SYGNIA

MARCH 2024

SYGNIA'S ANNUAL FIELD REPORT

THE EXECUTIVE'S PERSPECTIVE: LEGAL

The CISO's Expanding Universe: Navigating Liability and Risk in a Post-SolarWinds World

The recent SEC complaint against SolarWinds and its CISO, coupled with the 2022 Uber verdict, has ignited a firestorm of discussion surrounding the evolving role of the CISO and their expanding liability. No longer confined to the technical trenches, CISOs today are thrust into the spotlight, navigating a complex landscape of heightened scrutiny, expanded responsibilities, and potential personal liability. Below are the key takeaways from Sygnia's Engagement Managers after a year of helping C-level execs through the most challenging of times.

The SolarWinds Case: A Paradigm Shift

The SolarWinds incident, where a sophisticated supply chain attack infiltrated the company's software and impacted numerous government agencies and Fortune 500 companies, exposed the shortcomings of traditional cybersecurity approaches. The SEC complaint, alleging that CISO Tim Brown and SolarWinds deliberately downplayed cyber-risks and inflated their security posture, marked a significant shift in the legal landscape. This case sent a clear message: CISOs are not only responsible for implementing robust security measures but also for being transparent about cyber-risks and proactive in their mitigation.

The Uber Verdict: When Responsibility Extends Beyond the Firewall

The Uber verdict, which held the company liable for a data breach caused by a third-party vendor and its CISO personally liable for obstructing an active FTC investigation into Uber's security practices, has further amplified the scope of the CISO's responsibilities. This case highlights the need for CISOs to take a holistic approach to risk management, extending their purview beyond the organization's immediate perimeter and encompassing the entire ecosystem, including vendors, partners, and even customers. The CISO must now be the orchestrator of a comprehensive security program, ensuring that all actors within the organization's sphere of influence are adequately secured. And even more importantly, CISOs need to be honest.

Navigating the Labyrinth of Increased Liability

With the increasing scrutiny and broadened scope of their role, CISOs are facing potential personal liability for cybersecurity shortcomings. Legal scholars argue that the Uber verdict and the SolarWinds case could pave the way for a surge in lawsuits against CISOs, both from regulators and private plaintiffs. This necessitates a heightened awareness of legal obligations and the potential consequences of inaction or negligence.

From Tech Expert to Strategic Leader

To adapt to this evolving landscape, CISOs must shed the skin of a purely technical expert and embrace the role of a strategic leader. Here are some key areas of focus for the future CISO:

- **Risk Management:** CISOs must evolve beyond technical controls and implement a comprehensive risk management framework that identifies, assesses, and mitigates cybersecurity threats across the entire ecosystem, including third-party relationships.
- **Understanding Their Corporate Positioning:** The days of merely playing the role of a security expert are over, and as such it is imperative that the new CISO understand that their decisions and actions could have significant legal ramifications. The relationship between the CISO and General Counsel therefore is becoming paramount and giving closer attention to this synergy will only benefit the CISO as well as the legal and ethical resilience of the organization.
- **Championing Integrated Security:** The days of siloed security programs are over. CISOs must champion the integration of security into all aspects of the business, from product development to supply chain management. This necessitates collaboration across departments and a shift towards a "security first" mindset within the organization.
- **Building a Culture of Transparency:** The SolarWinds case has emphasized the importance of transparency in cybersecurity. CISOs must foster an environment where open communication about cyber-risks is encouraged, and information is readily shared with all stakeholders, including boards of directors.

> **Embracing Continuous Learning:** The cybersecurity landscape is a dynamic one, constantly evolving with new threats and vulnerabilities emerging. CISOs must commit to continuous learning and updating their knowledge base to stay ahead of the curve and ensure their organizations remain resilient.

The CISO role is transforming. No longer solely focused on technical measures, CISOs are now expected to be strategic leaders, risk management experts, and effective communicators. With increased scrutiny and potential liability looming, CISOs must embrace this evolving landscape by adopting a holistic approach to cybersecurity, fostering transparency, maintaining a clear and unfettered line of communication with the CEO, General Counsel and senior management, and remaining agile in the face of ever-changing threats. The future of organizational security rests largely (if not entirely) on their shoulders, and their success will be instrumental in navigating the challenges and seizing the opportunities of the digital age.

