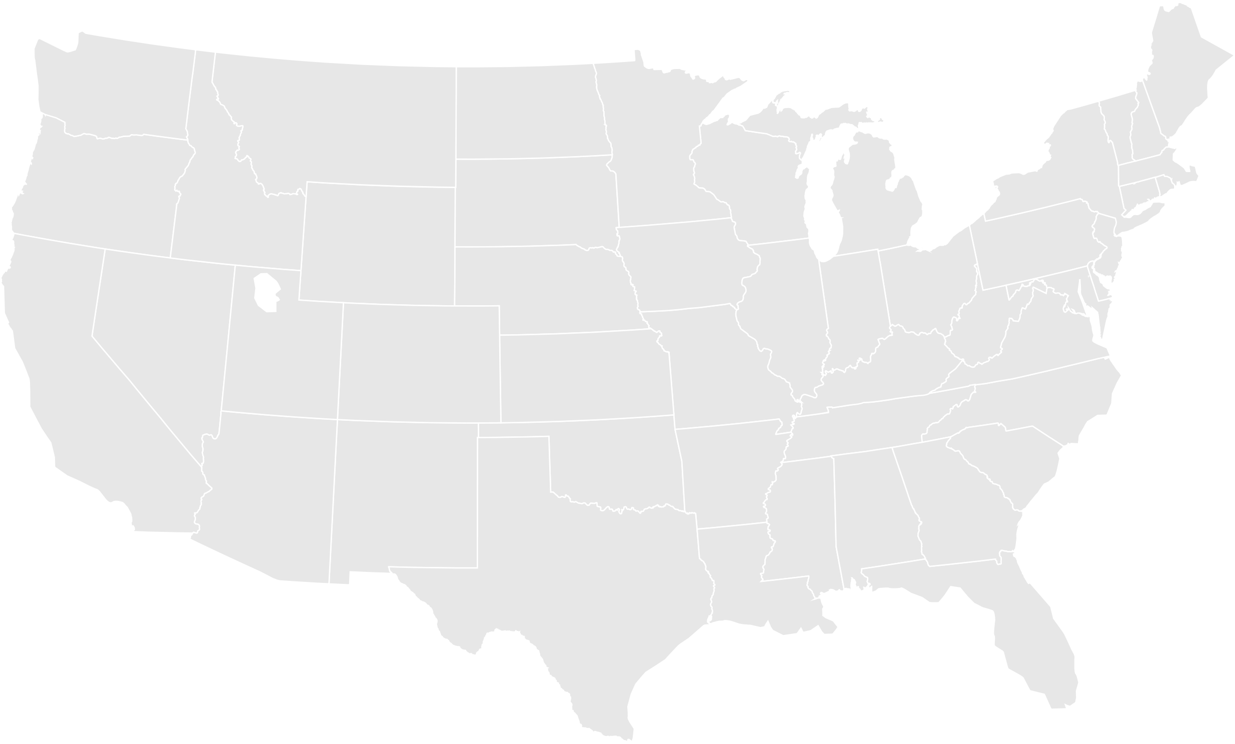
MAZEBOLT

A Comprehensive Guide to SEC Cyber Risk Management

Table of Contents



Introduction

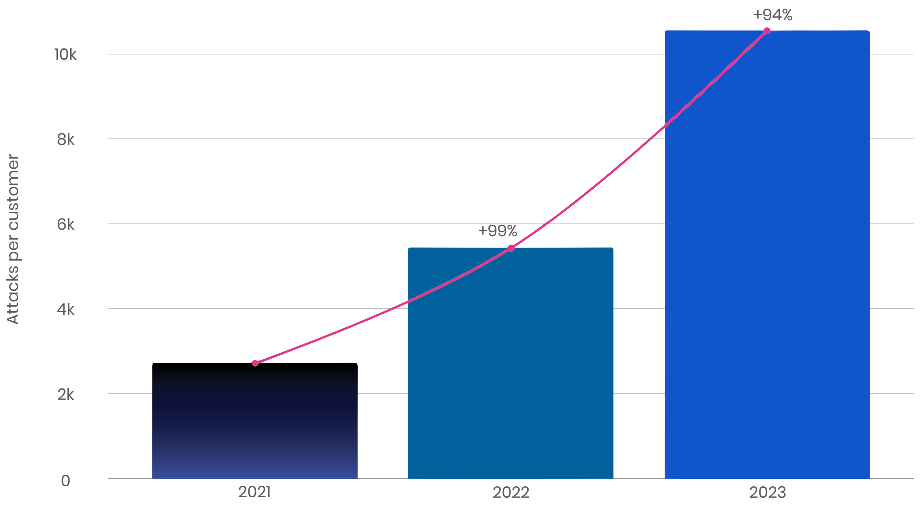
On July 26, 2023, the SEC issued a final rule that requires enhanced and standardized disclosures regarding cybersecurity risk management, strategy, governance, and incidents.

Are you prepared?

The increase in the number of cyber attacks, alongside the interconnected nature of the way organizations work means that digital resilience matters more than ever. For investors, shareholders, and consumers, companies that manage cyber risk effectively and have strategies and tools in place to support defense, mitigation and response are a far safer bet.

> ! The United States is the largest geographic target of DDoS attacks[1]

Attacks per Year (normalized per customer)



DDoS Attack Evolution (normalized per customer)

Source: Radware Threat Analysis Report 2024

Designed to encourage access to accurate and standardized information on cybersecurity risk management, the SEC's final rule is a response to the changing way we work. Today, the use of connected digital technologies, the growth in Artificial Intelligence, the shift to remote and hybrid work environments, and the increase in cybercrime has made cyber risk management more critical than ever.

The SEC's final rule establishes clear requirements for disclosing cybersecurity incidents, and changes the process for disclosures on risk management, testing and oversight. Reading its new guidelines, the final rule shines a light on the critical need for more comprehensive vulnerability testing on all online services, to reduce the growing risk of a DDoS attack, and to maintain business continuity and compliance.

[1] https://www.stationx.net/ddos-statistics/

!

94%

Increase in the average number of repeat DDoS attacks in 2023

196%

Increase in the average number of repeat DDoS attacks in 2023 in North America [2]

