White Paper

The Importance of Cyber Vigilance: Control Liability and Litigation Exposure

epiq
cyber
incident
response

BEST PRACTICES FOR APPROACHING

The Importance of Cyber Vigilance: Control Liability and Litigation Exposure

Cyber incidents occur daily. In its H1 2023 Data Breach Analysis, the Identity Theft Resource Center (ITRC) reported that data compromises are about to set a new record. There was an increase of 114 percent in reported data compromises from 2023 Q1 to Q2 reflecting the highest number of breaches ever during a quarter.[1] According to Cybercrime Magazine, by 2025 the global damage from cybercrimes is forecasted to reach $10.5 trillion.[2] Cyber incidents threaten an organization's data management and retention capabilities, business operations, and client relationships. Even organizations with sophisticated security systems can be at risk.

But what is worse than a breach and attack? That would be the resulting class action lawsuit or other liability for failing to prepare and respond well. This increases costs and can damage reputation, but the good news is it can be addressed with proactive planning. While no organization can eliminate cyber risk, applying professional teamwork to the problem can lessen the blow. Having professional staff and outside partners with the right knowledge and resources is the key to advancing good cyber health, remaining compliant, and avoiding that class action lawsuit.

[1] H1 2023 Data Breach Analysis: 2023 Data Compromises Are on a Blistering Pace to Set a New Record (Identity Theft Resource Center, 2023); Austin, Doug. Most Data Breaches in a Quarter Ever, Reports ITRC: Cybersecurity Trends (eDiscovery Today July, 12, 2023) https://ediscoverytoday.com/2023/07/12/most-data-breaches-in-a-quarter-ever-reports-itrc-cybersecurity-trends/

[2] Wise, Jason. 15 Urgent Cybersecurity Statistics in 2023 (Earthweb Aug. 17, 2023) https://earthweb.com/cybersecurity-statistics/

WARNING
Virus Detected
To Remove Virus Call Tech Support
Protect Your Personal Financial Information!!!
Security Risk

This white paper will cover cyber trends and tips for organizations to explore in order to be better equipped to anticipate and respond to cyber incidents before a devastating breach occurs. The outcome? Diminished chance of class action activity, compliance violations, lost business, and mounting costs.

PART ONE: TRENDING ATTACK METHODS

Bad actors are developing more sophisticated and strategic ways to target sensitive information, while organizations are simultaneously producing and storing a record amount of data. Think about the information stored by human resources departments for potential, past, and current employees. Or other data pertinent to daily operations like GPS tracking, healthcare patient information, and financial transactions. These are just a few examples. Digital footprints and technology usage will only keep expanding, which adds to vulnerability and presents more opportunities for compromises to occur. Since the cyber threat landscape is dynamic, it is crucial to keep informed on current threats and trends.

The Numbers

To ward off cyber incidents, organizations must keep tabs on trending attack methods when performing risk analysis and implementing security measures. On a broad scale, this can be accomplished by subscribing to industry reports and cyber news alerts. For example, the 2023 ITRC report shared some compelling and informative statistics:

- The first half of 2023 had 1,393 public data compromises with over 150 million known U.S. victims. The total number for all of 2022 was 1,802 with over 420 million known U.S. victims.
- Unsurprisingly, cyberattacks were the top attack vector followed by system and human error, physical attacks, and supply chain attacks. For cyberattacks, phishing and ransomware were the top method used by cybercriminals. Malware came in third, with a shocking 89 percent increase from H1 2022.
- Every sector had a higher number of public data compromises compared to H1 2022, with healthcare at the top of the list.
- There were 534 breaches with no information about the root cause, which was a 67 percent increase from the H1 2022 report.[3]

[3] H1 2023 Data Breach Analysis: 2023 Data Compromises Are on a Blistering Pace to Set a New Record (Identity Theft Resource Center, 2023); Austin, Doug. Most Data Breaches in a Quarter Ever, Reports ITRC: Cybersecurity Trends (eDiscovery Today July, 12, 2023) https://ediscoverytoday.com/2023/07/12/most-data-breaches-in-a-quarter-ever-reports-itrc-cybersecurity-trends/.

