Introduction to Cyber Crime

- Cyber crime and terrorism has escalated during recent years
- It is well-organized
- It is advanced technically
- It is well-financed
- It has adopted a new view
  - The old view: quick entry and exit
  - The new view: hidden long term presence
  - The best attack is undetected, and undetectable

Cyber Crime- It's a Big Deal!

- Forbes magazine, the global cost of cybercrime reached $2 trillion in 2019.
- Warren Buffett "cyber attacks a bigger threat to humanity than nuclear weapons"
- Ginni Rometty, IBM President & CEO, describes cybercrime as "the greatest threat to every profession, every industry, every company in the world."
- The National Computer Security Survey, conducted by the U.S. Department of Justice's Bureau of Justice Statistics, found approximately 68% of cyber theft victims will incur losses of $10,000 or more, and victims of cyber attacks will experience downtime of 24 hours or more.

Top Cyber Risks

- **Ignorance**: A cybersecurity company FireEye study found that 97% of 1,200 organizations studied had ***already*** been breached. If a company doesn't realize that it is at risk, then, it is not likely to take steps to identify and subsequently mitigate the risks.

- **Passwords**: A Verizon study found that 76% of corporate network breaches directly resulted from lost or stolen credentials. The impact of weak and repeated passwords is magnified now with so many cloud systems in use since hackers no longer have to be inside a company's network to use discovered passwords.

Top Cyber Risks

- **Vulnerabilities**: A vulnerability is a flaw or weakness in a system that hackers can exploit. Since software is written and released very quickly, the risk of security holes is greater. Periodic updates to operating systems (Windows XP, Windows 8, etc.) have diminished this risk so hackers are looking for vulnerabilities in applications, like Adobe Flash and Java, which users often do not update because they are unaware of the risk
- **A high personnel turnover**: Even within the company, there can be a high turnover and a reliance on subcontractors, making it difficult to arrange and deliver uniform IT and cybersecurity training.

Top Cyber Risks

- **A Virtual Workforce**
  - The fact that in today's environment most of the work is carried out in a variety of sites and locations can present a physical risk, it can also exacerbate the risks of cybercrime. Bases can often be temporary locations such as onsite cabins and trailers, with workers connecting to business networks and systems via laptops, tablets, and smartphones. Security can often be laxer than it would be in a permanent office, especially if there is a "bring your own device" (BYOD) policy in place, which allows workers to access critical systems on their own devices.

My Company is too Small to be Attacked

WRONG!!

- Small and mid-sized businesses are often prime targets because they have the “it won’t happen to me” approach on cybersecurity, despite the fact that more than **50%** of cyber-attacks are on small businesses.

Law Firms Beware

- The well-publicized June 2017 "Petya" malware attack on DLA Piper shut down the firm's email, phone systems, and operations for three consecutive days, and before being reconnected to the firm's network, all computers and devices had to be inspected and cleared.

- In 2016, the Federal Bureau of Investigation warned of a Ukraine-based Russian hacker known as "Oleras" who solicited other hackers to attack 48 top Chicago law firms, targeting company mergers and acquisitions information through phishing schemes. In the same year, Cravath Swaine & Moore LLP, Weil Gotshal & Manges LLP, and other major law firms were penetrated by unknown hackers possibly looking to profit from confidential or insider information for publicly traded companies.

  - Jeff John Roberts, "Law Firm DLA Piper Reels Under Cyber Attack, Fate of Files Unclear," Fortune (June 29, 2017)