Who is Impacted by the SEC's Final Rule?

While SEC regulations are primarily aimed at publicly-listed companies and foreign issuers, all organizations should be paying attention. Over the past few years, the SEC has extended their governance to levy penalties and take action against private companies, such as a fine of $225,000 to privately-held energy company Monolith[3], and action against law firm Covington[4] to obtain more information about data disclosure during a cyberattack.

> According to Senior Regulatory Intelligence experts at Thomson Reuters,
> *"Although the rules primarily target publicly listed companies, other private and smaller companies should familiarize themselves with the new rules, while preparing and monitoring their operations for their own security."* [5]

In addition to direct action, as many publicly-listed companies are heavily reliant on third parties along the supply chain, all organizations should be stepping up their game on compliance and resilience.

The Benefits of Increasing Regulation for Cyber Risk Management

1 **Enhanced security:**
A regulatory framework ensures companies are better prepared to withstand, respond to, and recover from cyber disruption and threat.

2 **Reduced risk to critical infrastructure:**
With regulation compliance in place, there is less risk of disruption from cyberattacks or IT failures.

3 **Protection of sensitive data:**
Clearer laws and stronger guidelines around data protection reduces the risk of unauthorized access, data leakage and data loss.

4 **Alignment with insurance guidelines:**
With stronger resilience, businesses looking to obtain comprehensive cyber insurance can receive premium reductions.

[2] https://www.radware.com/threat-analysis-report/

[3] https://www.sec.gov/news/press-release/2023-172

[4] https://www.sec.gov/litigation/litreleases/lr-25612

[5] https://www.thomsonreuters.com/en-us/posts/government/sec-cybersecurity-rules/

What is the SEC's Final Rule?

