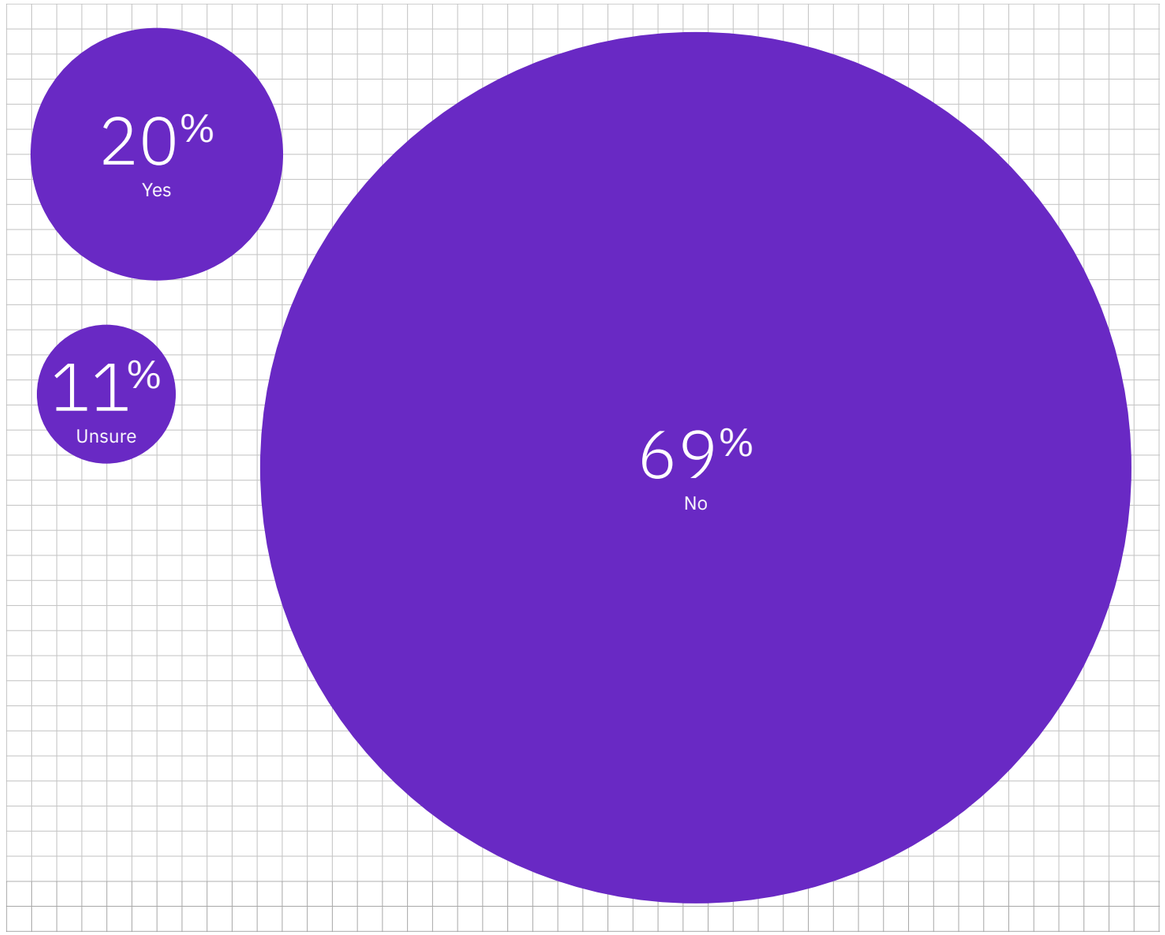


Figure 23.
Percentage of breaches involving shadow AI; only one response permitted

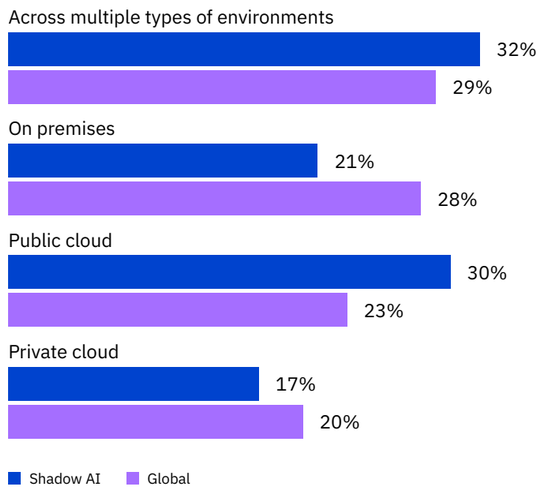
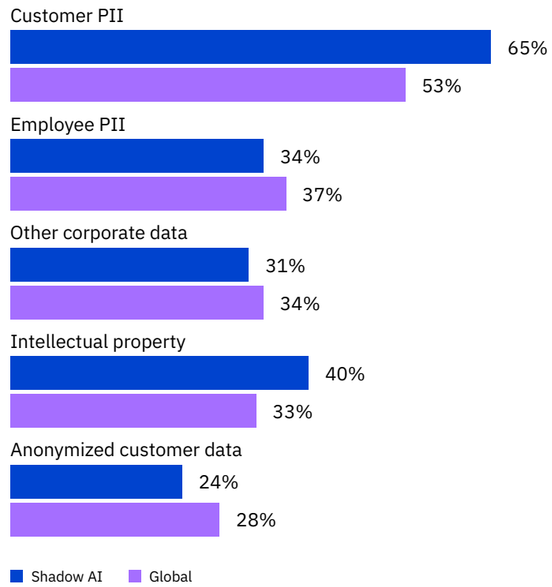


Figure 24.
Percentage of breaches involving shadow AI; more than one response permitted



Data stored across environments was the most breached in shadow AI incidents
Organizations that suffered a shadow AI security incident reported the breached data was most often stored across multiple environments and a public cloud (62%). See Figure 23.

Customer PII was the most common data compromised in shadow AI incidents
One of the most valuable types of data for attackers to target is customer PII. It can be used for financial and insurance fraud or for sale on the dark web. Likely because of those reasons, customer PII was the most compromised data type (65%). That figure is notably higher than the overall global share of PII reported compromised in this year's report (53%).
See Figure 24.

Customer PII was the most valuable record type compromised in a shadow AI incident
In addition to being the most compromised record type in a shadow AI security incident, customer PII was also the most expensive at USD 166 per record. That figure was slightly above the overall global average for this record type at USD 160. The cost of other record types was slightly lower in these security incidents than the overall global average. See Figure 25.

Internal security teams identified more shadow AI security incidents than did third parties
Organizations' security teams and tools identified most AI security incidents (57%), which was better than they did for overall breach discoveries (50%). Meanwhile, the share of AI security incidents attackers disclosed (12%) was lower than the overall global breach disclosure (19%). See Figure 26.

USD
200K
Added cost of a breach involving shadow AI

Shadow AI security incidents cost more
Security incidents involving shadow AI carried an added cost. They contributed USD 200,000 to the global average breach cost. This higher cost was likely driven by longer detection and containment times for these security incidents, approximately a week longer than the global average. See Figure 27.

Figure 25.
Measured in USD; more than one response permitted

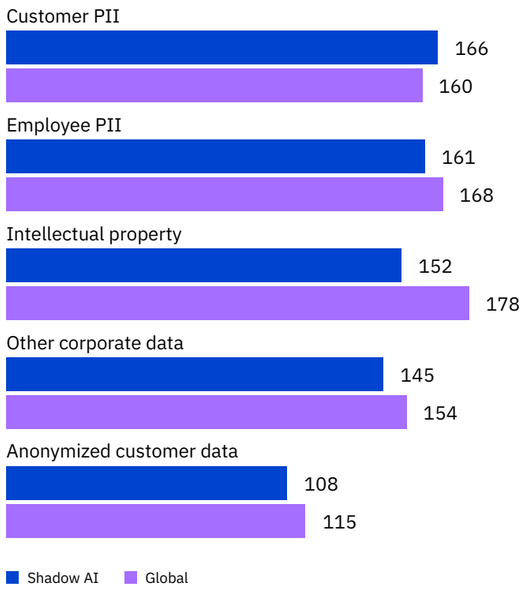


Figure 26.
Identification of breaches involving shadow AI

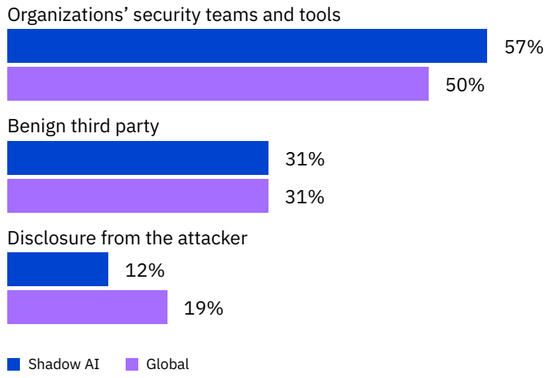
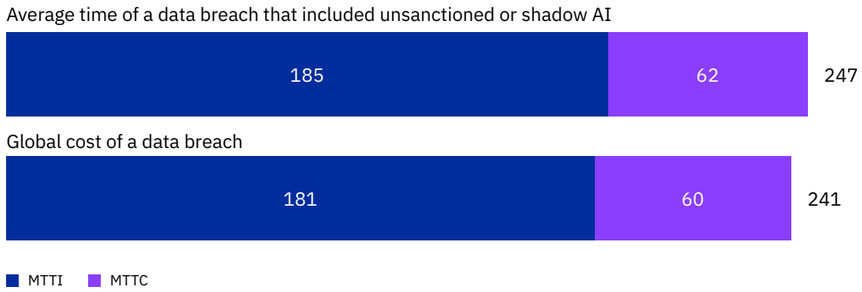


Figure 27.
Measured in days



AI governance

AI adoption has outpaced oversight. This year's research quantifies that governance gap and the costs it carries. Most organizations said they didn't have governance policies to mitigate or manage the risk to AI. For those that do, less than half have strict approvals for AI deployments. That deficiency had consequences. Not only do these organizations leave themselves open to security, operational and reputational risks, but they've paid a steeper cost than average when breached.

63%

Share of organizations that lacked AI governance policies

Most organizations lacked governance to manage AI or detect shadow AI

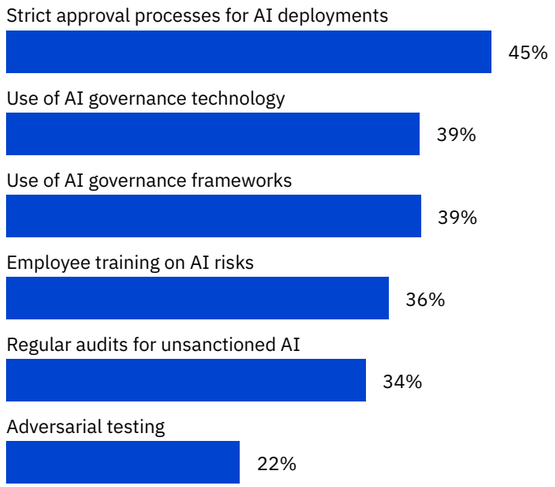
Oversight of AI—and the ability for IT and security teams to identify shadow AI—is essential for organizations to ensure the ethical, legal and responsible development and use of AI among employees. However, nearly two-thirds of organizations (63%) said they don't have governance policies in place to manage AI or detect shadow AI. See Figure 28.

Figure 28.
From all organizations

37%

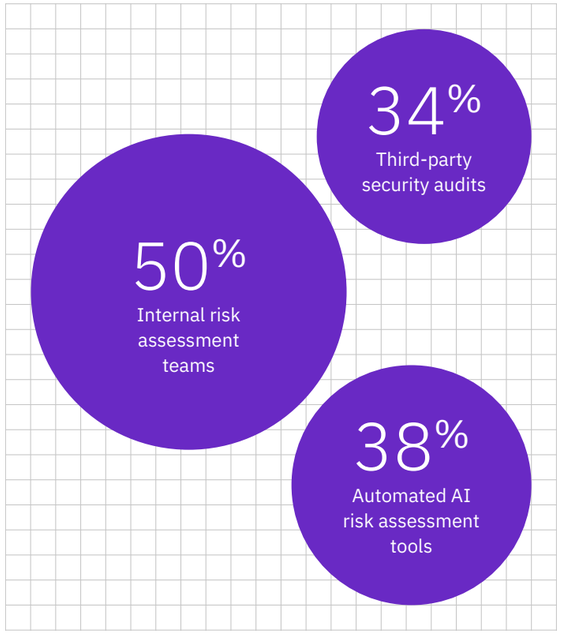
Share of organizations that had AI governance policies in place

Figure 29.
From organizations that had AI governance policies in place; more than one response permitted



Approval processes for AI were the top type of governance policy
AI governance technology, frameworks and employee training all play important roles in ensuring trustworthy and ethical AI. Among the 37% minority of organizations that had AI governance policies, these three areas had a nearly equal share of approximately one-third. But the most common AI governance policy reported among this group was strict approval procedures for AI deployments (45%). See Figure 29.

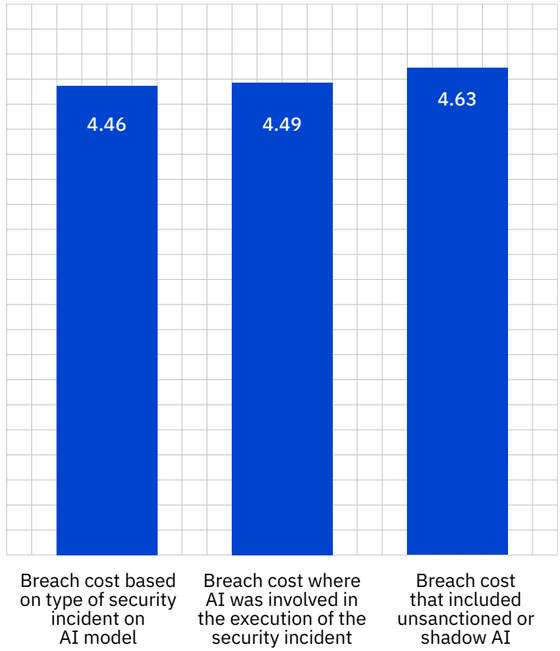
Figure 30.
From organizations that had AI governance policies in place; more than one response permitted



Half of all AI model evasion assessments come from internal teams
AI model evasion attacks—which attempt to make the AI model misbehave by manipulating data inputs—are relatively rare, but they carry a heavy risk. Researchers have previously shown these attacks can lead to financial loss, reputational damage and even endanger lives in critical applications, such as autonomous vehicles and medical diagnosis. This report found four out of five organizations have processes in place to assess the risk of these attacks, and half use internal risk assessment teams to do so. A further 38% use automated risk assessment tools, while 34% rely on third-party security audits. See Figure 30.

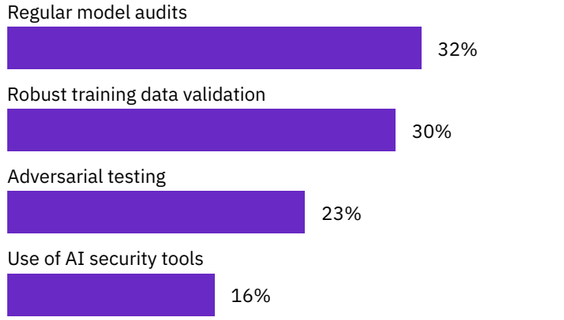
Effect of AI on data breach costs
Whether an attacker used AI against an organization—through phishing, for example—or targeted the organization's AI, the average cost of the breach was similar (USD 4.49 million and USD 4.46 million, respectively). However, if the breach involved a security incident with shadow AI, the average cost was higher (USD 4.63 million). See Figure 31.

