Modern Day Cyber Attacks

- Southwest Airlines – Pink Virus
- https://www.youtube.com/watch?v=RXW7dph8U-Q
- By 2021, 31 Percent of Companies Had Experienced a Data Breach
- With new cyber threats emerging daily both internally and externally, business leaders are juggling a full slate of concerns and challenges. Threats such as payment integrity (59%) and malware (58%) are the most cited concerns, with risk management (57%) cited as the biggest challenge leaders say their systems face. Companies also fear internal threats, with hospitality companies most frequently citing human error (86%) and lack of employee education (81%) as negatively impacting cybersecurity systems.

Ethical Duties

- As outlined in ABA Model Rule 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 a client.”
- This mandate extends beyond the protection of physical files to include digital data such as emails, electronic documents, and metadata. The rule emphasizes that these efforts must be “reasonable”—a flexible, fact-specific standard that depends on the circumstances, including the sensitivity of the client information, the level of risk, and prevailing technological norms. Rather than prescribing specific procedures, the rule expects lawyers to implement precautionary measures appropriate to their practice. This ethical obligation reinforces a lawyer’s broader duty to protect client confidentiality in the digital age.

Ethical Duties

- Ethical Duties to Clients
- Under Model Rule 1.4, lawyers must keep clients informed about significant developments in their representation, including data breaches that compromise confidential information.
- If a breach is discovered, firms must notify affected clients promptly, explaining what happened (*e.g.*, unauthorized access or exfiltration), what was affected (*e.g.*, categories of data, types of filings), and what the firm is doing (*e.g.*, containment measures, investigations, remediation steps).
- Failing to communicate transparently can violate the duties of competence, confidentiality, and communication, and may expose the firm to disciplinary or civil consequences.
- **Former Clients: A Best-Practice Imperative**
- For former clients, the Model Rules do not impose the same black-letter duty to notify. While Rule 1.9(c) prohibits revealing former clients' confidential information, it doesn't mandate breach notifications.
- However, ABA Formal Opinion 483 emphasizes that notification is often advisable. Former-client files may still contain sensitive personal or business information, and notice may likely be required by state and federal data breach laws, retention agreements or engagement letters, or common law duties of care.

Ethical Duties

- Sealed and Privileged Documents: Heightened Stakes
- When leaked files include sealed court filings or privileged materials, the breach implicates not only ethical obligations but also the integrity of ongoing litigation.
- **Continuing Confidentiality**
- Even when confidential materials surface publicly, courts continue to enforce sealing orders and protective designations. Protective orders often provide that inadvertent disclosure does not affect a document's confidential status or waive protections, and courts have upheld such provisions. Ramirez v. Clark Nissan, LLC, No. CV 25-32-M-KLD, 2025 WL 1755222, at *5 (D. Mont. June 25, 2025).
- Federal Rules of Civil Procedure 5.2(d) and 26(c) empower courts to keep filings under seal and control how sensitive information is used. Lawyers for each party subject to a sealing or protective order must continue treating these documents as confidential, even if hackers post them on the dark web.

Ethical Duties

- Obligations to the Court and Opposing Counsel
- When court-sealed or privileged documents are compromised, attorneys may have duties under Model Rules 1.4 (communication) and 3.3 (candor to the tribunal) to notify the court and, where appropriate, opposing counsel.
- Practical Takeaways for Firms
- Given these challenges, law firms should take proactive steps to minimize legal, ethical, and operational risks when breaches occur.
- Prepare in advance.
- Act quickly and transparently.
- Preserve privilege.
- Engage counsel and cybersecurity technical experts early.
- Monitor the dark web.
- A breach involving sealed or privileged client materials is among the most challenging scenarios a law firm can face. While courts have limited ability to claw back leaked documents from the dark web, ethical obligations remain clear: notify clients, preserve confidentiality, and work with courts to reinforce protective orders.

What is a Cyber Attack

- When there is an unauthorized system/network access by a third party, we term it as a cyber attack. The person who carries out a cyberattack is termed as a hacker/attacker.
- Cyber-attacks have several negative effects. When an attack is carried out, it can lead to data breaches, resulting in data loss or data manipulation. Organizations incur financial losses, customer trust gets hampered, and there is reputational damage. To put a curb on cyberattacks, we implement cybersecurity. Cybersecurity is the method of safeguarding networks, computer systems, and their components from unauthorized digital access.

Types of Data Breaches

- **DoS and DDoS Attacks -** A denial-of-service (DoS) attack is designed to overwhelm the resources of a system to the point where it is unable to reply to legitimate service requests.
- **MITM Attacks -** Man-in-the-middle (MITM) types of cyber attacks refer to breaches in cybersecurity that make it possible for an attacker to eavesdrop on the data sent back and forth between two people, networks, or computers.
- **Phishing Attacks -** A phishing attack occurs when a malicious actor sends emails that seem to be coming from trusted, legitimate sources in an attempt to grab sensitive information from the target.

Types of Data Breaches

- **Whale-phishing Attacks -** A whale-phishing attack is so-named because it goes after the “big fish” or whales of an organization, which typically include those in the C-suite or others in charge of the organization.
- **Spear-phishing Attacks -** Spear phishing refers to a specific type of targeted phishing attack. The attacker takes the time to research their intended targets and then write messages the target is likely to find personally relevant.
- **Ransomware -** With ransomware, the victim’s system is held hostage until they agree to pay a ransom to the attacker.

Types of Data Breaches

- **Password Attack -** Passwords are the access verification tool of choice for most people, so figuring out a target's password is an attractive proposition for a hacker.
- **SQL Injection Attack -** Structured Query Language (SQL) injection is a common method of taking advantage of websites that depend on databases to serve their users. Clients are computers that get information from servers, and an SQL attack uses an SQL query sent from the client to a database on the server. The command is inserted, or "injected", into a data plane in place of something else that normally goes there, such as a password or login. The server that holds the database then runs the command and the system is penetrated.

