GUTSY

NAVIGATING A NEW SECURITY GOVERNANCE REALITY:

A CISO's Guide to Cybersecurity Disclosure & Compliance

TABLE OF CONTENTS

AN INTRODUCTION

Navigating the New Security Governance Reality: A Guide for CISOs, CEOs, BODs, and Security Teams

First, the law came for Joe Sullivan. The former Uber Chief Information Security Officer (CISO) was convicted in 2022 of federal charges of covering up a cybersecurity incident resulting in the theft of Uber drivers' and customers' personal information.

Next on the docket is Tim Brown, the CISO of SolarWinds, which was the victim of a damaging supply chain attack. An SEC case against Brown alleges he is personally responsible for the network management company's cybersecurity posture and for the company's alleged downplaying of the severity of the attack, which left thousands of government networks exposed.

On the heels of these cases came a new rule from the SEC mandating four-day disclosure of material impacts of cybersecurity events. This rule puts an even heavier onus on the CISO and their team to detect, triage, and categorize breaches and incidents at a much faster pace. The cost of making a mistake or even hesitating increased, and with it, the pressure on CISOs, their Boards, and the CEOs they report to.

01

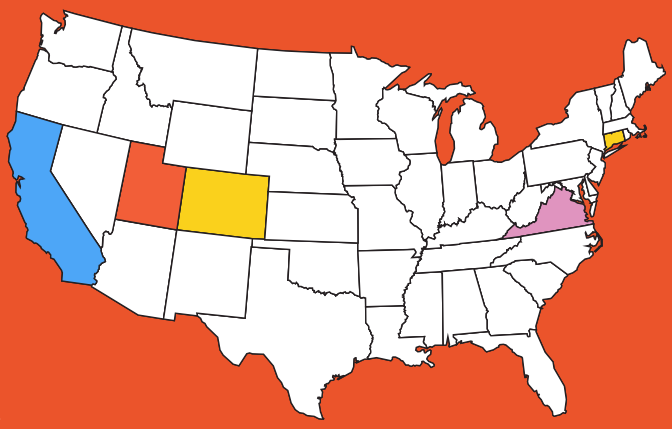
Disclosure Laws, Privacy Regulations Alter the Landscape

These cases are only one of the many developments in an accelerating trend toward more complexity and potential liability in security governance. More stringent expectations of company cybersecurity response and laws governing security practice are starting to bite hard.

In the European Union, a series of new laws, including the Cyber Resilience Act, are putting a heavier burden of security liability on companies building and selling technology gear. The existing EU umbrella law, the GDPR, is being more and more widely applied to fine companies that fail to quickly inform customers or users whose data might have been stolen or to mitigate root causes of cyberattacks. In 2023 alone, the EU levied roughly $2 billion in GDPR fines, including a whopping **$1.3 billion fine against Meta** and another **$345 million fine against TikTok** for data privacy and consumer protection violations.

In the U.S., the Food and Drug Administration levied a six-figure fine on a mid-sized healthcare organization for failure to comply with HIPAA guidelines due to a phishing incident. This was the first penalty for phishing-induced HIPAA violations and a wake-up call for healthcare CISOs and CEOs. More and more states are adding their own privacy laws, injecting greater and greater security governance complexity and making the life of a CISO ever more challenging.

These states include: **California, Virginia, Colorado, Utah & Connecticut**



These laws have considerable differences in definitions of covered data and acceptable disclosure periods. Some states cover medical and biometric information and even usernames and passwords. Others stick to more basic information like social security numbers and driver's license numbers. California's law also covers biometric data, email addresses with passwords, and health insurance information. Many state laws stipulate that companies tell potential victims as soon as possible and in no less than 30, 45, or 60 days of the breach and data loss, depending on the state.

The Uber CISO Case: **A Wake-Up Call**

The court ruling imposing personal and criminal liability on Uber's former CISO is a stark reminder of the personal stakes involved in cybersecurity governance. This precedent-setting case highlights the potential legal ramifications for CISOs whose organizations fail to disclose information about breaches and attacks (In this instance, the CEO drove the decision not to disclose but the CISO paid the price).