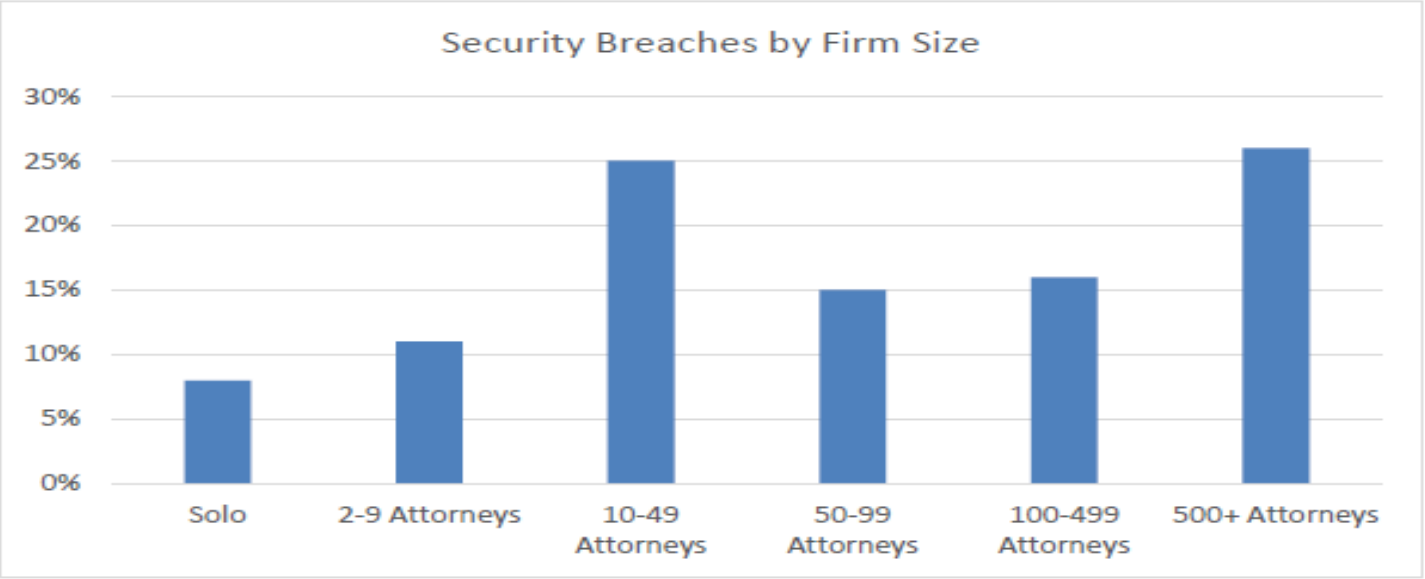
Law Firms Beware

- State-sponsored incursions from China, Russia and Iran continue to hack into the systems of a U.S. firm known for its expertise in intellectual property.

- As law firms and other businesses are relying more on third-party providers, like remote-access applications Citrix and LogMeIn, they have increased their vulnerability….And law firms may be especially appealing targets, not because of who they are, but because of the work they do for their clients. (The Recorded Future report described the targeted firm as “a U.S. law firm specializing in intellectual property law” that “has a dedicated China practice aimed at assisting Chinese companies entering the U.S. market.”)

  - ABA Cybersecurity and he Lawyer’s Standard of, May 22, 2018, https://www.americanbar.org/groups/litigation/committees/commercial-business/articles/2018/spring2018-cybersecurity-and-the-lawyers-standard-of-care/

American Bar Association's 2016 TechReport



What Type of Law Firm Information Is at Risk?

- Sensitive business data: projections, forecasts, M&A
- Intellectual Property
- Social Security and driver's license numbers
- Medical records (PHI, ePHI, PI)
- Financial information: bank/credit card accounts
- Personal information: email addresses, phone numbers and home addresses (if coupled with other information)

Consequences of a Data Breach

- Cost of issuance of breach notice
- Business interruption
- Media failure - damaged data, damaged hardware & cost of repair
- Additional business overhead
- Injury to business associates
- Reputational injury
- Ethical violations
- Ransom
- Civil penalties
- Audit of the firm's data security

Source of Potential Liability/Costs After a Cyber Attack

- FTC Enforcement
- State Attorney General/Other Consumer Protection Agencies Enforcement
- Class Action and Other Lawsuits
- Contractual Liability
- Data Breach Remediation and Related Costs
- Reputational Costs

Damages

- **Cost of remediation**
  - Depending on how many client and vendor files are compromised and how long it takes the company to identify the breach, the costs could mount quickly. And rarely do most companies notice breaches immediately – the average time between breach and identification is 197 days. Plus, remediation takes time – an average 69 days from discovery to containment.

Attorney Ethical & Legal Standards

Duty of Technological Competence

- Mo Rule 4-1.1Competence:

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

- ABA- Comment 15 :

  "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, and engage in continuing study and education."

