C-SUITE LIABILITY AND CYBERSECURITY

Strategies for Navigating a New Era of Enforcement

Steve Cobb, CISO, SecurityScorecard
Owen Denby, General Counsel, SecurityScorecard
Justin Daniels, Shareholder, Baker Donelson

Security Scorecard

Pressure mounts for CISOs

On October 30, 2023, the U.S. Securities and Exchange Commission (SEC) charged both SolarWinds and its Chief Information Security Officer (CISO) with fraud and internal control failures related to the company's cybersecurity practices leading up to the massive, years-long "SUNBURST" cyberattack.[1]

Specifically, the charge states:

> "SolarWinds made an incomplete disclosure about the SUNBURST attack in a December 14, 2020, Form 8-K filing, following which its stock price dropped approximately 25 percent over the next two days and approximately 35% by the end of the month."

This action by the SEC highlights two recent enforcement trends:

- Increasing scrutiny on corporate cybersecurity practices
- Personal liability for C-Suite officers for gaps in those practices

The role of the CISO was already a stressful one, with significant retention issues and burnout risk. In short, the personal and professional stakes for CISOs just got higher. A recent survey reveals that 62% of CISOs are concerned about being held personally liable for cyberattacks that occur on their watch.[2]

In the following pages, we'll explore strategies that CISOs and other C-Suite executives can use to boost their organizations' cyber resilience while also protecting themselves from legal fallout.

[1] "SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures," U.S. Securities and Exchange Commission, October 2023

[2] "2023 Voice of the CISO," Proofpoint, 2023

What are the new SEC cyber rules?

Cybersecurity breaches have increased 600% over the last decade, with total costs across the U.S. economy estimated at trillions of dollars per year. As a result, regulators are turning up the heat on cybersecurity programs as well as the boardrooms and officers who oversee them.[3]

In July, the SEC announced new cybersecurity rules that require publicly traded companies in the U.S. to disclose material cybersecurity incidents within four business days of determining whether the incident is material to the company's financial performance.

To meet this requirement, the CISO must work diligently with teams and stakeholders throughout their organization (including HR, finance, legal, and more) to determine the scope and cost of an attack.

What are boardrooms, key executives, and companies supposed to do in the face of multiplying threat actors and more aggressive cybersecurity enforcement?

> "Whether a company loses a factory in a fire — or millions of files in a cybersecurity incident — it may be material to investors."[4]
>
> **Gary Gensler**
> Chairperson, U.S. Securities and Exchange Commission

[3] "SEC Adopts Final Rules on Cybersecurity Disclosure," Harvard Law School Forum on Corporate Governance, August 2023

[4] "SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures," U.S. Securities and Exchange Commission, October 2023

Establishing materiality

Cybersecurity incident response involves large amounts of pressure and incomplete information that can change hourly. The SEC cyber regulation means that public companies must have in place a methodology to evaluate if the cyber event is or is not a material one.

The regulation calls for making this determination without undue delay, and being in constant communication with all affected parties.

That means planning for and executing a documented materiality analysis needs to be in place long before an incident happens.

According to the SEC, information is considered material if **"there is a substantial likelihood that a reasonable shareholder would consider it important"** in making an investment decision, or if it would have significantly altered the total mix of information made available.

Companies should consider the following when determining materiality:

- Financial impact
- Data theft
- Asset loss
- Intellectual property loss
- Reputational damage
- Litigation risk
- Reduction in competitiveness
- Impairment of customer or vendor relationships
- Business value loss

How can a public company tailor the SEC materiality standard — and the above factors — into a documentable process, while also responding to the cyber incident, all in a timely manner?

The solution may reside with a long-standing National Institute of Standards and Technology (NIST) framework, NIST FIPS 199. Read on for more information.

What is NIST FIPS 199?

FIPS 199 is the Federal Information Processing Standards publication series of NIST, first published in 2004. The purpose of NIST FIPS 199 was to create a framework for federal agencies to categorize all information and information systems they maintain to provide appropriate levels of security based on the risk level.[5]

The main elements evaluated in FIPS 199 are:

CONFIDENTIALITY:

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

INTEGRITY:

Guarding against improper information modification or destruction of data and includes ensuring information authenticity.