Types of Data Breaches

- **URL Interpretation -** With URL interpretation, attackers alter and fabricate certain URL addresses and use them to gain access to the target's personal and professional data. This kind of attack is also referred to as URL poisoning. The name "URL interpretation" comes from the fact that the attacker knows the order in which a web-page's URL information needs to be entered. The attacker then "interprets" this syntax, using it to figure out how to get into areas they do not have access to.
- **DNS Spoofing -** With Domain Name System (DNS) spoofing, a hacker alters DNS records to send traffic to a fake or "spoofed" website. Once on the fraudulent site, the victim may enter sensitive information that can be used or sold by the hacker. The hacker may also construct a poor-quality site with derogatory or inflammatory content to make a competitor company look bad.

Types of Data Breaches

- **Session Hijacking -** The attacker takes over a session between a client and the server. The computer being used in the attack substitutes its Internet Protocol (IP) address for that of the client computer, and the server continues the session without suspecting it is communicating with the attacker instead of the client. This kind of attack is effective because the server uses the client's IP address to verify its identity. If the attacker's IP address is inserted partway through the session, the server may not suspect a breach because it is already engaged in a trusted connection.
- **Brute force attack -** The attacker simply tries to guess the login credentials of someone with access to the target system, often using bots to do so.

Types of Data Breaches

- **Web Attacks -** Web attacks refer to threats that target vulnerabilities in web-based applications.
- **Insider Threats -** Sometimes, the most dangerous actors come from within an organization.
- **Trojan Horses -** A Trojan horse attack uses a malicious program that is hidden inside a seemingly legitimate one. When the user executes the presumably innocent program, the malware inside the Trojan can be used to open a backdoor into the system through which hackers can penetrate the computer or network.

Types of Data Breaches

- **Drive-by Attacks -** In a drive-by attack, a hacker embeds malicious code into an insecure website. When a user visits the site, the script is automatically executed on their computer, infecting it. The designation “drive by” comes from the fact that the victim only has to “drive by” the site by visiting it to get infected. There is no need to click on anything on the site or enter any information.
- **XSS Attacks -** With XSS, or cross-site scripting, the attacker transmits malicious scripts using clickable content that gets sent to the target’s browser. When the victim clicks on the content, the script is executed. Because the user has already logged into a web application’s session, what they enter is seen as legitimate by the web application. However, the script executed has been altered by the attacker, resulting in an unintended action being taken by the “user.”

Types of Data Breaches

- **Eavesdropping Attacks -** Eavesdropping attacks involve the bad actor intercepting traffic as it is sent through the network. In this way, an attacker can collect usernames, passwords, and other confidential information like credit cards. Eavesdropping can be active or passive.
- **Birthday Attack -**In a birthday attack, an attacker abuses a security feature: hash algorithms, which are used to verify the authenticity of messages. The hash algorithm is a digital signature, and the receiver of the message checks it before accepting the message as authentic. If a hacker can create a hash that is identical to what the sender has appended to their message, the hacker can simply replace the sender's message with their own. The receiving device will accept it because it has the right hash.

Types of Data Breaches

- **Malware Attack -** Malware is a general term for malicious software, hence the "mal" at the start of the word. Malware infects a computer and changes how it functions, destroys data, or spies on the user or network traffic as it passes through. Malware can either spread from one device to another or remain in place, only impacting its host device.

Recent Corporate Cyber Attacks

- More than 4,100 publicly disclosed data breaches occurred in 2022 equating to approximately 22 billion records being exposed.
- The latest increase comes on the heels of 2021's 68 percent increase in breaches over 2020, which beat the previous record, set in 2017, by 23 percent.

Recent Law Firm Cyber Attacks

- **Mossack Fonseca**
- In April 2016, journalists from German newspaper *Süddeutsche Zeitung*, Bastian Obermayer and Frederik Obermaier, **received approximately 11.5 million documents, later known as the Panama Papers,** belonging to the Panamanian law firm Mossack Fonseca.
- Among other forms of questionable activity, the documents detailed the widespread use of shell companies and complex transactions as means of committing tax fraud.
- While some claim that the 11.5 million records that ended up in the hands of the world press came from a leak from an anonymous insider, Mossack Fonseca claims that the firm **experienced a hack through an unauthorized breach of the e-mail server**.

Recent Law Firm Cyber Attacks

- **Appleby -** In 2016, Appleby, an offshore law firm located in Bermuda, experienced a cyber attack. News of the attack surfaced in 2017, when the hack attracted interest from the **ICIJ**. Known as the Paradise Papers, the law firm's breached records included **13.4 million files**. According to ***The Guardian***, a total of 96 media companies and 381 journalists reviewed the documents.
- **DLA Piper -** In June 2017, DLA Piper **suffered a ransomware attack** that first struck its Ukrainian offices during an upgrade of its payroll software. The attack involved malware known as NotPetya. The firm cited its "flat network structure" as a reason the infection spread so quickly. As a result of the attack, DLA Piper employees around the world could not use the firm's telephones or email system, and some struggled to access certain documents.

Recent Law Firm Cyber Attacks

- **Cravath Swaine & Moore and Weil Gotshal & Manges**
- To engage in **insider trading** and gather **confidential information** regarding pending mergers and acquisitions, three Chinese nationals targeted the law firms of Cravath Swaine & Moore and Weil Gotshal & Manges.
- According to the **U.S. government**, Iat Hong, Bo Zheng, and Chin Hung earned over $4 million in profits while trading on information they stole from the law firms. To gather such information, the perpetrators used their unauthorized access to **read emails belonging to partners** at both firms about pending transactions involving public companies.

