Tarter Krinsky & Drogin

THE BACHMAN LAW FIRM PLLC

The Coyle Group
RISK MANAGEMENT

BE CYBER AWARE. BE CYBER SECURE.

Amy B. Goldsmith, Esq.
Chair, Privacy and Cybersecurity
Tarter Krinsky & Drogin LLP
Judith Bachman, Esq.
The Bachman Law Firm PLLC
Gordon B. Coyle, CPCU, ARM, AMIM, PWCA
CEO, The Coyle Group

CYBERSECURITY: STATISTICS

3 seconds to encrypt

Attacks every 11 seconds

Ransomware = 2022

Average payment: $812,360

Total Average Cost: $4.5 million

CYBERSECURITY IS BOTH A LEGAL AND ETHICAL REQUIREMENT FOR LAWYERS

Statutory Framework

i. NY Shield Law

ii. Other laws

1. California
2. GDPR

NY SHIELD OBLIGATIONS

- Stands for: Stop Hacks and Improve Electronic Data Security Act
- N.Y. Gen. Bus. Law § 899-aa(1)(a), (b): Effective March 21, 2020
- Focuses on unauthorized access to or acquisition of New Yorker's electronic records which "compromises the security, confidentiality, or integrity of private information maintained by a business"
- Was the PI accessed or reasonably believed to have been accessed by an unauthorized person?
- ELECTRONIC RECORDS ONLY: NOT PRINTED PAPER!

WHO IS AFFECTED BY THE SHIELD ACT?

- Any person or business that owns, licenses, or for service businesses, maintains computerized data that includes the private information of New York residents
- individuals
- non-profits
- all businesses, big and small
- The entity does not have to be located in New York or conduct business in New York

NY SHIELD

Defines, documents, and supports the implementation and maintenance of the administrative, technical, and physical safeguards the company has selected to protect the personal information it collects, creates, uses, and maintains.

- **NY Shield**: "personal information" means any information concerning a natural person, which, because of name, number, personal mark, or other identifier, can be used to identify such natural person

- **NY Shield**: “private information” means either (i) personal information consisting of any information in combination with one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired:

NY SHIELD

(i) Social Security number;

(ii) Driver's license number or non-driver identification card number;

(iii) Account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account;

(iv) Account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password;

NY SHIELD

(v) Biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity; or

(vi) A username or e-mail address in combination with a password or security question and answer that would permit access to an online account.

(c) Private information does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.

WHEN DO OBLIGATIONS UNDER THE SHIELD ACT COME INTO EFFECT?

- Theft of a computer or another device
- Downloaded or copied records
- Creation of fraudulent accounts
- "indications that the information was viewed, communicated with, used, or altered without valid authorization."
- An entity that maintains computerized data that it does not own must notify the owner or licensee of the information of any breach of the security of the system immediately following discovery if the private information was, or is reasonably believed to have been, acquired by an unauthorized person

QUESTIONS

What information are you collecting about your clients?

Name

Address

Email

Phone

Driver's License

Social Security Number

Financial information: banking, credit union, insurance, investments, medical, health

WHAT IS PERSONAL INFORMATION?

any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person

WHAT IS PRIVATE INFORMATION?

PERSONAL INFORMATION PLUS A DATA ELEMENT WHEN EITHER THE DATA ELEMENT OR THE PI/DE COMBINATION IS NOT ENCRYPTED, OR, IF ENCRYPTED, THE "HACK" INCLUDED ACCESS TO THE ENCRYPTION KEY

social security number

driver's license number or non-driver ID

financial account information: credit, debit or bank account number

biometric information (fingerprint, voice print, retina/iris images or any other unique physical or digital way of finding out a person's identity)

MANDATORY SECURITY PROTOCOLS

Any business that fails to implement the below security protocols is also subject to action by the Attorney General.

Implement a Data Security Program, which:

(1) designates one or more employees to coordinate the security program;

(2) identifies reasonably foreseeable internal and external risks;

(3) assesses the sufficiency of safeguards in place to control the identified risks;

- (4) trains and manages employees in the security program practices and procedures;
- (5) selects service providers capable of maintaining appropriate safe-guards, and requires those safeguards by contract; and
- (6) adjusts the security program in light of business changes or new circumstances.

MANDATORY SECURITY PROTOCOLS

- Physical Safeguards, which:
- (1) assess of the risks of information storage and disposal;
- (2) detect, prevent and respond to intrusions;
- (3) protect against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and
- (4) disposes of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

Technical Safeguards, which:

(1) assess risks in network and software design;

(2) assess risks in information processing, transmission and storage;

(3) detect, prevent and respond to attacks or system failures; and

(4) regularly tests and monitors the effectiveness of key controls, systems and procedures.