The responsibility is now on companies to provide the SEC with accurate, standardized and relevant information regarding their cyber risk posture. Requirements can be split into three key areas, incident reporting, risk management, and governance.

Cyber incident reporting

Companies must use Form 8-K to report cybersecurity incidents that have been considered "material" within four business days. This report should include the nature of the attack, its scope and timing, and the impact on the business. Form 8-K can be amended at a later date when more information becomes available during incident response.

Security leaders need to focus on enhancing internal processes to meet the four-day disclosure requirement, and quickly manage compliance requirements when risk occurs. They should also be able to aggregate past incidents where they become material in combination.

What makes an attack material?

According to the SEC, both qualitative and quantitative analysis should be used to decide if an incident is material. This means even if there is a lack of quantifiable damage, an attack may still need to be disclosed. You should use a standardized framework to make this decision, including asking:

- Would a reasonable shareholder consider this important in making an investment decision?
- Would a reasonable investor feel the total mix of information made available has been significantly altered by this disclosure?

If the answer to either of these is yes, the SEC is likely to consider the incident material.

Cyber risk management and strategy

The SEC asks companies to describe the process in place for assessing, identifying and managing material risks in their annual 10-K filing. Companies must disclose what consultants, auditors and third parties are in place as part of risk management, and the processes in place to identify the risks of these third parties.

Companies are now asked to determine how cybersecurity threats affect or are likely to affect their business strategy, operations, and resilience. Mature companies will already be able to drive accountability over a strong cybersecurity posture, have a process in place to measure and monitor risks, and encourage regular reporting of the effectiveness of cyber programs in place.

Cyber governance

The final requirement in the SECs final rule relates to governance of cybersecurity risks. This means identifying who has oversight over risk management, whether that's the board, a specific committee, or managing agency. Companies must disclose their expertise in assessing and managing risk, and how they have implemented cybersecurity policies and procedures in line with that risk. To be ready ahead of time, companies should formalize disclosure statements, incorporate cyber risk into financial planning, and ensure robust reporting to executives.

Where Does DDoS Attack and Vulnerability Testing Come in?

The SEC is putting cyber risk under the spotlight, and inviting everyone from investors and shareholders to consumers and third parties to take a closer look.

There's no doubt that when a DDoS attack impacts business continuity and availability, this is likely to have material impact in the eyes of the SEC. Companies should develop a DDoS plan that includes the following key steps:

1 **Testing and validation of DDoS protections:**
How are your current DDoS mitigations performing, and is anything slipping through the cracks? This is the only way you can answer what threats are likely to impact your organization in line with the SEC regulations.

2 **Implementing a process for identifying and responding to DDoS attacks:**
DDoS attacks are growing in both number and sophistication. What is your process for identification and response, and is it effective enough to ensure business continuity?

3 **Documenting all DDoS incidents:**
Cyber incident reporting is a huge part of the SECs final rule. Even when incidents are not material, they will need logging and documenting, so they can be aggregated with future risk where relevant.

4 **Communicating DDoS incidents to stakeholders:**
Being transparent with stakeholders, from customers to partners and investors is an important SEC goal. To meet the guidelines for cyber governance, you need a plan in place for who is managing DDoS risk, and how.

For many, the answer to testing the resilience of the business lies in manual red team testing. However, with an emphasis on assessing, identifying and managing risk, the current approach for manual red team testing against DDoS attacks is not effective.