New SEC Cybersecurity Disclosure Requirements: 2023 and Beyond

In July 2023, the Securities and Exchange Commission (SEC) shook up the financial and legal landscape with its groundbreaking mandate for public companies to disclose cybersecurity incidents and risk management strategies. This landmark move aimed to equip investors with crucial information about cyber vulnerabilities and potential financial impacts, marking a significant step towards transparency in the digital age. However, as we enter 2024, questions abound about the future of these requirements and their evolving impact on companies and investors alike.

2023: Navigating the Initial Wave

The initial phase of these new regulations, which went into effect on December 18, 2023, focused on two key aspects:

> **Material Cybersecurity Incident Reporting:** Companies must disclose any incident deemed "material" within four business days on Form 8-K. This includes details about the nature, scope, timing, and potential financial impact of the incident; and

> **Annual Cybersecurity Risk Management Disclosures:** Within annual reports, companies must provide comprehensive information on their cybersecurity risk management strategies, governance practices, and risk assessment methodologies.

Predicting the Path Forward: 2024 and Beyond

As companies get comfortable with the new requirements and investors adjust their expectations, 2024 is expected to witness several interesting trends:

1. **Refining the "Materiality" Lens:** With initial filings underway, the SEC might issue further guidance or rulemakings to clarify the definition of a "material" incident. This will provide greater certainty for companies in determining when disclosure is necessary.

2. **Deep Dive into Incident Response:** Expect investors to go beyond initial incident reports, demanding insights into response effectiveness, remediation efforts, and long-term consequences. Companies will need to demonstrate their preparedness and recovery skills.
3. **Spotlight on Governance and Leadership:** Board involvement in cybersecurity, CISO expertise, General Counsel oversight, and cybersecurity culture will likely take center stage. Investors will seek evidence of strong leadership and commitment to cyber resilience.
4. **Data-Driven Disclosures and Benchmarking:** Companies will likely leverage automation and data analytics to enhance incident detection, risk assessment, and disclosure preparation. Industry-specific comparisons and best practices might emerge, leading to more tailored and relevant information for investors.
5. **Cyber Insurance and Resource Allocation:** The role of cyber insurance in risk mitigation and response might receive increased attention in disclosures. Additionally, investors might look for information about how companies are allocating resources to manage cyber risks effectively.

Beyond the Horizon: Regulatory Landscape and Global Collaboration

2024 may also witness:

- **Potential for Additional SEC Rulemaking:** The SEC might fine-tune specific aspects of the requirements,addressing areas like third-party vendor risk management or sensitive data handling.
- **Heightened Litigation Risk:** Companies may face increased legal challenges over allegedly inadequate disclosures or mismanagement of cyber risks.
- **Global Harmonization Efforts:** International collaboration to harmonize cybersecurity disclosure requirements across jurisdictions might gain momentum.

The SEC's cybersecurity disclosure requirements are a crucial step towards increasing transparency and accountability in the face of ever-evolving cyber threats. As we move into 2024, these requirements are likely to evolve, driven by investor demand, technological advancements, and regulatory developments. Companies (both public and private) that embrace proactive risk management and prioritize clear, informative disclosures will be well-positioned to navigate this dynamic landscape and foster investor confidence in the digital age.

Emerging Trends in Third-Party Risk Management

In the rapidly evolving landscape of cybersecurity, organizations face a multitude of challenges in safeguarding their digital assets. As businesses increasingly rely on third-party vendors for various services, the importance of effective Third-Party Risk Management (TPRM) has never been more critical. Here are a few anticipated trends we expect to see and which should be taken into consideration when developing strategies and methodologies around TPRM.

1. **Elevated Complexity in Vendor Ecosystems:** As organizations expand their operations, the intricacies of managing diverse and extensive vendor ecosystems grows. We will witness an increased demand for comprehensive TPRM services aimed at ,addressing the complexity of interconnected supply chains and ensuring a robust defense against evolving cyber threats.