Duty of Technological Competence

- E-Discovery
- Electronic filing of court documents
- Communicating with clients and third-parties
- Use of social media
- Knowledge of client's technology
- Use of courtroom technology

Duty of Confidentiality

- Rule 4-1.6(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 the client.

Duty of Confidentiality

- Rule 4-1.(6) Comment 15:

  “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 4-1.1, 4-5.1, and 4-5.3. 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.”

Duty of Confidentiality

- Comment 15 to Rule 4.1.6:
  - Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to,
    - 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).

Duty of Confidentiality

- Comment 16 Rule 4.1.6

  “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.”

Non-Lawyer Assistants

- **Rule 4.5.3-Responsibilities Regarding Non-lawyer Assistants**

With respect to a non-lawyer employed or retained by or associated with a lawyer:

(a) a partner, 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 the person's conduct is compatible with the professional obligations of the lawyer;

(b) a lawyer having direct supervisory authority over the non-lawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and

(c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:

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

(2) the lawyer is a partner, or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

Non-Lawyer Assistants

- Rule 4-4.3 Comment 1:

  "Paragraph (a) requires lawyers with managerial authority within a law firm to make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that non-lawyers ***in the firm*** and non-lawyers ***outside*** the firm who work on firm matters act in a way compatible with the professional obligations of the lawyer."

Non-Lawyer Assistants

- Rule 4-5.3 Comment 2 (Inside Firm):

  "Lawyers generally employ assistants in their practice, including secretaries, investigators, law student interns, and paraprofessionals. Such assistants, whether employees or independent contractors, act for the lawyer in rendition of the lawyer's professional services. A lawyer ***must give such assistants appropriate instruction and supervision concerning the ethical aspects of their employment***, particularly regarding the obligation not to disclose information relating to representation of the client, and should be responsible for their work product. The measures employed in supervising non-lawyers should take account of the fact that they do not have legal training and are not subject to professional discipline."

Non-Lawyer Assistants

- Rule 4-5.3 Comment 3 (Outside Firm):

  "When using such services outside the firm, a lawyer must make ***reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations***. The extent of this obligation will depend upon the circumstances, including the education, experience and reputation of the non-lawyer; 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."

Recognize Different Types of Cybercrime

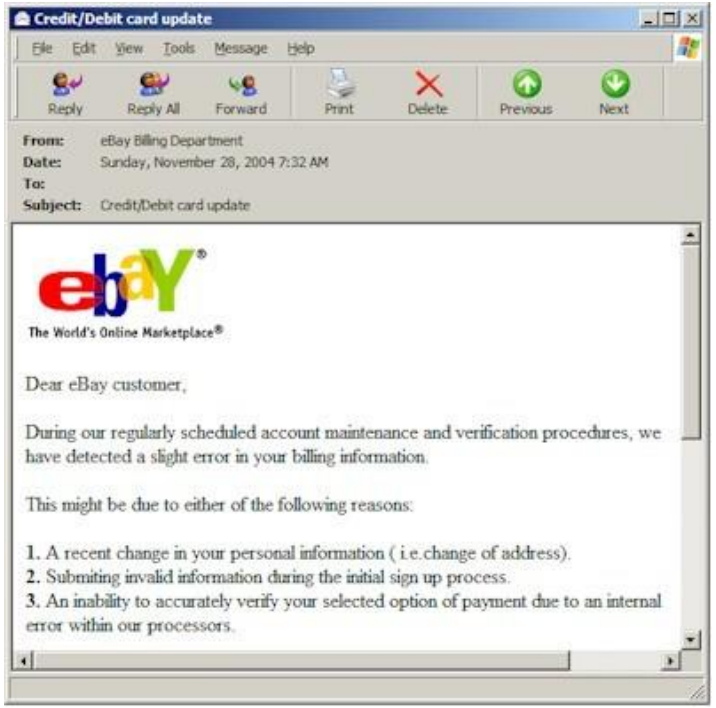
Phishing

- According to Digital Guardian, 91% of cyber attacks start with a phishing email, making it the number one threat to a business.
- **Phishing** is a computer scam that uses SPAM, SPIM & pop-up messages to trick us into disclosing private information (Social Security Number, Credit Cards, banking data, passwords, etc)
  - Often sent from someone that we “trust” or are in some way associated with us
  - Appears to be a legitimate website
  - Embedded in links emails & pop-up message
  - Phishing emails often contain spyware designed to give remote control to our computer or track our online activities
  - **Emails sent from a co-worker but not the same email extension**

Phishing: Counterfeit Email

- **Phishing:**

  A seemingly trustworthy entity asks for sensitive information such as SSN, credit card numbers, login IDs or passwords via e-mail.