Figure 31.
Measured in USD millions



Most organizations have no governance in place to mitigate AI risk
87% of organizations said they have no governance policies or processes to mitigate AI risk. Nearly two-thirds of breached organizations didn't perform regular audits on their AI models to mitigate risk. And over three-quarters reported not performing adversarial testing on their AI models. See Figure 32.

Figure 32.
Percentage of breaches involving an AI model; more than one response permitted



AI-driven attacks

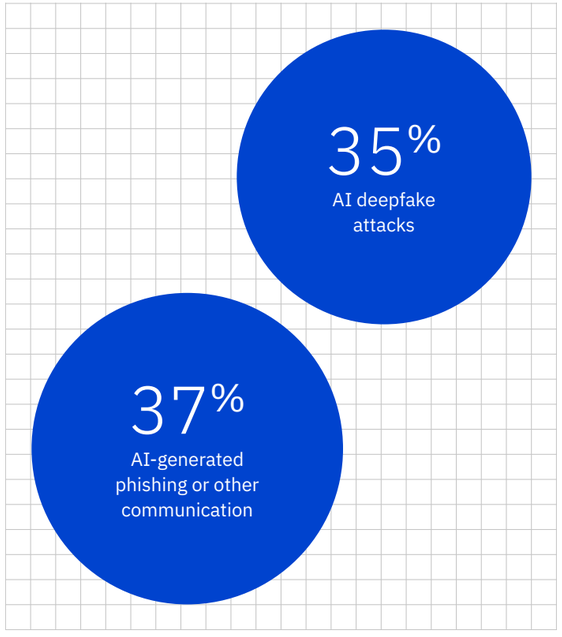
Attackers are using gen AI to improve and scale their creative writing and image generation. By crafting highly personalized emails, voices and videos mimicking real people or brands, attackers can make their fake appeals harder to detect. For the first time, this report's research analyzed the prevalence of those AI-driven attacks.

Attackers are using AI to manipulate humans
Researchers found 16% of breaches involved attackers using AI. Most of these breaches focused on human manipulation through phishing (37%) or deepfake attacks (35%). See Figure 33.

16%

Share of breaches that involved attackers using AI

Figure 33.
Types and percentages of AI-driven attacks used on organizations that experienced a breach

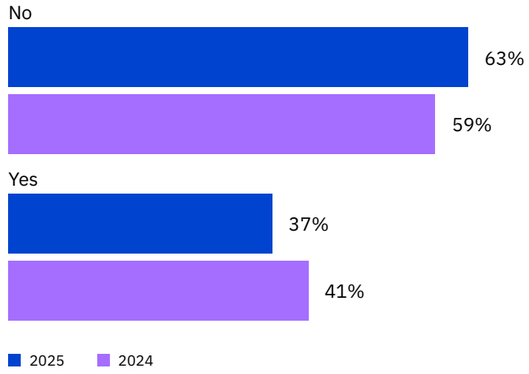


Ransomware attacks

Ransomware fatigue appears to be growing. More organizations are opting not to pay the ransom demands, even as the cost of an extortion or ransomware incident remains high. Also, more organizations are deciding against involving law enforcement, even as researchers found last year that calling in law enforcement dramatically reduced the global average cost of a breach.

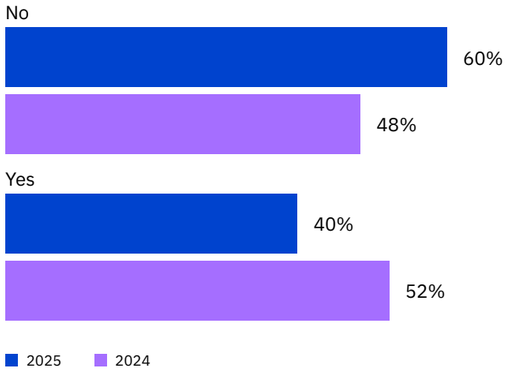
Nearly two-thirds of ransomware victims refused to pay the ransom
Organizations pushed back against ransom demands, with more opting not to pay (63%) compared to the previous year (59%). However, even though more organizations refuse to pay ransom demands, the average cost of an extortion or ransomware incident remained high, particularly when disclosed by an attacker. See Figure 34.

Figure 34.
If your organization was hit with a ransomware attack, did your organization pay the ransom?



Fewer organizations involved law enforcement
Last year, organizations saw an average cost savings of USD 1 million when they involved law enforcement in ransomware attacks. However, they didn't see—or realize—that benefit this year: the share of organizations that involved law enforcement fell to 40%, down from 52% in 2024. See Figure 35.

Figure 35.
Was law enforcement contacted and involved following the ransomware attack?



Raising prices post-breach

By nature, data breaches are costly. Organizations looking to recover those costs might choose to pass them on to customers. However, in price-sensitive markets or moments, that strategy may backfire. In this year's report, compiled during a period when inflation was—and is—top of mind for many consumers, organizations appeared less likely than before to pass along breach costs in the form of price hikes.

Fewer organizations plan to pass breach costs to customers
The share of organizations that said they would pass breach costs on to customers fell by nearly a third to 45% in this year's report, down from 63% last year. However, approximately a third said they would hike prices more than 15%. See Figures 36 and 37.

Figure 36.
Did the data breach result in your organization increasing the cost of its services and products?

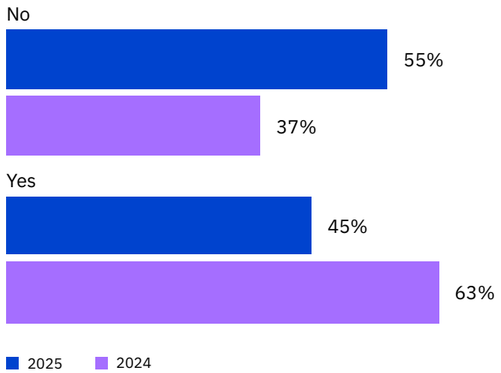
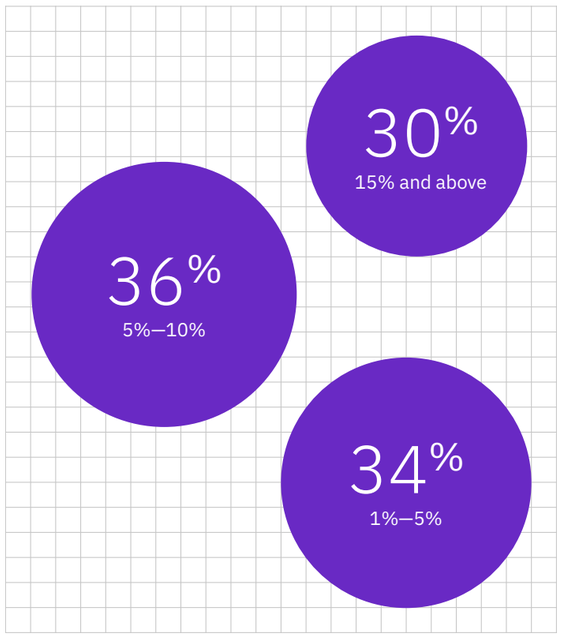


Figure 37.
If yes, by what percent were costs increased?



Business disruption

Breaches can happen in seconds, but the ripple effect can last for months or even years. As a result, most breached organizations in this year's report suffered operational disruption. The growth of AI complicates this picture further by expanding and introducing new and potentially fragile interdependent and interconnected systems that are linked to operational activities.

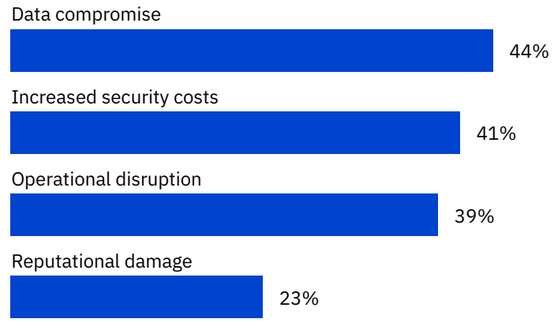
A majority of data breaches disrupted operations
Data breaches can disrupt the ability of organizations to process sales orders, provide customer services and keep their production lines running. This year's report found 86% of organizations experienced this sort of operational disruption.

86%

Share of businesses that experienced a disruption due to a data breach

Impacts of security incidents involving shadow AI
Among organizations that experienced a security incident involving shadow AI, 44% suffered data compromise. Another 41% reported increased security costs as a result of those incidents. Operational disruption was more widespread than incidents involving authorized AI. These results suggest shadow AI incidents have an outsized impact on downstream breach issues that extend beyond data security. See Figure 38.

Figure 38.
Impact of a shadow AI incident; more than one response permitted



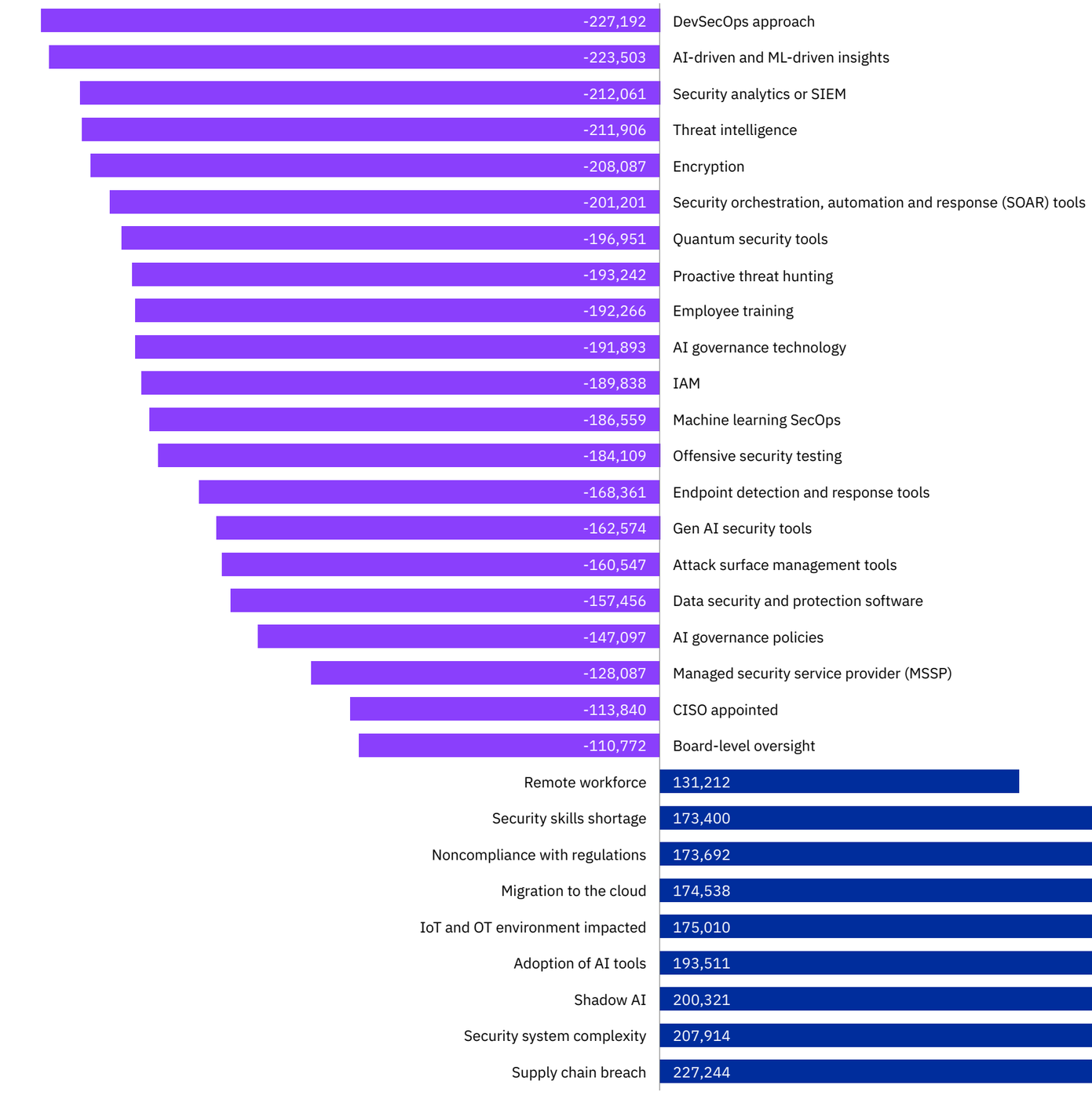
Factors that increase or decrease breach costs

When analyzing breach costs, it's important security leaders understand which technologies or events tend to lower or raise those costs. One constant we've found year over year: security AI and automation lowers costs. This year we also found the use of shadow AI raises costs. Our analysis examined 30 contributing factors and the impact of each in isolation against the global average. Also included are the top three factors found to amplify or mitigate the average data breach cost.

Key factors that reduced costs
Taking a DevSecOps approach to software development was the number one factor that reduced breach costs in this year's report. The use of AI and machine-learning insights, as well as having a security information and event management (SIEM) platform for detecting and responding to threats, rounded out the top three cost-reducing factors. All three of these security approaches center around and strengthen insight, intelligence and coordination. See Figure 39.

Key factors that increased costs
Security system complexity and supply chain breaches continue to challenge security teams and add to the average cost of a data breach. Both involve systems, networks and workflows with potential blind spots that can lead to vulnerability. The new addition to this year's top three costliest factors is shadow AI. Its presence within an organization is an added blind spot, another attack surface that is hard to police. As we've shown elsewhere in this report, organizations often don't look for shadow AI, so it remains undetected. See Figure 39.

Figure 39.
Cost difference from USD 4.88M breach average; measured in USD

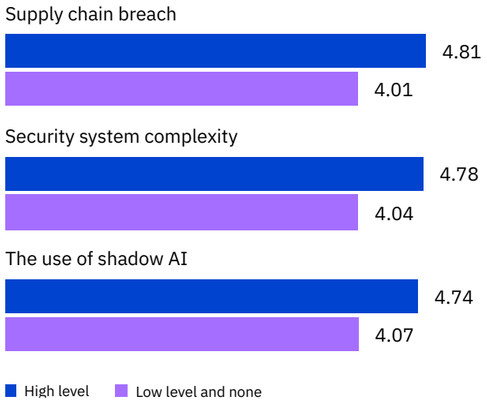


670K

Added cost of a breach, in USD, for organizations with high levels of shadow AI versus those that had low levels or none

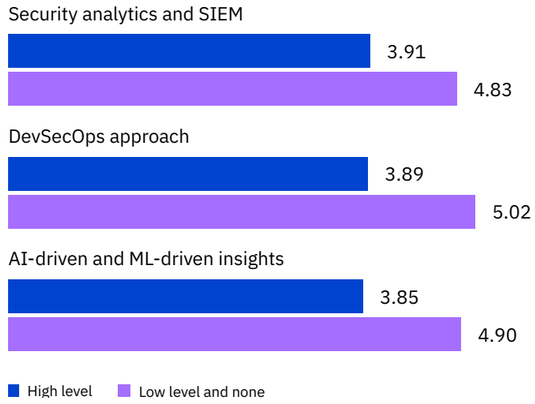
High levels of shadow AI drove up costs
When organizations used a high level of shadow AI, their average breach costs were USD 4.74 million, which is USD 670,000 higher than organizations that had a low level or no shadow AI (USD 4.07 million). Similar disparities were seen with the other two key cost amplifying factors. See Figure 40.