2. **Regulatory Compliance Takes Center Stage:** With the global landscape of data protection and privacy regulations becoming increasingly stringent, cybersecurity firms will play a pivotal role in assisting organizations in enforcing compliance within their vendor networks. Expect a surge in demand for services that evaluate and ensure third-party adherence to regulatory frameworks, reducing the risk of legal and financial consequences.

3. **Technological Integration for Efficiency:** Automation and advanced technologies are poised to revolutionize TPRM. Cybersecurity firms will harness the power of artificial intelligence and machine learning to enhance the efficiency of risk assessments, monitoring processes, and incident response planning. The integration of cutting-edge solutions will enable real-time threat detection and response, mitigating risks before they escalate.

4. **Resilience and Incident Response Planning:** In response to the ever-evolving threat landscape, the focus of TPRM will extend beyond risk assessment to building resilience and effective incident response capabilities. We expect to see the development and testing of even more robust incident response plans, ensuring a swift and coordinated response to cyber threats.

5. **Supplier Diversity and Inclusion Considerations:** Beyond cybersecurity risks, organizations are increasingly mindful of the broader impact of their vendors on business operations and reputation. We will see organizations adapting their data security and privacy methodologies to assess not only technical risks but also factors such as supplier diversity and inclusion, aligning with their broader ESG objectives. As such, cybersecurity firms will be required to take these factors into consideration when addressing the needs of the organization.

6. **Continuous Monitoring and Threat Intelligence Sharing:** Proactive measures will become paramount in an organization's effective and continuous monitoring of third-party vendors. This involves not only assessing the current risk posture but also staying ahead of emerging threats through effective threat intelligence sharing within industries.

7. **Educational Initiatives for a Resilient Workforce:** Recognizing the role of human factors in cybersecurity incidents, organizations will likely need to implement more robust education and training programs. These initiatives will encompass awareness training, simulated phishing exercises, and best practices for secure collaboration, fortifying both the client organization and its vendors against social engineering and human error.

In conclusion, the trends in Third-Party Risk Management are dynamic and closely aligned with the evolving threat landscape. Cybersecurity firms will continue to play a pivotal role in guiding organizations towards a future where resilience, compliance, and technological innovation are at the forefront of effective TPRM strategies. As the digital realm continues to expand, the collaboration between organizations and cybersecurity experts becomes integral to navigating the complex and ever-changing cybersecurity terrain.

Disclaimer: This article provides general information and does not constitute legal advice. For specific legal guidance, please consult with qualified legal professionals.

Executive perspective – Engagement Managers

Top lessons learned in 2023 in terms of Global Cybersecurity tabletop exercises

Having worked with some of the most mature customers in the world and experienced both real and simulated cyber crisis events, I often get asked what the top lessons learned are. Below are the most common challenges, allies and items that are underestimated by customers globally.

CHALLENGES: Time & Perfection
To quote one of the most respected CISO in the world, Equifax's CISO Jamil Farshchi - "Time and perfection will ultimately crush you." Customers do not realize how quickly a crisis can escalate to the point that they lose control of the situation. This is why cybersecurity requires a full business response. Secondly, the stakeholders will demand all information right away so they think they can make perfect decisions and perfect solutions. You will never have enough time for perfection. I tell customers that they need to become comfortable being "uncomfortable" with the lack of information during a crisis. Account for this in your leadership strategy.

ALLIES: Communications & Options & Preparedness
The most oft repeated feedback after a crisis or simulation was how critical the role of communications became. Companies who communicate a daily "North Star" of the current priorities are the most successful. Build your Incident response plans, business continuity plans, and other solutions with flexibility in mind, to quote Jamil Farshchi again "optionality… [become] comfortable rolling them [decisions / solutions] back or tailoring them as you learn more, and as things progress". Another key lesson was the understanding how much could be done ahead of time vs during a crisis. Bringing all of these allies together is why you create a security culture focusing on continuous cyber preparedness.