SMALL BUSINESS AND COMPLIANCE

- Businesses who are subject to and already in compliance with GLB, HIPAA/HITECH or New York's rules for financial service companies, or any other federal or New York agency data security statutes, rules or regulations are considered to be compliant with these SHIELD Act provisions.

What is a small business? Fewer than 50 employees, less than $3 million dollars in gross annual revenues for the last three years or less than $5 million dollars in total assets

Does the small business's security program contain reasonable administrative, technical and physical safeguards that are appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers?

CALIFORNIA

Is your revenue over $25 million?

Do you have PII of California residents?

Do you sell PII?

GDPR

Do you have the PII (or PD) of any European residents?

Do you enter into contracts with European companies?

CYBERSECURITY REQUIREMENTS: WHAT ARE LAWYERS REQUIRED TO DO?

ETHICAL OBLIGATIONS: A LAWYER MUST BE PROFICIENT IN CYBERSECURITY AND PROTECT CLIENT INFORMATION

Lawyer's cybersecurity ethical obligations under the Rules* stem from requirements as to, among other things,:

- competence,
- client communication, and
- confidentiality.

These rule based obligations are fortified by ethics opinions; for example:

- Remote access to client files and cloud data storage is permissible if the particular technology used provides reasonable protection to client confidential information. NYSBA Opinion 1019, 1020;
- Particular cybersecurity safeguards that lawyers must employ. ABA Formal Opinion 477R; and
- What lawyer's must do after a hack. ABA Formal Opinion 483.

*R. 1.0, 1.1, 1.4, 1.6, 5.1, 5.2, 5.3 of the Rules of Professional Conduct (22 N.Y.C.R.R. §1200)

LAWYERS AND TECHNOLOGY: WHAT DO YOU KNOW?

ARTIFICIAL INTELLIGENCE

USE CASES: Lawgeex, Westlaw Edge

ESL: DOCUMENT REVIEW, LEGAL RESEARCH, CONTRACT REVIEW; CONTRACT DRAFTING, EVALUATE LEGAL OUTCOMES

Issues: inherent bias

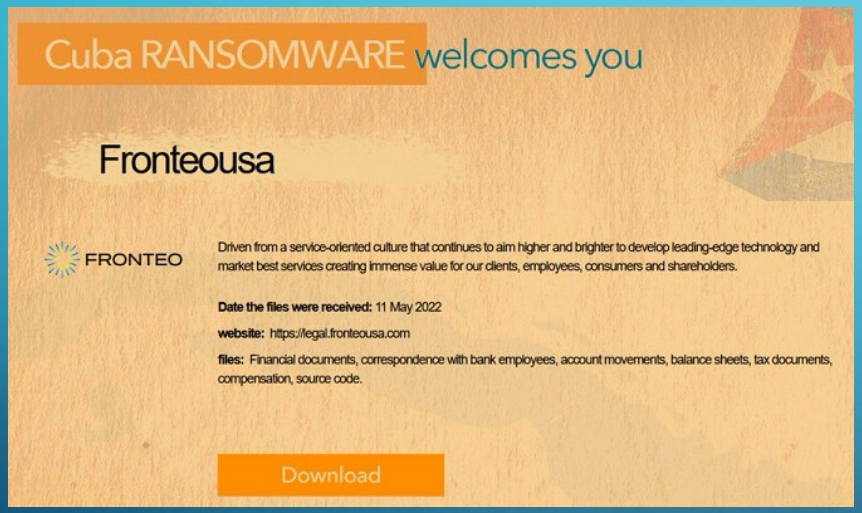
CHATGPT

USE CASES: automated legal brief writing; discovery requests, case summaries

Issues: do you have your own instance to preserve confidentiality?

What if the results are "fictional"?

