


WHITE PAPER

How New SEC Disclosure Rules Move Beyond the Checkbox

By Dr. James Norrie, Founder

A hand is shown placing a white block on top of a stack of six other white blocks. The blocks are stacked vertically and labeled with the following terms from top to bottom: Regulations, Rules, Standards, Policies, Compliance, and Law. The background is a blurred image of a person in a white lab coat and a patterned tie, suggesting a professional or scientific setting.

Regulations

Rules

Standards

Policies

Compliance

Law

Executive Summary

- 1 **SEC's Regulatory Shift:** On September 5, 2023, the SEC introduced new rules requiring public corporations to disclose cybersecurity incidents promptly and provide annual cybersecurity risk management disclosures, marking a significant regulatory change. ([8-K Form Sample here](#))
- 2 **Increased Responsibilities:** CISOs, CEOs, and Board members will face heightened pressure to apply advanced cyber expertise, model cyber risk, integrate it into overall business risk, and manage and report new cyber risks and mitigating investments under the new SEC guidelines.
- 3 **Complex Frameworks:** Many companies currently use multiple security frameworks for compliance, but the focus is shifting from mere, 'check the box' compliance, to demonstrating the deployment of tactics, techniques, and procedures (TTPs) for comprehensive cybersecurity risk mitigation.

The cybersecurity world changed on September 5, 2023 when the SEC issued new rules affecting public corporations ([33-11216-fact-sheet.pdf - sec.gov](#)). These mandate public disclosure of cybersecurity incidents within **four business days** of determining a material event; and **annual disclosure** regarding cybersecurity risk management, strategy, and governance. This is an important regulatory shift.

The new SEC guidelines will be **more pressure** on the CISO, CEO and the Board to apply sophisticated cyber expertise to stochastically model cyber risk; understand cyber as a critical component of overall reportable business risk; and task management to identify, track and clearly report on new cyber risks and how their Board will approve mitigating investments to minimize that risk to acceptable levels.

To date, many companies are either required to or voluntarily apply one or more **security frameworks** such as NIST, ISO27001/2, CoBiT, CIS 20, PCI, and others to assess their security program maturity. These overlapping standards can be overwhelming if the organization is simply trying to 'check the box' for compliance. That only measures activity as an input rather measuring reduced risk as an outcome.

In our view, this important shift by the SEC to force public companies to not simply report how they manage their cybersecurity program today but instead to prove that enterprise tactics, techniques and procedures (TTP's) are being deployed to fully mitigate, transfer or accept the remaining residual cybersecurity risk as being within your total business risk tolerances and why that is the case.

cyberconIQ® offers the **Human Defense Platform** and our **cybermetrIQs™** dashboard, both of which can help pinpoint and reduce cybersecurity risk across the enterprise and measures the risk-adjusted ROI of your cyber investments. Our focus is to help any business to move 'beyond the checkbox' by embedding a **security first culture** that minimizes risk and maximizes compliance under these new rules.

For more information on how cyberconIQ can help your enterprise, please visit cyberconIQ.com.