Looking at cost, below are some key observations from IBM's 2023 Cost of a Data Breach report[4]:

- The global average breach cost was $4.45 million, representing a 15 percent increase in three years. The healthcare sector had the highest data breach costs at $10.93 million, representing an 8.2 percent increase in just a year's time.
- The top attack vectors were phishing at 16 percent and compromised/stolen credentials at 15 percent, both in the high-cost categories.
- For malicious attacks, ransomware came in at 24 percent with a significant average cost increase of 13 percent from the prior year ($5.13 million).
- For 82 percent of breaches, the data was stored in the cloud. This included public cloud, private cloud, and attacks across multiple environments. Breaches in the public cloud and across environments proved to cost more and take longer to contain.
- Customer and employee personally identifiable information (PII) were the most commonly breached information categories and the costliest.

> "Threat actors will unfortunately continue to evolve their capabilities and find more ways to penetrate systems – whether it be a completely new attack method or variations of current ones."

Considerations

The statistics above illustrate how monitoring industry trends from reputable sources can provide actionable intel. Organizations can see that more breaches are occurring across all sectors, they are costlier, the types of trending attack methods, the heightened risk of storing data in the public cloud, and that threat actors are attempting PII retrieval more often.

It is critical to determine how these trends fit in with specific risk profiles, security controls, and priorities. Then, organizations can make changes accordingly to protect data and control litigation exposure. For example, attack vectors such as ransomware and phishing have been preferred by cybercriminals for years. According to the SonicWall 2023 Cyber Threat report, in 2022 there were 493.3 million identified ransomware attempts.[5] Demands previously in the thousands are now in the millions, proving to be a very costly breach in many instances.

With ransomware attacks trending, cyber risk elevates dramatically as organizations across industries of all sizes can fall victim. This will likely be a part of all risk profiles across the board. However, trends may change as organizations are better prepared to avoid certain threats or limit exposure risk. Even so, threat actors will unfortunately continue to evolve their capabilities and find more ways to penetrate systems – whether it be a completely new attack method or variations of current ones.

[4] Cost of a Data Breach Report 2023 (IBM Security, 2023).
[5] Wise, Jason. 15 Urgent Cybersecurity Statistics in 2023 (Earthweb Aug. 17, 2023) https://earthweb.com/cybersecurity-statistics/

PART TWO: OTHER FACTORS THAT ELEVATE RISK

While staying on top of trending attack methods is crucial, considering less popular ways threat actors may penetrate an organization's systems is just as important. According to a report released in summer 2023, federal data breach class action filings have risen 154 percent in a year's time.[6] The 2022 FBI Internet Crime Report shockingly reported that there were 800,944 cybercrime complaints in 2022.[7] These statistics are indicative of the growing threat landscape, with so many potential avenues available to attack and increase the chance of liability.

Here are three out-of-the-box areas to consider when performing cyber risk analysis:

#1: Deepfakes

Deepfakes are videos, pictures, or audio that have been convincingly manipulated to misrepresent a person saying something they never said or doing something they never did. Machine learning tools make connections between the subject's physical attributes, sounds, and other unique identifiers to create extremely realistic outputs. Some may wonder, is this really a threat to business operations? Analysts would say yes, with 66 percent of participants in a 2022 VMware survey reporting that their organization experienced a deepfake incident. This represented a 13 percent increase over the year prior.[8]

> "Putting extra effort into cybersecurity review fosters successful, secure transactions and ensures everyone at the table is comfortable or has the opportunity to tailor strategy before it is too late."

Cybercriminals can access public company data and make changes or synthesize new content via a deepfake. This can lead to financial and reputational loss that can be hard to detect. Some examples of how threats can materialize include:

- Using manipulated audio to sound like a direct manager, member of the legal team, or client to deceive that person into revealing sensitive information or accessing funds. This could lead to a data leak, fraudulent financial transactions, and more. In 2023 the CEO of Zscaler, a large cloud security company, disclosed that he was the target of a deepfake. The threat actor created a convincing voice deepfake with intent to extort funds.[9]
- Creating a fake video or audio recording of a C-Suite member to paint the organization in a bad light or make statements that do not align company culture, product launches, or that otherwise damage reputation.
- Enabling various phishing campaigns and business email compromises.
- Perpetrating fake interviews, taking a licensing examination under a false identity, or bypassing authentication controls to access personal identifiers or sensitive business data.