Recent Law Firm Cyber Attacks

- **Moses Afonso Ryan Ltd.**
- The law firm Moses Afonso Ryan Ltd. had its critical files locked down for three months due to a **ransomware attack** in 2016. Specifically, the firm's billing system and documents were frozen, so they could not be paid by clients and key financial information could not be accessed.
- After the system was disabled, the law firm was forced to negotiate a ransom, which was paid in Bitcoin. In total, nearly $700,000 was lost in client billings, as well as the undisclosed ransom cost.

Recent Law Firm Cyber Attacks

- **GozNym Malware**
- In 2016, two undisclosed law firms **experienced attacks** involving malware known as GozNym, which criminals used to covertly steal banking login and password information.
- To trick law firm personnel into providing their banking credentials, the criminals sent a phishing email that directed the recipient to web pages designed to look like their bank's website. The scheme used keystroke logging, which recorded the keys entered when victims visited the fake bank site. It then sent that information surreptitiously to the cybercriminals.
- The attack targeted bank accounts at Bank of America and Brookline Bank. Once the criminals gained access to the law firm's bank accounts, they transferred funds to other U.S. and foreign bank accounts they controlled.

Recent Law Firm Cyber Attacks

- **Jenner & Block and Proskauer Rose**
- Jenner & Block admitted that in response to a request that appeared legitimate, the firm had "mistakenly transmitted" **employee W-2 forms** to "an unauthorized recipient" in 2017. The phishing scheme resulted in the inadvertent sharing of personal information of 859 individuals, including their Social Security numbers and salaries.
- Proskauer Rose experienced a **similar attack**, involving what appeared to be a routine request from a senior executive within the firm. In this case, the firm lost control of more than 1,500 W-2s.

Recent Law Firm Cyber Attacks

- **Oleras**
- In 2016, a cybercriminal using the alias Oleras allegedly **targeted 50 law firms** to steal confidential information to facilitate insider trading. The hacker attempted to hire accomplices via the criminal underground to help breach the law firms' defenses and then use keywords to search for pending deals
- To entice others to join, Oleras advertised a plan that detailed the names, email addresses, and social media accounts of the law firm employees to be targeted.
- One of the phishing emails associated with the scheme appeared to originate from a business journal asking to run a profile of the recipient about their work in mergers and acquisitions.

Recent Law Firm Cyber Attacks

- **Fragomen, Del Rey, Bernsen & Loewy**
- Fragomen, Del Rey, Bernsen & Loewy confirmed it was the victim of a data breach on September 24, 2020. The law firm was heavily involved with Google, and the **data breach** involved personal information for both current and former Google employees.
- An unauthorized third party was able to access at least one file that contained personal information on **several Google employees**, such as driver's license numbers and other personally identifiable information. This placed certain Google employees at risk for identity theft or other forms of fraud.

Recent Law Firm Cyber Attacks

- **Grubman Shire Meiselas & Sacks**
- In May 2020, Grubman Shire Meiselas & Sacks, which offers legal services to the entertainment and media industries, acknowledged having experienced a ransomware attack. To exert pressure, the hackers leaked information involving Lady Gaga, who is a client of the law firm. They also threatened to release information involving other celebrities.
- The attackers asked for a **ransom payment of $42 million** to prevent the release of the documents to the public. The perpetrators originally asked for $21 million, then doubled their payment demand.
- According to news outlets, the criminals behind the attack **reported having received $365,000** from the firm. They threatened to release additional data, much of which involves celebrities, if they didn't receive payment in full.

Recent Law Firm Cyber Attacks

- **Campbell Conroy & O'Neil P.C.**
- The law firm Campbell Conroy & O'Neil P.C. was subject to a data breach on February 27, 2021. The firm became aware of **unusual activity**, then conducted an investigation and discovered it had unwittingly been a ransomware victim.
- The ransomware attack prevented Campbell Conroy & O'Neil P.C. from accessing critical files in its system. Although the full extent and impact of the attack have not yet been determined, Campbell Conroy & O'Neil P.C. speculates that the attacker had access to clients' names, Social Security numbers, driver's license numbers, dates of birth, and other key identifying facts.

Top Hacks of 2024

- Top 10 Biggest Cyber Attacks, Data Breaches and Ransomware Attacks of 2024

1. Change Healthcare Ransomware Attack - A major processor of U.S. medical claims, fell victim to a ransomware attack. The attackers infiltrated the company's systems. They exfiltrated sensitive data and deployed ransomware that crippled operations.
2. Snowflake Ransomware Attack - The breach was orchestrated by hackers who exploited compromised credentials of a Snowflake employee account. This unauthorized access led to the exfiltration of vast amounts of sensitive data. Billions of call records from AT&T and personal information from Ticketmaster and Santander Bank customers was stolen. The attackers employed extortion tactics, demanding ransoms ranging from $300,000 to $5 million from affected companies to prevent the public release of the stolen data.
3. UK MoD Data Breach - the UK's Ministry of Defence (MoD) experienced a significant data breach when a contractor-operated payroll system was compromised by a cyber attack. This system contained personal information—including names, bank details, and, in some cases, home addresses—of approximately 270,000 current and former UK military personnel.
4. Ascension Ransomware Attack - The leading U.S. healthcare system experienced a crippling ransomware attack in May 2024. As is usually the case with attacks on the healthcare industry, this one too disrupted operations across multiple states. The attack made the MyChart electronic health record (EHR) system inaccessible.
5. MediSecure Data Breach - MediSecure, a prominent electronic prescription service provider, suffered a significant ransomware attack. This resulted in the theft of personal and health information of approximately 12.9 million individuals. The compromised data included names, dates of birth, addresses, phone numbers, Medicare numbers, prescription details, and reasons for medication.