Concrete Next Steps

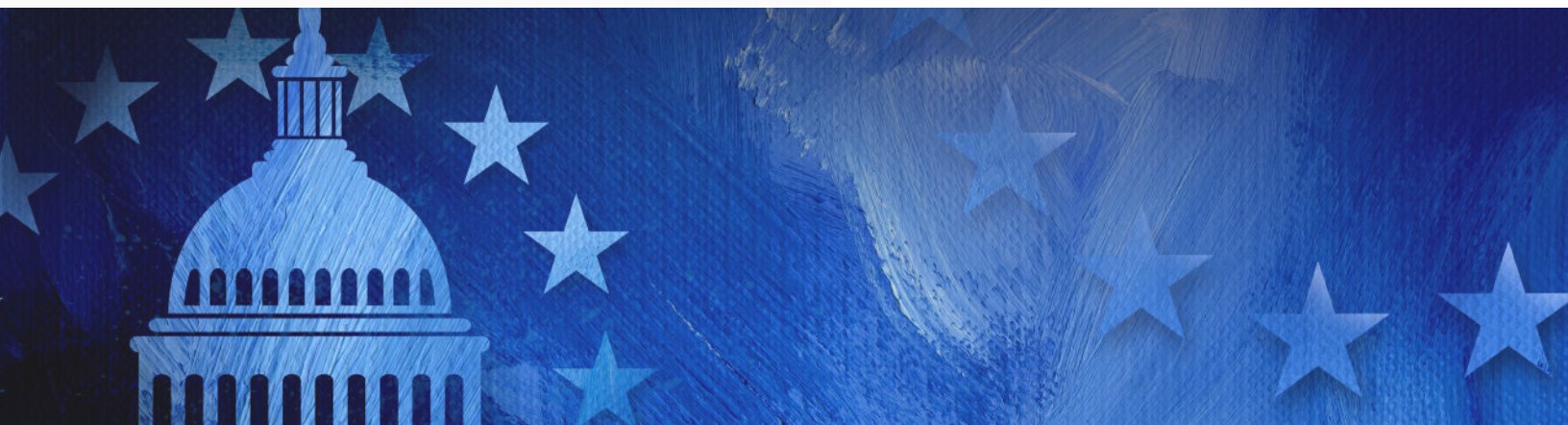
As is often the case when an important regulator like the SEC changes step, many organizations struggle to interpret the practical actions necessary to move into compliance with the new regulatory cadence. Furthermore, we frequently note that regulators move to impose new guidelines often without clear accompanying definitions of what is acceptable to avoid litigation or criminal pursuit as a result of failing to meet these new guidelines. This often creates consternation, frustration and anxiety as Boards and Directors struggle to respond to new responsibilities without concrete next steps to undertake. To help, instead of offering a summary of the changes in the underlying SEC guidelines themselves – information already available and digested by all concerned – we opted to turn our efforts towards early actions a Board of Directors can consider to avoid becoming an early victim of SEC enforcement efforts.

While nobody knows for sure what will happen, there is past precedent, common law tradition and critical legal reasoning to credibly apply. They indicate the SEC Enforcement Division will be looking for early egregious breach examples to engage both their civil and criminal enforcement powers to heave clarity into what is expected of a company claiming compliance with these new guidelines. Therefore, our objective is to examine the possible perceived purpose of these new guidelines, focusing on noted cybersecurity gaps the SEC is signaling it intends as the scope of this enhanced regulatory oversight.

Let's consider actions under the new guidelines by grouping them into three distinct categories which highlight what we feel are the most obvious and compelling focus areas under the new guidelines:

1. **Timely Disclosure of Material Cybersecurity Incidents (Form 8-K)**
2. **Annual Disclosure or Risk Management, Strategy & Governance (Form 10-K)**
3. **Managing Risk Beyond Your Existing Perimeter and Tactical Edge**

For each one, to reduce the risk of becoming an early litigant under these new guidelines, we offer one or more concrete steps an enterprise can take within the next **90 days** to get ahead of looming reporting deadlines and put forward evidence of solid governance action to meet the spirit of these guidelines.



Implications of #1: Timely Disclosure of Material Incidents

The SEC now mandates a **4-day reporting** requirement for a material event (with limited exceptions for national security or law enforcement impact). Combined with the instruction “time is of the essence”, an enterprise must move swiftly upon first detection of a cyber event to assess and document materiality without delay. These two legal requirements coalesce to create an expectation of more timely public disclosure that is both internally challenging and may have unintended consequences.

Frequently with any new guideline issued by the SEC, there are no rules given to Executives and Boards on what defines “**materiality**”. The SEC opted instead to suggest the “reasonable investor” test – a legal standard previously imposed by the Supreme Court – requiring materiality to be viewed through the lens of a typical investor: would the estimated impact of the attack or a series of attacks cause an investor to question buying, holding, or selling your stock? If so, you must immediately disclose on Form 8-K which becomes public information and can provoke potential negative media coverage obviously.