Even after a deepfake is proven false, damage occurs and sometimes it is hard to overcome the mistrust, rebuild image, or execute necessary financial mitigation.

#2: Mergers and Acquisitions

Threat actors watch for talk of M&A activity and view this as an opportunity to attack. There are a lot of moving parts and data transfers, which can lead to diminished security awareness and more vulnerability. This increases the likelihood of ransomware attacks, phishing, and other attempts to access sensitive or proprietary information.

[6] Austin, Doug. Data Breach Class Actions Are Surging: Cybersecurity Trends (eDiscovery Today July, 14, 2023) https://ediscoverytoday.com/2023/07/14/data-breach-class-actions-are-surging-cybersecurity-trends/
[7] Wise, Jason. 15 Urgent Cybersecurity Statistics in 2023 (Earthweb Aug. 17, 2023) https://earthweb.com/cybersecurity-statistics/
[8] Global Incident Response Threat Report p. 6 (VMware 2023).

[9] Columbus, Louis. IBM study reveals how AI, automation protect enterprises against data breaches (VentureBeat July 31, 2023) https://venturebeat.com/security/ibm-study-reveals-how-ai-automation-protect-enterprises-against-data-breaches/

Besides the nature of the transaction heightening risk, it is crucial to identify data breach history, dark web exposure, supply chain activity, contractual obligations, and pending legal action. Being aware of these factors helps teams understand where risk exists and what action to effectuate in order to avoid compromise or remediate before moving to the next stage.

It is essential to perform inquiries into cyber risk as a separate category of due diligence review and also throughout the life of the transaction. Putting extra effort into cybersecurity review fosters successful, secure transactions and ensures everyone at the table is comfortable or has the opportunity to tailor strategy before it is too late. Proactive cyber screening before jumping into a transaction should be included.

Here are five steps that can lessen cyber exposure during M&A transactions:

- Take a collaborative approach. Create a playbook outlining roles for key stakeholders and who should come to the table at each phase. Make sure cyber has a presence at each phase.
- Develop strategy with "security by design" to align expectations and ensure that cyber risks are at the forefront of due diligence investigations so teams can identify gaps and react accordingly.
- Dive deep into the acquiree's cyber program to determine what to address in order to maintain uniform security practices. This also diminishes the chance of overlooking a major responsibility or gap prior to integration.
- Maintain an agnostic approach to technology. Key stakeholders can discuss assessments, determine risk tolerance, and consider alternative approaches that lessen risk while still advancing goals. Do not forget to consider whether the people coming over will need certain solutions to continue thriving and contributing in the manner expected after a deal closes.
- Consider how privacy fits into cyber risk due diligence, as current and future legislation around the globe will continue to influence the level of cybersecurity needed to protect sensitive information. Discounting this step and similar obligations such as contractual mandates can result in legal exposure after the deal closes.

> "Timely notification, quality care, and support of these contacts is essential. This minimizes damage, protects brand trust, and helps avoid regulatory fines."

This is just one illustration of how certain dealings will inherently create opportunities for threat actors to strike. Being aware is half the battle, allowing for more strategic and thoughtful decisions during times of heightened cyber risk.

#3 Opportunistic Events

Certain events can cause widespread attacks that quickly place a large number of organizations at risk. For example, in May 2023 the MOVEit hack began. This transfer file management program developed by Progress Software experienced a breach compromising over six hundred organizations globally as of August 2023.[10] MOVEit users transfer sensitive data from their internal systems and from third-parties. An article by Reuters proclaimed, "the sheer variety of victims of the MOVEit compromise, from New York public school students to Louisiana drivers to California retirees, have made it one of the most visible examples of how a single flaw in an obscure piece of software can trigger a global privacy disaster." This is an example of how a small vulnerability can quickly turn into a disaster that highly increases litigation exposure.

[10] Satter, Raphael and Siddiqui, Zeba Analysis: MOVEit hack spawned over 600 breaches but is not done yet -cyber analysts (Reuters Aug. 8, 2023) https://www.reuters.com/technology/moveit-hack-spawned-around-600-breaches-isnt-done-yet-cyber-analysts-2023-08-08/.

