TANIUM

WHITEPAPER

# How Tanium Helps Organizations Comply with the New SEC Cyber Disclosure Requirement

CONTENTS



# Introduction

Significant new **SEC cybersecurity disclosure regulations** went into effect in December 2023 for all public companies in the U.S:

- Cybersecurity incidents must be publicly disclosed on Form 8-K, within four business days of being determined to be material
- Cybersecurity processes and governance must be disclosed annually on Form 10-K

These rules make public companies responsible for providing timely and consistent information about cyber incidents and risk management that is relevant to their investors. Structured as amendments to existing securities laws, any failure to comply with the new regulations will be subject to the same significant consequences that apply to traditional financial reporting requirements.

Even though material cyber-related items were previously required to be disclosed in accordance with general rules on communication of material information, the SEC determined a lack of uniformity and consistency around cyber disclosures combined with the growing importance of and risk surrounding information technology activities warranted a dedicated set of cyber disclosure rules.

## Overview – Disclosure of material cybersecurity incidents

Public companies are now required to disclose material cybersecurity incidents. An incident is an unauthorized occurrence impacting a company's information systems that jeopardizes the systems or the information. Information systems include those owned or used by the company, thereby encompassing incidents at third parties, such as cloud service providers. Incidents also include a series of related unauthorized occurrences, which even if not individually material, require disclosure if material when considered together. Examples of related occurrences include where the same malicious actor or same vulnerability is involved.

Materiality is not defined in the new rules, but the SEC pointed to general 'reasonable investor' standards that are used throughout existing securities laws. Thus, an incident must be deemed material when a reasonable investor would have considered it important in making an investment decision. However, the SEC specifically pointed to immediate and longer-term effects for consideration, including impact on operations, finances, brand, reputation, and customer relationships.

> "Whether a company loses a factory in a fire — or millions of files in a cybersecurity incident — it may be material to investors."

**Gary Gensler**
SEC Chair

Upon detection of an incident, the company must determine whether it is material without unreasonable delay. Once materiality is determined, the incident must be disclosed within four business days. The SEC expects the materiality determination to be made through an informed and deliberative process and not rushed. However, a lack of complete information is not a reason to delay the determination. Rather, the initial disclosure must identify information not yet obtained and that information should be disclosed in an amendment to the original filing when available.

There are only two exceptions to the 4-day disclosure requirement. First, in cases of national security or public safety, disclosure may be delayed if the US Attorney General determines that disclosure would cause a substantial risk. And for companies subject to the FCC rules on notifications of breaches of customer proprietary network information, disclosure may be delayed in accordance with those regulations.

The disclosure itself must describe the material aspects of the nature, scope, and timing of the incident and its impact on the company. The SEC intentionally focuses the required disclosure on the impact of the incident rather than its details to avoid the risk of sharing information that could be useful to bad actors.

## Overview – Disclosure of cybersecurity risk processes & governance

In addition to incident disclosure, public companies are now also required annually to describe their processes for identifying, assessing, and managing material cybersecurity risks and the governance around those processes.

The final rules focus on the disclosure of processes rather than more detailed descriptions of how a company plans for, defends against, and responds to cyberattacks, as originally proposed. Similarly, the final rules call for disclosure of "processes" rather than "policies and procedures". There was concern that disclosure of greater detail had the potential to assist threat actors. But even though those details are not required to be disclosed, it is implicit that internal written policies describing them are an important part of the risk management process.

The annual disclosure must include whether and how the processes have been integrated into the company's overall risk management activities, whether third-party services are used to support the processes, and whether the company has processes to manage cybersecurity risks in connection with any third-party service providers.

Companies must include in the disclosure how their board of directors exercises oversight of cybersecurity risk and how the board is informed of these risks. Management's role in assessing and managing these risks must be described, including their expertise and processes to understand and monitor the prevention, detection, mitigation, and remediation of incidents and whether they report information about these risks to the board or a board committee.

## Steps that should be taken by companies considering the new rules

Critical to being able to effectively implement the new incident disclosure rules is understanding how the company detects incidents, the process for escalating to those responsible for the materiality determination, and collecting the information necessary to make that judgment. Also, appropriate contemporaneous records of incidents must be kept and monitored to determine whether a series of occurrences may be related for reporting purposes and in the event of a subsequent data request from the SEC. It is also important to understand how materiality determinations will be made and whether the company is capable of disclosing the incident within four days of that determination. Importantly, these processes all need to be tested and determined to be effective.