Figure 40.
Measured in USD millions



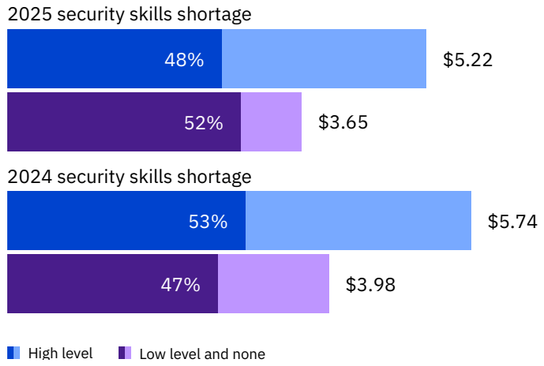
High versus low levels of key cost mitigating factors
When organizations used AI or machine-learning insights in their security, their average breach costs were USD 3.85 million, compared to USD 4.9 million for organizations that used these technologies at a low level or not at all. For the other two cost mitigating factors, DevSecOps created a similar difference, while SIEM created slightly less of a difference, at USD 3.91 million versus USD 4.83 million. See Figure 41.

Figure 41.
Measured in USD millions



Security skills shortages remain costly
The cybersecurity skills shortage has challenged the industry for years. This year's report found 48% of organizations had a high level of security skills shortage, down from 53% last year. However, those high skills shortages continue to exert pressure, equating to USD 5.22 million in average breach costs compared to USD 3.65 million for organizations that had a low level or no skills shortage. See Figure 42.

Figure 42.
Measured in USD millions

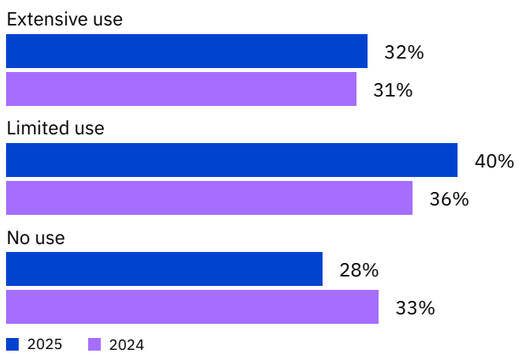


Security AI and automation

AI and automation play an increasingly crucial role in security, providing defenders with speed and scale. Both are necessary for securing organizations and detecting and responding to AI-driven threats from attackers. Since AI tools act as a skills multiplier, security teams can oversee more systems and react quickly to possible threats. While this year's report found these technologies accelerated the work of identifying and containing breaches and reducing costs, adoption rates appear to be uneven.

Extensive AI and automation use remained constant
The share of organizations that used security AI and automation extensively ticked up slightly to 32% in this year's report compared to 31% last year. Organizations that used these tools in a limited way rose to 40% from 36%. Although that increase is just a four-percentage-point difference, it represents an 11% increase in use. Correspondingly, those claiming no use dropped to 28% in this year's report from 33% last year. See Figure 43.

Figure 43.
Percentage of organizations per usage level



More AI and automation equaled lower breach costs

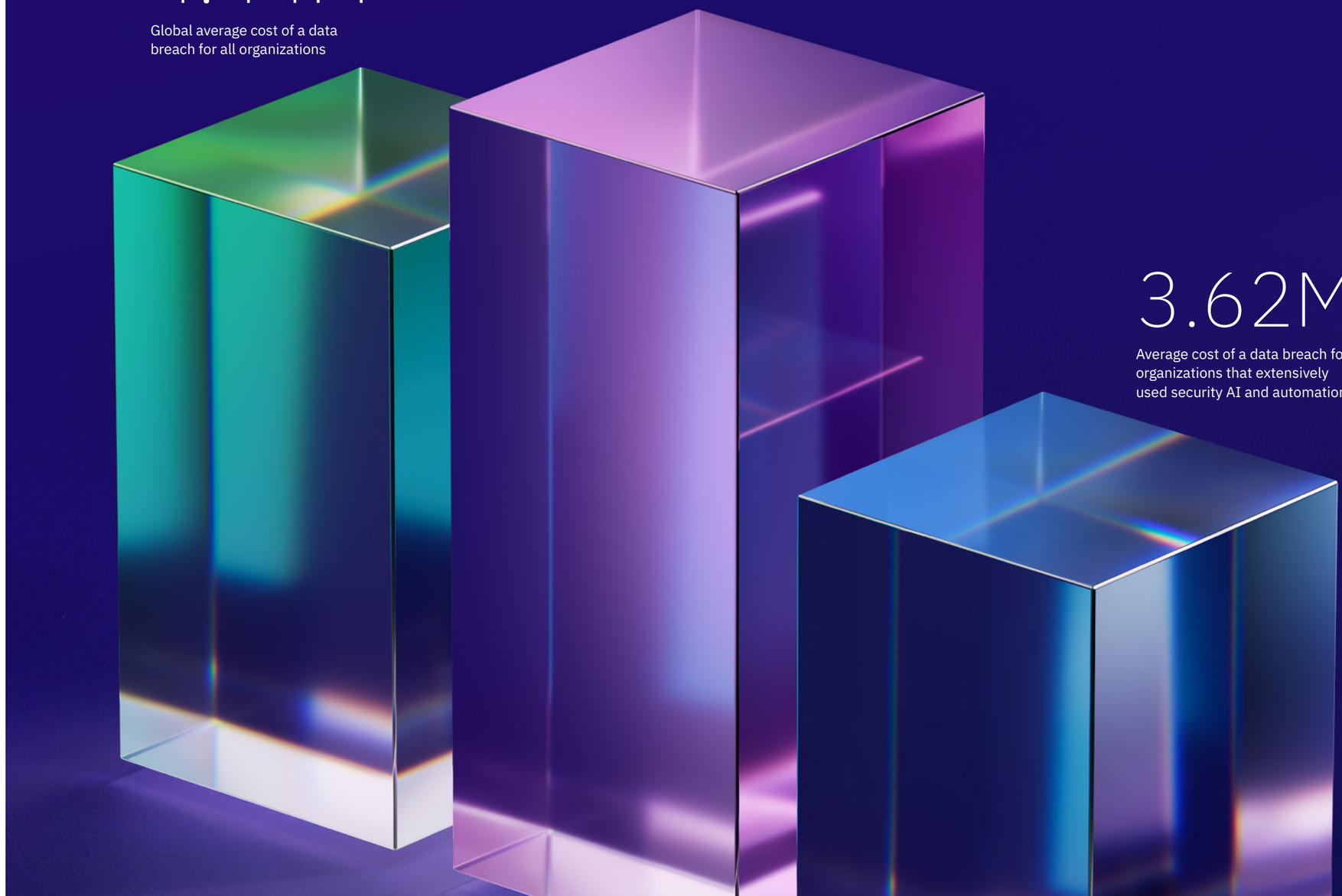
Security AI and automation continue to drive down breach costs. This correlation was noted last year and gained momentum this year. Organizations that didn't use AI or automation had an average breach cost of USD 5.52 million, while those that used these technologies extensively had an average breach cost of USD 3.62 million. These figures represent a USD 200,000 improvement over last year, and a savings of USD 1.9 million. See Figure 44.

Figure 44.
Measured in USD

4.44M
Global average cost of a data breach for all organizations

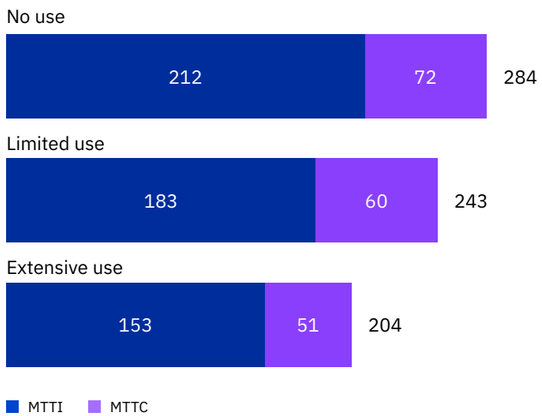
5.52M
Average cost of a data breach for organizations that didn't use security AI and automation

3.62M
Average cost of a data breach for organizations that extensively used security AI and automation



More AI and automation meant faster identification and containment
By extensively using AI and automation, organizations drove down the time it took to identify and contain a breach by an average of 80 days compared to those that didn't use AI and automation. Those quicker speeds directly equated to cost savings. See Figure 45.

Figure 45.
Time to identify and contain a breach with and without AI and automation; measured in days



Security teams used AI and automation evenly across workflows
Among organizations that said they used AI and automation extensively, nearly one-third did so across the full cybersecurity lifecycle: prevention, detection, investigation and response. Meanwhile, organizations that used these technologies in a limited way reported the same level of dispersion across the security lifecycle, but at slightly over 40%. See Figure 46.

Figure 46.
Percentage of organizations per usage level

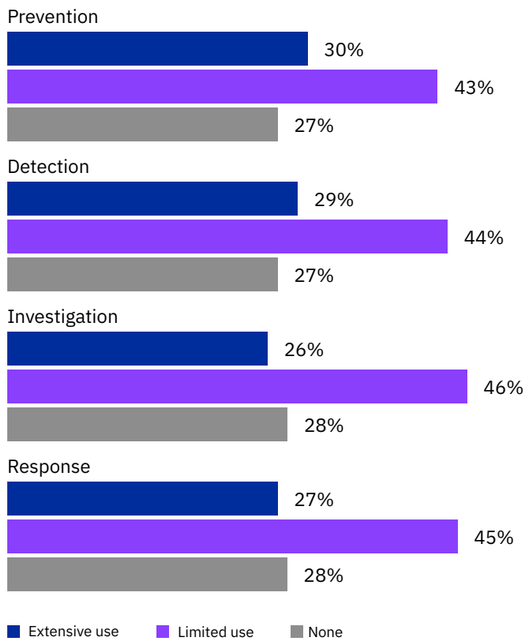
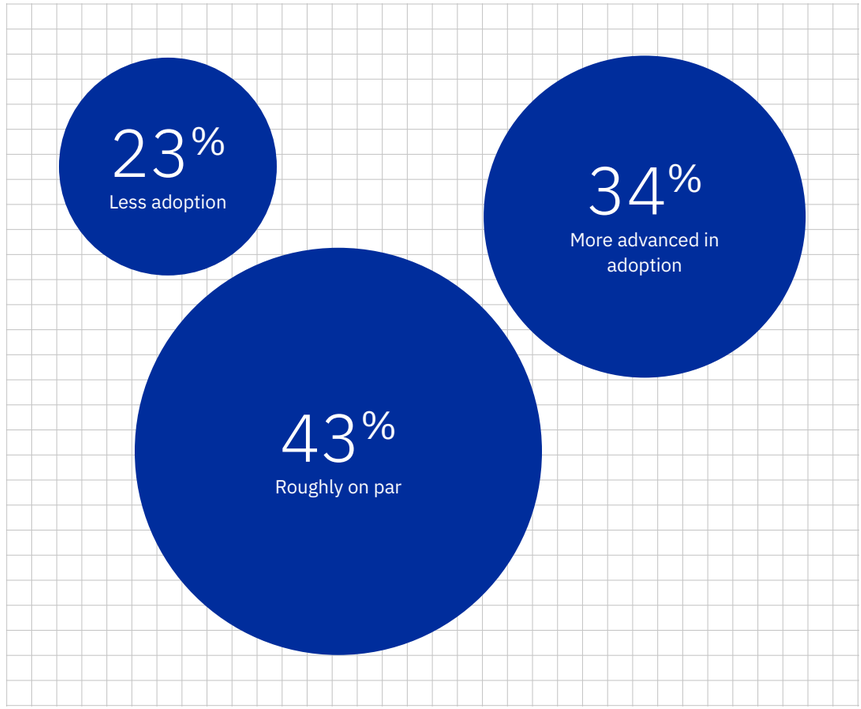


Figure 47.
Percentage of all organizations



Security teams adopted AI at the same rate as other business functions
This year's report aimed to discover if security teams were adopting AI at the same pace as other business units and functions in the wider organization. They are. A combined 77% were either adopting these technologies on par with (43%) or more advanced than (34%) their wider organization.
See Figure 47.

Security investments

Following a breach, security and IT leaders often turn their attention to fortifying their security defenses. Each year, organizations are asked if they plan to invest in new security measures and if so, where. Organizations in this study were allowed to choose more than one area of investment.

Post-breach investment declined
Less than half of organizations (49%) said they would increase security investments following a breach, a 22% drop over last year. While we saw more expected security investments post-breach last year, this year's anticipated slowdown might be attributed to organizations taking a more disciplined approach to evaluating which security initiatives deliver impact. For those organizations that do plan to increase security spending, the top three areas of investments were: threat detection (43%), data security and protection tools (37%), and IR planning and testing (35%). See Figures 48 and 49.

Figure 48.
Following the data breach, will your organization increase its security investment?

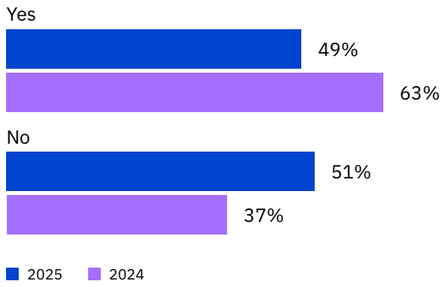
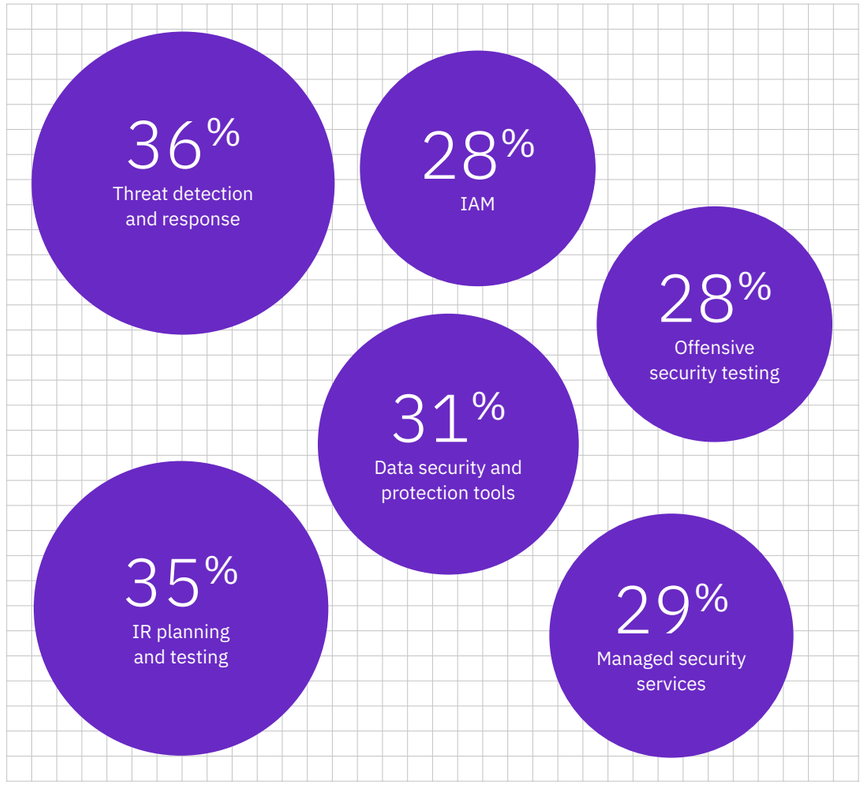


Figure 49.
Categories among organizations that will increase security investment; more than one response permitted

Figure 50.
Categories among post-breach organizations that plan to invest in AI-driven solutions, by percentage; more than one response permitted



AI-driven security solution investments remain strong
For organizations that plan to invest in security after a breach, 45% said they would choose AI-driven solutions. They also said they would do so fairly evenly across threat detection and response (36%), IR planning and testing (35%) and data security and protection tools (31%). See Figure 50.