Companies deploy DDoS protection solutions both on premises, and in the cloud. These solutions are intended to block DDoS attacks in real time, but in reality — even the best mitigation products have intrinsic misconfigurations and vulnerabilities that can be exploited by cyber attackers. In addition, these solutions are only able to identify and remediate vulnerabilities once an attack is already happening. The sheer volume of DDoS attacks, the varied attack vectors, and the sophistication of new and emerging tools that utilize AI technologies mean that, like your network itself, the threat landscape is dynamic and ever-changing. MazeBolt research shows that even organizations that deploy DDoS protection solutions still experience 40-75% vulnerability exposure of their online services [6]. The most common reasons include misconfigurations, lack of software patching and insufficient protections deployed.

Today's businesses need compliance certification so that they can operate. The legacy approach to prove compliance was to run manual red team testing, and obtain a certificate that claimed they could withstand an attack. This would involve intentionally attacking their networks once or twice a year to test resilience, which resulted in downtime to online services.

The main problem with this approach is the limited time frame that red teams have to do their job. Once or twice each year, the business gets the approvals necessary to allow for potential business disruption, and red teams spend no more than 3-4 hours attacking with intensity. During that window, there's no way to attack all online services, as many enterprises will have hundreds in place. There's also no time to try all attack vectors on all targets. On average, red team tests may cover between 10-15 methods of attack on a singular domain. To compare, at MazeBolt we have more than 150 types of attack vectors listed in our knowledgebase, allowing thousands of simulations to be run to ensure full coverage against all DDoS attack types and trends — because any one of them could be your next attack.

In addition, the rise in AI tools is introducing endless "mutating" variants of malware code[7.] evading detection from red teams who only have time to look for what they know during a single "snapshot" in time.

While your certificate may claim that your business, data and customers are secure, in reality all you can say is you had point-in-time protection against a small number of specific DDoS variants. That's certainly not good enough for the SEC. Is it good enough for you?

> *"The ultimate objective [of the SEC final rule] should be building and employing an effective cyber-risk management program that goes beyond completing compliance checklists. Firms and companies must ensure that best practices are in place across the enterprise to prevent cyberattacks and ensure that a proper response plan is in place that effectively stops or quickly remediates real threats when attacked"* [8]
>
> **Todd Ehret, Senior Regulatory Intelligence Expert, Thomson Reuters**

[6] https://mazebolt.com/radar-testing/

[7] CSO Online, ChatGPT and Mutating Malware

[8] https://www.thomsonreuters.com/en-us/posts/

MazeBolt: Providing Business Continuity and Cyber-Resilience

With new SEC regulations in place, it's time for companies both public and private to shift their strategy from reactive to proactive.

The main reason why enterprises can't run more frequent or expansive red team testing is the fear of disruption to business continuity. MazeBolt has removed that limitation with a completely new continuous and non-disruptive approach that proactively prevents DDoS attacks. This one-of-a-kind technique gives organizations the freedom to test continuously, across all online services, and against all known attack vectors — with no downtime to online services.

If a vulnerability is detected, your company can implement our recommended mitigation steps and then test immediately to validate that the issue has been resolved.

Benefits for compliance with SEC regulations:

1. **Boosted resilience:** Simulations of tens of thousands of distinct DDoS attacks, with no disruption to business continuity.
2. **Streamlined risk management:** Continuous attack and vulnerability simulations that run 24/7 to find the gaps in current mitigation tools.
3. **Accurate reporting:** A direct view into the impact and 'materiality' of an incident, as well as a complete reporting history and logs in case of an audit
4. **A view of third-party risk:** Challenging the efficacy of third-party DDoS mitigation products, and documenting and reviewing vulnerabilities.
5. **Smart information sharing:** Partnerships with mitigation vendors offer the community a proactive approach to fixing issues once identified

The SEC's final rule impacts all publicly-listed companies in the US, as well as private companies that are connected across the supply chain. Without the right testing procedures and reporting capabilities in place — your organization may be directly in the line of fire.

Running manual red team testing once or twice a year to cover only 0.5% of your attack surface doesn't mean your online services are resilient. MazeBolt's RADAR™ does.

Assess your DDoS vulnerability rating with our free DDoS Threat Rating Tool

Learn more