Email Account Takeover

- A cybercriminal hacks an email account and searches for emails involving correspondence between the client and their financial institutions. Their goal is to learn about the victim and their habits so they can pose as the victim to steal money.
- Because the cybercriminal has access to our client's email and can impersonate him/her, you are likely to believe the correspondence came from the client. The cybercriminal may provide instructions within the email to transfer funds to a fraudulent account.

Email Account Takeover (etc.)

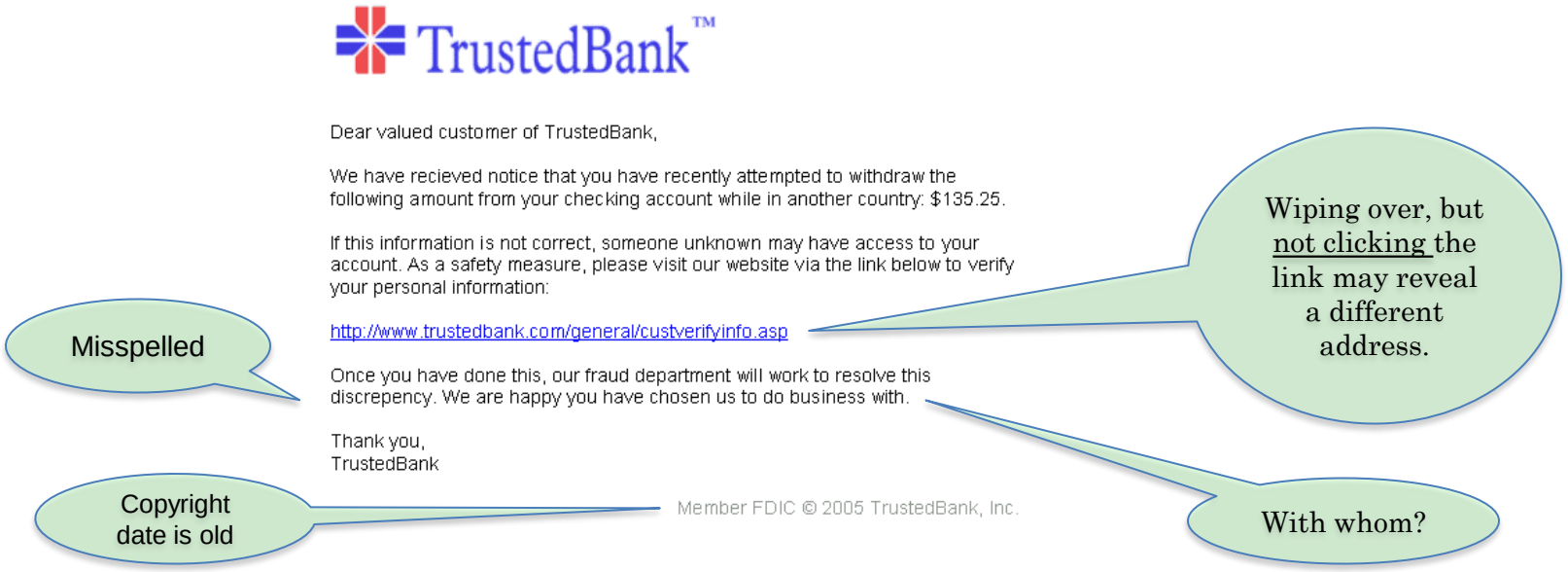
- Without proper verification, the money is transferred and stolen.

In the end, your company may be held responsible for any client/vendor losses if you did not have in place the proper safety measures.