Public companies already have disclosure controls and procedures (DCPs) in place, but they must be updated to reflect cyber disclosure requirements, including the addition of a cyber representative to the disclosure committee. In cases of potential national security or public safety impact of a cyber incident disclosure, relationships with federal law enforcement must be sufficient to escalate the dialogue in a timely manner and request a determination from the US Attorney General's office whether a disclosure delay is appropriate. The **FBI recommends** that all public companies establish a relationship with the cyber squad at their local field office.

### Example cybersecurity incident disclosure - Microsoft Corporation Form 8-K filed with the SEC on Jan. 19, 2024

**Item 1.05. Material Cybersecurity Incidents**

On January 12, 2024, Microsoft (the "Company" or "we") detected that beginning in late November 2023, a nation-state associated threat actor had gained access to and exfiltrated information from a very small percentage of employee email accounts including members of our senior leadership team and employees in our cybersecurity, legal, and other functions, on the basis of preliminary analysis. We were able to remove the threat actor's access to the email accounts on or about January 13, 2024. We are examining the information accessed to determine the impact of the incident. We also continue to investigate the extent of the incident. We have notified and are working with law enforcement. We are also notifying relevant regulatory authorities with respect to unauthorized access to personal information. As of the date of this filing, the incident has not had a material impact on the Company's operations. The Company has not yet determined whether the incident is reasonably likely to materially impact the Company's financial condition or results of operations.

## Tanium's role

To accurately disclose incidents, companies must be able to detect, correlate, and assess unauthorized occurrences. To accurately determine materiality, companies must have sufficient insight into the scope and reach of the occurrences to understand their potential impact. Companies must have access to sufficient contemporaneous data to determine when, where, and how an occurrence may have been initiated and evolved.

Similarly, in annually disclosing processes for identifying, assessing, and managing material cyber risks, a company is really describing its ability to access, assess, and react to timely, accurate data about the state of its IT environment.

These capabilities require companies to define a desired state of the environment at each of the assets, applications, files, and process levels, often done in accordance with an industry-recognized framework such as NIST or ISO. However having determined the desired state, the company must be able to monitor for deviations from that state confidently and reliably. On top of that, standard configurations across each of those layers must be defined, monitored, and maintained. To fully achieve these goals, there first must be full visibility into the entire estate across those same layers – assets, applications, files, and processes.

**"Currently, many public companies provide cybersecurity disclosure to investors. I think companies and investors alike, however, would benefit if this disclosure were made in a more consistent, comparable, and decision-useful way. Through helping to ensure that companies disclose material cybersecurity information, today's rules will benefit investors, companies, and the markets connecting them."**

**Gary Gensler**
SEC Chair

For more information please contact **Mark Millender, Global Executive Engagement** at

mark.millender@tanium.com

By relying on Tanium's Converged Endpoint Managment (XEM) platform, companies will have confidence that the desired state is being accurately monitored across the entirety of the environment, that deviations are detected quickly, and remediation is made available. Reports can be run daily on critical assets (e.g., servers) or alert in seconds, and at appropriate intervals on other assets. Deviations can automatically trigger mitigation tickets, and timely remediation can be actioned.

Importantly, when unexpected deviations from the desired state happen (i.e., an unauthorized occurrence), Tanium will provide the data to understand the nature, scope, and timing of the incident, driving both the materiality determination as well as any required disclosure. The real-time, reliable, comprehensive data will provide visibility into whether the system was breached, where the attackers went, and where they were not able to get. When new vulnerabilities or zero days are discovered, or known vulnerabilities are being exploited, Tanium can tell you whether and where those vulnerable files may exist in your environment, which versions of affected software may be present, and whether and when related patches have been deployed.

## Conclusion

The SEC has recognized that in today's digital world, IT systems are more critical and more vulnerable than ever. Given that reality, investors must be able to evaluate a company's cyber risk management approach to make a reasonable investment decision. Therefore, they must have access to current, regular, and uniform disclosures to allow that evaluation.

With Tanium comes the power of certainty – real-time visibility into every device connected to the corporate network. This includes the power to query and take action on every endpoint, at scale, instantly. In effect, the new SEC rules have significantly increased the stakes of an enterprise not having full visibility into its IT estate. Full visibility in this sense includes accurate, real-time data about every device and service that has the potential to allow an unauthorized occurrence impacting IT systems or data. While these new SEC rules are all about disclosure, inherent in the requirements is full, accurate, real-time knowledge and the ability to act on it. Tanium will deliver on both of those requirements like no other tool can.