In addition, it might drive CISOs towards overly conservative behaviors. An unintended consequence might be that the ruling makes it more challenging to recruit good CISOs for jobs that are perceived to be more challenging and risky. This case, too, was questioned by many CISOs as conflating hesitancy and a cautious approach to disclosure with dishonesty and rule-breaking.

The reality is no breach or loss disclosure happens in a business vacuum and many actors may seek to influence the course of a cyber response. In this case, however, the lack of a rigorous set of processes and the absence of compliance mechanisms to validate appropriate breach disclosure processes came back to haunt Uber — and, in turn, to haunt the CISO profession.

This precedent-setting case highlights the potential legal ramifications for CISOs whose organizations fail to disclose information about breaches and attacks.

Whistleblower Complaints: **A New Threat Vector**

The recent developments in the U.S. Securities and Exchange Commission's (SEC) cybersecurity incident disclosure rules have introduced new risks. In November 2023, AlphV reportedly breached the information systems of MeridianLink, a software company providing digital lending solutions. After exfiltrating data, the group not only demanded a ransom but also took the unprecedented step of filing a whistleblower tip with the SEC against MeridianLink. This action was based on the alleged failure of the company to disclose the cybersecurity incident publicly within the mandated time frame as per the SEC's new rule.

The SEC had adopted final rules mandating the disclosure of material cybersecurity incidents, which requires registered companies to disclose information about a material cybersecurity incident within four business days. AlphV's move to file a whistleblower complaint represents an escalation in ransomware tactics. By leveraging the SEC's regulations, the group aimed to increase the pressure and potential costs for MeridianLink by raising the likelihood of regulatory investigation, which could be costly and damaging to the company's reputation and business operations.

This approach illustrates how threat actors are becoming increasingly sophisticated, not only in their technical capabilities but also in their understanding of regulatory and corporate pressures.

The SEC has not publicly commented on how it will handle whistleblower complaints initiated by threat actors, and the likelihood that AlphV would ever directly profit from the filing is slim. (In the U.S., whistleblowers can receive a percentage of a fine should their claim hold up in court). However the law of unintended consequences implies this is likely one of many unforeseen complications resulting from the new policies and environment.

The Cost of Breaches Soar: **Boards and Investors are on Alert**

High-profile breaches and disclosure failures at companies like MGM, Clorox, Boeing, and particularly Okta — which suffered a $2 billion market capitalization loss following its breach announcement — illustrate the substantial financial and reputational risks involved. In particular, the growing wave of ransomware attacks is causing material harm.

Okta's breach appeared to be more reputational damage after attackers leveraged inconsistencies in security processes to steal session tokens and download sensitive information. The incident impacted all Okta customers.

Clorox and MGM suffered ransomware attacks that caused massive business interruptions. MGM slot machines and IT systems were offline for extended periods, and Clorox was forced to warn of a $100 million potential revenue hit caused by delays in shipping products.

More recently, financial services provider Mr Cooper warned shareholders of a **$25 million cleanup** after what appeared to be a ransomware attack. These impacts, and the increasing sophistication of attacks ratchet up pressure on CISOs. They need to not only ensure security processes are properly followed, but also to put in place air-tight forensics and process capture to document any incident.

High-profile breaches and disclosure failures illustrate the substantial financial and reputational risks involved. In particular, the growing wave of ransomware attacks is causing material harm.

A New Landscape Means New Models

Organizations must now consider the new landscape of personal and corporate liability.

The new landscape demands a reevaluation of traditional security governance models. Organizations must now consider the new landscape of personal and corporate liability, the realities imposed by new disclosure laws, and the required processes and tooling to meet the needs of these new landscapes.

For CISOs, CEOs, BODs, and security teams, the new security governance landscape presents a markedly more complex array of challenges and responsibilities. Staying ahead of these changes requires a proactive approach with a focus on compliance, transparency, and strategic risk management.