Recommendations

To help prevent, mitigate and reduce the costs of a data breach, as well as secure and govern AI models, applications and usage, IBM experts suggest these five successful approaches.

Fortify identities—human and machine

Many organizations operate with lax access controls, over-permissioned accounts and low visibility into who has access to critical systems. In many cases, different departments and tools are used for identity and access management (IAM). All these factors create openings attackers are actively exploiting, so it's essential to limit such openings. Meanwhile, AI models and infrastructure are rapidly growing, offering attackers a new, high-value attack surface.

Fortifying identity security with the help of AI and automation can improve IAM without overburdening chronically understaffed security teams. And as AI agents begin to play a larger role in organizational operations, the same rigor must be applied to protecting agent identities as to protecting human identities. Just like human users, AI agents increasingly rely on credentials to access systems and perform tasks. So, it's essential to implement strong operational controls, or services that can help you do so, and maintain visibility into all non-human identity (NHI) activity. Organizations must be able to distinguish between NHIs using managed (vaulted) credentials and those using unmanaged credentials.

Once credentials are brought under management, it's crucial to protect and enforce proper lifecycle management and governance. It includes provisioning, rotation, auditing, protection and decommissioning of credentials, as well as monitoring the behavior of NHIs to ensure they operate within expected parameters. By doing so, organizations can reduce the risk of credential misuse and maintain a secure and compliant environment.

Today, many attackers are logging in rather than hacking in. To combat this issue, it's critical to prevent attackers from obtaining those credentials in the first place. One of the most effective ways to do so is by ensuring all human users adopt modern, phishing-resistant authentication methods, such as passkeys. These technologies are designed to eliminate the vulnerabilities of traditional passwords and one-time codes, making it significantly harder for attackers to intercept or misuse login credentials.

Elevate AI data security practices

Organizations have now moved beyond the experimentation phase with gen AI and AI agents into real-world innovation, weaving the technology deep into the fabric of their businesses. But the speed of adoption is outpacing security. This year's report found 97% of organizations that experienced an AI-related incident lacked proper access controls on AI systems. And because data is the fuel for AI, it's a prime target for attackers.

Securing AI data is essential not just for privacy and compliance, but also to protect data integrity, maintain organizational trust and avoid data compromise. This approach means going beyond surface-level controls and implementing strong data security fundamentals: data discovery and classification, as well as data protections, such as access control, encryption and key management. It can also include the use of data and AI security services. These measures aren't unique to securing AI, but the rise of AI as both a threat vector and security helper means they're more important than ever before.

Connect security for AI and governance for AI

Security for AI and governance for AI are complementary disciplines. When organizations keep them in silos, they increase risk, complexity and cost. Unfortunately, AI adoption is outpacing security and governance adoption: 41% of organizations in this year's report said they didn't have such policies in place, and 22% are still developing them.

Organizations must ensure chief information security officers (CISOs), chief revenue officers (CROs) and chief compliances officers (CCOs)—and their teams—collaborate regularly. Investing in integrated security and governance software and processes to bring these cross-functional stakeholders together can help organizations automatically discover and govern shadow AI. Such investments can also help them:

- Gain visibility into all AI deployments.
- Identify and mitigate vulnerabilities.
- Protect the prompts and data generated from unintended use.
- Use observability tools to improve compliance and detect anomalies.

Use AI security tools and automation to move faster

AI is already helping attackers move faster—for example, making deepfakes easy to create with just a few prompts, or cutting the time needed to produce a realistic phishing message from hours to minutes. As attackers turn to AI to produce and distribute more adaptive attacks, security teams should also embrace AI technologies. Security teams can use AI to reduce or prevent attacks and their business impacts, proactively employing measures that improve the accuracy of detection (threat hunting) and reduce the time to respond.

Security tools and managed security services, including those powered by AI and automation, can augment already overburdened security teams. They can significantly reduce the volume of alerts; identify at-risk data; spot security gaps and threats earlier; detect in-progress breaches; and enable faster, more precise attack responses.

Improve resilience

On a long enough timeline, data breaches are inevitable. They happen despite strong preventative measures. While it's important to try to block threats, it can't be an organization's only focus. They must also focus on, and plan for, minimizing damage once an attack gets through and a breach occurs.

Building resilience means being able to detect issues quickly, contain them before they cause significant impact and recover operations quickly with minimal disruption. A plan for building resilience should include regularly testing IR plans and restoration of backups, ensuring clear roles and responsibilities during crisis response—even for nontechnical leaders—and limiting high-level access to reduce the scope of a potential problem. In-person or virtual training can be essential in helping security teams understand their roles and execute in a crisis. To enhance their ability to handle attacks, organizations can also participate in cyber range crisis simulation exercises.

Organization demographics

This year's study examined 600 organizations of various sizes across 16 countries and geographic regions and 17 industries. This section explores the breakdown of organizations in the study by geography and industry and defines the industry classifications.

Geographic demographics

The 2025 study was conducted across 16 countries and geographic regions. For the second year the study included Benelux, the economic union of Belgium, the Netherlands and Luxembourg.

ASEAN is a cluster sample of organizations located in Singapore, Indonesia, Philippines, Malaysia, Thailand and Vietnam. Latin America is a cluster sample of organizations located in Mexico, Argentina, Chile and Colombia. Middle East is a cluster sample of organizations located in Saudi Arabia and the United Arab Emirates.

Distribution by sample or region

ASEAN	4%	Australia	5%
US	11%	Benelux	5%
India	9%	Canada	5%
Brazil	8%	LATAM	5%
UK	8%	South Korea	5%
Germany	7%	ASEAN	4%
Japan	7%	Italy	4%
Middle East	7%	South Africa	4%
France	6%		

Industry demographics

The selection of 17 industries has been consistent across multiple years of the study. This year, the top 4 industries—financial, industrial, professional services and technology—accounted for 47% of the 600 organizations studied.

Industry

Financial	14%	Consumer	4%
Industrial	12%	Hospitality	4%
Services	11%	Media	3%
Technology	10%	Pharma	3%
Energy	8%	Education	3%
Public	7%	Research	2%
Communications	6%	Healthcare	2%
Transportation	5%	Entertainment	1%
Retail	5%		

Industry definitions

Healthcare
Hospitals and clinics

Financial
Banking, insurance and investment companies

Energy
Oil and gas companies, utilities and alternative energy producers and suppliers

Pharmaceuticals
Pharmaceutical companies, including biomedical life sciences

Industrial
Chemical processing and engineering, and manufacturing companies

Technology
Software and hardware companies

Education
Public and private universities and colleges, and training and development companies

Professional services
Services such as legal, accounting and consulting firms

Entertainment
Movie production, sports, gaming and casinos

Transportation
Airlines, railroads and trucking, and delivery companies

Communications
Newspapers, book publishers, and public relations and advertising agencies

Consumer
Manufacturers and distributors of consumer products

Media
Television, satellite, social media and internet

Hospitality
Hotels, restaurant chains and cruise lines

Retail
Brick and mortar and e-commerce

Research
Market research, think tanks, and research and development

Public
Federal, state and local government agencies, and nongovernmental organizations

Research methodology

The numerical value obtained from the number line, rather than a point estimate for each presented cost category, preserved confidentiality and ensured a higher response rate. The benchmark instrument also required respondents to provide a second separate estimate for indirect and opportunity costs.

In the interest of maintaining a manageable dataset for benchmarking, the report included only those cost activity centers with a crucial impact on data breach costs. Based on discussions with experts, a fixed set of cost activities was chosen. After collecting benchmark information, each instrument was carefully reexamined for consistency and completeness.

The scope of data breach cost factors was limited to known categories that apply to a broad set of business operations involving personal information. We chose to focus on business processes instead of data protection or privacy compliance activities because we believed the process study would yield better-quality results.

How we calculate the cost of a data breach

To calculate the average cost of a data breach, we excluded very small and very large breaches. Data breaches examined in the 2025 report ranged in size between 2,960 and 113,620 compromised records.

We used activity-based costing, which identifies activities and assigns a cost according to actual use. Four process-related activities drove a range of expenditures associated with an organization's data breach: detection and escalation, notification, post-breach response and lost business.

Detection and escalation
Activities that enable an organization to detect the breach include:

- Forensic and investigative activities
- Assessment and audit services
- Crisis management
- Communications to executives and boards

Notification
Activities that enable an organization to notify data subjects, data protection regulators and other third parties include:

- Emails, letters, outbound calls or general notices to data subjects
- Determination of regulatory requirements
- Communication with regulators
- Engagement of outside experts

Post-breach response
Activities to help victims of a breach communicate with an organization and conduct redress activities to victims and regulators include:

- Help desk and inbound communications
- Credit monitoring and identity protection services
- Issuing of new accounts or credit cards
- Legal expenditures
- Product discounts
- Regulatory fines

Lost business
Activities that attempt to minimize the loss of customers, business disruption and revenue losses include:

- Business disruption and revenue losses due to system downtime
- Cost of losing customers and acquiring new customers
- Reputational damage and diminished goodwill

Data breach FAQs

What's a data breach?
A data breach is defined as an event in which records containing PII; financial or medical account details; or other secret, confidential or proprietary data are potentially put at risk. These records can be in electronic or paper format. Breaches included in the study ranged between 2,960 and 113,620 compromised records.

What's a compromised record?
A record is information that reveals confidential or proprietary corporate, governmental or financial data, or identifies an individual whose information has been lost or stolen in a data breach. Examples include a database with an individual's name, credit card information and other PII, or a health record with the policyholder's name and payment information.

How do you collect the data?
Our researchers collected in-depth qualitative data over 3,470 separate interviews with individuals at 600 organizations that suffered a data breach between March 2024 and February 2025. Interviewees were familiar with their organization's data breach and the costs associated with resolving the breach. These interviewees included CEOs or executives, heads of operations, controllers or heads of finance, IT practitioners, business unit leaders and general managers, and risk management and cybersecurity practitioners. For privacy purposes, we didn't collect organization-specific information.

What's included in the cost of a data breach?
We collected both the direct and indirect expenses incurred by the organization. Direct expenses included engaging forensic experts, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and services. Indirect costs included in-house investigations and communications along with the extrapolated value of customer loss resulting from turnover or diminished customer acquisition rates.

This research represented only events directly relevant to the data breach experience. Regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), may encourage organizations to increase investments in their cybersecurity governance technologies. However, such activities didn't directly affect the cost of a data breach for this research. For consistency with prior years, we used the same currency translation method rather than adjusting accounting costs.

How does benchmark research differ from survey research?
The unit of analysis in the Cost of a Data Breach Report was the organization. In survey research, the unit of analysis is the individual. We recruited 600 organizations to participate in this study.

Can the average per-record cost be used to calculate the cost of breaches involving millions of lost or stolen records?
It's not consistent with this research to use the overall cost per record as a basis for calculating the cost of single or multiple breaches totaling millions of records. The per-record cost is derived from our study of hundreds of data breach events in which each event featured a maximum of 113,000 compromised records.

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 477 **May 11, 2017**

Securing Communication of Protected Client Information

A lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

I. Introduction

In Formal Opinion 99-413 this Committee addressed a lawyer's confidentiality obligations for e-mail communications with clients. While the basic obligations of confidentiality remain applicable today, the role and risks of technology in the practice of law have evolved since 1999 prompting the need to update Opinion 99-413.

Formal Opinion 99-413 concluded: "Lawyers have a reasonable expectation of privacy in communications made by all forms of e-mail, including unencrypted e-mail sent on the Internet, despite some risk of interception and disclosure. It therefore follows that its use is consistent with the duty under Rule 1.6 to use reasonable means to maintain the confidentiality of information relating to a client's representation."[1]

Unlike 1999 where multiple methods of communication were prevalent, today, many lawyers primarily use electronic means to communicate and exchange documents with clients, other lawyers, and even with other persons who are assisting a lawyer in delivering legal services to clients.[2]

Since 1999, those providing legal services now regularly use a variety of devices to create, transmit and store confidential communications, including desktop, laptop and notebook computers, tablet devices, smartphones, and cloud resource and storage locations. Each device and each storage location offer an opportunity for the inadvertent or unauthorized disclosure of information relating to the representation, and thus implicate a lawyer's ethical duties.[3]

In 2012 the ABA adopted "technology amendments" to the Model Rules, including updating the Comments to Rule 1.1 on lawyer technological competency and adding paragraph (c)

---

1. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413, at 11 (1999).

2. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2008); ABA COMMISSION ON ETHICS 20/20 REPORT TO THE HOUSE OF DELEGATES (2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120508_ethics_20_20_final_resolution_and_report_outsourcing_posting.authcheckdam.pdf.

3. *See* JILL D. RHODES & VINCENT I. POLLEY, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 7 (2013) [hereinafter ABA CYBERSECURITY HANDBOOK].

and a new Comment to Rule 1.6, addressing a lawyer's obligation to take reasonable measures to prevent inadvertent or unauthorized disclosure of information relating to the representation.

At the same time, the term "cybersecurity" has come into existence to encompass the broad range of issues relating to preserving individual privacy from intrusion by nefarious actors throughout the Internet. Cybersecurity recognizes a post-Opinion 99-413 world where law enforcement discusses hacking and data loss in terms of "when," and not "if."[4] Law firms are targets for two general reasons: (1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and (2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client.[5]

The Model Rules do not impose greater or different duties of confidentiality based upon the method by which a lawyer communicates with a client. But how a lawyer should comply with the core duty of confidentiality in an ever-changing technological world requires some reflection.

Against this backdrop we describe the "technology amendments" made to the Model Rules in 2012, identify some of the technology risks lawyers' face, and discuss factors other than the Model Rules of Professional Conduct that lawyers should consider when using electronic means to communicate regarding client matters.

II. Duty of Competence

Since 1983, Model Rule 1.1 has read: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[6] The scope of this requirement was clarified in 2012 when the ABA recognized the increasing impact of technology on the practice of law and the duty of lawyers to develop an understanding of that technology. Thus, Comment [8] to Rule 1.1 was modified to read:

> To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (Emphasis added.)[7]

---

4. "Cybersecurity" is defined as "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack." CYBERSECURITY, MERRIAM WEBSTER, http://www.merriam-webster.com/dictionary/cybersecurity (last visited Sept. 10, 2016). In 2012 the ABA created the Cybersecurity Legal Task Force to help lawyers grapple with the legal challenges created by cyberspace. In 2013 the Task Force published The ABA Cybersecurity Handbook: A Resource For Attorneys, Law Firms, and Business Professionals.

5. Bradford A. Bleier, Unit Chief to the Cyber National Security Section in the FBI's Cyber Division, indicated that "[l]aw firms have tremendous concentrations of really critical private information, and breaking into a firm's computer system is a really optimal way to obtain economic and personal security information." Ed Finkel, Cyberspace Under Siege, A.B.A. J., Nov. 1, 2010.

6. A LEGISLATIVE HISTORY: THE DEVELOPMENT OF THE ABA MODEL RULES OF PROFESSIONAL CONDUCT, 1982-2013, at 37-44 (Art Garwin ed., 2013).

7. *Id.* at 43.