AVAILABILITY:

Ensuring timely and reliable access to and use of information.

The standard is applied in the context of three potential impact levels:

1 LOW IMPACT:

The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

2 MODERATE IMPACT:

The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

3 HIGH IMPACT:

The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

In 2023, FIPS 199 can be repurposed to provide a framework that public companies can use to document a process to determine whether a cyber incident is or is not material.

On this same note, companies must think through the process of evaluating the data they get for materiality purposes to investigate further. In the event of a breach, the SEC may investigate and want to know why some pattern of network activity that resulted in a breach was not treated more seriously.

[5] "Standards for Security Categorization of Federal Information and Information Systems," National Institute of Standards, February, 2004

Moving forward with metrics that matter

Incident response requires tough decisions to be made in a pressure cooker; which is why every company would benefit from having a materiality framework. In addition, the need for objective assessment tools such as Cybersecurity Ratings for continuous monitoring of cybersecurity programs has never been more critical.[6]

Consistent and data-driven Cybersecurity Ratings enable all stakeholders to understand the vulnerabilities in their own environment as well as those of their third and fourth parties. A standard A-F grading scale streamlines cyber risk communication and empowers risk mitigation across the entire vendor ecosystem.

Security Ratings are becoming a trusted barometer of cyber resilience because they provide a standard unit of measurement and transparency. With this common language and level of insight, organizations can identify their own vulnerabilities in addition to the cyber risks posed by their suppliers and make informed decisions to strengthen their cyber defenses.

The focus on cybersecurity risk at the C-Suite will only continue to grow as the regulatory landscape expands, with the passage of laws at home and abroad (GDPR[7], DORA[8], and CCPA[9], for instance). So now is the time for organizations to **build repeatable processes and establish effective communication channels to improve safety, preserve trust, and enhance cyber resilience.**

[6] 6 Myths About Cybersecurity Ratings (and 1 Truth)," SecurityScorecard, August, 2023

[7] General Data Protection Regulation - Regulation (EU) 2016/679) - European Union, May, 2018

[8] Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554 - European Union, September, 2020

[9] California Consumer Privacy Act (CCPA) - Resolution AB-375, State of California Department of Justice, June, 2018

HOW SECURITYSCORECARD CAN HELP

About SecurityScorecard's

Partner with SecurityScorecard to maximize your executive-level reporting and cybersecurity compliance.

Remember, cybersecurity is a critical concern that impacts organizations at every level. It's important to take proactive steps to protect your organization and yourself. Implement the strategies discussed in this eBook to strengthen your cyber resilience and mitigate risks.

Our team is dedicated to helping organizations enhance their security posture and navigate the complexities of today's cybersecurity landscape.

SERVICES

Executive-level reporting

Cyber risk affects the growth and sustainability of organizations, and it's now an executive-level discussion topic. Demonstrate to boards and business leaders the value of your security program with SecurityScorecard's actionable data and reporting capabilities.

Cyber Risk Reporting

The nature of cyber risk is complex. Security leaders need to put security into the context of business problems when presenting to stakeholders. Our Cyber Risk Reporting Center enables you to easily interpret and share SecurityScorecard findings.

Cyber Risk Quantification

Cyber risk is no longer just an IT problem. Holistic conversations about the financial impact of cyber risk are needed to ensure the sustainability of the business. Start using cyber risk quantification to drive risk management strategies and translate cyber risk into dollars.

Digital Forensics & Incident Response Services

Be ready to respond to any threat confidently and mitigate business interruptions from a cyberattack by partnering with industry-leading experts in digital forensic and incident response services. Integrate data forensics and incident response (DFIR) capabilities to augment your security team's capabilities with SecurityScorecard on demand.

Tabletop Exercises

Improve your cyber readiness with real-life incident scenarios and hands-on training to respond effectively and efficiently

Board Reporting Template

Be seen as a business leader and justify your security budget to the board with the most scalable and actionable cyber risk quantification solution. Use this template to build a deck that will make you look like a champion when you report to the board on the effectiveness of your security program.

Partner with SecurityScorecard to maximize your executive-level reporting and cybersecurity compliance.

GET STARTED

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.com

United States: (800) 682-1707
International: +1(646) 809-2166