02

Redefining Security Governance for the Modern Era

Security governance has existed for decades as a subset of technology governance and compliance. However, security governance has remained a slow-moving, static, and reactive practice. The old ways of thinking about governance and approaching the practice are no longer sufficient and cannot keep up with modern requirements. A raft of new disclosure rules and privacy laws mandate that CISOs have real-time insights into cybersecurity practices and processes. Understanding when, where, and how a breach or infiltration occurred within a few days of discovery is now table stakes. Failure to do this can result in both corporate and personal liability for CISOs.

Old Security Governance: **Static, Slow, Manual**

For decades, security governance lived inside general IT governance processes and moved at a similar pace. Governance reviews were semi-annual or annual. Governance processes were often survey or examination-based and conducted annually or semi-annually alongside traditional compliance processes. Governance policies were used to inform and configure policy engines and other technology controls. However, policies were complex to update and rarely changed. This made sense in the older "Defend The Castle" era of IT security, where assets and activity inside the walls were trusted and less scrutinized, employees used fewer and more tightly controlled systems, and physical boundaries separated enterprise assets from the outside world.

All CISOs recognize that this dated approach to security is no longer viable. APIs punching holes in the firewalls, distributed applications running both on-prem and in the cloud, employees accessing SaaS applications for a growing portion of their workflows, and the explosion of connected devices and traffic all force CISOs to adopt a new mindset and approach. Securing the modern environment requires "Zero Trust" continuous verification, ubiquitous security controls, and always-on intelligence. Zero Days are more common, and threats revealed are quickly exploited in the wild. To address this change, CISOs have adopted numerous new security technologies.

Unfortunately, security governance approaches have failed to keep up. Even today, most security governance remains siloed in various playbooks, spreadsheets, communications tools, and ticketing systems. Processes for governance may be stated once but are rarely tracked, monitored, and verified. As a result, security governance often becomes a security risk in its own right. In its **2023 State of Security report, logging, and security company Splunk found that only 31%** of respondents

had a formal cyber resilience strategy and program. **According to ISACA's 2023 State of Cybersecurity report**, 62% of respondents believe that organizations are under-reporting attacks due to concerns over brand reputation or legal consequences. These findings demonstrate that security governance is failing to keep up.

With the recent issuance of a new rule by the **U.S. Security and Exchange Commission**, pressure on CISOs to improve security governance will dramatically increase. The new rule mandates disclosure of material security incidents within four days of discovery. Equally important, part of this rule, Regulation S-K Item 106, requires registered companies to "describe their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats, as well as the material effects or reasonably likely material effects of risks from cybersecurity threats and previous cybersecurity incidents." In other words, transparency and process are no longer "nice-to-haves." Every CISO must be prepared to explain their approach directly to shareholders. Given the tight timetable for disclosure, under the new rule, the only viable path is to automate and instrument security governance processes. The upshot? Security governance must up its game and enter the modern age of continuous cybersecurity. What's more, the process of security governance must change in order to match this new higher bar.

62% of respondents believe that organizations are under-reporting attacks

Modern Security Governance: **Real-time, Automated, Transparent, Verifiable**

The core definition of security governance remains the same — the practice of providing governance and oversight for security-specific processes and workflows. Modern security governance, however, goes beyond this bare-bones description. CISOs looking to modernize their security governance should consider four fundamental tenets: real-time, transparent, automated, and verifiable.

Real-time Means Faster Governance Metabolism

In a world where Zero Day attacks and ransomware continue to increase, and dangerous nation-state threat actors rapidly iterate on exploits and attack TTPs, security governance must up its metabolism to keep pace. Annual or semi-annual policy updates no longer suffice and CISOs must be equipped to quickly shift governance approaches to counter fast-moving adversaries. Closely related, faster governance means that security teams must accelerate the processes and workflows required for proper governance, moving from paper-based and semi-manual processes to on-demand checks and integrated monitoring of governance metrics.

