McKinsey
& Company

Cybersecurity Practice

Cybersecurity legislation: Preparing for increased reporting and transparency

To get ready for compliance with new US regulations, companies can segment their preparation into stages and take both short- and long-term actions to increase preparedness.

by Tucker Bailey, Justin Greis, Matt Watters, and Josh Welle

© Gorodenkoff/Getty Images

June 2022

Cybersecurity incidents have been taking place for years, but most have remained out of the public spotlight until the past decade. Recent high-profile incidents that affected large numbers of everyday citizens have catapulted the issue into the national discourse and the legislative and regulatory spotlight. We are now entering a new era in cybersecurity—one in which governments, regulatory agencies, and companies around the world work to increase oversight of cybersecurity incidents.

Companies may regard new regulations as an opportunity to prepare for greater cybersecurity transparency. In the United States, two cybersecurity regulations are likely to have an impact on multiple industries in the commercial sector. First, the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), signed into law in March 2022, will require critical infrastructure companies,[1] including financial services, to report cybersecurity incidents, such as ransomware attacks, to the Cybersecurity and Infrastructure Security Agency (CISA). In addition, the US Securities and Exchange Commission (SEC) in March 2022 proposed a rule requiring publicly listed companies to report to the SEC cybersecurity incidents, their cybersecurity capabilities, and their board's cybersecurity expertise and oversight (see sidebar, "CISA and SEC will create US cybersecurity reporting requirements").

Entities in the 16 critical infrastructure sectors defined by CISA and all registrants with the SEC should consider acting now to prepare for CIRCIA and the expected SEC rule. Where appropriate, companies may consider providing their valuable input on the shape of the regulations' detailed rules as they are formed in the months ahead. Regardless of how the final regulations are put into practical enforcement, organizations can benefit from establishing or fine-tuning cyber-crisis management programs that will help prepare for increased regulatory requirements and improve their cyber-defense posture.

This article lays out the new context of cybersecurity and the contents of the anticipated new US regulations. It then proposes for a three-step approach to preparing organizations for readiness, response, and remediation.

Organizations can benefit from establishing or fine-tuning cyber-crisis management programs that will help prepare for increased regulatory requirements.

[1] Critical infrastructure sectors, as defined in Presidential Policy Directive 21, are chemicals; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

This article constitutes general business information, not legal, regulatory, or cybersecurity advice.

CISA and SEC will create US cybersecurity reporting requirements

The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), signed into law in March 2022, requires critical infrastructure companies to report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency (CISA). In addition, the US Securities and Exchange Commission (SEC) proposed a rule requiring publicly listed companies to report to the SEC cybersecurity incidents, their cybersecurity capabilities, and their board's cybersecurity expertise and oversight (see table).

	CIRCIA	**SEC cyber-disclosure rule**
Implications for companies	— Organizations need capability to report covered incidents within the required time frame — Transparency must increase; quietly paying ransom when attacked will not be an option — Stakeholders can participate in specific rulemaking, which will take place through 2025	— Incident and defense information will become publicly available to investors — Boards will likely need to understand and describe their company's cybersecurity posture — Boards will likely have to engage on cybersecurity matters more closely than ever
Affected organizations	Covered critical infrastructure entities: chemicals; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems	Publicly listed companies
Reporting requirements	— Covered cyberincidents within 72 hours — Ransomware payments within 24 hours	**Incidents** — Material cybersecurity breaches within four days of discovery — Immaterial incidents that collectively become material **Capabilities** — Existence of a cyberrisk assessment program — Board governance and oversight of cyberrisk (eg, cyber expertise of individual board members)
Penalties for noncompliance	— CISA can issue a subpoena to compel disclosure — Failure to comply can result in referral to the DOJ	Rulemaking process pending; fines are possible

This article constitutes general business information, not legal, regulatory, or cybersecurity advice.

Cybersecurity incident and response playbooks are top of mind for companies

While government organizations, companies, and private citizens have all been the targets of cybercrime in the last decade, some of the most significant compromises of essential services or information have been through attacks against large US companies:

- In 2021, a large energy supplier shut down a major eastern US fuel pipeline to control an incident in its network. Compromises to its critical business systems and the resulting shutdown brought about in fuel shortages across the eastern United States.[2]

- In 2021, a major US insurance carrier fell victim to a double extortion ransomware attack and paid millions of dollars in ransom to the threat actors. The attack shut down business systems, and thousands of records reportedly were stolen.[3]

- In 2019, attackers targeted a large financial-services firm and accessed the personal information of millions of credit card customers and applicants. The attack was enabled by a misconfigured web application firewall (WAF) that allowed the attackers to obtain the data from cloud storage services.[4]

These incidents, while notable and significant, are not isolated and are only increasing in prevalence. In 2021, the FBI received the highest number of cybercrime complaints and reported total losses in history—nearly 850,000 complaints reflecting more than $6.9 billion in losses. The preceding four years averaged about 480,000 complaints with roughly $2.95 billion in losses per year.[5] Yet these figures represent a small fraction of true crime statistics. In 2016, the FBI estimated it received complaints for only 10 to 12 percent of all cybercrimes.[6] The United Kingdom, which tracked 30,000 cyber-complaint filings in 2020, estimated it received complaints for only about 2 percent of all incidents.[7]

Why does cybercrime so often go unreported? There could be many reasons, including that victims frequently do not recognize that they were a victim of an attack or scam. Another major reason is that companies may have declined to report cybercrimes due to reputational concerns or the potential for customer or investor backlash. Companies may also have determined that paying a ransom would be an easier or faster path to resolution. However, these responses may become unavailable in the United States under CIRCIA and the SEC's planned cyber-disclosure rule.