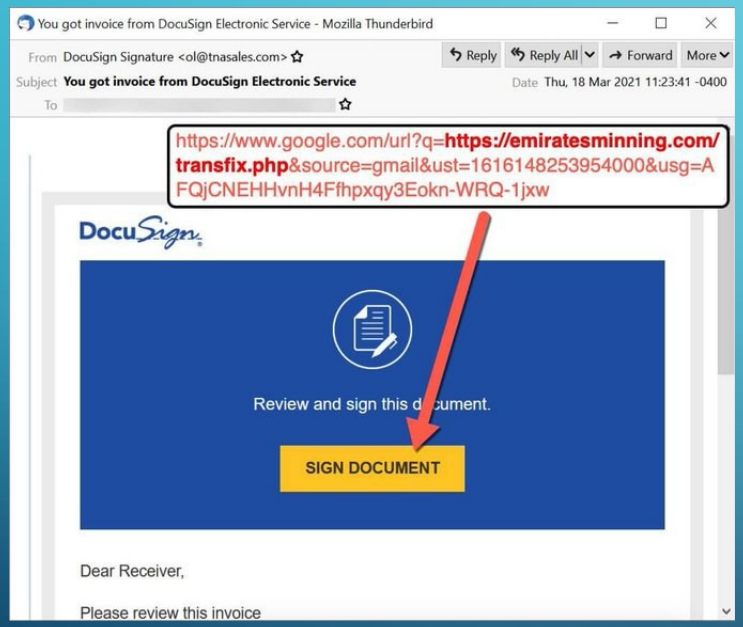
A RECENT HACK



"Here is a screen shot of what was supposedly displayed on the FRONTEO site (courtesy of this tweet from DailyDarkWeb), as you can see, it has a "Download" button, which implies the data could be downloaded but might simply be a subterfuge for stealing a password (see below)."

https://ediscoverytoday.com/2022/05/20/cuba-ransomware-group-hacked-fronteo/

DOCUSIGN: OR IS IT?



De Grasse confirmed the approach of the Cuba Ransomware group, stating: "The Cuba M.O. is to install password-stealers, like Pony, Ficker, or their Cobalt Strike and is usually distributed through malicious spam campaigns pretending to be DocuSign invoices. That is where they excel. As our Group has noted before, document signing services are an easy cyber attack route."

https://ediscoverytoday.com/2022/05/20/cuba-ransomware-group-hacked-fronteo/

WHO HAS BEEN HACKED? YOU'LL BE SURPRISED…

COVINGTON

CADWALADER

troutman pepper

WHO HAS BEEN HACKED? YOU'LL BE SURPRISED….

Campbell Conroy & O'Neil, P.C. (2021)

Grubman Shire Meiselas & Sacks (2020)

Fragomen (Form I9s, 2020)

Seyfarth Shaw (malware, 2020)

DLA Piper (malware, 2017)

Jenner & Block (phishing, 2017)

Proskauer Rose (phishing, 2016)

LAW FIRMS: WHAT ARE THE STATISTICS?

2020 ABA report: 29% of law firms reported a security breach, 36% reported past malware infections

File encryption: 43%

Device Recovery: 27%

Email encryption: 39%

Web Filtering: 26%

Whole/Full Disk encryption: 26%

Employee Monitoring: 23%

Two-Factor Authentication: 39%

Biometric Login: 12%

Intrusion Prevention or Detection: 29%

Remote Device Management and Wiping: 28%

DEFINITIONS

- Hackers: persons who compromise digital devices and networks through unauthorized access to an account or computer system

DEFINITIONS

Smart Devices	smart phones and pads (Android and Apple operating systems)
Webcams	a camera attached to your computer
Router	box that allows all the wired and wireless devices to simultaneously use the Internet connection and talk to the other without using the Internet
Software	code that runs operating systems

RECOGNIZING ENTRY POINTS

Remote access gateways, such as those that support:

- telecommuting through dial-up or virtual private network (VPN) connections; and
- mobile devices.
- Wireless networks at an organization's facilities or events.
- Extranet connections that link an organization's internal network to vendors' or business partners' networks.

Hackers often exploit vulnerabilities in common network entry points, including:

Internet connections, such as those that support:

an organization's website, apps, or other e-commerce capabilities;

email;

web surfing and access to cloud computing resources; and

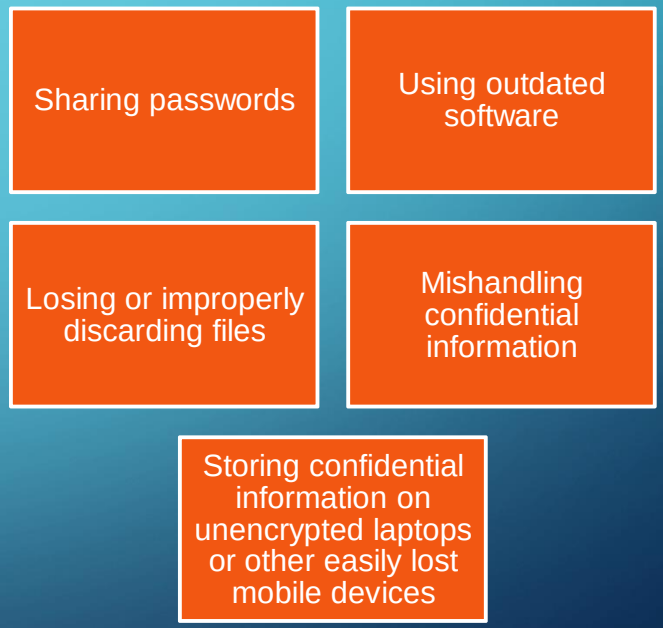
file transfer, instant messaging, VoIP, or other internet-based services.