In the MOVEit breach response landscape, many incidents are involving more than 1 million impacted contacts and threat actors will continue to trickle out impacts utilizing the vast amounts of data they have exfiltrated. The types of data impacted tend to be rich files with complete contact data, such as complete client or employee lists containing full PII sets. If protected data is exfiltrated or accessed from compromised MOVEit environments, accurate and effective review is essential to create clean lists of affected contacts, including employees and customers requiring notification. Timely notification, quality care, and support of these contacts is essential. This minimizes damage, protects brand trust, and helps avoid regulatory fines. Providers offering a breadth of services such as data mining, review, notification, call center, and credit monitoring can be valuable to limit litigation risk when opportunistic events such as MOVEit occur.

Takeaways

The above are some prime examples of where cyber risk may exist. There are so many areas to consider, both broadly and at an organization-specific level. Keeping on top of the changing landscape will help improve policies and procedures related to managing threats and risks. Also, do not discount the fact that cyber risk is also present in everyday activities in absence of an attack. For example, an employee sending out the wrong file or losing their laptop could lead to a data compromise. These are areas requiring continuous monitoring.

Addressing cyber risks in the specific supply chain of professional services, maintenance contracts, and software plays a role in staying cyber aware. All of this sets the stage for a robust and effective program and will inform strategy and beneficial partnerships, making for a stronger culture of cybersecurity and diminished litigation exposure.

> "Failure to maintain proper controls or act in accordance with the policy could result in denied coverage or dropped policies, which in turn ties into liability exposure levels"

PART THREE: BEST PRACTICES

With all the cyber risk that exists in the world today, it may seem difficult to formulate a plan. There has been an uptick of class actions because organizations are not putting enough prevention in place or when a breach occurs, there is failure to determine its cause and remediate it effectively. When this is the case, there is higher risk for multiple breaches leading to litigation and liability. However, more are looking to invest in cyber preparedness as demonstrated in the IBM report where 51 percent of organizations said they plan to increase cybersecurity spending because of an internal breach.[11]

The first step is to accept that breaches cannot be eliminated, but they can be controlled both proactively and after an event occurs. The next is to determine the best combination of security controls that fall within an organization's risk tolerance. From training to threat detection software, mock breach exercises, and beyond – the possibilities are plentiful and flexible.

Additionally, there is a growing trend where insurance carriers are starting to demand illustrations of cyber preparedness before they provide new or renewal cyber coverage. Underwriters are looking closely at the controls in place that would prevent an attack or foster rapid remediation and recovery. As the cyber insurance market matures, new ways to evaluate risk and manage policies will emerge. Bi-annually, quarterly, or even monthly premiums are in the realm of possibilities. Insurers may require more

[11] Cost of a Data Breach Report 2023 p. 49 (IBM Security, 2023).

"Tabletop exercises are a great place to start, as they validate which processes are sufficient and shine light on areas needing improvement. Some key people that should come to the table for these exercises include IT staff, executives, human resources, management, and counsel."

frequent audits that can result in discounts for sound security demonstrations. Failure to maintain proper controls or act in accordance with the policy could result in denied coverage or dropped policies, which in turn ties into liability exposure levels.

Cost is also a factor, as breaches can be expensive. In the recent IBM report, organizations that had the tools and processes in place to identify breaches internally saved $1 million on average compared to breaches disclosed by attackers.[12] Additionally, savings for those using security AI and automation tools extensively was $1.76 million and these organizations could contain breaches much faster.[13]

Below are five approaches that organizations can undertake to remain cyber vigilant with the underlying goal of limiting litigation exposure, controlling liability, and reducing breach-related costs. These suggestions are in addition to monitoring cyber-attack trends and understanding any unique vulnerabilities that may exist, as discussed above.

#1: Implement robust internal programs to ensure cyber awareness.