UNDERESTIMATION: Deeper level details & authorization & human factor
In the majority of IR, BCM, and crisis documentation reviewed the customers have a certain level of details. But they underestimate the need for more details - one to two layers deeper – during a crisis. For example, the need to communicate to employees during the crisis in an out of band platform when laptops are encrypted. Who has the latest contact list? When was the last time it was updated? Where is that list stored and is that also encrypted? Understanding someone's roles and responsibilities is fundamental but it is the one layer deeper this is most critical; who is "authorized" to take significant actions. For example, it's who can take down a server, talk to the media and explain to customers and clients that needs to be clearly defined. Lastly, one of the most overlooked aspects of a crisis is the human factor. The first hours of a crisis is when the greatest number of mistakes are made due to the increased stress. Your team will need to sleep, eat, and go home to their families. Prepare for that.

Sygnia focused on four major areas during cybersecurity exercises in 2023;

- First was preparing for the new SEC cybersecurity reporting requirements with an emphasis on determining "materiality" of the incident. Who is authorized to make the determination and who is responsible for the disclosure to the SEC. What makes this challenging are the opposing legal, financial and operational points of view all colliding while trying to provide some level of trust and accountability on the investor side.
- Second was new cybersecurity crisis playbooks and runbooks that are tested and immersed in a customized tabletop exercise. The majority of the client's maturity show their continuous cybersecurity preparedness strategy by upgrading their documentation and placing it under live fire simulations.
- Third was greater understanding of the multiple stakeholders' roles and responsibilities especially when the leadership team has new executives who have never done an exercise together. A lot of the foundation is to build trust and understanding amongst the new executives and to feel that they have a seat at the table.
- Finally the validation of the customer's current posture and strategy followed by an understanding of how they compare to their peers and what are the key gaps that need to be addressed. The most mature customers are not only doing tabletop exercises with internal stakeholders but are also including their top business partners. In other words, they are comparing runbook to runbook to make sure that their processes, escalation, authority and strategy are aligned.

Building a security team

The role of the CISO has been evolving over the years as cybersecurity has taken on a greater role for organizations as they try to become more competitive and efficient. Navigating cybersecurity challenges through digitalization and cloud adoption and innovating with emerging technologies are just some business drivers' where CISOs and their security teams are contributing their expertise. Today's CISO should be able to gather the support of their security program and effectively drive security culture within their organization as they move closer in reporting to the C-level executive management team.

Cyber risks are getting more disruptive and costly. The C-suite and the board are getting serious about the realities of securing the organization, especially with legislation is penalizing them for negligence. CISOs will need to ensure that cybersecurity is discussed and forms sufficient consideration in the decision-making process at the C-suite and board level, where they are relied on for guidance to effectively influence the security culture. It is then important for the CISO to justify their budget spending, through an effective security program that supports maximum business growth and protects the bottom line.

Developing an effective cybersecurity program is often challenged with building the appropriate organization structure for a security team. Where cybersecurity aligns with the business, building a security team requires consideration for the security strategy, technologies, and objectives to support the security program. The security strategy determines how the organization is going to secure and defend against cyberattacks and position the security services to meet the business needs. Technologies define what skillsets and training is required to appropriately deploy and adopt secure systems. And objectives allow security leaders to align their internal teams to sustain business operations and defend against cyber-attacks.

Core to building a security team is aligning business needs with the C-Suite and the board. The CISO role is pivotal for influencing changes of the security culture across the organization through executive awareness and training.

Creating a resilient security team involves a combination of strategic planning, talent acquisition and ongoing training. Organizations will need to start building their security teams to support their cybersecurity program with a well-defined structure to ensure that team members understand their specific contributions to the overall cybersecurity program and seek individuals with problem solving abilities and an understanding of emerging threats. Cybersecurity remains a dynamic field, so training and skillset development is essential to staying ahead of the evolving threat landscape to maximize the benefits when investing in cutting-edge technologies. Security teams must foster a collaborative culture to ensure resilience across the organization with IT operations, development teams and enterprise architects. With higher levels of collaboration across the organization, it will be easier to instill a culture of cybersecurity and promote security awareness.