ENTRY POINTS

IT'S ALL ABOUT PEOPLE AND THE MISTAKES THEY MAKE

People use poor judgment and make mistakes by:

- Circumventing information security controls;
- intentionally for criminal purposes;
- in the mistaken belief that they can improve efficiency; and
- narrow mindedly thinking that they "just need to get the job done" regardless of risk.



SO HOW DOES HACKING HAPPEN?

- INFILTRATE: Access and assess the company's IT networks and systems to find vulnerabilities
- ESCALATION: Exploitation of vulnerabilities by inserting malware
- ESCALATION: grab passwords and Confidential Information; establish backdoors
- AVOID DETECTION: resetting configurations and removal of evidence

COMMON VULNERABILITIES AND HACKING METHODS

Unsecured Communications

1. Are your communications unencrypted? (public WiFi)
2. Are your smart devices (phones, webcams, modems, routers) unsecured?
3. Are your passwords following the KISS principle?
4. Is the software you use continuously updated?

- Remote Access Trojan malware enables spying on users, reach messages, take screenshots, hijack webcams
- Connecting to unsecured networks creates an open road for a hacker

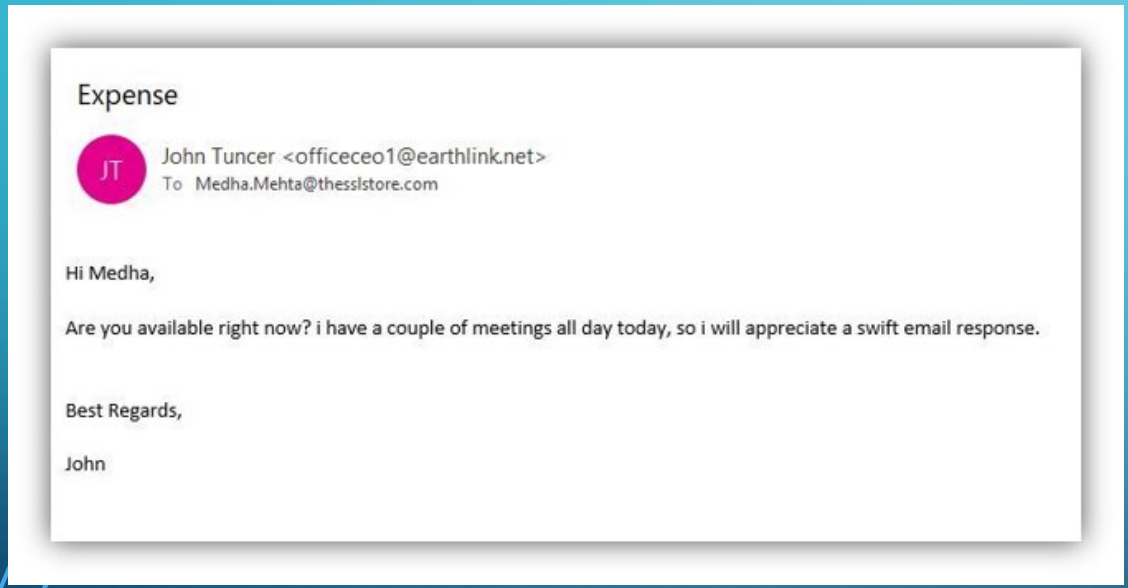
UNDERSTANDING MALWARE AND END USER ATTACKS

- Data theft
- Attacks from the inside
- DoS and DDoS attacks
- Advanced persistent threats
- Malware

DATA THEFT: HOW CAN IT OCCUR?

- **Wiretaps**: any IoT device, including Alexa and Google, are vulnerable
- **Domain Name Hijacking**: without permission, the ownership or administration of a domain name is changed
- **Spoofing**: an email is sent from a false sender address which may mimics an internal company address; it could contain a link to malware
- **Phishing**: emails that look like they are from reputable companies; it could contain a link to malware
- **Dark web**: company data is already compromised and available for sale on the dark web