Automated Governance Moves from Human Error to Machine Readable

In technology, every error-prone process is shifting from overreliance on humans to programmatic approaches. Infrastructure-as-Code, GitOps, and other operational processes have shifted manual application delivery management to scripts and automation. More advanced security teams are automating security processes by automating workflows and linking together different systems to unify security operations. Whereas security monitoring and reporting focuses on Indicators of Compromise and evidence of breach or exfiltration, security governance automation will need to focus on automating all the steps teams take to maintain security, investigate anomalies, and then disclose or report findings. Naturally, security cannot be completely automated; human judgment will continue to play a central role. But just as all other areas of operations and security (and even marketing and IT processes) are becoming automated, so too must security governance.

Transparency for Easy Reporting, Observability, and Drill-Down

When organizations wanted to audit security governance processes, traditionally, this meant poring over log files for many different systems and looking over interactions in communications channels or ticketing systems. It was insecurity through obscurity, making it impossible to quickly and efficiently execute forensic investigations. Modern security governance requires greater transparency, making it possible even for CISOs or CIOs to drill down into individual aspects of security governance process conformance and execution. An additional benefit of transparency is simplified reporting, which can be tuned to highlight anomalies and serve to focus organizational efforts on outliers.

Verifiable Governance to Reduce Liability and Simplify Audits

With increasing regulatory scrutiny and legal risk, CISOs must be able to demonstrate and verify security governance. Many of the state laws in the U.S. leave considerable room for interpretation of "best efforts" in security response and disclosure. Verifiable security governance establishes a tamper-resistant logging mechanism to capture and safeguard governance process records. Making governance verifiable provides legal protection and simplifies auditing and compliance procedures, enabling more frequent audits of security governance practices to help organizations maintain compliance.

New Rules, New Possibilities

While this ongoing shift requires considerable organizational energy and significant change management, a faster, more automated and more transparent security governance approach empowers a raft of new possibilities. Faster metabolism and response times and ability to quickly modify governance will lead to more responsive security posture management and a rapid feedback loop. Automation and transparency will lead to a reduction in human error, less toil and trouble for stretched security teams, and simplified analysis of security response processes. Verifiable security governance will reduce liability, build traceable processes, and eliminate gray areas where CISOs might unfairly be held liable. Ultimately, this new approach to security governance will affect cybersecurity teams for the better and make governance less painful, more proactive, and more effective.

A faster, more automated and more transparent security governance approach empowers a raft of new possibilities.

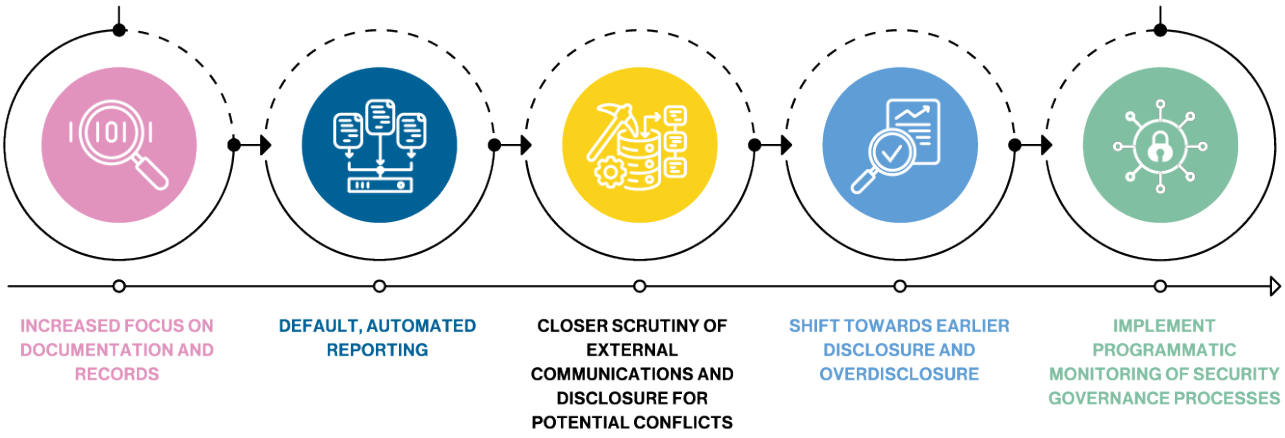
0 3

The New Liability Reality for CISOs

The conviction of former Uber CISO Joseph Sullivan by a jury in a Federal Court was the first time someone in this role was **convicted of a felony** resulting from their actions in responding to a cyberattack. At its core, the case hinged more on Sullivan's failure to disclose a new breach to Federal investigators shortly after they had interviewed him for an ongoing investigation at Uber. A second pending case against Timothy Brown, the CISO of SolarWinds, indicates that CISOs can expect greater personal liability for their actions in reporting and mitigating security breaches.