Notably, after detecting an indicator of compromise or breach, even the most sophisticated and well-resourced company often requires time for digital forensics and proper investigation by their incident response team to be completed. This process also engages external experts, legal counsel and potentially law enforcement, with the attendant delays those broad consultations take to complete.

While cybersecurity attacks have significant hard costs (approximately \$9M per incident for a public company according to the SEC’s own research in proposing these guidelines) the potentially more difficult impact to assess are soft costs related to incident disclosure, much less easily defined.

Companies often fear reputation and brand damage incurred from public disclosure of a cybersecurity incident more than the hard remediation and recovery expenses. In highly targeted industries, where successful attacks naturally do occur, currently they can be mitigated and responded to without the full scope of the attack ever being made **fully public**. This discretion helped companies contain soft costs and prevented or reduced reputational harm. But under the new guidelines, if the disclosure of an attack is likely to affect the public perception of your company by a reasonable investor, doesn’t practically every attack now become material? How’s that for a legal catch-22? At least until we see what starts to occur post-disclosure, how materiality was determined by the company making that report, and how the SEC responds.



But can you afford to wait for litigation to clarify all this?

Apparent SEC Objective:

The SEC wants the window of investigation and judgment shortened. While companies do not have to disclose defensive tactics as part of their filing, the timeline to disclose attacks increases scrutiny on your internal cybersecurity practices. This implies the most likely risk of early litigation will be found in gaps in the effectiveness of accelerated SOC, SIEM, SOAR and MDR processes to meet these new mandated timelines. To **enhance legal defenses**, management actions must be guided by both informed standards and frameworks (such as the AICPA's cybersecurity risk management reporting framework) and robust internal enterprise risk management and measurement frameworks to support faster and more certain incident detection, attendant decision-making and reporting.

Our Advice:

This aspect of SEC guidance becomes a mandated requirement mid-December of this year. Executive teams and boards are now on a three-month countdown to develop, implement and test new internal workflows, processes, and procedures before they are needed. As a board, mandate and fund this work immediately, using experienced external resources to provide independent advice and guidance that you can legally rely on if challenged. Then **test these for effectiveness by running an internal incident response simulation (IRS) of actual attack conditions and document the results**. While this won't guarantee you avoid early litigation on material disclosure, it is the optimal path to avoid it, and provides a valid and reliable legal defense should litigation occur. Better to be safe than sorry here.



Implications of #2: Reporting Risk Management, Strategy & Governance

The second fundamentally important shift under these new guidelines is the specific and separate scrutiny to which your cybersecurity risk management practices, strategy and governance will come under, beyond what was typically disclosed in annual reports, financial statements and attached notes.

Let's be honest: every company has gaps in their cybersecurity practices. No one can reduce the probability of a data breach to zero. As an ever-present risk, your cybersecurity maturity always required constant attention and innovation to right the balance between attackers and defenders. Now the SEC has also mandated attention on governance of those actions to defend against legal liability.

To illustrate this point, I turn to the example of cyberconIQ's own **Human Defense Platform**. We developed this platform in response to the conclusion that traditional, generic security awareness training was failing to determinedly prevent enough attacks. The proof of that? Despite companies electing universal employee security training for well over a decade, the incidents of successful human factors attacks have only increased significantly. And as perimeter security has become so much more effective, the risk of an accidental insider being the cause of a successful breach now represents **70 – 90%** of your attack risk. In the age of AI-enabled cybersecurity attacks, both the quantity and quality of attacks targeting your employees is going up, while the cost to deliver them is going down, making no organization too small to attack. So, human beings really do become our last line of defense, and we must rely on their confidence, judgment, and cyber intuition to keep us safe.

If your company has ticked the proverbial box and is training everyone, are Directors asking the question why human factor attacks are still increasing? Since that risk is growing, how do you as a company target more effort on this fast-growing attack vector? Can you prove not just that you offer security awareness training to all employees, but that you have **measured the effectiveness** of this intervention and it works? If you mandate it for employees, do you require it for all Directors? Does management compare proxy risk measures like phishing simulation failure rates to industry and global benchmarks to ensure the company is achieving its lowest practical level of human factors risk? And what is that level, why was it selected and how was it achieved and is it being maintained? These in-depth conversations with management must happen with more of a determination to map and document actual risk impact that manifests in an improved security posture, or else you risk litigation.