Ransomware

- 400,000 new strains of ransomware are detected daily making the attacks more sophisticated and harder to respond to.

Pharming: Counterfeit Web Pages

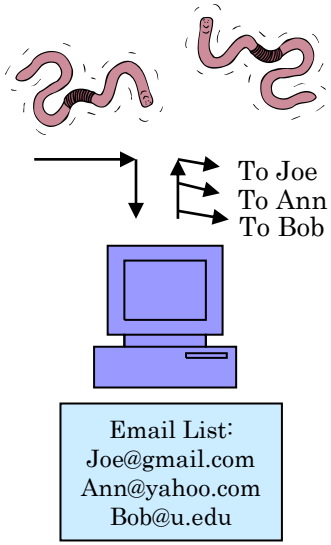


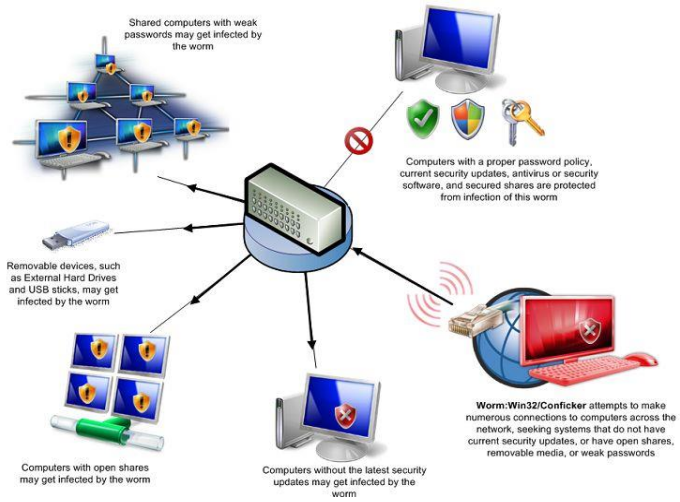
Viruses

- A virus attaches itself to a program, file, or disk.
- When the program is executed, the virus activates and replicates itself.
- The virus may be benign or malignant but executes its payload at some point (often upon contact).
  - Viruses can cause computer crashes and loss of data.
- In order to recover or prevent virus attacks:
  - Avoid potentially unreliable websites/emails.
  - System Restore.
  - Re-install operating system.
  - Use and maintain anti-virus software.

Worms

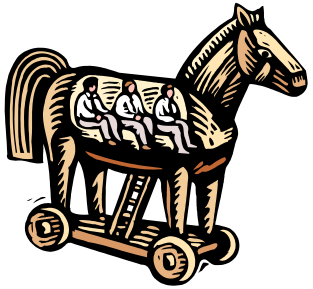
- Independent program that replicates itself and sends copies from computer to computer across network connections. Upon arrival, the worm may be activated to replicate.





Logic Bombs and Trojan Horses

- **Logic Bomb:** Malware logic executes upon certain conditions. The program is often used for otherwise legitimate reasons.
  - Examples:
  - Software which malfunctions if maintenance fee is not paid.
  - Employee triggers a database erase when he is fired.



- **Trojan Horse:** Masquerades as a benign program while quietly destroying data or damaging your system.
  - Download a game: It may be fun but contains hidden code that gathers personal information without your knowledge.

Social Engineering

- Social engineering manipulates people into performing actions or divulging confidential information. Similar to a confidence trick or simple fraud, the term applies to the use of deception to gain information, commit fraud, or access computer systems.

Social Engineering (cont.)

Phone Call: This is John, the System Administrator. What is your password?

In Person: What ethnicity are you? Your mother's maiden name?