Regarding the change to Rule 1.1's Comment, the ABA Commission on Ethics 20/20 explained:

> Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [6] specifies that, to remain competent, lawyers need to "keep abreast of changes in the law and its practice." The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today's environment without knowing how to use email or create an electronic document.[8]

III. Duty of Confidentiality

In 2012, amendments to Rule 1.6 modified both the rule and the commentary about what efforts are required to preserve the confidentiality of information relating to the representation. Model Rule 1.6(a) requires that "A lawyer shall not reveal information relating to the representation of a client" unless certain circumstances arise.[9] The 2012 modification added a new duty in paragraph (c) that: "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[10]

Amended Comment [18] explains:

> Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

---

8. ABA COMMISSION ON ETHICS 20/20 REPORT 105A (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf. The 20/20 Commission also noted that modification of Comment [6] did not change the lawyer's substantive duty of competence: "Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase 'including the benefits and risks associated with relevant technology,' would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent."

9. MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2016).

10. *Id.* at (c).

At the intersection of a lawyer's competence obligation to keep "abreast of knowledge of the benefits and risks associated with relevant technology," and confidentiality obligation to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," lawyers must exercise reasonable efforts when using technology in communicating about client matters. What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors. In turn, those factors depend on the multitude of possible types of information being communicated (ranging along a spectrum from highly sensitive information to insignificant), the methods of electronic communications employed, and the types of available security measures for each method.[11]

Therefore, in an environment of increasing cyber threats, the Committee concludes that, adopting the language in the ABA Cybersecurity Handbook, the reasonable efforts standard:

> . . . rejects requirements for specific security measures (such as firewalls, passwords, and the like) and instead adopts a fact-specific approach to business security obligations that requires a "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments.[12]

Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c) includes nonexclusive factors to guide lawyers in making a "reasonable efforts" determination. Those factors include:

- the sensitivity of the information,
- the likelihood of disclosure if additional safeguards are not employed,
- the cost of employing additional safeguards,
- the difficulty of implementing the safeguards, and
- the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).[13]

---

11. The 20/20 Commission's report emphasized that lawyers are not the guarantors of data safety. It wrote: "[t]o be clear, paragraph (c) does not mean that a lawyer engages in professional misconduct any time a client's confidences are subject to unauthorized access or disclosed inadvertently or without authority. A sentence in Comment [16] makes this point explicitly. The reality is that disclosures can occur even if lawyers take all reasonable precautions. The Commission, however, believes that it is important to state in the black letter of Model Rule 1.6 that lawyers have a duty to take reasonable precautions, even if those precautions will not guarantee the protection of confidential information under all circumstances."

12. ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 48-49.

13. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [18] (2013). "The [Ethics 20/20] Commission examined the possibility of offering more detailed guidance about the measures that lawyers should employ. The Commission concluded, however, that technology is changing too rapidly to offer such guidance and that the particular measures lawyers should use will necessarily change as technology evolves and as new risks emerge and new security procedures become available." ABA COMMISSION REPORT 105A, *supra* note 8, at 5.

A fact-based analysis means that particularly strong protective measures, like encryption, are warranted in some circumstances. Model Rule 1.4 may require a lawyer to discuss security safeguards with clients. Under certain circumstances, the lawyer may need to obtain informed consent from the client regarding whether to the use enhanced security measures, the costs involved, and the impact of those costs on the expense of the representation where nonstandard and not easily available or affordable security methods may be required or requested by the client. Reasonable efforts, as it pertains to certain highly sensitive information, might require avoiding the use of electronic methods or any technology to communicate with the client altogether, just as it warranted avoiding the use of the telephone, fax and mail in Formal Opinion 99-413.

In contrast, for matters of normal or low sensitivity, standard security methods with low to reasonable costs to implement, may be sufficient to meet the reasonable-efforts standard to protect client information from inadvertent and unauthorized disclosure.

In the technological landscape of Opinion 99-413, and due to the reasonable expectations of privacy available to email communications at the time, unencrypted email posed no greater risk of interception or disclosure than other non-electronic forms of communication. This basic premise remains true today for routine communication with clients, presuming the lawyer has implemented basic and reasonably available methods of common electronic security measures.[14] Thus, the use of unencrypted routine email generally remains an acceptable method of lawyer-client communication.

However, cyber-threats and the proliferation of electronic communications devices have changed the landscape and it is not always reasonable to rely on the use of unencrypted email. For example, electronic communication through certain mobile applications or on message boards or via unsecured networks may lack the basic expectation of privacy afforded to email communications. Therefore, lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters, applying the Comment [18] factors to determine what effort is reasonable.

While it is beyond the scope of an ethics opinion to specify the reasonable steps that lawyers should take under any given set of facts, we offer the following considerations as guidance:

1. Understand the Nature of the Threat.

   Understanding the nature of the threat includes consideration of the sensitivity of a client's information and whether the client's matter is a higher risk for cyber intrusion. Client matters involving proprietary information in highly sensitive industries such as industrial designs, mergers and acquisitions or trade secrets, and industries like healthcare, banking, defense or education, may present a higher risk of data theft.[15] "Reasonable efforts" in higher risk scenarios generally means that greater effort is warranted.

---

14. See item 3 below.

15. *See, e.g.*, Noah Garner, *The Most Prominent Cyber Threats Faced by High-Target Industries*, TREND-MICRO (Jan. 25, 2016), http://blog.trendmicro.com/the-most-prominent-cyber-threats-faced-by-high-target-industries/.

2. Understand How Client Confidential Information is Transmitted and Where It Is Stored.

A lawyer should understand how their firm's electronic communications are created, where client data resides, and what avenues exist to access that information. Understanding these processes will assist a lawyer in managing the risk of inadvertent or unauthorized disclosure of client-related information. Every access point is a potential entry point for a data loss or disclosure. The lawyer's task is complicated in a world where multiple devices may be used to communicate with or about a client and then store those communications. Each access point, and each device, should be evaluated for security compliance.

3. Understand and Use Reasonable Electronic Security Measures.

Model Rule 1.6(c) requires a lawyer to make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client. As comment [18] makes clear, what is deemed to be "reasonable" may vary, depending on the facts and circumstances of each case. Electronic disclosure of, or access to, client communications can occur in different forms ranging from a direct intrusion into a law firm's systems to theft or interception of information during the transmission process. Making reasonable efforts to protect against unauthorized disclosure in client communications thus includes analysis of security measures applied to both disclosure and access to a law firm's technology system and transmissions.

A lawyer should understand and use electronic security measures to safeguard client communications and information. A lawyer has a variety of options to safeguard communications including, for example, using secure internet access methods to communicate, access and store client information (such as through secure Wi-Fi, the use of a Virtual Private Network, or another secure internet portal), using unique complex passwords, changed periodically, implementing firewalls and anti-Malware/Anti-Spyware/Antivirus software on all devices upon which client confidential information is transmitted or stored, and applying all necessary security patches and updates to operational and communications software. Each of these measures is routinely accessible and reasonably affordable or free. Lawyers may consider refusing access to firm systems to devices failing to comply with these basic methods. It also may be reasonable to use commonly available methods to remotely disable lost or stolen devices, and to destroy the data contained on those devices, especially if encryption is not also being used.

Other available tools include encryption of data that is physically stored on a device and multi-factor authentication to access firm systems.

In the electronic world, "delete" usually does not mean information is permanently deleted, and "deleted" data may be subject to recovery. Therefore, a lawyer should consider

whether certain data should *ever* be stored in an unencrypted environment, or electronically transmitted at all.

4. Determine How Electronic Communications About Clients Matters Should Be Protected.

Different communications require different levels of protection. At the beginning of the client-lawyer relationship, the lawyer and client should discuss what levels of security will be necessary for each electronic communication about client matters. Communications to third parties containing protected client information requires analysis to determine what degree of protection is appropriate. In situations where the communication (and any attachments) are sensitive or warrant extra security, additional electronic protection may be required. For example, if client information is of sufficient sensitivity, a lawyer should encrypt the transmission and determine how to do so to sufficiently protect it,[16] and consider the use of password protection for any attachments. Alternatively, lawyers can consider the use of a well vetted and secure third-party cloud based file storage system to exchange documents normally attached to emails.

Thus, routine communications sent electronically are those communications that do not contain information warranting additional security measures beyond basic methods. However, in some circumstances, a client's lack of technological sophistication or the limitations of technology available to the client may require alternative non-electronic forms of communication altogether.

A lawyer also should be cautious in communicating with a client if the client uses computers or other devices subject to the access or control of a third party.[17] If so, the attorney-client privilege and confidentiality of communications and attached documents may be waived, and the lawyer must determine whether it is prudent to warn a client of the dangers associated with such a method of communication.[18]

---

16. *See* Cal. Formal Op. 2010-179 (2010); ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 121. Indeed, certain laws and regulations require encryption in certain situations. *Id.* at 58-59.

17. *See, e.g.*, ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-459 (2011) (discussing the duty to protect the confidentiality of e-mail communications with one's client); Scott v. Beth Israel Med. Center, Inc., Civ. A. No. 3:04-CV-139-RJC-DCK, 847 N.Y.S.2d 436 (Sup. Ct. 2007); Mason v. ILS Tech., LLC, 2008 WL 731557, 2008 BL 298576 (W.D.N.C. 2008); Holmes v. Petrovich Dev Co., LLC, 191 Cal. App. 4th 1047 (2011) (employee communications with lawyer over company owned computer not privileged); Bingham v. BayCare Health Sys., 2016 WL 3917513, 2016 BL 233476 (M.D. Fla. July 20, 2016) (collecting cases on privilege waiver for privileged emails sent or received through an employer's email server).

18. some state bar ethics opinions have explored the circumstances under which e-mail communications should be afforded special security protections, *See, e.g.*, Tex. Prof'l Ethics Comm. Op. 648 (2015) that identified six situations in which a lawyer should consider whether to encrypt or use some other type of security precaution:

- communicating highly sensitive or confidential information via email or unencrypted email connections;
- sending an email to or from an account that the email sender or recipient shares with others;
- sending an email to a client when it is possible that a third person (such as a spouse in a divorce case) knows the password to the email account, or to an individual client at that client's work email account, especially if the email relates to a client's employment dispute with his employer...;
- sending an email from a public computer or a borrowed computer or where the lawyer knows that the emails the lawyer sends are being read on a public or borrowed computer or on an unsecure network;

5. Label Client Confidential Information.

Lawyers should follow the better practice of marking privileged and confidential client communications as "privileged and confidential" in order to alert anyone to whom the communication was inadvertently disclosed that the communication is intended to be privileged and confidential. This can also consist of something as simple as appending a message or "disclaimer" to client emails, where such a disclaimer is accurate and appropriate for the communication.[19]

Model Rule 4.4(b) obligates a lawyer who "knows or reasonably should know" that he has received an inadvertently sent "document or electronically stored information relating to the representation of the lawyer's client" to promptly notify the sending lawyer. A clear and conspicuous appropriately used disclaimer may affect whether a recipient lawyer's duty under Model Rule 4.4(b) for inadvertently transmitted communications is satisfied.

6. Train Lawyers and Nonlawyer Assistants in Technology and Information Security.

Model Rule 5.1 provides that a partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct. Model Rule 5.1 also provides that lawyers having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct. In addition, Rule 5.3 requires lawyers who are responsible for managing and supervising nonlawyer assistants to take reasonable steps to reasonably assure that the conduct of such assistants is compatible with the ethical duties of the lawyer. These requirements are as applicable to electronic practices as they are to comparable office procedures.

In the context of electronic communications, lawyers must establish policies and procedures, and periodically train employees, subordinates and others assisting in the delivery of legal services, in the use of reasonably secure methods of electronic communications with clients. Lawyers also must instruct and supervise on reasonable measures for access to and storage of those communications. Once processes are established, supervising lawyers must follow up to ensure these policies are being

---

- sending an email if the lawyer knows that the email recipient is accessing the email on devices that are potentially accessible to third persons or are not protected by a password; or
- sending an email if the lawyer is concerned that the NSA or other law enforcement agency may read the lawyer's email communication, with or without a warrant.

19. *See* Veteran Med. Prods. v. Bionix Dev. Corp., Case No. 1:05-cv-655, 2008 WL 696546 at *8, 2008 BL 51876 at *8 (W.D. Mich. Mar. 13, 2008) (email disclaimer that read "this email and any files transmitted with are confidential and are intended solely for the use of the individual or entity to whom they are addressed" with nondisclosure constitutes a reasonable effort to maintain the secrecy of its business plan).

implemented and partners and lawyers with comparable managerial authority must periodically reassess and update these policies. This is no different than the other obligations for supervision of office practices and procedures to protect client information.

7. Conduct Due Diligence on Vendors Providing Communication Technology.

Consistent with Model Rule 1.6(c), Model Rule 5.3 imposes a duty on lawyers with direct supervisory authority over a nonlawyer to make "reasonable efforts to ensure that" the nonlawyer's "conduct is compatible with the professional obligations of the lawyer."

In ABA Formal Opinion 08-451, this Committee analyzed Model Rule 5.3 and a lawyer's obligation when outsourcing legal and nonlegal services. That opinion identified several issues a lawyer should consider when selecting the outsource vendor, to meet the lawyer's due diligence and duty of supervision. Those factors also apply in the analysis of vendor selection in the context of electronic communications. Such factors may include:

- reference checks and vendor credentials;
- vendor's security policies and protocols;
- vendor's hiring practices;
- the use of confidentiality agreements;
- vendor's conflicts check system to screen for adversity; and
- the availability and accessibility of a legal forum for legal relief for violations of the vendor agreement.

Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education.[20]

Since the issuance of Formal Opinion 08-451, Comment [3] to Model Rule 5.3 was added to address outsourcing, including "using an Internet-based service to store client information." Comment [3] provides that the "reasonable efforts" required by Model Rule 5.3 to ensure that the nonlawyer's services are provided in a manner that is compatible with the lawyer's professional obligations "will depend upon the circumstances." Comment [3] contains suggested factors that might be taken into account:

- the education, experience, and reputation of the nonlawyer;
- the nature of the services involved;
- the terms of any arrangements concerning the protection of client information; and
- the legal and ethical environments of the jurisdictions in which the services will be performed particularly with regard to confidentiality.

20. MODEL RULES OF PROF'L CONDUCT R. 1.1 cmts. [2] & [8] (2016).

Comment [3] further provides that when retaining or directing a nonlawyer outside of the firm, lawyers should communicate "directions appropriate under the circumstances to give reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer."[21] If the client has not directed the selection of the outside nonlawyer vendor, the lawyer has the responsibility to monitor how those services are being performed.[22]

Even after a lawyer examines these various considerations and is satisfied that the security employed is sufficient to comply with the duty of confidentiality, the lawyer must periodically reassess these factors to confirm that the lawyer's actions continue to comply with the ethical obligations and have not been rendered inadequate by changes in circumstances or technology.

IV. Duty to Communicate

Communications between a lawyer and client generally are addressed in Rule 1.4. When the lawyer reasonably believes that highly sensitive confidential client information is being transmitted so that extra measures to protect the email transmission are warranted, the lawyer should inform the client about the risks involved.[23] The lawyer and client then should decide whether another mode of transmission, such as high level encryption or personal delivery is warranted. Similarly, a lawyer should consult with the client as to how to appropriately and safely use technology in their communication, in compliance with other laws that might be applicable to the client. Whether a lawyer is using methods and practices to comply with administrative, statutory, or international legal standards is beyond the scope of this opinion.

A client may insist or require that the lawyer undertake certain forms of communication. As explained in Comment [18] to Model Rule 1.6, "A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule."

---

21. The ABA's catalog of state bar ethics opinions applying the rules of professional conduct to cloud storage arrangements involving client information can be found at: http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html.