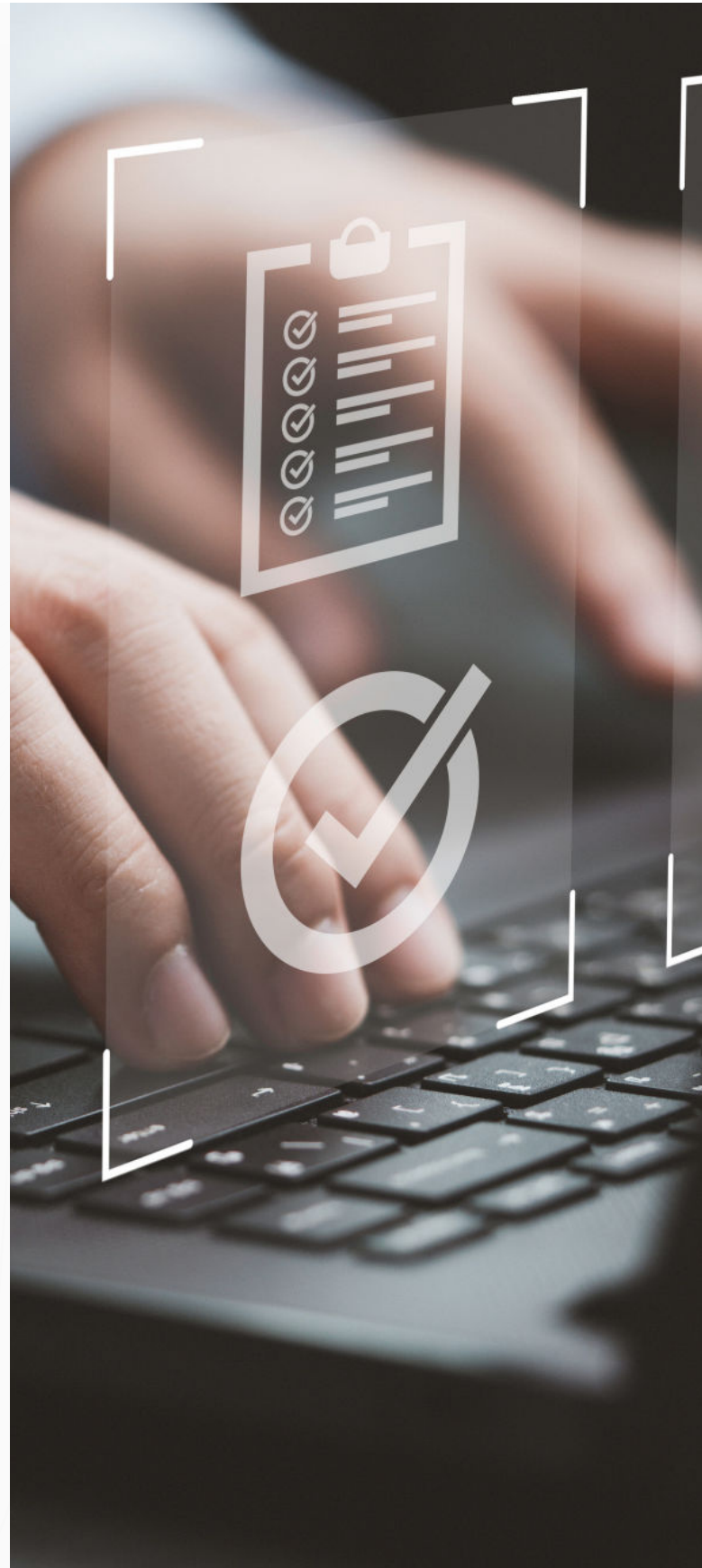


Apparent SEC Objective:

The guidelines suggest moving from an input-based to an **outcome-based risk mitigation model**. This requires a more concrete understanding of which TTP's have the highest measurable impact on reducing your cybersecurity risk exposure. This cybersecurity expertise should be resident at the board level or procured externally. A public company's Board of Directors is now expected to be able to make a specific decision regarding acceptable levels of corporate cybersecurity risk tolerance and to answer to this on the public record as part of on-going SEC reporting requirements.