Top Hacks of 2024

6. Synnovis-NHS UK Ransomware Attack - On June 4, 2024, the NHS in the UK declared a ‘critical incident’. Its pathology services provider, Synnovis, had become victim of a ransomware attack by Qilin Ransomware Gang. What followed was utter chaos and a direct impact on human life and wellbeing.
7. CrowdStrike-Microsoft Outage - On July 19, 2024, a faulty update from CrowdStrike's Falcon Sensor software caused widespread disruptions for Microsoft Windows users globally.
8. TfL Cyber Attack - The attack had allegedly compromised the personal data of approximately 5,000 customers, including sensitive information such as home addresses and banking details. A 17-year-old individual was identified as the perpetrator of the attack and was subsequently released on bail.
9. Ivanti Mass Zero-Day Exploits - Initially exploited by a suspected Chinese state-sponsored group known as UNC5221, these vulnerabilities allowed attackers to deploy custom malware, including web shells and credential harvesters, compromising numerous organisations worldwide.
10. Salt Typhoon Attacks - Alleged Chinese-backed state hackers, Salt Typhoon, intensified their cyber espionage efforts targetting major U.S. telecommunications companies, including AT&T, Verizon, T-Mobile, and Lumen Technologies in December 2024.

Large Business Cyber Attacks

- **Target -** A 2013 cyber attack involving Target exposed 41 million payment cards and contact information for approximately 70 million customers. The attack focused on a third-party vendor via a **spear-phishing attack designed to steal user credentials** . Once threat actors compromised Target's network, they installed malware to seize customer data over the course of two months.
- **Home Depot – In 2014, u**sing a third-party vendor's login credentials, **attackers gained access to Home Depot's network** , then deployed malware designed to infect the retail giant's POS system and gather customer payment information. Between **April and September 2014** , the breach impacted 52 million customers.

Large Business Cyber Attacks

- **Neiman Marcus Group -**In September 2021, upscale retailer **Neiman Marcus notified 4.6 million customers** that a hacker had compromised online accounts in May 2020, gaining access to personal data such as usernames and passwords, customer names, contact information, credit card numbers, as well as expiration dates and virtual card numbers.
- **eBay -**Using compromised employee credentials, **attackers accessed approximately 145 million eBay accounts** in 2014. The online auction company acknowledged that attackers managed to copy much of the data tied to the accounts, including email addresses, birth dates, and mailing addresses.

Large Business Cyber Attacks

- **CVS Health -** A misconfigured database with **204 gigabytes and 1.1 billion records**, including customer email addresses, user IDs, and customer online search information gathered from CVS Health and CVS.com, was found publicly available and unsecured in 2021 by cybersecurity researchers.
- **Saks Fifth Avenue/Lord & Taylor -** A 2018 malware attack against these Hudson Bay Corporation retailers' POS resulted in the theft of more than **five million credit and debit card numbers** . The attackers subsequently attempted to **sell the stolen data via the dark web** .

Large Business Cyber Attacks

- **Under Armour -** Usernames, email addresses, and hashed passwords for approximately **150 million users of Under Armour's MyFitnessPass** were compromised when an unauthorized third party accessed the data in February 2018. The company discovered the breach on March 25, 2018.
- **Bonobos -** It's not only a company's own network and systems that risk exposing sensitive data, but also those of its partners, especially when operating in the cloud. In January 2021, a **70-gigabyte SQL backup file** belonging to Bonobos, the apparel subsidiary of Walmart, was stolen from a third-party cloud provider and posted in a hacker forum. The file contained 7 million shipping addresses, 1.8 million registered customer accounts, and 3.5 million partial credit card records.

Large Business Cyber Attacks

- **Forever 21 -** In 2018, over the course of seven months, **attackers accessed payment card data of Forever 21 customers** . After obtaining network access, the threat actors deployed malware to gather credit card data from the fashion retailer's point-of-sale (POS) system. Forever 21 admitted to not previously encrypting some of its POS devices.
- **Guess -** Between February 2 and February 23, 2021, denim and apparel giant Guess experienced a ransomware attack that included the **theft of customer data** . The compromised information included Social Security numbers, driver's license numbers, passport numbers, and financial account numbers.

Small Business Cyber Attacks

- When it comes to data security, a restaurant's defense is only as good as the weakest link in the system. Large franchised restaurant chains offer many points of entry for would-be hackers. Plus, their fractured security systems could differ across regions, by individual franchisees or even store-by-store.
- When you have lots of employees and outlets, employees who don't have a lot of experience in security and hundreds of devices, a hacker just needs to get into one. The attackers are looking for the weakest link.

Small Business Cyber Attacks

- Because of the unique structure of the franchisee model, quick-serve companies need to build in tangible rewards for partners who maintain formidable security protections.
- It’s in the best interest of franchisees and franchisors to double down on security because data breaches have consequences for individual stores and their global brands.

Fast Food Cyber Attacks

- McDonald's was breached by hackers in 2021, with data theft occurring in three separate countries. Wendy's was another victim and its breaches back in 2015 and 2016. One of the largest fast food chain data breaches may have been the related attacks that involved multiple franchises – including Arby's, Chili's, and Chipotle.
- Customers of the popular chicken chain Chick-fil-A could be the latest victims of hackers, where the fast food brand is looking into possible mobile app breaches that may have exposed customers' private information.

Sophisticated Cyber Attacks

- Since at least 2015, FIN7—also known as Carbanak Group and the Navigator Group—used a malware campaign to attack U.S. companies in the restaurant, gambling, and hospitality industries. The group crafted email messages that appeared genuine to employees and accompanied those messages with phone calls to further legitimize the email. Once a file attached to the fraudulent email was opened and activated, FIN7 used its malware to steal payment card data from the business' customers.

Sophisticated Cyber Attacks

- CRM platform “Seven Rooms”, recently suffered a serious data breach, one they only acknowledged after their data was found being sold on the dark web.
- Seven Rooms is a restaurant customer management platform used by international restaurant chains and hospitality service providers. Notable clients include MGM Resorts, Mandarin Oriental, and Black Sheep Restaurants.
- Seven Rooms did confirm that the data being sold was theirs, and it had been caused by unauthorized access into the systems of one of their vendors. This data breach is notable, as Seven Rooms confirmed that their systems have not been breached, but rather an organization in their supply chain has flawed cyber security in place.