EXAMPLES: SPOOFING



Expense

JT

John Tuncer <officeceo1@earthlink.net>
To Medha.Mehta@thesslstore.com

Hi Medha,

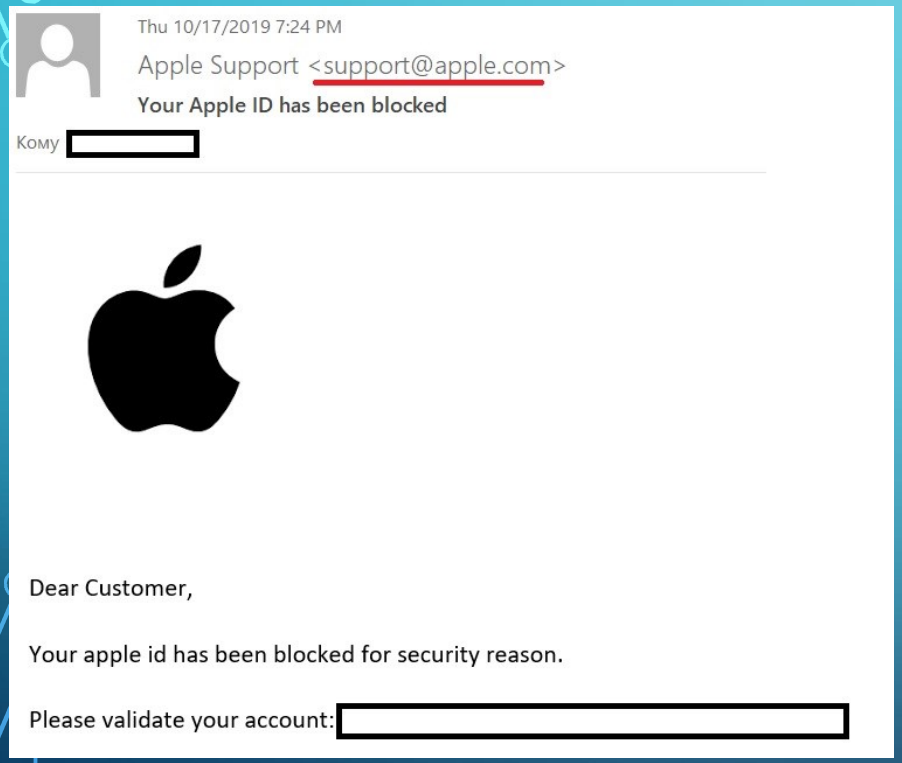
Are you available right now? i have a couple of meetings all day today, so i will appreciate a swift email response.

Best Regards,

John

https://securityboulevard.com/2020/01/email-spoofing-101-how-to-avoid-becoming-a-victim/

EXAMPLES: PHISHING



Thu 10/17/2019 7:24 PM

Apple Support <support@apple.com>

Your Apple ID has been blocked

Кому [redacted]

Dear Customer,

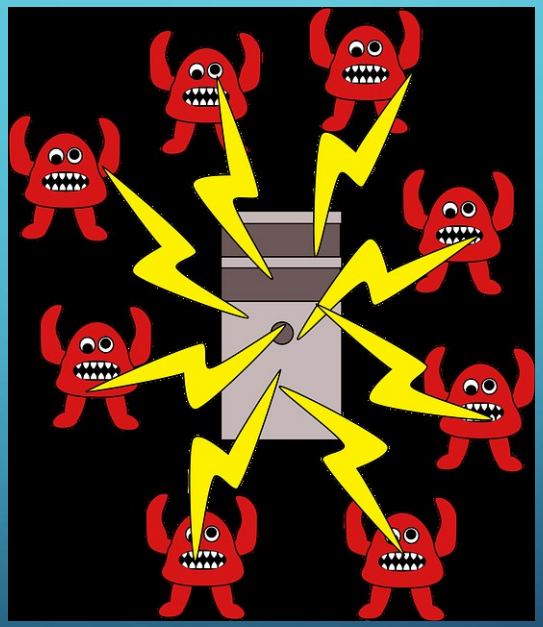
Your apple id has been blocked for security reason.

Please validate your account: [redacted]