This is new territory, CISOs have not traditionally been thought of as personally liable for security incidents or the responses to them. Corporations often did not purchase Directors & Operators liability insurance for CISOs, reserving that for other C-Suite occupants. While CISOs worked closely with legal teams to determine the right policies for complying with the law, the Uber case involved company attorneys accepting immunity in exchange for testimony against Sullivan. With the SEC case against Brown, the charges allege that public statements made by SolarWinds about incident impacts contradicted internal statements. These cases are forcing a reckoning in the CISO community and a **new approach to security governance** to minimize personal liability.

Ways CISOs Should Change Security Governance to Reduce Liability



There are five common sense changes to security governance CISOs can pursue to reduce their legal exposure.

Increased Focus on Documentation and Records:

To minimize liability, CISOs must improve documentation of security processes and keep detailed records of actions taken and team communications during incident responses and other critical security operational activities. CISOs should preserve presentations, emails, and other communications for extended periods to better enable due diligence and create a clear record of their actions and intent. For their own well-being, CISOs should insist on robust enterprise knowledge management and document and communications indexing to ensure that internal communications are easy to search and navigate.

Default, Automated Reporting:

CISOs should implement detailed, automated reporting using security governance and operations aggregation tools. Reports should be system-generated from ongoing metrics capture and security observations. This approach ensures that notification is transparent and automated and puts the onus on all recipients to remain informed. Recipient lists should be determined by the CISO, legal team, and C-Suite to match best practices for disclosure and security governance as determined by the legal team.

Closer Scrutiny of External Communications and Disclosure for Potential Conflicts:

In the case of SolarWinds, the SEC specifically cited internal presentations by the CISO voicing concerns about the security of systems against external attackers. Such concerns were not included in SolarWinds' public risk statements. The key problem is the disconnect between what the CISO states internally and what the organization states publicly. Often a CISO has no control over public statements. For that reason, a CISO should assume that any internal presentation could ultimately become discoverable for litigation or published online. To cover their liabilities, CISOs should make explicit statements in any internal documents indicating what information is material and should be disclosed to comply with the law.

Shift Towards Earlier Disclosure and Overdisclosure:

In most cases where CISOs are faulted, the point of contention is not how incident response is conducted but when an incident or data breach is disclosed and the degree of disclosure. The hesitancy to disclose for fear of reputational and damage leading to lost customers and revenues is counterbalanced by stronger legal requirements to disclose and the resulting bad publicity of "disclosure sprawl". An example of this is the Okta incident in the fall of 2023 when the company slowly widened its admissions from a few customers to all customers subject to information leakage from a breach. A better approach is to detail the known scope of exposure and concede that the final scope is unknown and may be revised upwards.

Implement Programmatic Monitoring of Security Governance Processes:

To ensure that they have good information on what is really happening in security governance, CISOs must monitor processes programmatically to verify that incident response playbooks are followed. This includes monitoring engagement with legal teams to document when they are informed and how their inputs inform incident response efforts. Newer forms of artificial intelligence make analysis of conversational data more accessible and applicable. This type of monitoring also simplifies post-incident audits required by law enforcement. It also facilitates third-party investigations, something that Uber was criticized for failing to accommodate as it worked through root cause and response analysis of its data breaches.