Sophisticated Cyber Attacks

- Payment card details from customers of more than 300 restaurants have been stolen in two web-skimming campaigns targeting three online ordering platforms.
- Web-skimmers, or Magecart malware, are typically JavaScript code that collects credit card data when online shoppers type it on the checkout page.
- Magecart campaigns were discovered, injecting malicious code into the online ordering portals of MenuDrive, Harbortouch, and InTouchPOS.
- As a result, 50,000 payment cards were stolen and have already been offered for sale on various marketplaces on the dark web.

Cyber Attacks on Federal Courts

- The federal judiciary's system known as PACER CM/ECF – short for Public Access to Court Electronic Records and Case Management/Electronic Case Files – it was thought that the system was compromised during the massive U.S. cybersecurity breach in 2020 that targeted SolarWinds Orion products, as the software had utilized the Orion IT tool before the breach.
- Both government and private networks were compromised in the hack "beginning in at least March 2020," the Cybersecurity and Infrastructure Security Agency said in an alert, which acknowledged that there is still much to learn about the difficult-to-detect attack.

Cyber Attacks on Federal Courts

- January 6, 2021 Announcement - In December 2020, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency issued an emergency directive regarding "a known compromise involving SolarWinds Orion products that are currently being exploited by malicious actors." The Administrative Office of the U.S. Courts (AO) immediately notified courts of this development and in response, the Judiciary has suspended all national and local use of this IT network monitoring and management tool.
- The AO is working with the Department of Homeland Security on a security audit relating to vulnerabilities in the Judiciary's Case Management/Electronic Case Files system (CM/ECF) that greatly risk compromising highly sensitive non-public documents stored on CM/ECF, particularly sealed filings. An apparent compromise of the confidentiality of the CM/ECF system due to these discovered vulnerabilities currently is under investigation. Due to the nature of the attacks, the review of this matter and its impact is ongoing.

Cyber Attacks on Federal Courts

- Under the new procedures announced, highly sensitive court documents (HSDs) filed with federal courts will be accepted for filing in paper form or via a secure electronic device, such as a thumb drive, and stored in a secure stand-alone computer system. These sealed HSDs will not be uploaded to CM/ECF. This new practice will not change current policies regarding public access to court records, since sealed records are confidential and currently are not available to the public.
- On July 28, 2022, the chairman of the House Judiciary Committee, Congressman Jerry Nadler, disclosed for the first time that actually three hostile foreign actors breached the federal courts document management system via “an incredibly significant and sophisticated” cyberattack more than 18 months ago, the chairman of the House Judiciary Committee.

Cyber Attacks on Federal Courts

- Representative Nadler said that his committee learned in March 2022 of “the startling breadth and scope of the courts’ documents management system security failure.” He added the hack had a “disturbing impact” on both pending civil and criminal litigation and national security.
- Nadler said the breach wasn’t related to a cyber-espionage campaign that was revealed in December 2020 and affected nine federal agencies -- including the Department of Justice -- and about 100 businesses. US officials blamed that attack, which partially relied on installing malicious code in updates for software made by SolarWinds Corp., on Russian state-sponsored hackers.

Cyber Attacks on Federal Courts

- Senator Ron Wyden said the federal judiciary has yet to publicly explain what happened and has refused multiple requests to provide unclassified briefings to Congress. He accused the federal judiciary of concealing what happened and demanded more information.
- Wyden said the judiciary's decentralized court system is flawed and has opposed congressional efforts to modernize, creating unmanageable security risks. He urged the federal judiciary to adopt a set of mandatory cybersecurity standards and audits that all federal courts would be required to follow.

Cyber Attacks on Federal Courts

- David Sellers, a spokesperson for the Administrative Office of the U.S. Courts, pointed to the January 2021 statement in noting that “the Judiciary faces a significant threat to our electronic case management system.” Sellers said that U.S. Courts had taken steps since then to protect its networks, including through working with the Department of Homeland Security to address vulnerabilities, and establishing the Judiciary IT Security Task Force to make recommendations for ways to strengthen security further.
- “Cybersecurity is one of our highest priorities,” Sellers said. “We continue to work closely with our executive branch partners, take precautions to protect our systems, and engage in the modernization of the existing CM/ECF system.”

Cyber Attacks on Federal Courts

- The federal judiciary will receive a big boost in spending for court security and cybersecurity as part of the $1.66 trillion government spending bill that passed the U.S. Congress in December 2022. The $8.46 billion also includes $106 million for cybersecurity and information technology modernization projects within the federal court system.
- The judiciary sought the funding citing the need to guard against cyberattacks on its aging, vulnerable computer systems.

Response to Cyber Attacks

- Engage a data forensics investigation team
- Determine the type of attack
- Contain the threat
- Assess and repair the damage
- Notify the proper authorities
- Communicate with affected parties
- Learn from the experience

Cyber Security

- Security Awareness Training
- Phishing Training & Tools
- Security Assessments
- Compliance & Advanced Monitoring
- Cyber Liability Insurance Management
- Penetration Testing & Threat Hunting
- Security Information and Event Management as-a-Service
- Password Protection

Cyber Security – ISO Certification

- ISO/IEC 27001 is an Information security management standard that structures how organizations should manage risk associated with information security threats; including policies, procedures and staff training.
- ISO 27001 is the internationally recognized best practice framework for an ISMS and one of the most popular information security management standards worldwide.