Prioritizing security budget

Cybersecurity is functioning more as a business driver in today's organizations. Budgets however remain a concern and during an economic downturn are often a candidate for cuts. C-Suites and boards who are hampered by a lack of understanding the cybersecurity program may be more concerned with compliance than security best practices. CISOs must justify the security budget and position their program as a business driver rather than as a cost center.

Security teams should be able to adopt a cyber risk approach that is relevant to their environmental threats, address regulatory requirements and minimize negative business impact. The security posture should be continuously assessed and monitored against security industry best practices and relevant threats to establish a clear understanding of the cyber risks that needs to be addressed. Cyber assessments should address business risks as they are prioritized to protect and maximize the organizations bottom line with a clearly defined roadmap addressing cyber risks.

As cyberattacks increase and security budgets are cut, organizations should focus more on prevention and detection capabilities to maintain their security posture. Prevention reduces the chances of threat actors infiltrating and moving through the organization, cutting them off early in the attack chain. And when a threat actor can perform malicious activities in the organization, early detection can help to mitigate the consequences of a cyberattack.

To justify the security budget, the program must be communicated to the C-Suite and board through a prioritized cyber risk approach that is aligned with the business needs. A comprehensive methodology for discovering threats and relevant vulnerabilities while translating the cyber risks into business risks needs to be clear and concise so that C-Suite and Board can effectively advocate for budget because it is aligned with business objectives.

Development of KPIs to measure effectiveness/fulfillment of the cyber security program

Maintaining an effective cybersecurity program builds cyber resilience into an organization and establishes quantifiable metrics for success that influence security culture and emphasize the importance of cybersecurity in the organization. Cybersecurity awareness plays a large role, and the security team needs to be transparent and aligned with Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) that matter to the C-Suite and the board.

Security controls should be developed to support the cyber security program and security metrics must be aligned and tracked to understand how effective the controls are. Security controls must be adaptable to the ever-changing threat landscape and business environment. And the security team must be able to adopt the appropriate controls as cybersecurity challenges arise. It is essential for security teams to measure and monitor the effectiveness of security controls through KPIs and KRIs to enable strategic decision making towards achieving the objectives of the cybersecurity program.

By having security metrics that are transparent and precise, the cybersecurity program can be validated for its effectiveness and credibility. C-suite and the board will have a better appreciation as to where the organization's security performance stands and able to drive key cybersecurity decisions. More importantly, this will build organizational security confidence through tracking and continuous improvement of the cybersecurity program. Security metrics provide insights into areas that require attention and improvement, here are some examples of commonly developed KPIs & KRIs:

KPIs:

1. Incident Response Time: time it takes for detection and response to security incidents.
2. Phishing Resistance Rate: success rate of organization resisting phishing attempts.
3. Patch Management Compliance: Percentage of systems and software that are up to date with latest security patches.
4. Threat Detection Accuracy: Accuracy of threat detection systems
5. Employee Training Effectiveness: Success of cybersecurity awareness training by tracking employee behavior, such as recognizing and reporting suspicious activities.

KRIs:

1. Vulnerability Exposure Rate: Rate of new vulnerabilities discovered within the organization systems.
2. Third-Party Security Risk: Security posture of third-party vendors and partners.
3. Data Breach Cost: Quantify potential financial impact of a breach.
4. User Account Anomalies: Usual activities related to user accounts, i.e., multiple login failures / unauthorized access attempts.
5. Regulatory Compliance Violations: Compliance with industry regulations and legal requirements.

Security metrics are important for making cybersecurity decisions with foundational KPI and KRI data, moving security teams into proactive approaches for dealing with any cyber threats and vulnerabilities. Well-defined security metrics can illustrate the overall security posture to the C-suite and the board to highlight the most pressing cybersecurity matters and justification of the cybersecurity budget. Regularly reassess and update security metrics to stay resilient against evolving cyber threats.

WANT TO KNOW MORE ABOUT ONE OF OUR SOLUTIONS?

As the trusted advisor and cybersecurity service provider of leading organizations worldwide, Sygnia protects the enterprise through a variety of solutions that are aligned with the current threat landscape. From OT and Cloud Security to Ransomware Readiness, our Enterprise Solutions are borne out of frontline experience and a deep understanding of the threat actor mindset.