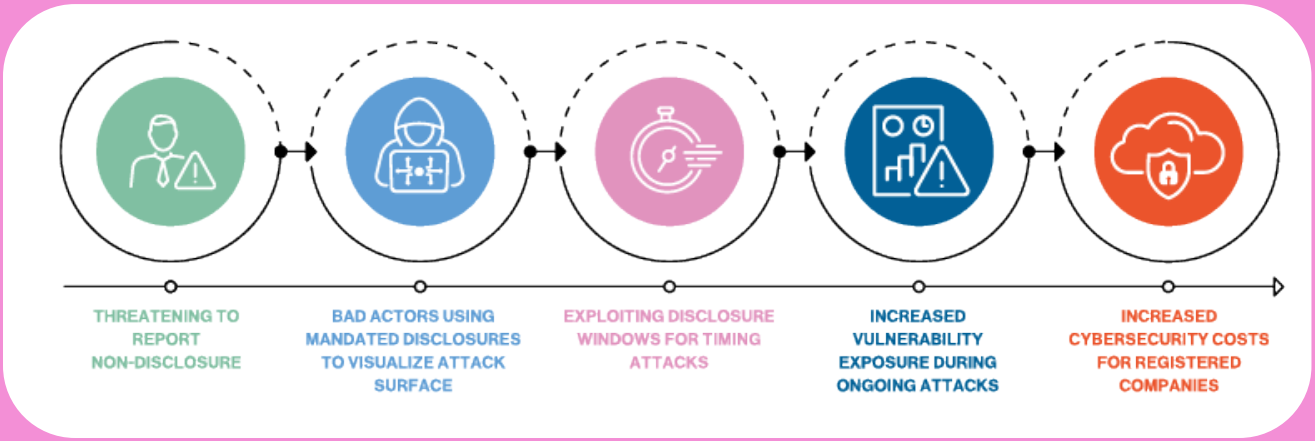
CISOs Can Address Liability Through Common Sense Changes

Security is a messy business. Incident responses are chaotic. Communications and information sharing between humans are inexact and may create false impressions of malicious intent. Projecting increased personal liability in this already unsettled environment raises the stakes for CISOs. Shifting security governance to emphasize early and complete disclosure, monitoring and capture of processes, eliminating discrepancies in reporting, and automating the reporting process help contain CISOs' personal liability.

Increased personal liability in this already unsettled environment raises the stakes for CISOs.

04

Five Unintended Consequences of the New SEC Cybersecurity Disclosure Rule



The November 2023 **whistleblower complaint by the ALPHV/Blackcat ransomware** crime syndicate to the U.S. Securities and Exchange Commission broke new ground in the rapidly evolving world of cybersecurity. ALPHV filed the complaint alleging that a publicly traded company, MeridianLink, had failed to make a timely disclosure of a material cyberattack. This would violate a **new SEC rule that took effect in July 2023 mandating disclosure of attacks** within four days. ALPHV clearly wanted Meridian to pay their ransom to make the attack go away, but the way it chose to leverage the new SEC rules was perhaps the first case of unintended consequences.

A ransomware gang turned government whistleblower is unexpected, to say the least. But CISOs seeking to maintain a tight security governance ship will be facing an entirely new and unfamiliar landscape as additional unintended consequences of the new rules play out in 2024 and beyond. In this post, we'll examine a few of the potential unintended consequences and their impact.

Threatening to Report Non-Disclosure

As we already discussed, this surprising tactic has been used by the ransomware group ALPHV/Blackcat. It is likely that other ransomware gangs will adopt similar tactics because their chances of collecting payment from victims are directly proportional to the pain, bad publicity, and cost created. The SEC stipulates $25,000 per day fines for the first 30 days of non-disclosure, adding to financial pain. The SEC also states that failure to properly disclose material incidents in a timely fashion could negatively impact the ability of public companies to fundraise. To be clear, this threat of regulatory disclosure merely adds a new wrinkle to attack tactics; disclosure of attacks has long been used as a weapon against victims who stand to suffer reputational or other damage when a cyber breach hits the news. But the SEC angle ratchets up the pressure and adds an additional pain point.