Email: ABC Bank has noticed a problem with your account…

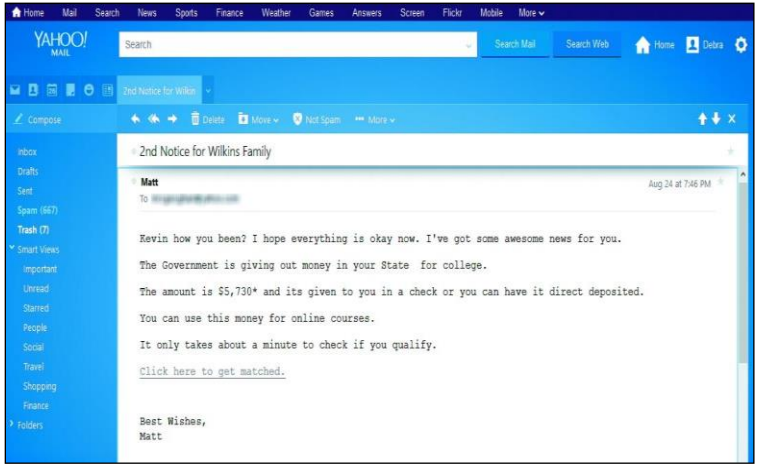
and have some lovely software patches!

I have come to repair your machine…

SANDBERG PHOENIX

Fraud

- Schemes that convince you to give money or property to a person
- Shill bidding is fake bidding to drive up the price of an item



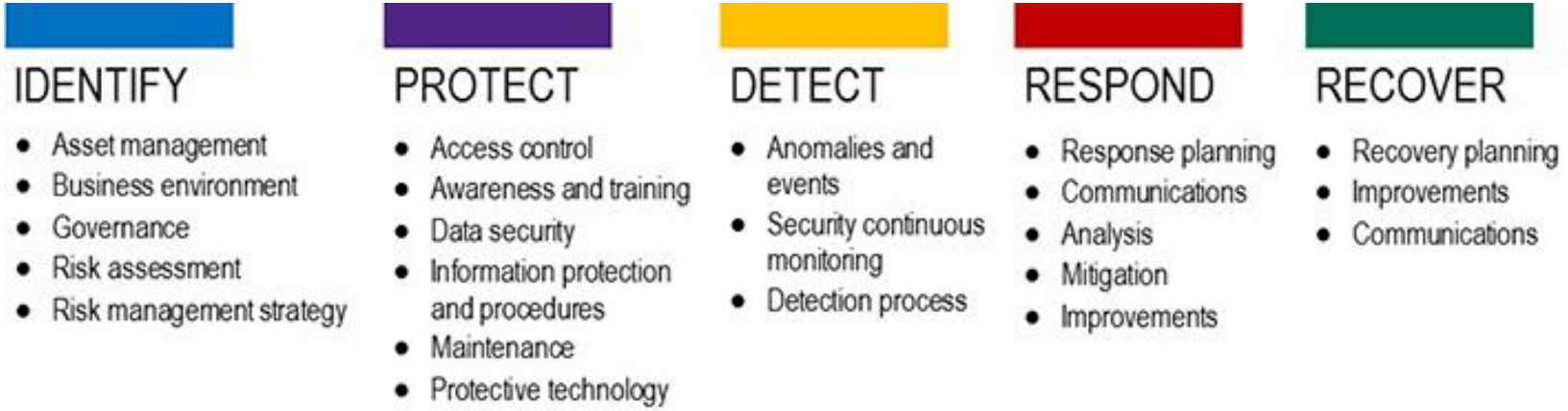
Components of a Cybersecurity Program

NIST Implementation

- **The National Institute of Standards and Technology (NIST) Implementation**
  - NIST developed the initial implementation guidance:
    - ***"Framework for Improving Critical Infrastructure Cybersecurity"***
    - Also known as, "**The Cybersecurity Framework**" or **CSF**

The Cybersecurity Framework

The framework aligns with the common Cybersecurity functions:



Protect –Cybersecurity Program

- Implement clear and Comprehensive Cybersecurity Program
  - Identify an individual within the organization to be responsible for the development and implementation of the organization's security policies and procedures.
  - Regular risk assessments addressing vulnerabilities
  - Audit Controls to monitor activity within computer systems.
  - Incident Response Plan
  - Training

Protect- Software/Hardware Management

- Install , maintain, and update anti-virus and anti-spyware software
- Make sure your firewalls are enabled and updated regularly with security patches
- Secure your company's Wi-Fi network, both at the office and at the jobsite, by encrypting your wireless signal, securing your router with a password and filter MAC addresses of devices so only employees and authorized personnel can access your network.