22. By contrast, where a client directs the selection of a particular nonlawyer service provider outside the firm, "the lawyer ordinarily should agree with the client concerning the allocation of responsibility for monitoring as between the client and the lawyer." MODEL RULES OF PROF'L CONDUCT R. 5.3 cmt. [4] (2017). The concept of monitoring recognizes that although it may not be possible to "directly supervise" a client directed nonlawyer outside the firm performing services in connection with a matter, a lawyer must nevertheless remain aware of how the nonlawyer services are being performed. ABA COMMISSION ON ETHICS 20/20 REPORT 105C, at 12 (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105c_filed_may_2012.authcheckdam.pdf.

23. MODEL RULES OF PROF'L CONDUCT R. 1.4(a)(1) & (4) (2016).

V. Conclusion

Rule 1.1 requires a lawyer to provide competent representation to a client. Comment [8] to Rule 1.1 advises lawyers that to maintain the requisite knowledge and skill for competent representation, a lawyer should keep abreast of the benefits and risks associated with relevant technology. Rule 1.6(c) requires a lawyer to make "reasonable efforts" to prevent the inadvertent or unauthorized disclosure of or access to information relating to the representation.

A lawyer generally may transmit information relating to the representation of a client over the Internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

21st-Century Standards

Lawyers must secure client communications from cyber breaches

By David L. Hudson Jr.

Ethics

In May, the ABA Standing Committee on Ethics and Professional Responsibility released an opinion that says lawyers must make reasonable efforts to ensure that communications with their clients are secure and not subject to inadvertent or unauthorized cybersecurity breaches.

Formal Opinion 477 updates Formal Opinion 99-413, which was issued in 1999 before the widespread use of tablet devices, smartphones and cloud storage.

"It is an important opinion because there have been many changes in the cybersecurity realm," says Peter Geraghty, senior counsel and ETHICSearch director with the ABA Center for Professional Responsibility. "There have been all kinds of new applications that have come into play. It is important to address these new developments and how they might apply to lawyers' day-to-day practices."

The new opinion explains: "Each device and each storage location offer an opportunity for the inadvertent or unauthorized disclosure of information relating to the representation and thus implicate a lawyer's ethical duties."

These duties include competency, confidentiality and communication. In the ABA Model Rules of Professional Conduct, Rule 1.1, which focuses on competency, includes a technology clause added in 2012. Comment 8 to the rule provides that lawyers must stay abreast of "the benefits and risks associated with relevant technology."

Ethics expert Peter A. Joy, a professor at Washington University School of Law in St. Louis, thinks the opinion should have done more to discuss competency.

"The opinion quotes the comment to Model Rule 1.1 on keeping up with technology, but few lawyers really understand what keeping abreast of technology really means," he says. "Some may think knowing how to use the technology, like the internet or email, is enough. They may fail to realize that using the internet provided by their favorite coffee shop or at the airport to communicate with clients is not secure."

'REASONABLE EFFORTS' APPROACH

The bulk of the opinion addresses lawyers' obligations to ensure the confidentiality of client information. In 2012, Rule 1.6 was amended to add a new paragraph (c): "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Comment 18 to the rule says such unauthorized access or inadvertent or unauthorized disclosure of client info "does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure."

Citing the *ABA Cybersecurity Handbook*, the opinion explains that reasonable effort is a fact-specific inquiry. It requires examining the sensitivity of the information, the risk of disclosure without additional precautions, the cost of extra measures, the difficulty of adding safeguards, and whether more safeguards adversely affect the lawyer's ability to represent the client. The opinion adds that lawyers must adopt a process to systematically assess and address cyberrisks.

Generally, lawyers may use unencrypted email when they communicate with clients routinely, the opinion says, but only if they have "implemented basic and reasonably available methods of common electronic security measures."

The phenomenon of cyberthreats, particularly in "highly sensitive industries, such as industrial designs, mergers and acquisitions or trade secrets, and industries like health care, banking, defense or education, may present a higher risk of data theft." In such higher-risk scenarios, reasonable effort will likely mean that "greater effort is warranted." For example, "particularly strong protective measures, like encryption, are warranted in some circumstances."

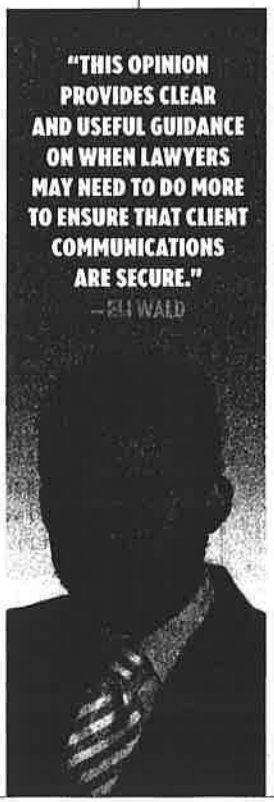


PHOTO COURTESY OF UNIVERSITY OF DENVER STURM COLLEGE OF LAW

The opinion provides seven considerations for guidance, including understanding the nature of the threat; how client confidential information is transmitted and stored; the use of reasonable electronic security measures; how electronic communications should be protected; the need to label client information as privileged and confidential; the need to train lawyers and nonlawyer assistants in technology and cybersecurity; and the need to conduct due diligence on vendors who provide technology services.

"Overall, I think it is a fantastic opinion, particularly with regard to its treatment of lawyers' obligations regarding confidentiality," says legal ethics scholar Eli Wald, a professor at the University of Denver's Sturm College of Law. "In general, ethics opinions are meant to explain the applicable rules of professional conduct. Facing increased

cyberrisks, this opinion provides clear and useful guidance on when lawyers may need to do more to ensure that client communications are secure. The opinion does a great job of clarifying and explaining in practical terms what lawyers must do to comply with the confidentiality and competence rules pertaining to cybersecurity."

WHEN TO PIPE UP

The opinion also briefly addresses communication, covered by Rule 1.4. The opinion says lawyers should inform clients about inherent risks when they transmit "highly sensitive confidential client information." The opinion notes that "Model Rule 1.4 may require a lawyer to discuss security safeguards with clients."

For example, the opinion says that if a lawyer reasonably thinks highly sensitive confidential client information is being transmitted such that "extra measures" are needed for protection, the lawyer should inform the client and discuss options.

"The lawyer and client then should decide whether another mode of transmission, such as high-level encryption or personal delivery, is warranted," the opinion reads. "Similarly, a lawyer should consult with the client as to how to appropriately and safely use technology in their communication, in compliance with other laws that might be applicable to the client."

"Lawyers need to communicate with clients about cyberrisks from the initial meeting and then periodically thereafter," Joy says. "First and foremost, there needs to be a discussion about whether and when email will be used."

Wald thinks the opinion could have done a better job of explaining when lawyers must communicate to clients in the event of a security or a data breach. In a 2016 law review article, "Legal Ethics' Next Frontier: Lawyers and Cybersecurity," published in the *Chapman Law Review*, Wald argues that legal ethics rules should mandate that lawyers disclose "to clients when their confidential information was, or is, reasonably believed to have been accessed by an unauthorized party."

The difficulty in this area for lawyers, Wald says, is that often with a security breach, lawyers don't know who hacked their devices or server, nor do they know exactly what confidential client information was accessed.

"The opinion correctly points out that Model Rule 1.4 may require a lawyer to discuss security safeguards with a client," Wald says. "However, after reading this opinion, a lawyer may reasonably ask, 'When exactly do I need to communicate to a client about security risks and breaches?' The opinion could have given more guidance to lawyers as to under what circumstances they should communicate with clients about cyberthreats, security breaches, compromised confidential information and possible remedies." ■

RULE 1.1:
COMPETENCE

(a) A lawyer should provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

(b) A lawyer shall not handle a legal matter that the lawyer knows or should know that the lawyer is not competent to handle, without associating with a lawyer who is competent to handle it.

(c) A lawyer shall not intentionally:

(1) fail to seek the objectives of the client through reasonably available means permitted by law and these Rules; or

(2) prejudice or damage the client during the course of the representation except as permitted or required by these Rules.

Comment

Legal Knowledge and Skill

[1] In determining whether a lawyer employs the requisite knowledge and skill in a particular matter, relevant factors include the relative complexity and specialized nature of the matter, the lawyer's general experience, the lawyer's training and experience in the field in question, the preparation and study the lawyer is able to give the matter, and whether it is feasible to associate with a lawyer of established competence in the field in question. In many instances, the required proficiency is that of a general practitioner. Expertise in a particular field of law may be required in some circumstances. One such circumstance would be where the lawyer, by representations made to the client, has led the client reasonably to expect a special level of expertise in the matter undertaken by the lawyer.

[2] A lawyer need not necessarily have special training or prior experience to handle legal problems of a type with which the lawyer is unfamiliar. A newly admitted lawyer can be as competent as a practitioner with long experience. Some important legal skills, such as the analysis of precedent, the evaluation of evidence and legal drafting, are required in all legal problems. Perhaps the most fundamental legal skill consists of determining what kinds of legal problems a situation may involve, a skill that necessarily transcends any particular specialized knowledge. A lawyer can provide adequate representation in a wholly novel field through necessary study. Competent representation can also be provided through the association of a lawyer of established competence in the field in question.

[3] [Reserved.]

[4] A lawyer may accept representation where the requisite level of competence can be achieved by adequate preparation before handling the legal matter. This applies as well to a lawyer who is appointed as counsel for an unrepresented person.

Thoroughness and Preparation

[5] Competent handling of a particular matter includes inquiry into and analysis of the factual and legal elements of the problem, and use of methods and procedures meeting the standards of competent practitioners. It also includes adequate preparation. The required attention and preparation are determined in part by what is at stake; major litigation and complex transactions ordinarily require more extensive treatment than matters of lesser complexity and consequence. An agreement between the lawyer and the client may limit the scope of the representation if the agreement complies with Rule 1.2(c).

Retaining or Contracting with Lawyers Outside the Firm

[6] Before a lawyer retains or contracts with other lawyers outside the lawyer's own firm to provide or assist in the provision of legal services to a client, the lawyer should ordinarily obtain informed consent from the client and should reasonably believe that the other lawyers' services will contribute to the competent and ethical representation of the client. *See also* Rules 1.2 (allocation of authority), 1.4 (communication with client), 1.5(g) (fee sharing with lawyers outside the firm), 1.6 (confidentiality), and 5.5(a) (unauthorized practice of law). The reasonableness of the decision to retain or contract with other lawyers outside the lawyer's own firm will depend upon the circumstances, including the needs of the client; the education, experience and reputation of the outside lawyers; the nature of the services assigned to the outside lawyers; and the legal protections, professional conduct rules, and ethical environments of the jurisdictions in which the services will be performed, particularly relating to confidential information.

[6A] Client consent to contract with a lawyer outside the lawyer's own firm may not be necessary for discrete and limited tasks supervised closely by a lawyer in the firm. However, a lawyer should ordinarily obtain client consent before contracting with an outside lawyer to perform substantive or strategic legal work on which the lawyer will exercise independent judgment without close supervision or review by the referring lawyer. For example, on one hand, a lawyer who hires an outside lawyer on a per diem basis to cover a single court call or a routing calendar call ordinarily would not need to obtain the client's prior informed consent. On the other hand, a lawyer who hires an outside lawyer to argue a summary judgment motion or negotiate key points in a transaction ordinarily should seek to obtain the client's prior informed consent.

[7] When lawyer from more than one law firm are providing legal services to the client on a particular matter, the lawyers ordinarily should consult with each other about the scope of their respective roles and the allocation of responsibility among them. *See* Rule 1.2(a). When allocating responsibility in a matter pending before a tribunal, lawyers and parties may have additional obligations (*e.g.*, under local court rules, the CPLR, or the Federal Rules of Civil Procedure) that are a matter of law beyond the scope of these Rules.

[7A] Whether a lawyer who contracts with a lawyer outside the firm needs to obtain informed consent from the client about the roles and responsibilities of the retaining and outside lawyers will depend on the circumstances. On one hand, of a lawyer retains an outside lawyer or law firm to work under the lawyer's close direction and supervision, and the retaining lawyer closely reviews the outside lawyer's work, the retaining lawyer usually will not need to consult with the client about the outside lawyer's role and level of responsibility. On the other hand, if the outside lawyer will have a more material role and will exercise more autonomy and responsibility, then the retaining lawyer usually should consult with the client. In any event, whenever a retaining lawyer discloses a client's confidential information to lawyers outside the firm, the retaining lawyer should comply with Rule 1.6(a).

[8] To maintain the requisite knowledge and skill, a lawyer should (i) keep abreast of changes in substantive and procedural law relevant to the lawyer's practice, (ii) keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information, and (iii) engage in continuing study and education and comply with all applicable continuing legal education requirements under 22 N.Y.C.R.R. Part 1500.

RULE 1.4:
COMMUNICATION

(a) A lawyer shall:

(1) promptly inform the client of:

(i) any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(j), is required by these Rules;

(ii) any information required by court rule or other law to be communicated to a client; and

(iii) material developments in the matter including settlement or plea offers.

(2) reasonably consult with the client about the means by which the client's objectives are to be accomplished;

(3) keep the client reasonably informed about the status of the matter;

(4) promptly comply with a client's reasonable requests for information; and

(5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by these Rules or other law.

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

Comment

[1] Reasonable communication between the lawyer and the client is necessary for the client to participate effectively in the representation.

Communicating with Client

[2] In instances where these Rules require that a particular decision about the representation be made by the client, paragraph (a)(1) requires that the lawyer promptly consult with the client and secure the client's consent prior to taking action, unless prior discussions with the client have resolved what action the client wants the lawyer to take. For example, paragraph (a)(1)(iii) requires that a lawyer who receives from opposing counsel an offer of settlement in a civil controversy or a proffered plea bargain in a criminal case must promptly inform the client of its substance unless the client has previously made clear that the proposal will be acceptable or unacceptable or has authorized the lawyer to accept or to reject the offer. *See* Rule 1.2(a).

RULE 1.6:
CONFIDENTIALITY OF INFORMATION

(a) A lawyer shall not knowingly reveal confidential information, as defined in this Rule, or use such information to the disadvantage of a client or for the advantage of the lawyer or a third person, unless:

(1) the client gives informed consent, as defined in Rule 1.0(j);

(2) the disclosure is impliedly authorized to advance the best interests of the client and is either reasonable under the circumstances or customary in the professional community; or

(3) the disclosure is permitted by paragraph (b).

"Confidential information" consists of information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential. "Confidential information" does not ordinarily include (i) a lawyer's legal knowledge or legal research or (ii) information that is generally known in the local community or in the trade, field or profession to which the information relates.

(b) A lawyer may reveal or use confidential information to the extent that the lawyer reasonably believes necessary:

(1) to prevent reasonably certain death or substantial bodily harm;

(2) to prevent the client from committing a crime;

(3) to withdraw a written or oral opinion or representation previously given by the lawyer and reasonably believed by the lawyer still to be relied upon by a third person, where the lawyer has discovered that the opinion or representation was based on materially inaccurate information or is being used to further a crime or fraud;

(4) to secure legal advice about compliance with these Rules or other law by the lawyer, another lawyer associated with the lawyer's firm or the law firm;

(5) (i) to defend the lawyer or the lawyer's employees and associates against an accusation of wrongful conduct; or

(ii) to establish or collect a fee; or

(6) when permitted or required under these Rules or to comply with other law or court order.

(c) A lawyer make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to, information protected by Rules 1.6, 1.9(c), or 1.18(b).