Bad Actors Using Mandated Disclosures to Visualize Attack Surface

The new SEC rules also require companies to provide detailed information about their cybersecurity risk management, strategy, and governance practices. The full extent of what is acceptable remains a work in progress and will evolve over time. The risk of these disclosures is potentially providing bad actors with detailed insights into a company's cybersecurity practices, making it easier for them to plan and execute attacks. For example, a significant percentage of serious attacks involve sophisticated social engineering and attempts to exploit known processes, identities, and behaviors. With AI and deep fakes, social engineering and spear-phishing will become easier to execute. If a company is required to disclose significant details of who or what teams must be involved in cybersecurity processes, then attackers will surely seek to exploit that new knowledge.

Exploiting Disclosure Windows for Timing Attacks

In some cybersecurity incidents, the share prices of the victim company fall on news of the attack. This is more true with companies that have small or medium market capitalization. Now that the SEC has instituted a four-day notice mandate, attackers could conceivably exploit an anticipated disclosure window to sell the victim's shares short, profiting when they fall. In another scenario, attackers might hit a victim organization on the eve of an important shopping day or, if bids are due for a critical contract, in the week before that deadline. By putting a timeline on disclosure and making it non-negotiable, the SEC makes timing attacks far more powerful.

Increased Vulnerability Exposure During Ongoing Attacks

As a former CISO, I can say for sure that it may not be possible to fully block an attack in four days. An attack might require updating software and endpoints across tens of thousands of devices and systems around the world. Not all those devices are even online or connected to the Internet — in factories, for example. If a company is forced to disclose an attack even as it continues, this could encourage other attackers to pile on.This could either be to exploit the same ongoing vector or via other vectors under the premise that security response teams are already stretched, so responding to an additional response would likely be beyond their capacity. Because of the nature of shareholder lawsuits and recent court rulings, non-disclosure that material attacks are still ongoing could put litigation crosshairs on the backs of breached organizations.

Increased Cybersecurity Costs for Registered Companies

Security response is costly. It requires lots of time and often requires a surge in resources. Putting a four-day window on identifying, cataloging, and mitigating security incidents is the equivalent of moving from ground shipping to next-day air delivery. Speed is expensive. It can also result in waste if a wrong path is undertaken in the response and forensics and resources are poured into a dead end. Unfortunately, this budget item is likely to be lumpy and unpredictable, making it harder for CISOs to properly budget for the new security governance landscape.

Other Unintended Shoes Likely to Drop

These are just five potential unintended consequences of the new SEC disclosure rules. One of them has come to pass. However, attackers are creative and will likely identify other ways to exploit the new rules to gain an advantage. CISOs will face not only pressure to move quickly and comply more broadly, but also to redesign their teams and processes for forensics and disclosure. CISOs will also have to find a way to strike a balance between disclosing cybersecurity practices and processes to potential investors while shielding critical information about attack surfaces and processes from bad actors. The inevitable unintended consequences inject a new wildcard into the equations that will make security governance still more complicated going forward.

The inevitable unintended consequences inject a new wildcard into the equations.

05

Reshaping Security Governance to Meet the New Challenges

We have covered changes to the security governance landscape, the reality for CISOs in the wake of critical legal rulings and SEC rule changes, how they face greater liability, and potential unintended consequences of the SEC disclosure mandates. Now it's time to explore specific recommendations to improve security governance to reduce personal and corporate risk.

CISOs can actually transform the new requirements into a thoughtful mechanism to create greater efficiencies around security governance processes, metrics, and workflows.

Update your security incident response playbook

To meet the new reality of faster and more detailed disclosures as well as to mitigate personal legal risk, CISOs need to update their security response playbooks. To meet the new SEC requirements, you may need to change many practices to better hit the four-day disclosure window. That could mean increasing the frequency of log analysis,closing gaps in log collection, putting in place better observability and data aggregation to speed up forensics, or automating key parts of your reporting process. In addition, you may need to allocate more resources to the initial response, by assigning additional headcount or putting in place a resource burst capability through a third party.