Protect- Data Controls

- Silo data through servers/accounts
- Tiered password protection: Limit an individual's access privileges to the files, data, and documents necessary to the individual's job function.
- Assigning unique names or identification numbers to each user to track user identity.
- **Establish multi-factor authentication procedures that include passwords, PINs, or fingerprints.**

Protect- Data Controls (cont.)

- Encryption of files containing confidential information.
- Implementing technical solutions to determine whether personal information has been altered or destroyed in an unauthorized manner
- Regularly backup data offsite or with a trusted cloud storage provider.

Protect- Access Controls

- Establishing access controls (for example, visitor logs, photo IDs, and electronic badge systems) that allow people with legitimate business interests to access business facilities but prevent uncontrolled access to sensitive documents or files.
- Implement security measures, such as locked doors, surveillance cameras, alarms, and signs indicating restricted areas.
- Document repairs and modifications to security-related physical components of a system (for example, hardware, doors, and locks).

Protect- Access Controls (cont.)

- information should be shredded or wiped before final disposal.
- Automating workstation security controls (for example, requiring passwords, disk encryption, and automatic screen locks as default settings).
- Conduct periodic evaluations of security policies and procedures.

Internal Controls—H.R.

- Providing security awareness training programs that educate personnel on information security, including topics such General Privacy Principals
  - Types of Cyber-attacks
  - Identifying a cyberattack
  - Avoiding cybersecurity attacks
  - Implement security policies to manage the prevention, detection, and response to information security issues
  - Draft and Implement privacy /confidentiality polices and practices (continued on next slide)

Internal Controls—H.R. (cont.)

- Draft and Implement privacy/confidentiality polices and practices includes:
  - Confidentiality & Trade Secrets
  - E-Mail use and prohibitions
  - Internet use and prohibitions
  - BYOD policies/protecting mobile devices
  - Social Media
  - Strong Passwords

Internal Controls—H.R. (cont.)

- Require each employee to sign a statement/agreement to comply with the company's information security policies and procedures
- Apply appropriate sanctions against personnel failing to comply with information security policies and procedures.
- Implement procedures for quickly terminating access to corporate systems and personal information when an individual's employment ends

Third Party Vendor Management

- The growing use of external service providers presents new and difficult challenges for organizations, especially in the area of information system security.
- Relationships with external service providers can be established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (*i.e.*, through contracts, interagency agreements, lines of business arrangements, service-level agreements), licensing agreements, and/or supply chain exchanges.

Vendor Contracts: Key Tasks

- Identify actual/full scope of **dependencies on third-party IT service providers**, such as data center operators and cloud services.
- Ensure contracts are reviewed by knowledgeable personnel.
  - Ensure contract reviewers are adequately trained regarding standards and risk areas.
- Design standards for assessing vendor risk:
  - Checklists for business team when considering vendors
  - "Disclosure" form for vendors to complete prior to review of service agreement
- Devise reasonable process for review of information collected.

Vendor Contracts

- Specific data security/protection issues to review include:
  - Security and data protection expectations
  - Substantive notification obligations (e.g., information to be provided and shared by vendor)
  - Coordination of security incident response
  - Sharing of information regarding/performance of ongoing risk assessments and audits
  - Vendor data storage and data destruction practices
  - Level of customer data segregation
  - Termination/ unwinding/ transition requirements
  - Indemnification, limitation of liability, and insurance provisions

Who You Gonna Call?

- Data breach coach (**Attorney**)
- **Timing is critical**
- Forensic support
- Public relations
- Insurance company
- IT Support
    - Don’t wipe the system clean;
    - Preserve all evidence for further investigation
    - If overwriting data, make sure to create a backup copy

Stay Informed - Follow Me……

- **LinkedIn:**
  https://www.linkedin.com/in/tschowalter

- **Twitter:**
  TimmSchowalter@tschowalter

- **Sandberg Phoenix: Employer's Blog**
  http://www.employerlawblog.com/

THANK YOU.

Timm W. Schowalter, CIPP/US
600 Washington Avenue, 15th Floor
St. Louis, MO 63101
314.425.4910- Direct
314.609.7552- Mobile
tschowalter@sandbergphoenix.com
https://www.linkedin.com/in/tschowa