https://securelist.com/email-spoofing-types/102703/

ATTACK FROM THE INSIDE

DOS AND DDOS ATTACKS



APT: ADVANCED PERSISTENT THREATS

Targeted Industries

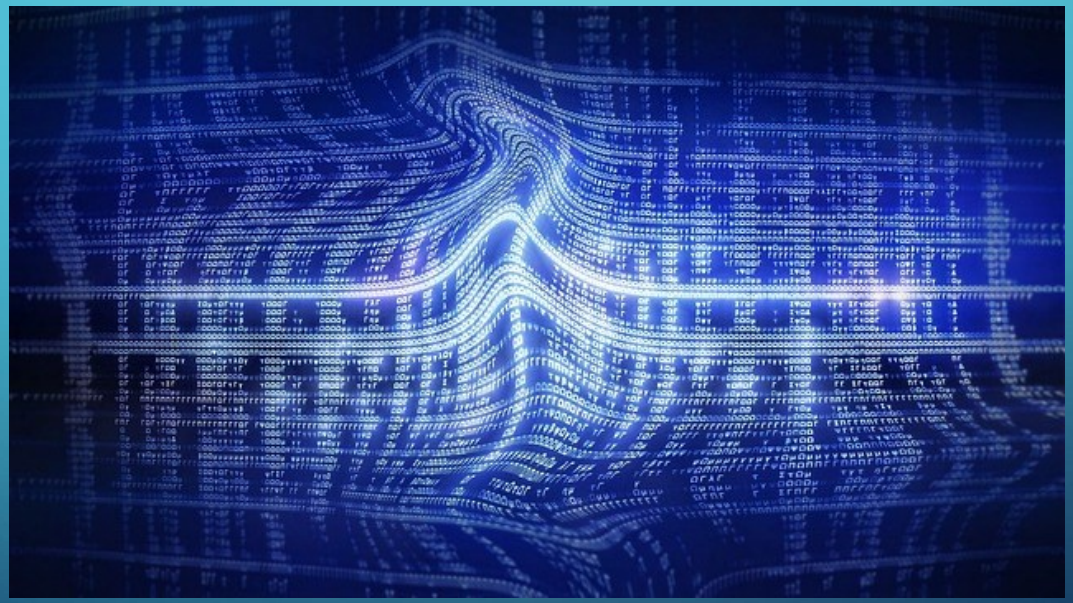
- **Financial:** 238% increase in cyber attacks, average cost of a data breach tops $5 million dollars
- **Aviation:** millions of breached records
- **Healthcare:** 2020: 270 breaches of 8 million patient data records
- **Manufacturing:** data breaches are rising and are major
- **Telecom:** T-Mobile, Verizon, AT&T, Sprint have all been the victim of DDoS attacks

NATION STATES

China, Russia, North Korea

PRIVATE BAD ACTORS (sometimes state supported)

MALWARE



TYPES OF ATTACKS

Viruses: malicious code is attached to a host (file, program, document)

Worms: do not need a host program; can self-replicate and rapidly move through networks and infect machines by exploiting unsecured communications channels

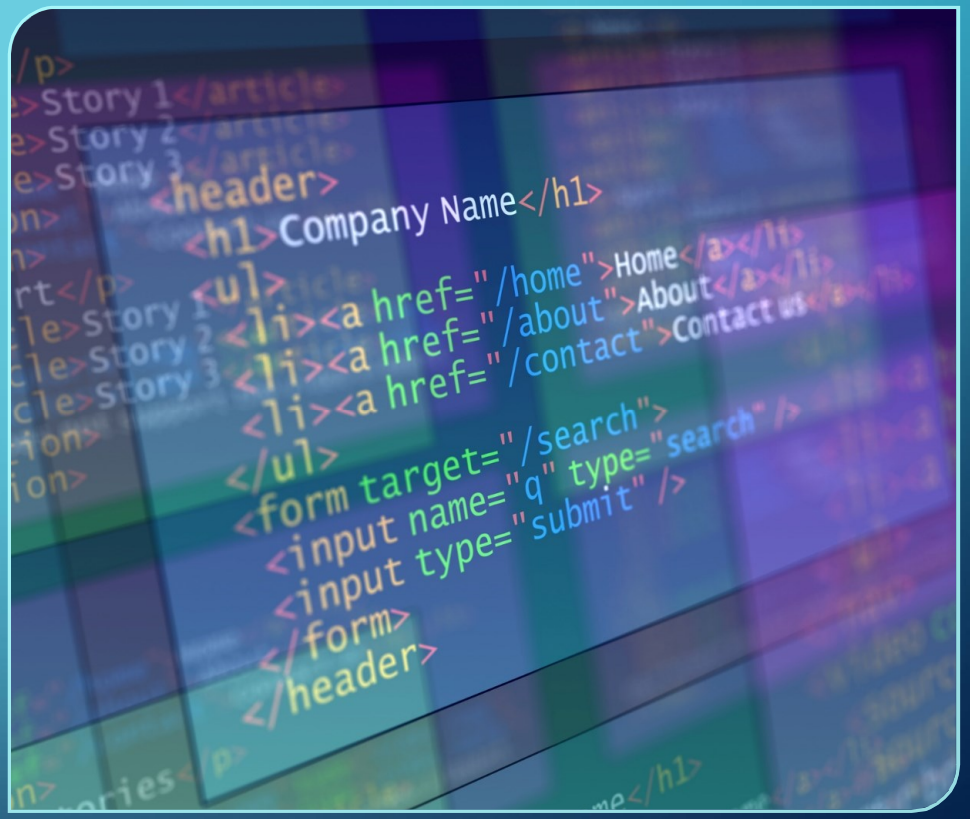
Bots: type of malware that allows the hacker to send more command and control codes into the system; used to send spam or to launch DoS or DDoS attacks