Update your compliance and risk management practices

CISOs will need to have a new set of compliance and risk practices to accommodate the new SEC rules and legal risks. For their organizations, the SEC rules accelerate timetables for any compliance activities required to report a material attack. At the same time, due to the fast turnaround time required by the SEC, CISOs may consider increasing the frequency of compliance exercises such as audits to increase their team's ability to move quickly and reset organizational expectations. In terms of risk management and disclosure, the new landscape for personal and corporate liability requires significantly more care to be applied in all internal communications.

When CISOs do make internal presentations or provide recommendations about cybersecurity policies and practices, they should err on the side of caution. CISOs should advocate for disclosure early and often, even with incomplete information, because the alternative is far greater legal exposure. CISOs should also work closely on disclosure playbooks with the CEO and communications teams of their organizations in order to better manage reputational risks and potential financial impacts resulting from any disclosed breach or attack.

Instrument your playbooks and processes so you can objectively verify compliance

What is not measured does not matter, and what is not instrumented cannot be measured. Rather than prioritize purchasing more defensive security tools, CISOs should consider investments into systems that can programmatically collect, categorize, and report on security response and compliance processes. Such systems exist today but a wide gap remains in understanding how teams behave, whether they follow policies in reality, what the workflows actually look like under fire, and where bottlenecks and gaps may lie.

Enter security process capture, the last mile for security governance. Process capture has long existed in other fields, but it is only now becoming more of a focus in security governance, driven by the SEC rules and the changing landscape. Process capture means instrumenting

the different workflows and tools that security teams use to monitor and validate that proper processes are followed and to identify ways processes can be improved. In reality, security controls are only a part of the toolchain essential to security governance and compliance. Messaging and chat tools, ticketing systems, software repositories, and CI/CD tools all play critical parts in security operations and governance. Instrumenting the tools that are used puts in place a mechanism to develop process centric understanding and also a more detailed record of team actions and behaviors. This record can be used to fulfill audit and compliance requirements by demonstrating policy execution and conformance.

That said, simply capturing the process and making it visible is a necessary but not sufficient step. CISOs will also need to deploy a new set of security process metrics to spot trends, find outliers, and measure averages. Some existing security metrics would clearly apply — such as mean-time-to-detect, mean-time-to-fix, mean-time-to-contain, and mean-time-to-update.

Some new potential security metrics might include:

Mean-time-to-triage — How much time it takes to appropriately identify and escalate a security event is a critical capability to be able meet new disclosure requirements. Without rapid triage, a serious incident might not be escalated in a timely fashion.

Mean-time-to-validate — From triage to validating that an attack is underway is another critical metric along the path to a four-day notification capability.

Mean-time-to-blast-radius — Mapping the full blast radius of an attack can be challenging to measure, but having an accurate read on the full extent of an attack will make rapid reporting less daunting and risky.

Playbook-compliance-percentage — What percentage of security responses follow the prescribed playbook determines both how well a team is performing but also the viability of a playbook and supporting processes and tools.

An Opportunity to Make Security Governance Transparent & Efficient

While all of the discussed changes will put stress on security, compliance, and risk management teams, this transitional period also offers a rich opportunity to elevate, streamline, and automate security governance. What the SEC and shareholders want to know is whether CISOs and their teams prepared and responded correctly. For CISOs, this knowledge will also help them understand how effective their team is and whether the processes put in place are viable and followed. The most important capability of any security team is tight coordination and cooperation. While every team has many tools and controls, those controls are only as good as the processes that surround them.

While every team has many tools and controls, those controls are only as good as the processes that surround them.

Instrumenting security and compliance processes makes security more transparent and efficient by allowing CISOs to monitor and observe coordination and cooperation. Transforming previously manual event log analysis and interviewing processes into systems will also enable faster audits and reduce compliance and risk management costs over time, all while delivering improved security. Automated security process monitoring and reporting will enable nearly real-time readouts on process compliance and behaviors, allowing CISOs to oversee critical security response and even enabling CEOs to track security governance. The logical end game for CISOs is to have a clear line of sight into the inner workings of their security response and compliance processes, making visible the vague and predictable the previously opaque — all while reducing cost and risk.

GUTSY

www.gutsy.com