Cyber Security – ISO Certification

- The International Standard Organization (ISO) created a comprehensive set of guidelines called the ISO/IEC 27001:2013 (a.k.a. ISO 27001). These standards help global businesses establish, organize, implement, monitor and maintain their information security management systems.
- Unlike standards such as GDPR or HIPAA that primarily focus on one type of data (customer information or personal health privacy), the ISO 27001 encompasses all kinds of business data that is stored electronically, in hard copies (physical copies like paper and post) or even with third-party suppliers.
- The ISO 27001 certification is applicable to businesses of all sizes and ensures that organizations are identifying and managing risks effectively, consistently and measurably.

Cyber Security - ISO Certification

- Organizations can enjoy a number of benefits from being ISO 27001 certified.
- 1. Certification helps to identify security gaps and vulnerabilities, protect data, avoid costly security breaches and improve cyber resilience.
- 2. Certified organizations demonstrate that they take information security extremely seriously and have a structured approach towards planning, implementing and maintaining ISMS.
- 3. Certification serves as a seal of approval (or proof) that an independent third-party certified body is routinely assessing the security posture of the business and finds it to be effective.
- 4. It boosts confidence, demonstrates credibility and enhances brand reputation in the eyes of customers, partners and other stakeholders that their information is in safe hands.
- 5. It helps comply with other frameworks, standards and legislation such as GDPR, HIPAA, the NIST SP 800 series, the NIS Directive and others while helping to avoid costly fines and penalties.

Cyber Security – ISO Certification

- An ISO 27001 audit involves a competent and objective auditor reviewing:
- The ISMS or elements of it and testing that it meets the standard's requirements,
- The organization's own information requirements, objectives for the ISMS,
- That the policies, processes, and other controls are practical and efficient.
- In addition to the overall compliance and effectiveness of the ISMS, as ISO 27001 is designed to enable an organization to manage it's information security risks to a tolerable level, it will be necessary to check that the implemented controls do indeed reduce risk to a point where the risk owner(s) are happy to tolerate the residual risk.

- Poor coding practices
- Poor configurations
- Poor maintenance
- Apathy vs automation
- Lack of user training


Only human…

- **Internal Network**
  - Weak and default passwords
  - Lack Isolation
  - WIFI keys not rotated
  - Lack Audits
  - Lack onboard/offboard processes

- **Data partners**
  - Food delivery Services
  - Vendors
  - POS system
  - Partner Business Email Compromise
  - Owner/Executive Impersonation
  - Rewards programs
  - Reservation systems
  - Lack 3rd Party Risk assessments
  - Lack awareness of data residency, flow and spread

restech

- **Cloud services**
  - Payroll
  - CPA
  - Email
  - Marketing
  - Etc…

- **Loss of business** due to inadequate security and business controls
- **Loss of insurability** due to carriers experiencing high loss rates.

Defensibility is the idea that you are doing well known actions to prepare for well known threats.

The three main interested parties:

1) Your Clients
2) Your insurance carrier
3) Cyber Thieves

restech

Insurance companies are now dictating very high standards before they issue Cyber Security Insurance coverage.

American Property Casualty Insurance Association 2022

Your client are more frequently sending out security questionnaires to cover their compliance efforts.

restech

All of this equates to very well-known practices that insurance carriers & clients are expecting from their vendors or data partners.

A company's credibility is now graded by their data security. a.k.a Defensibility.

restech

- **Protect Users** – *users' identity is #1 target.*
  - Strong Passphrases
  - Multi Factor Authentication
  - Password Vaults
  - Anti-Phishing
  - Cyber Defense Training

restech

- **Protect Data** – *thieves #1 objective, and your #1 responsibility*
  - Asset Inventory - Know where all the data lives
  - Access Controls- Know who can access data/systems and how
  - Administrative Controls – Who is granting and validating access?
  - Anomaly Detection – known baseline vs deviations
  - Backup and Recovery– Are systems in place to recover data and how long will that take? Tested?

- **Protect Network** – *can you detect a breach?*
  - Harden systems and devices
  - Limit access
  - Capture and Analyze Event Logs
  - Know and test your systems vulnerabilities (including people)

- **Executives are at greatest risk**
  - Resistance to security controls
  - Hold sensitive information
  - Do not manage data sprawl or asset disposal
  - Have the most to lose
  - Unqualified assumptions

C-level executives were twelve times more likely to be the target of social incidents and nine times more likely to be the target of social breaches than in years past. To further underline the growth of financial social engineering attacks, both security incidents and data breaches that compromised executives rose from single digits to dozens in this report

2019 Verizon Data Breach Report Exec Summary

Cyber Insurance Coverage:

Crisis Management Costs — Attorneys, IT Forensics Investigators, credit monitoring firms, mailing and call centers, public relations experts