Comment

Scope of the Professional Duty of Confidentiality

[1] This Rule governs the disclosure of information protected by the professional duty of confidentiality. Such information is described in these Rules as "confidential information" as defined in this Rule. Other rules also deal with confidential information. See Rules 1.8(b) and 1.9(c)(1) for the lawyer's duties with respect to the use of such information to the disadvantage of clients and former clients; Rule 1.9(c)(2) for the lawyer's duty not to reveal information relating to the lawyer's prior representation of a former client; Rule 1.14(c) for information relating to representation of a client with diminished capacity; Rule 1.18(b) for the lawyer's duties with respect to information provided to the lawyer by a prospective client; Rule 3.3 for the lawyer's duty of candor to a tribunal; and Rule 8.3(c) for information gained by a lawyer or judge while participating in an approved lawyer assistance program.

[2] A fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, or except as permitted or required by these Rules, the lawyer must not knowingly reveal information gained during and related to the representation, whatever its source. See Rule 1.0(j) for the definition of informed consent. The lawyer's duty of confidentiality contributes to the trust that is the hallmark of the client-lawyer relationship. The client is thereby encouraged to seek legal assistance and to communicate fully and frankly with the lawyer, even as to embarrassing or legally damaging subject matter. The lawyer needs this information to represent the client effectively and, if necessary, to advise the client to refrain from wrongful conduct. Typically, clients come to lawyers to determine their rights and what is, in the complex of laws and regulations, deemed to be legal and correct. Based upon experience, lawyers know that almost all clients follow the advice given, and the law is thereby upheld.

[3] The principle of client-lawyer confidentiality is given effect in three related bodies of law: the attorney-client privilege of evidence law, the work-product doctrine of civil procedure and the professional duty of confidentiality established in legal ethics codes. The attorney-client privilege and the work-product doctrine apply when compulsory process by a judicial or other governmental body seeks to compel a lawyer to testify or produce information or evidence concerning a client. The professional duty of client-lawyer confidentiality, in contrast, applies to a lawyer in all settings and at all times, prohibiting the lawyer from disclosing confidential information unless permitted or required by these Rules or to comply with other law or court order. The confidentiality duty applies not only to matters communicated in confidence by the client, which are protected by the attorney-client privilege, but also to all information gained during and relating to the representation, whatever its source. The confidentiality duty, for example, prohibits a lawyer from volunteering confidential information to a friend or to any other person except in compliance with the provisions of this Rule, including the Rule's reference to other law that may compel disclosure. *See* Comments [12]-[13]; *see also* Scope.

[4] Paragraph (a) prohibits a lawyer from knowingly revealing confidential information as defined by this Rule. This prohibition also applies to disclosures by a lawyer that do not in themselves reveal confidential information but could reasonably lead to the discovery of such information by a third person. A lawyer's use of a hypothetical to discuss issues relating to the representation with persons not connected to the representation is permissible so long as there is no reasonable likelihood that the listener will be able to ascertain the identity of the client.

[4A] Paragraph (a) protects all factual information "gained during or relating to the representation of a client." Information relates to the representation if it has any possible relevance to the representation or is received because of the representation. The accumulation of legal knowledge or legal research that a lawyer acquires through practice ordinarily is not client information protected by this Rule. However, in some circumstances, including where the client and the lawyer have so agreed, a client may have a proprietary interest in a particular product of the lawyer's research. Information that is generally known in the local community or in the trade, field or profession to which the information relates is also not protected, unless the client and the lawyer have otherwise agreed. Information is not "generally known" simply because it is in the public domain or available in a public file.

Use of Information Related to Representation

[4B] The duty of confidentiality also prohibits a lawyer from using confidential information to the advantage of the lawyer or a third person or to the disadvantage of a client or former client unless the client or former client has given informed consent. See Rule 1.0(j) for the definition of "informed consent." This part of paragraph (a) applies when information is used to benefit either the lawyer or a third person, such as another client, a former client or a business associate of the lawyer. For example, if a lawyer learns that a client intends to purchase and develop several parcels of land, the lawyer may not (absent the client's informed consent) use that information to buy a nearby parcel that is expected to appreciate in value due to the client's purchase, or to recommend that another client buy the nearby land, even if the lawyer does not reveal any confidential information. The duty also prohibits disadvantageous use of confidential information unless the client gives informed consent, except as permitted or required by these Rules. For example, a lawyer assisting a client in purchasing a parcel of land may not make a competing bid on the same land. However, the fact that a lawyer has once served a client does not preclude the lawyer from using generally known information about that client, even to the disadvantage of the former client, after the client-lawyer relationship has terminated. *See* Rule 1.9(c)(1).

Authorized Disclosure

[5] Except to the extent that the client's instructions or special circumstances limit that authority, a lawyer may make disclosures of confidential information that are impliedly authorized by a client if the disclosures (i) advance the best interests of the client and (ii) are either reasonable under the circumstances or customary in the professional community. In some situations, for example, a lawyer may be impliedly authorized to admit a fact that cannot properly be disputed or to make a disclosure that facilitates a satisfactory conclusion to a matter. In addition, lawyers in a firm may, in the course of the firm's practice, disclose to each other

information relating to a client of the firm, unless the client has instructed that particular information be confined to specified lawyers. Lawyers are also impliedly authorized to reveal information about a client with diminished capacity when necessary to take protective action to safeguard the client's interests. See Rules 1.14(b) and (c).

Disclosure Adverse to Client

[6] Although the public interest is usually best served by a strict rule requiring lawyers to preserve the confidentiality of information relating to the representation of their clients, the confidentiality rule is subject to limited exceptions that prevent substantial harm to important interests, deter wrongdoing by clients, prevent violations of the law, and maintain the impartiality and integrity of judicial proceedings. Paragraph (b) permits, but does not require, a lawyer to disclose information relating to the representation to accomplish these specified purposes.

[6A] The lawyer's exercise of discretion conferred by paragraphs (b)(1) through (b)(3) requires consideration of a wide range of factors and should therefore be given great weight. In exercising such discretion under these paragraphs, the lawyer should consider such factors as: (i) the seriousness of the potential injury to others if the prospective harm or crime occurs, (ii) the likelihood that it will occur and its imminence, (iii) the apparent absence of any other feasible way to prevent the potential injury, (iv) the extent to which the client may be using the lawyer's services in bringing about the harm or crime, (v) the circumstances under which the lawyer acquired the information of the client's intent or prospective course of action, and (vi) any other aggravating or extenuating circumstances. In any case, disclosure adverse to the client's interest should be no greater than the lawyer reasonably believes necessary to prevent the threatened harm or crime. When a lawyer learns that a client intends to pursue or is pursuing a course of conduct that would permit disclosure under paragraphs (b)(1), (b)(2) or (b)(3), the lawyer's initial duty, where practicable, is to remonstrate with the client. In the rare situation in which the client is reluctant to accept the lawyer's advice, the lawyer's threat of disclosure is a measure of last resort that may persuade the client. When the lawyer reasonably believes that the client will carry out the threatened harm or crime, the lawyer may disclose confidential information when permitted by paragraphs (b)(1), (b)(2) or (b)(3). A lawyer's permissible disclosure under paragraph (b) does not waive the client's attorney-client privilege; neither the lawyer nor the client may be forced to testify about communications protected by the privilege, unless a tribunal or body with authority to compel testimony makes a determination that the crime-fraud exception to the privilege, or some other exception, has been satisfied by a party to the proceeding. For a lawyer's duties when representing an organizational client engaged in wrongdoing, see Rule 1.13(b).

[6B] Paragraph (b)(1) recognizes the overriding value of life and physical integrity and permits disclosure reasonably necessary to prevent reasonably certain death or substantial bodily harm. Such harm is reasonably certain to occur if it will be suffered imminently or if there is a present and substantial risk that a person will suffer such harm at a later date if the lawyer fails to take action necessary to eliminate the threat. Thus, a lawyer who knows that a client has accidentally discharged toxic waste into a town's water supply may reveal this information to the authorities if there is a present and substantial risk that a person who drinks the water will contract a life-threatening or debilitating disease and the lawyer's disclosure is necessary to

eliminate the threat or reduce the number of victims. Wrongful execution of a person is a life-threatening and imminent harm under paragraph (b)(1) once the person has been convicted and sentenced to death. On the other hand, an event that will cause property damage but is unlikely to cause substantial bodily harm is not a present and substantial risk under paragraph (b)(1); similarly, a remote possibility or small statistical likelihood that any particular unit of a mass-distributed product will cause death or substantial bodily harm to unspecified persons over a period of years does not satisfy the element of reasonably certain death or substantial bodily harm under the exception to the duty of confidentiality in paragraph (b)(1).

[6C] Paragraph (b)(2) recognizes that society has important interests in preventing a client's crime. Disclosure of the client's intention is permitted to the extent reasonably necessary to prevent the crime. In exercising discretion under this paragraph, the lawyer should consider such factors as those stated in Comment [6A].

[6D] Some crimes, such as criminal fraud, may be ongoing in the sense that the client's past material false representations are still deceiving new victims. The law treats such crimes as continuing crimes in which new violations are constantly occurring. The lawyer whose services were involved in the criminal acts that constitute a continuing crime may reveal the client's refusal to bring an end to a continuing crime, even though that disclosure may also reveal the client's past wrongful acts, because refusal to end a continuing crime is equivalent to an intention to commit a new crime. Disclosure is not permitted under paragraph (b)(2), however, when a person who may have committed a crime employs a new lawyer for investigation or defense. Such a lawyer does not have discretion under paragraph (b)(2) to use or disclose the client's past acts that may have continuing criminal consequences. Disclosure is permitted, however, if the client uses the new lawyer's services to commit a further crime, such as obstruction of justice or perjury.

[6E] Paragraph (b)(3) permits a lawyer to withdraw a legal opinion or to disaffirm a prior representation made to third parties when the lawyer reasonably believes that third persons are still relying on the lawyer's work and the work was based on "materially inaccurate information or is being used to further a crime or fraud." *See* Rule 1.16(b)(1), requiring the lawyer to withdraw when the lawyer knows or reasonably should know that the representation will result in a violation of law. Paragraph (b)(3) permits the lawyer to give only the limited notice that is implicit in withdrawing an opinion or representation, which may have the collateral effect of inferentially revealing confidential information. The lawyer's withdrawal of the tainted opinion or representation allows the lawyer to prevent further harm to third persons and to protect the lawyer's own interest when the client has abused the professional relationship, but paragraph (b)(3) does not permit explicit disclosure of the client's past acts unless such disclosure is permitted under paragraph (b)(2).

[7] [Reserved.]

[8] [Reserved.]

[9] A lawyer's confidentiality obligations do not preclude a lawyer from securing confidential legal advice about compliance with these Rules and other law by the lawyer, another lawyer in the lawyer's firm, or the law firm. In many situations, disclosing information to secure

such advice will be impliedly authorized for the lawyer to carry out the representation. Even when the disclosure is not impliedly authorized, paragraph (b)(4) permits such disclosure because of the importance of a lawyer's compliance with these Rules, court orders and other law.

[10] Where a claim or charge alleges misconduct of the lawyer related to the representation of a current or former client, the lawyer may respond to the extent the lawyer reasonably believes necessary to establish a defense. Such a claim can arise in a civil, criminal, disciplinary or other proceeding and can be based on a wrong allegedly committed by the lawyer against the client or on a wrong alleged by a third person, such as a person claiming to have been defrauded by the lawyer and client acting together or by the lawyer acting alone. The lawyer may respond directly to the person who has made an accusation that permits disclosure, provided that the lawyer's response complies with Rule 4.2 and Rule 4.3, and other Rules or applicable law. A lawyer may make the disclosures authorized by paragraph (b)(5) through counsel. The right to respond also applies to accusations of wrongful conduct concerning the lawyer's law firm, employees or associates.

[11] A lawyer entitled to a fee is permitted by paragraph (b)(5) to prove the services rendered in an action to collect it. This aspect of the rule expresses the principle that the beneficiary of a fiduciary relationship may not exploit it to the detriment of the fiduciary.

[12] Paragraph (b) does not mandate any disclosures. However, other law may require that a lawyer disclose confidential information. Whether such a law supersedes Rule 1.6 is a question of law beyond the scope of these Rules. When disclosure of confidential information appears to be required by other law, the lawyer must consult with the client to the extent required by Rule 1.4 before making the disclosure, unless such consultation would be prohibited by other law. If the lawyer concludes that other law supersedes this Rule and requires disclosure, paragraph (b)(6) permits the lawyer to make such disclosures as are necessary to comply with the law.

[13] A tribunal or governmental entity claiming authority pursuant to other law to compel disclosure may order a lawyer to reveal confidential information. Absent informed consent of the client to comply with the order, the lawyer should assert on behalf of the client nonfrivolous arguments that the order is not authorized by law, the information sought is protected against disclosure by an applicable privilege or other law, or the order is invalid or defective for some other reason. In the event of an adverse ruling, the lawyer must consult with the client to the extent required by Rule 1.4 about the possibility of an appeal or further challenge, unless such consultation would be prohibited by other law. If such review is not sought or is unsuccessful, paragraph (b)(6) permits the lawyer to comply with the order.

[14] Paragraph (b) permits disclosure only to the extent the lawyer reasonably believes the disclosure is necessary to accomplish one of the purposes specified in paragraphs (b)(1) through (b)(6). Before making a disclosure, the lawyer should, where practicable, first seek to persuade the client to take suitable action to obviate the need for disclosure. In any case, a disclosure adverse to the client's interest should be no greater than the lawyer reasonably believes necessary to accomplish the purpose, particularly when accusations of wrongdoing in the representation of a client have been made by a third party rather than by the client. If the disclosure will be made in connection with an adjudicative proceeding, the disclosure should be

made in a manner that limits access to the information to the tribunal or other persons having a need to know the information, and appropriate protective orders or other arrangements should be sought by the lawyer to the fullest extent practicable.

[15] Paragraph (b) permits but does not require the disclosure of information relating to a client's representation to accomplish the purposes specified in paragraphs (b)(1) through (b)(6). A lawyer's decision not to disclose as permitted by paragraph (b) does not violate this Rule. Disclosure may, however, be required by other Rules or by other law. *See* Comments [12]-[13]. Some Rules require disclosure only if such disclosure would be permitted by paragraph (b). *E.g.*, Rule 8.3(c)(1). Rule 3.3(c), on the other hand, requires disclosure in some circumstances whether or not disclosure is permitted or prohibited by this Rule.

Withdrawal

[15A] If the lawyer's services will be used by the client in materially furthering a course of criminal or fraudulent conduct, the lawyer must withdraw pursuant to Rule 1.16(b)(1). Withdrawal may also be required or permitted for other reasons under Rule 1.16. After withdrawal, the lawyer is required to refrain from disclosing or using information protected by Rule 1.6, except as this Rule permits such disclosure. Neither this Rule, nor Rule 1.9(c), nor Rule 1.16(e) prevents the lawyer from giving notice of the fact of withdrawal. For withdrawal or disaffirmance of an opinion or representation, see paragraph (b)(3) and Comment [6E]. Where the client is an organization, the lawyer may be in doubt whether the organization will actually carry out the contemplated conduct. Where necessary to guide conduct in connection with this Rule, the lawyer may, and sometimes must, make inquiry within the organization. *See* Rules 1.13(b) and (c).