Our Advice:

Immediately change the internal conversation in both the C-Suite and Boardrooms to orient everyone to measuring **results achieved** instead of just actions taken. Put more attention on prevention. Then properly **track and document** all reflections and decisions taken in board and committee minutes, including proof of tangible internal actions taken in the event of a query from the Enforcement Division. As well as an effective short-term governance strategy, this is simply best practice. Now is the time to infuse this new outcome-based approach into existing practices quickly.



Implications of #3: Managing Risk Beyond the Existing Tactical Edge

The new guidelines also infer that companies go beyond their own perimeter and accept that their level of risk has as much to do with their supply chain, vendors and extended technical architecture as it does with their own internal systems and employees. You will likely have to extend your current tactical edge outward. Cybersecurity contagions now easily flow across domains; among networks; through systems integrations; and from a growing list of new sources. Especially if you are a manufacturer, manage critical infrastructure, or are part of a highly attacked and regulated industry such as Financial Services or Healthcare, it is no longer practical to just manage your own risk. You now need to measure third party risk and have methods to assess and mitigate their direct impact on your own risk level. Yet, any cybersecurity professional will attest to the fact that reliable and easy **third-party risk assessment (TPRA)** that properly extends your risk insight beyond your current perimeter is a newer frontier.

Apparent SEC Objective:

As air-gapping and isolating infrastructure become impractical strategies in an inter-connected world (such as are now seeing emerge between OT and IT for instance), the SEC seems concerned about how companies plan to protect ourselves from the sneaky cross-domain contagions we have already seen? What constitutes risky versus rewarding systems integration and how does that amplify or mitigate co-dependent cyber risk? Of the three domains discussed herein, this one is likely the place of least certainty across the profession – never mind those tasked with governing us. So efforts to share early learning as we all consider proactively managing third party risk in our technical and physical supply chains is critical – and as of Tuesday, is now also a required practice for some.

Our Advice:

Immediately deepen internal awareness of this new legal risk across the enterprise. While existing 3rd party integrations may reduce costs and improve efficiencies, do these benefits outweigh potential security risks? How did we measure that? Should past decisions be reviewed under these new guidelines? Do you need to offer new resources, define new methods or install vendor-provided solutions to measure and manage third party risk? With active reflection and fast deliberation between management and the board, the enterprise should **document decisions** taken to support this new guideline to **immediately show effort to mitigate and manage this new risk category**. Look for easy wins to establish sector leadership here. Remember that early mitigation often dints early litigation.



Conclusion: Integration of Cybersecurity into ERM and GRC

An early implication of the new SEC guidelines – and interestingly a component from the original draft that was significantly softened on final adoption – was the requirement for all public Boards to have “internal cybersecurity expertise”. Often this requirement is associated with technical expertise; but what about the impact of psychology on online behavior? Technology is operated by humans – and how we operate wisely when online – is more important today than purely technical factors in reducing cybersecurity risk. Within our methodology, we refer to this as establishing a “security-first culture” – where a focus on culture and behavior moves employees, executives and board members from simply knowing about online risks to becoming aware of how their behaviors and choices can mitigate them.

My first reading of these SEC guidelines demands that we build security into everything we do both inside and outside the enterprise perimeter. We must consider not just the technical but also the human risks and **move beyond the checkbox** and start to deliver proven, repeatable results from methods that measurably mitigate risk. As a Board, it is time to do so proactively before your company becomes that first legal test case who sets the precedents from which the rest of us will learn.

To learn more about our Human Defense Platform and Advisory Services, please visit cyberconIQ.com and book your free consultation today.