Extortion Costs — Immediate access to Bitcoin and trained negotiators

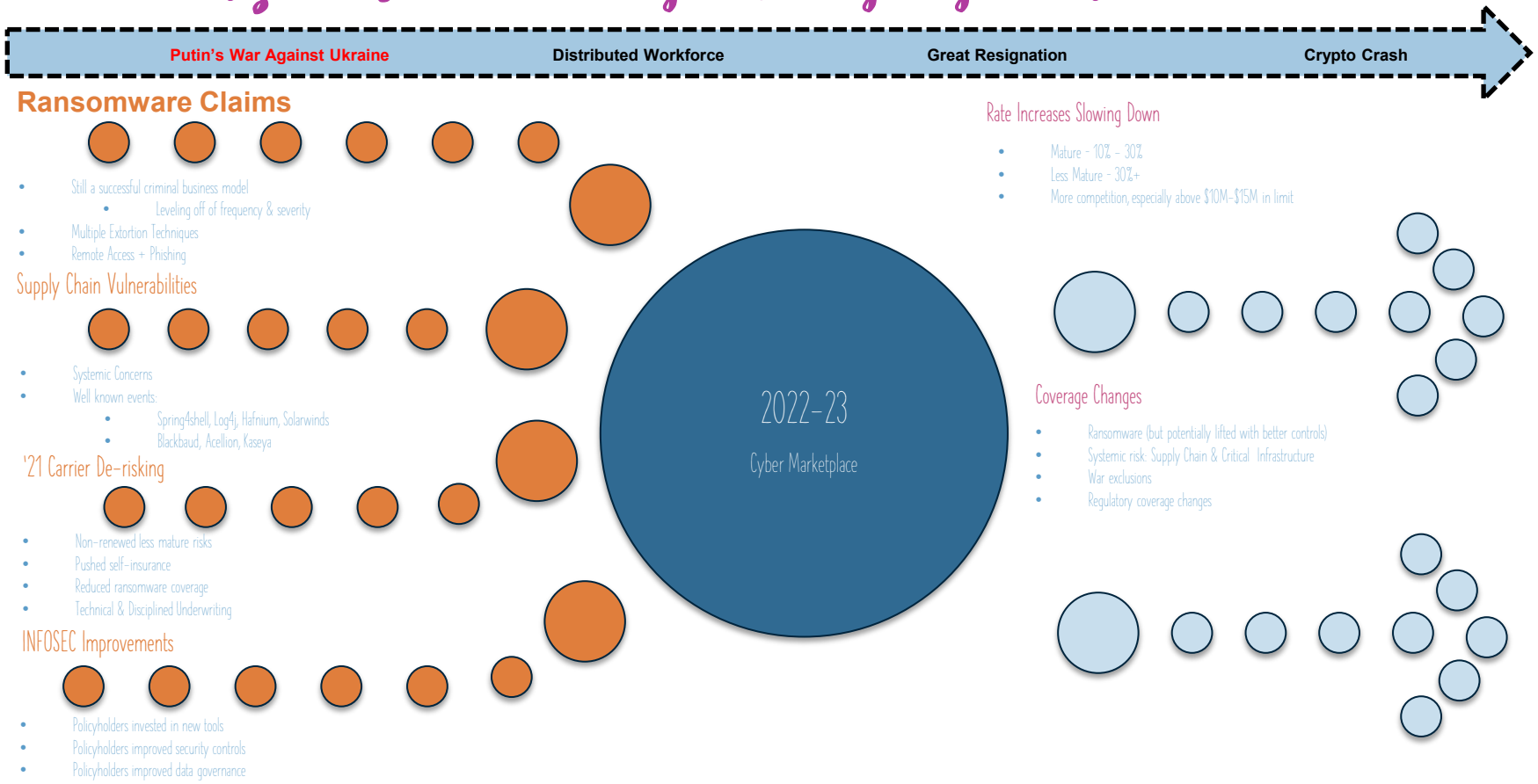
Business Interruption — Lost income due to downtime

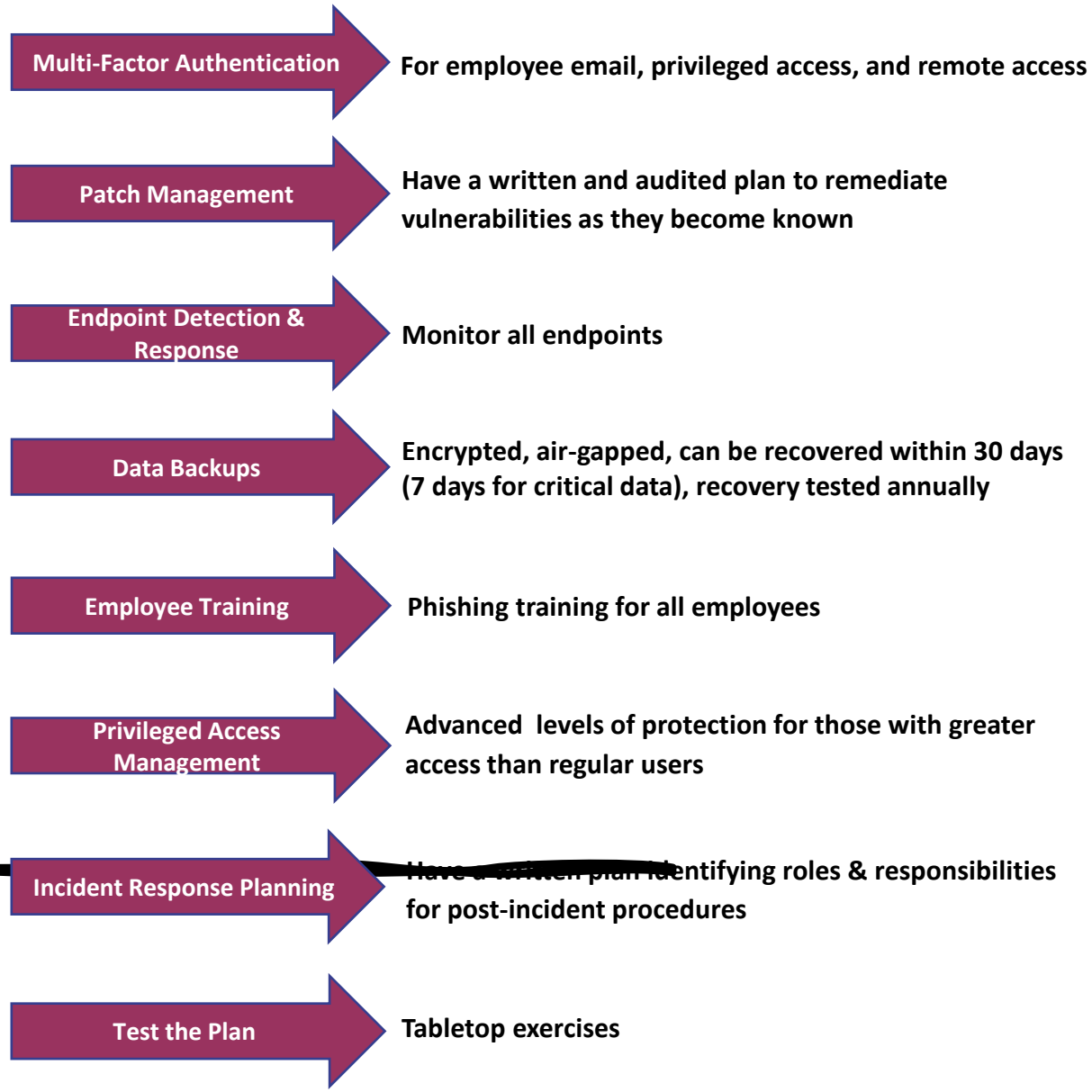
Data Asset Restoration — Restoring data that is damaged or destroyed