Spyware and Keyloggers: spyware = hacker's eyes into the system; keyloggers record keystrokes (what is being typed) and clicks so that the hacker can keep a record of them; used to grab passwords, access credentials of high value people (checkbook, confidential information/trade secrets, reputational information)

TYPES OF ATTACKS

- **Trojans**: malware is disguised as a game or App that one downloads; then the malicious code is in your system

- **Adware**: advertisements may contain Adware, gathering data for marketing purposes, but Confidential Information may be gathered too; Adware could also contain Trojans or other types of malicious code



TYPES OF ATTACKS

- **Social engineering**
- Phishing, spoofing, phone calls

  - Goals:
    - The hacker wants personally identifiable information such as names, license and social security numbers, financial account information; credit cards, tax forms of employees
    - The hacker wants usernames, passwords, any other credential
    - The hacker wants information about the it systems, data, and networks
    - The hacker wants money wired

RANSOMWARE

LOCKER

- The device is locked
- Ransom must be paid to unlock the device
- Ransom messages may mimic law enforcement
- Hackers may release embarrassing content
- Data is not destroyed and may be able to be retrieved

CRYPTO

- Access to files is locked, not access to the device
- Data cannot be read without the hacker's decryption key
- Ransom messages say "Give me money, I'll give you the key"

BEING CYBER AWARE AND CYBER SECURE

- **Prevention, Detection and Response**
- Authentication to access system remotely

- b) Update browser and web server software; be aware of all Microsoft and Apple vulnerabilities

- c) Robust protocols for all transactions for disclosing sensitive data and making payments; double authentication, review and approval

BEING CYBER AWARE AND CYBER SECURE

- Registration of like-kind domain names
- Implementation of cybersecurity measures
- Periodic Drills and Training

BEING CYBER AWARE AND CYBER SECURE

Best Practices

- Software updates and patches continuously
- Train your people to use unique passwords for different accounts
- USE HTTPS ENCRYPTION: https://www.tarterkrinsky.com
- Don't click on strange links or pop-up ads
- Router and smart devices: create a new username and password, don't use the ones that were assigned
- Downloads should only be from trusted businesses; consider having it in control of all downloads
- Install anti-virus software on all systems, including personal laptops and phones
- Use a virtual private network
- Do not use 'admin' as a default for your IT department
- Assign strong passwords to employees; use a password manager
- Authentication: 2 factor (pushing a code to a phone, for instance)

WHAT POLICIES ARE RECOMMENDED?

- Written Information Security Program
- Cyber and Information Security Policy
- Incident Response Plan
- Business Continuity Plan
- Vendor Contract Management Plan

GOALS OF THE WRITTEN PROGRAMS

(1) Protect the security and confidentiality of the information;

(2) Protect against any anticipated threats or hazards to the security or integrity of the information;

(3) Protect against unauthorized access to and acquisition of the information that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates.

WHO IS RESPONSIBLE?

- INFORMATION SECURITY COORDINATOR
- Initial implementation of WISP and other documents
- Risk assessment
- Develop, design, distribute and maintain information security
- Oversight of internal/external IT and Cyber
- Monitor, test and train
- Incident response plan

CONFIDENTIAL INTERNAL POLICIES

- Written Information Security Program
- Purpose: teach the employee about the company's rules to keep its information safe
- No expectation of privacy when an employee uses the company's network or systems
- Company has the right to monitor the employee's use of the company's network and systems and personal phone if it is being used by the employee to access the company
- Appointment of Information Security Officer
- Establishes classification of information: public, confidential, trade secrets and safeguards and who needs to know

WRITTEN INFORMATION SECURITY PROGRAM

- defining, documenting, and supporting the implementation and maintenance of the administrative, technical, and physical safeguards company has selected to protect the personal information it collects, creates, uses, and maintains.

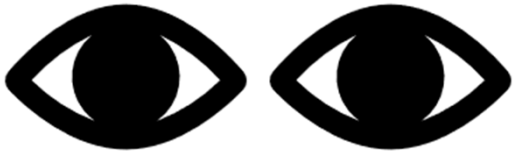
WISP

Ensures security, confidentiality, integrity and availability of personal and other sensitive information the company collects, creates, uses and maintains.

Protects against any anticipated threats or hazards to the security, confidentiality, integrity, or availability of such information.

Protect against unauthorized access to or use of company maintained personal and other sensitive information that could result in substantial harm or inconvenience to any customer or employee.

Define an information security program that is appropriate to company's size, scope, and business, its available resources, and the amount of personal and other sensitive information that company owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.