Duty to Preserve Confidentiality

[16] Paragraph (c) imposes three related obligations. It requires a lawyer to make reasonable efforts to safeguard confidential information against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are otherwise subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. Confidential information includes not only information protected by Rule 1.6(a) with respect to current clients but also information protected by Rule 1.9(c) with respect to former clients and information protected by Rule 1.18(b) with respect to prospective clients. Unauthorized access to, or the inadvertent or unauthorized disclosure of, information protected by Rules 1.6, 1.9, or 1.18, does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the unauthorized access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to: (i) the sensitivity of the information; (ii) the likelihood of disclosure if additional safeguards are not employed; (iii) the cost of employing additional safeguards; (iv) the difficulty of implementing the safeguards; and (v) the extent to which the safeguards adversely affect the lawyer's ability to represent clients (*e.g.*, by making a device or software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule, or may give informed consent to forgo security measures that would otherwise be required by this Rule. For a lawyer's duties when sharing information with nonlawyers inside or outside the lawyer's own firm, see Rule 5.3, Comment [2].

[17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. Paragraph (c) does not ordinarily require that the lawyer use special security measures if the method of communication affords a reasonable expectation of confidentiality. However, a lawyer may be required to take specific steps to safeguard a client's information to comply with a court order (such as a protective order) or to comply with other law (such as state and federal laws or court rules that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information). For example, a protective order may extend a high level of protection to documents marked "Confidential" or "Confidential – Attorneys' Eyes Only"; the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") may require a lawyer to take specific precautions with respect to a client's or adversary's medical records; and court rules may require a lawyer to block out a client's Social Security number or a minor's name when electronically filing papers with the court. The specific requirements of court orders, court rules, and other laws are beyond the scope of these Rules.

Lateral Moves, Law Firm Mergers, and Confidentiality

[18A] When lawyers or law firms (including in-house legal departments) contemplate a new association with other lawyers or law firms though lateral hiring or merger, disclosure of limited information may be necessary to resolve conflicts of interest pursuant to Rule 1.10 and to address financial, staffing, operational, and other practical issues. However, Rule 1.6(a) requires lawyers and law firms to protect their clients' confidential information, so lawyers and law firms may not disclose such information for their own advantage or for the advantage of third parties absent a client's informed consent or some other exception to Rule 1.6.

[18B] Disclosure without client consent in the context of a possible lateral move or law firm merger is ordinarily permitted regarding basic information such as: (i) the identities of clients or other parties involved in a matter; (ii) a brief summary of the status and nature of a particular matter, including the general issues involved; (iii) information that is publicly available; (iv) the lawyer's total book of business; (v) the financial terms of each lawyer-client relationship; and (vi) information about aggregate current and historical payment of fees (such as realization rates, average receivables, and aggregate timeliness of payments). Such information is generally not "confidential information" within the meaning of Rule 1.6.

[18C] Disclosure without client consent in the context of a possible lateral move or law firm merger is ordinarily *not* permitted, however, if information is protected by Rule 1.6(a), 1.9(c), or Rule 1.18(b). This includes information that a lawyer knows or reasonably believes is protected by the attorney-client privilege, or is likely to be detrimental or embarrassing to the client, or is information that the client has requested be kept confidential. For example, many clients would not want their lawyers to disclose their tardiness in paying bills; the amounts they spend on legal fees in particular matters; forecasts about their financial prospects; ir information relating to sensitive client matters (e.g., an unannounced corporate takeover, an undisclosed possible divorce, or a criminal investigation into the client's conduct).

[18D] When lawyers are exploring a new association, whether by lateral move or by merger, all lawyers involved must individually consider fiduciary obligations to their existing firms that may bear on the timing and scope of disclosures to clients relating to conflicts and financial concerns, and should consider whether to ask clients for a waiver of confidentiality if consistent with these fiduciary duties – *see* Rule 1.10(e) (requiring law firms to check for conflicts of interest). Questions of fiduciary duty are legal issues beyond the scope of the Rules.

[18E] For the unique confidentiality and notice provisions that apply to a lawyer or law firm seeking to sell all or part of its practice, see Rule 1.17 and Comment [7] to that Rule.

[18F] Before disclosing information regarding a possible lateral move or law firm merger, law firms and lawyers moving between firms – both those providing information and those receiving information – should use reasonable measures to minimize the risk of any improper, unauthorized or inadvertent disclosures, whether or not the information is protected by Rule 1.6(a), 1.9(c), or 1.18(b). These steps might include such measures as: (1) disclosing client information in stages; initially identifying only certain clients and providing only limited information, and providing a complete list of clients and more detailed financial information only at subsequent stages; (2) limiting disclosure to those at the firm, or even a single person at the firm, directly involved in clearing conflicts and making the business decision whether to move forward to the next stage regarding the lateral hire or law firm merger; and/or (3) agreeing not to disclose financial or conflict information outside the firm(s) during and after the lateral hiring negotiations or merger process.

RULE 4.4:
RESPECT FOR RIGHTS OF THIRD PERSONS

(a) In representing a client, a lawyer shall not use means that have no substantial purpose other than to embarrass or harm a third person or use methods of obtaining evidence that violate the legal rights of such a person.

(b) A lawyer who receives a document, electronically stored information, or other writing relating to the representation of the lawyer's client and knows or reasonably should know that it was inadvertently sent shall promptly notify the sender.

Comment

[1] Responsibility to a client requires a lawyer to subordinate the interests of others to those of the client, but that responsibility does not imply that a lawyer may disregard the rights of third persons. It is impractical to catalogue all such rights, but they include legal restrictions on methods of obtaining evidence from third persons and unwarranted intrusions into privileged relationships, such as the client-lawyer relationship.

[2] Paragraph (b) recognizes that lawyers and law firms sometimes receive a document, electronically stored information, or other "writing as defined in Rule 1.0(x), that was mistakenly sent, produced, or otherwise inadvertently made available by opposing parties or their lawyers. A document, electronically stored information, or other writing is "inadvertently sent" within the meaning of paragraph (b) when it is accidentally transmitted, such as when an email or letter is misaddressed or a document or other writing is accidentally included with information that was intentionally transmitted. One way to resolve this situation is for lawyers and law firms to enter into agreements containing explicit provisions as to how the parties will deal with inadvertently sent documents. In the absence of such an agreement, however, if a lawyer or law firm knows or reasonably should know that such a document or other writing was sent inadvertently, this Rule requires only that the receiving lawyer promptly notify the sender in order to permit that person to take protective measures. Although this Rule does not require that the receiving lawyer refrain from reading or continuing to read the document, a lawyer who reads or continues to read a document that contains privileged or confidential information may be subject to court-imposed sanctions, including disqualification and evidence-preclusion. Whether the lawyer or law firm is required to take additional steps, such as returning the document or other writing, is a matter of law beyond the scope of these Rules, as is the question whether the privileged status of a document or other writing has been waived. Similarly, this Rule does not address the legal duties of a lawyer who receives a document or other writing that the lawyer knows or reasonably should know may have been inappropriately obtained by the sending person. For purposes of this Rule, "document, electronically stored information or other writing" includes not only paper documents, but also email and other forms of electronically stored information – including embedded data (commonly referred to as "metadata") – that is subject to being read or put into readable form. *See* Rule 1.0(x).

[3] Refraining from reading or continuing to read a document or other writing once a lawyer realizes that it was inadvertently sent and returning the document to the sender or permanently deleting electronically stored information, honors the policy of these Rules to

RULE 5.0:

RULE 5.1:
RESPONSIBILITIES OF LAW FIRMS, PARTNERS, MANAGERS AND SUPERVISORY LAWYERS

(a) A law firm shall make reasonable efforts to ensure that all lawyers in the firm conform to these Rules.

(b) (1) A lawyer with management responsibility in a law firm shall make reasonable efforts to ensure that other lawyers in the law firm conform to these Rules.

(2) A lawyer with direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the supervised lawyer conforms to these Rules.

(c) A law firm shall ensure that the work of partners and associates is adequately supervised, as appropriate. A lawyer with direct supervisory authority over another lawyer shall adequately supervise the work of the other lawyer, as appropriate. In either case, the degree of supervision required is that which is reasonable under the circumstances, taking into account factors such as the experience of the person whose work is being supervised, the amount of work involved in a particular matter, and the likelihood that ethical problems might arise in the course of working on the matter.

(d) A lawyer shall be responsible for a violation of these Rules by another lawyer if:

(1) the lawyer orders or directs the specific conduct or, with knowledge of the specific conduct, ratifies it; or

(2) the lawyer is a partner in a law firm or is a lawyer who individually or together with other lawyers possesses comparable managerial responsibility in a law firm in which the other lawyer practices or is a lawyer who has supervisory authority over the other lawyer; and

(i) knows of such conduct at a time when it could be prevented or its consequences avoided or mitigated but fails to take reasonable remedial action; or

(ii) in the exercise of reasonable management or supervisory authority should have known of the conduct so that reasonable remedial action could have been taken at a time when the consequences of the conduct could have been avoided or mitigated.

RULE 5.3:
LAWYER'S RESPONSIBILITY FOR CONDUCT OF NONLAWYERS

(a) A law firm shall ensure that the work of nonlawyers who work for the firm is adequately supervised, as appropriate. A lawyer with direct supervisory authority over a nonlawyer shall adequately supervise the work of the nonlawyer, as appropriate. In either case, the degree of supervision required is that which is reasonable under the circumstances, taking into account factors such as the experience of the person whose work is being supervised, the amount of work involved in a particular matter and the likelihood that ethical problems might arise in the course of working on the matter.

(b) A lawyer shall be responsible for conduct of a nonlawyer employed or retained by or associated with the lawyer that would be a violation of these Rules if engaged in by a lawyer, if:

> **(1) the lawyer orders or directs the specific conduct or, with knowledge of the specific conduct, ratifies it; or**
>
> **(2) the lawyer is a partner in a law firm or is a lawyer who individually or together with other lawyers possesses comparable managerial responsibility in a law firm in which the nonlawyer is employed or is a lawyer who has supervisory authority over the nonlawyer; and**
>
> > **(i) knows of such conduct at a time when it could be prevented or its consequences avoided or mitigated but fails to take reasonable remedial action; or**
> >
> > **(ii) in the exercise of reasonable management or supervisory authority should have known of the conduct so that reasonable remedial action could have been taken at a time when the consequences of the conduct could have been avoided or mitigated.**

Comment

[1] This Rule requires a law firm to ensure that work of nonlawyers is appropriately supervised. In addition, a lawyer with direct supervisory authority over the work of nonlawyers must adequately supervise those nonlawyers. Comments [2] and [3] to Rule 5.1, which concern supervision of lawyers, provide guidance by analogy for the methods and extent of supervising nonlawyers.

[2] With regard to nonlawyers, who are not themselves subject to these Rules, the purpose of the supervision is to give reasonable assurance that the conduct of all nonlawyers employed by or retained by or associated with the law firm, including nonlawyers outside the firm working on firm matters, is compatible with the professional obligations of the lawyers and firm. Lawyers typically employ nonlawyer assistants in their practice, including secretaries, investigators, law student interns and paraprofessionals. Such nonlawyer assistants, whether they are employees or independent contractors, act for the lawyer in rendition of the lawyer's professional services. Likewise, lawyers may employ nonlawyers outside the firm to assist in

CYBERSECURITY LAW ALERT

March 3, 2026

By: Steven J. Kuperschmid, Esq.
Nicole E. Osborne, Esq.
Tyla R. Phillip, Esq.

RUSKIN MOSCOU FALTISCHEK P.C.
Smart Counsel. Straight Talk.

Practical Cybersecurity Measures Amid Heightened Global Risk

Recent geopolitical developments, including escalating global tensions, have increased the risk of cyber threat activity directed at U.S. businesses and institutions. Cyber threat actors, whether they are foreign state-sponsored or domestic criminals, exploit uncertainty and often take time to "study" an organization before they plan an attack. Most often, threat actors are looking for organizations that handle sensitive and valuable data which may include, but are not limited to, professional services firms, financial institutions, healthcare providers, and middle-market companies. This alert outlines practical steps that organizations should consider taking to reduce risk and strengthen their cybersecurity posture.

The first practical way to increase your organization's cybersecurity is to improve your company's access controls for both in-person and remote work. This may include implementing multi-factor authentication (MFA) wherever available, particularly for email logins, remote access to servers, cloud services, and financial systems where any sensitive data may be held. A good way to gauge if your organization has some unwanted cyber visitors is investigating unexpected MFA prompts. Companies should also require employees to use unique and strong passwords that are distinct from any other password used by the employee. Another small but highly impactful tip is requiring all employees to change their passwords at least once a quarter, if not more frequently.

Where employees are permitted to work from home, companies must also take important safeguards to protect information accessible to employees remotely. Simple ways to boost cybersecurity for remote workers include requiring a VPN or similar protections and prohibiting the use of public Wi-Fi without appropriate safeguards. Laptops and mobile devices should also be encrypted and protected with strong authentication measures.

Second is educating employees of how threat actors gain access to the system by gaining their trust, usually by a phishing attempt or social engineering. Organizations should remind employees to be extra cautions of emails that: (1) create a sense of urgency or pressure to respond; (2) request login credentials, wire transfers, or other sensitive information; (3) contain unexpected attachments or links; or (4) appear to come from executives, vendors, or clients but contain subtle inconsistencies. It is important that employees are adequately trained to be able to identify and promptly report any suspicious communications sent to them. Businesses should be engaging in regular testing of their employees through the use of mock, but realistic, phishing attempt emails, especially in light of an increase in sophistication and accuracy due to the use of Artificial Intelligence by threat actors.

Third, ensure timely patching and updates. Many successful attacks exploit known vulnerabilities for which patches already exist. To ensure compliance, companies should conduct an internal audit to ensure their network is secure. This may entail confirming that operating systems, servers, applications, and network devices are fully up to date, and applying security patches promptly, particularly for internet-facing systems and remote access tools.

Any internal audit should also remove or isolate unsupported software and legacy systems where possible. For example, backups should be stored in isolated environments away from the primary network. Restoration procedures should also be tested frequently to ensure backups are accessible to keep your business running in case of an emergency.

Fourth is protecting sensitive data in every communication. While this goes without saying, it is nonetheless important to use encryption for data at rest and in transit. Emails that contain highly confidential or sensitive information should also be sent via encrypted email for an added layer of protection. Companies should also only permit employees to access data necessary to perform their roles. This is particularly important as social engineering attempts are often geared at those with the most access, so by limiting the number of employees who have access, you limit the pool of ideal candidates to threat actors.

Fifth is ensuring your business partners are also protected. Many cyber incidents originate through vendors or service providers. Companies should ensure they are adequately vetting any external or third-party vendor they share data with, in any capacity. It is important to ensure that these vendors are also investing in maintaining cybersecurity safeguards. Any contracts with external companies or vendors should appropriately address data protection and incident notification obligations.

Finally, every organization should have a clear plan for responding to cybersecurity incidents. While no company hopes to be involved in a cybersecurity incident, the response is much smoother when there is a clear and accessible plan to look to for next steps. This plan should be memorialized and should identify key personnel within your organization and any external assistance your company may need with respect to a technical response, legal review, and any reporting requirements. Education and training are also key components to incident response. Organizations should ensure decision-makers understand escalation procedures and consider tabletop exercises to test readiness before an actual incident occurs. In the event of any incident, organizations should always contact their own outside counsel first, in an attempt to maintain privilege over the breach investigation.

Periods of global instability often heighten cyber risk, as they tend to create opportunities for malicious actors to exploit uncertainty and gaps in preparedness. The measures outlined above are practical to implement for most organizations and with proper guidance, they can drastically improve your company's cybersecurity posture. If you need assistance with cybersecurity preparedness, incident response, regulatory considerations, or want to memorialize an incident response plan for your company, please contact:

Nicole E. Osborne, Esq.
516.663.6687
nosborne@rmfpc.com

Steven J. Kuperschmid, Esq.
516.663.6686
skuperschmid@rmfpc.com

Tyla R. Phillip, Esq.
516.663.6503
tphillip@rmfpc.com