3rd Party Liability — Coverage for lawsuits from regulators, business partners and affected individuals

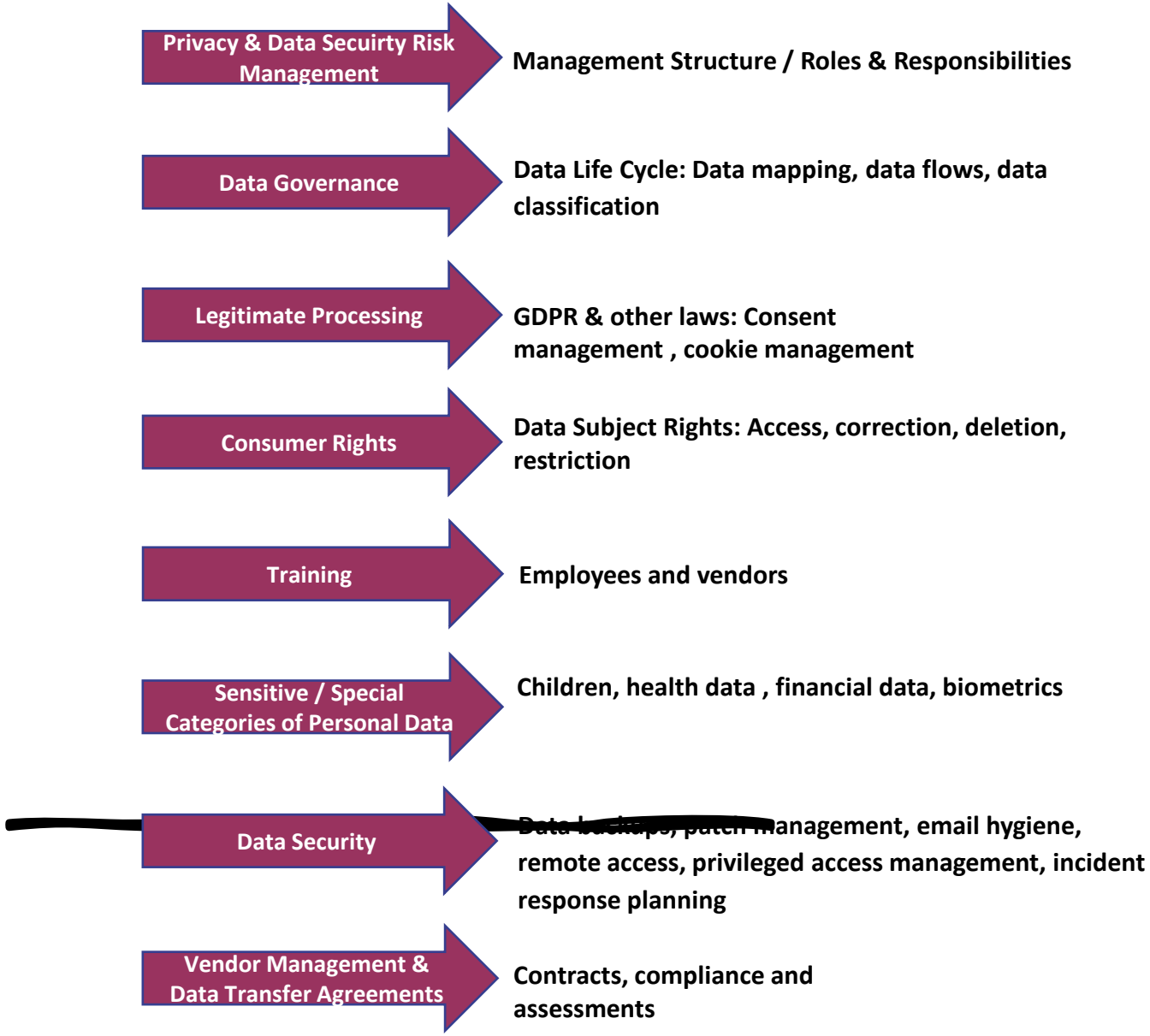
Cyber Insurance Market Conditions

Market Stabilization Yet Encountering Some Lingering Turbulence





Source: Coveware Q3 2021 Ransomware Report



Source: Coveware Q3 2021 Ransomware Report

Cyber Security – Top 10 Tips

- You are a target to hackers
- Keep software up-to-date
- Avoid Phishing scams - beware of suspicious emails and phone calls
- Practice good password management
- Be careful what you click
- Never leave devices unattended
- Safeguard Protected Data
- Use mobile devices safely
- Install antivirus/anti-malware protection
- Back up your data

Cyber Security Extra Tip – Avoid QR Codes

Although QR codes have numerous useful applications, bad actors can also use them for malicious purposes. In January 2022, the FBI released a warning that **cybercriminals may tamper with QR codes to direct victims to malicious websites**. Scammers often look to the latest trends for new cybercrime tactics.

NINJIO To Scan, Or Not to Scan S6E12

Be Vigilant to Avoid Falling Prey!

- Scott R. Wolf
- Cook, Yancey, King & Galloway
- Shreveport, Louisiana
- Scott.wolf@cookyancey.com
- (318) 227-7769

- Thank you!!!!