CYBER AND INFORMATION SECURITY POLICY

- Outlines how the personal information and sensitive information is protected
- States that employees have no expectation of privacy and explains monitoring
- Lists applicable regulations particular to the company's business
- Explains Data Information Classification and Risk Based Controls

INCIDENT RESPONSE PLAN

Incident Response Plan

(a) Define the Company's cyber incident response process and provide step-by-step guidelines for establishing a timely, consistent, and repeatable incident response process.
(b) Assist the Company and any applicable third parties in quickly and efficiently responding to and recovering from different levels of information security incidents.
(c) Mitigate or minimize the effects of any information security incident on the Company, its clients, employees, and others.

INCIDENT RESPONSE PLAN

- (d) Help the Company consistently document the actions it takes in response to information security incidents.

- (e) Reduce overall risk exposure for the Company.

- (f) Engage stakeholders and drive appropriate participation in resolving information security incidents while fostering continuous improvement in the Company's information security program and incident response process.

NOTICE OF BREACH

What is an acceptable notice of a breach?

The type of notice required depends on the number of consumers affected and the size of the business. Depending on these factors, it may be acceptable to notify consumers: in writing; via e- mail or electronic notice; over the phone; through the local newspaper; on the business's website; or through notification to major media outlets in the area where the entity is located.

How does notice occur?



Substitute Notice under certain circumstances

BUSINESS CONTINUITY PLAN

- COVID-19 forced companies to quickly develop and implement business continuity plans. Did you have one? If not, how fast did you develop it and what does it contain?

- Emergency contact information for internal and external personnel
- Insurance information
- Landlord information
- Tenant information
- Team members
- Meeting schedules
- Critical Assets: People, Physical Structures, Equipment, Data, Inventory, Operations, Vendors, Customers

VENDOR MANAGEMENT PROGRAM

Vendor Management Program

- Purpose: to outline the business relationship and expectations between the company and the vendor and to mitigate cyber security risks
  - Determine how the company and vendor will handle data transfers and data security
  - Require the vendor to explain how the vendor handles its own data security
  - Review the vendor's cyber security policies and insurance
  - What industry standards apply? What Government standards apply?

PRIVACY POLICY REQUIREMENTS

EMPLOYEE TRAINING AND RESPONSIBILITIES

- Familiarity with all policies
- Training
- Don’t share passwords; deactivate anti-malware software; remove or modify secure configurations; make unauthorized copies of secured information; create any unauthorized network connections

EMPLOYEE TRAINING AND RESPONSIBILITIES

Classification of and Safeguarding Information and Risk Management

a) Public Information

b) Confidential Information

c) Highly Confidential Information

d) Role Based Access Control

e) User Accounts

EMPLOYEE TRAINING AND RESPONSIBILITIES

f) Limits on Personal Use of Network Resources

g) System Controls on desktop, laptop, mobile devices

h) Information handling and storage: what is and isn't permitted?

i) Information Security Controls

j) Purchase/Download of information assets: software and hardware

CUSTOMER DATA

Review of All Contracts with Customers and Vendors: what are your company's obligations?

Responding to questionnaires:

- ❑ Do you perform penetration testing?
- ❑ Who performs the tests? How often?
- ❑ Do you have a formal information security policy?
- ❑ Do you have a policy to review user access?
- ❑ Do you use "least privilege" and multi-factor authentication?
- ❑ How do you protect data in transit from your company to other companies?
- ❑ Do you require your vendors or customers to be cyber aware and secure?
- ❑ How do you dispose of expired hard drives, flash drives, documents?
- ❑ How do you implement security training?
- ❑ Do you have an incident management program?
- ❑ What prevention measures does your internal or external IT vendor use?

CYBER INSURANCE

What questions are you likely to face?

What happens if you say “no”?

CYBER INSURANCE QUESTIONNAIRE

- What is your revenue?
- How many offices do you have?
- How many employees do you have?
- Is personally identifiable information encrypted by your company? Entire records or parts?
- How many PII records does your company maintain?

QUESTIONNAIRE

- What training do you provide? Does your training include recognizing phishing and spoofing? Incident response protocols? How often is it conducted?
- Is there an Information Security Coordinator (Officer)?
- If not, who performs this function at the company?
- How many internal IT personnel do you have? Outline their functions.

QUESTIONNAIRE

- Do you have external IT assistance?
- Does your company have a WISP, CISP, IRP, BCP, pen/vulnerability testing, intrusion detection, information back up protocols? How long would it take to restore information?
- Who assists in establishing the plans? Is your Board involved?
- Is the Board informed of cyber risks?
- Are you PCI DSS compliant?

CYBER INSURANCE AND THIRD PARTIES

- List all third parties (cloud service providers, cyber security and privacy service providers)
- Do you use due diligence measures when you share PII with third parties?
- Do you require indemnification if those third parties have a security breach involving your PII? If no, what is their obligation to you?

Contact

Amy Goldsmith

agoldsmith@tarterkrinsky.com

212-216-1135