Being proactive starts with solid training programs and creating an internal culture of cyber awareness. Without proper communication on cyber controls, reporting procedures, and companywide responsibilities – an organization opens the door to claims that could be avoided or remedied prior to regulatory involvement. Here are some initiatives to consider:

- **Enhanced cyber training programs.** There need to be thoughtful and mandatory education that will promote transparency and expand cyber knowledge for everyone in the organization. This should be included past onboarding and be embedded into daily activities via mandatory training, open forums, cyber alerts, simulations, and other educational opportunities. Also ensure that managers regularly talk about cyber responsibility to their teams and how to report suspected issues via the appropriate channels.
- **Complaint handling protocols.** Everyone should know where to escalate cyber reports so the appropriate team can determine which issues are actual threats, everyday IT issues, or instances of whistleblowing. Risk analysis and legal obligations will feed into these designations. Having policies around following up with individuals who report is also a good idea to keep decisions transparent and defensible.

[12] Cost of a Data Breach Report 2023 p. 6 (IBM Security, 2023).
[13] Cost of a Data Breach Report 2023 p. 5 (IBM Security, 2023).

The above can also help control unsubstantiated claims, such as reports by cyber whistleblowers. Sometimes, people report suspected cyber issues to regulatory agencies or the public but do not have all the information relating to business risk decisions or complex technologies involved. The resulting investigatory response and reputation repair will utilize a lot of resources. This can be counterbalanced with valuable education that will promote transparency and expand cyber knowledge for everyone in the organization.

#2: Maintain strong incident prevention and response programs.

Proactively performing cyber risk analysis goes hand in hand with incident response efforts. This includes identifying the key players, having the right tech stack, and maintaining strong partnerships with outside consultants.

Tabletop exercises are a great place to start, as they validate which processes are sufficient and shine light on areas needing improvement. Some key people that should come to the table for these exercises include IT staff, executives, human resources, management, and counsel. Even if not included, it would be beneficial to share findings with legal services providers that will participate in breach response to confirm role comprehension and compliance.

IBM found that incident response planning was a top three cost mitigator and that organizations deploying high levels of breach countermeasures on average saved $1.49 million in breach costs and came to a resolution 54 days faster. The report highlighted best practices including forming a dedicated response team, drafting playbooks, regularly testing incident response plans in tabletop exercises or simulated environments, and having an incident response vendor on retainer.[14] For example, the respondents using automated response playbooks or workflows specific to ransomware attacks contained breaches 68 days faster.[15]

It is also critical not to discount legal's involvement. While incident response heavily relies on technical and forensic actions, legal implications are just as important and will come into play at every phase. Breach notification, impact assessment, privacy law compliance, and regulatory reporting are a few areas where the legal team will have an integral role in response efforts.

> "Having consistent counsel to contact about cybersecurity issues will help ensure that an organization's infrastructure, policies, and practices promote data protection."

On July 26, 2023 the Securities and Exchange Commission (SEC) adopted new cybersecurity rules. A major change is that when a material cybersecurity incident occurs, organizations registered under the SEC need to disclose it within four days after deeming it material. There are also new categories of information to include in annual reports. The first is all active processes for assessing, identifying, and managing material risks from cybersecurity threats. The second is any material effects of risks from cybersecurity threats and prior incidents. The last is a description of the board of directors' oversight of cybersecurity risks stemming from threats and management's role and expertise in assessing and managing material cyber risk from these threats.[16]

[14] Cost of a Data Breach Report 2023 p. 66 (IBM Security, 2023).
[15] Cost of a Data Breach Report 2023 p. 35 (IBM Security, 2023).
[16] SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (U.S. Securities and Exchange Commission July 26, 2023) https://www.sec.gov/news/press-release/2023-139

This is an example of regulatory reporting that must be considered during incident response. There are expanded requirements with nuances and compressed timelines to consider where legal's involvement will be crucial. Understand this is a C-suite level initiative so there needs to be board-level attention on minimizing, managing, and responding to cyber risk. This greatly increases responsibility on an organization's board of directors to maintain cyber knowledge and expertise. Having a relationship with a provider that can offer both proactive planning and response efforts can help ensure that the C-suite, legal, and other important actors are aligned on cybersecurity initiatives and ready to respond in the event of a breach.

> "Material changes to laws, regulations, and best practices will continue to surface. Organizations need to be nimble and prepared to adapt expediently to the changing cyber landscape. Formulating a robust plan is possible with the right internal and external resources, changing cyber habits, and preparation."

#3: Information governance and cybersecurity need to intertwine.

In addition to having robust investigatory and breach plans, clear information governance is critically important to limit the consequences that could result from a substantial data breach. As companies continue to move to the cloud and attempt to reduce spend on information technology, it is becoming more important to be creative in where investments are made across people, process and technology. Information governance is an area of opportunity to invest in to reduce the risk associated with cyber events.

An outside consultant can help mitigate the risk of cyber incidents by reducing the volume of data stored in a legally defensible manner. The stronger the retention policies are, the less data that will be available to intercept in the event of the breach. Sometimes organizations already own technology that can help with these efforts, but they are not taking advantage of the full potential. For example, in the Microsoft 365 environment there are several options available to better leverage an organization's investment in this technology. Some areas to explore related to information governance include:

- **Data Classification:** Consider implementing sensitivity labels, sensitive information types, and trainable classifiers to foster cybersecurity readiness.
- **Data Lifecycle Management:** Leverage M365 retention policies and labels to place the organization in a better position to defensibly delete data and reduce risks associated with over retention.
- **Records Management:** There are file plan capabilities and label policies that allow organizations to build a comprehensive solution to manage business-critical data in compliance with regulations, laws, and unique records retention policies.

All of this can feed into cyber initiatives by allowing organizations to leverage the value in their data while effectively managing security and compliance.

#4: Vet all vendors and third-party relationships.

As the MOVEit breach demonstrated, organizations are dependent on the security habits of their vendors and other third parties. Before partnering with another organization, investing in new technologies, or otherwise transferring sensitive data – it is crucial to advance a thorough vetting process to understand all cyber risks. This helps with the selection process and opens dialogue on optimal solutions that will safeguard sensitive and proprietary data. Also consider involving vendors in tabletop exercises to align expectations. Taking this action before an incident makes for less to do when that stressful event occurs and once again may help avoid that class action from coming down the pipeline.

#5: Retain cyber counsel.

Organizations should consider retaining outside counsel specializing in cybersecurity or hire a staff attorney practicing in this area. The relationship can be scaled according to the company's size and specific security needs to stay within budget while still improving security practices to protect sensitive data. Some advantages are having attorney-client privilege available for sensitive cyber matters, access to industry connections, and expanded legal knowledge. Overall, having consistent counsel to contact about cybersecurity issues will help ensure that an organization's infrastructure, policies, and practices promote data protection. This is important pre-incident in the planning phase to the post-incident response phase to combat threats and expedite remediation efforts.

This can serve a dual purpose by also helping meet compliance obligations. Some global data privacy regulations obligate organizations to have a designated data privacy officer on staff or engage cyber counsel. For example, under the new India data privacy law if an organization receives a significant data fiduciary designation, one requirement imposed is to appoint an India-based data protection officer.[17]

According to an article by CSO, a recent industry study by the law firm of Womble Bond Dickinson concluded that only roughly half of businesses executives are very prepared to reach compliance in the EU, U.K. and U.S. data privacy landscapes. Cybersecurity was the top data privacy concern in this study. One best practice noted to help tackle the evolving global data privacy landscape was to engage outside counsel to advise on compliance in this regard.[18]

CONCLUSION

Nobody wants to deal with class action or other liability stemming from a breach – especially when it could have been prevented or better controlled. New digital threats are constantly surfacing and cyber vigilance should be top of mind. Organizations have to balance these threats against budget constraints, risk profile, resources, regulations, and data indicating attack probabilities. This is also a field experiencing quick and continual evolution. Material changes to laws, regulations, and best practices will continue to surface. Organizations need to be nimble and prepared to adapt expediently to the changing cyber landscape. Formulating a robust plan is possible with the right internal and external resources, changing cyber habits, and preparation.

[17] Landaw, Max. 6 Things You Need to Know About India's Digital Personal Data Protection Bill of 2023 (Lexology Aug. 27, 2023) https://www.lexology.com/library/detail.aspx?g=a7ddfd7c-caba-4a90-8460-1a1dd32e4fce
[18] Hill, Michael. Only half of organizations "very prepared" to meet global data privacy laws (CSO July 18, 2023) https://www.csoonline.com/article/646475/only-half-of-organizations-very-prepared-to-meet-global-data-privacy-laws.html