CIRCIA and SEC regulations will change how companies address cybercrime

The CIRCIA legislation and expected SEC cyber-disclosure rule have significant implications for companies in the areas of reporting, disclosure, and governance. In addition, companies may determine they should be more engaged with government and review their insurance needs.

Reporting, disclosures, and the board

Under CIRCIA, companies in the critical-infrastructure sectors will need to establish and support a capability to report incidents within the required time frames (24 or 72 hours, depending on the event). The reporting requirements will make it impossible to pay ransom demands quietly when attacked. Therefore, it will be important

[2] Kartikay Mehrotra and William Turton, "Hackers breached Colonial Pipeline using compromised password," *Bloomberg*, June 4, 2021.
[3] Kartikay Mehrotra and William Turton, "CNA Financial paid $40 million in ransom after March cyberattack," *Bloomberg*, May 20, 2021.
[4] Jennifer Surane, "Capital One settles class-action cyber lawsuit for $190 million," *Bloomberg*, December 23, 2021.
[5] FBI Internet Crime Report, 2021.
[6] Al Baker, "An 'iceberg' of unseen crimes: Many cyber offenses go unreported," *New York Times*, February 5, 2018.
[7] Crime Survey for England and Wales, UK Office of National Statistics, 2021.

This article constitutes general business information, not legal, regulatory, or cybersecurity advice.

to establish a unified strategy for cybersecurity defense and response.

Under the SEC rules, all publicly listed companies must disclose their incident and defense information to their investors and shareholders. Board members will therefore need to understand and be able to describe—and likely defend—their company's cybersecurity posture. To do this, boards will likely have to engage on cybersecurity matters more closely than ever.

Going forward, companies could benefit from increasing their cybersecurity defense and response posture while simultaneously considering steps to prepare for compliance with pending regulations.

Disclosure criteria and transparency

Under CIRCIA and the SEC regulation, companies will also need to determine how and when to comply without sharing sensitive company information. At the present stage of the SEC rulemaking process, the proposed rule does has no hard-and-fast threshold for the materiality of cybersecurity incidents. Companies will likely need to work across their information security and legal departments to establish the threshold for reporting. Ideally, they would consider the potential need to report major cyberincidents but be able to avoid oversharing information that is not required by disclosure regulations and manage reputational risk.

Similarly, as companies comply with new reporting requirements regarding cybersecurity incident response capabilities, they need to manage the risk of oversharing their intellectual property and their cyber-defense posture. Overreporting intellectual-property risks divulging corporate secrets could enable competitors to gain a potential advantage; oversharing about cyber defenses could give hackers an opportunity to leverage the disclosed information to compromise company networks. IT and cybersecurity should collaborate with company leadership—especially chief risk officers (CROs) and legal—to enable regulatory compliance without putting the company at further risk.

Collaborative relationships and cyber insurance

Covered organizations could consider bolstering their collaboration with the government and nongovernment regulatory organizations to improve their security posture. Cybersecurity organizations could establish clear and regular reporting between their company and their local CISA point of contact. Depending on how CISA's role may evolve, working side by side with the Department of Homeland Security (DHS)[8] could help firms prepare for any regulatory questions or operational growing pains that may occur as CISA's role grows. Close contact with CISA may also be a boon to companies if CISA's new repository of cybersecurity incident information could be accessed for threat intelligence. Companies could have close contact with CISA to ingest incident information, obtaining constant, up-to-the-minute updates on cyberthreats to support making the necessary adjustments to their program.

Companies could also prepare for close collaboration with sector-specific cybersecurity organizations. CIRCIA requirements and the SEC rule may have a disparate impact on companies' cybersecurity postures, especially in the critical infrastructure sectors. Companies may want to work with their industry's information-sharing and analysis center (ISAC)[9] to determine how to improve their internal security and reporting to comply with these laws.

Finally, companies may also need to prepare for fluctuations in the prices charged by providers of cyber insurance. Depending on the level of information provided by CIRCIA and the SEC, insurance providers could have more information

[8] The White House established CISA as a subcomponent of DHS in 2018.

[9] ISACs, or information sharing and analysis centers, are "nonprofit organizations that are a resource for compiling information on cyber threats relative to critical infrastructure." "What is an ISAC?," Space ISAC, accessed on May 1, 2022.

This article constitutes general business information, not legal, regulatory, or cybersecurity advice.

As companies comply with new reporting requirements, they also need to manage the risk of oversharing their intellectual property and their cyber-defense posture.

about how they should price policies offered to individual firms. While this could improve margins for insurance providers, insured companies could see their premiums go up if they—or even their peers in a sector—have recently been hit by attacks.

Adopting an approach to readiness and preparing for compliance

While CIRCIA and SEC regulations target cyberincident reporting, reporting is but one component of a larger framework for cyberincident *readiness*, *response*, and *remediation*. Companies could increase readiness through program assurance, verifying processes and capabilities to detect and identify potential cyberattacks and create reporting infrastructure and processes. Existing processes may be exercised, tested, and refined through simulation and tabletop exercises. Companies could increase their response capability during a crisis by growing their capabilities to identify, contain, eradicate, and recover from a cyberattack. This could include (but is not limited to) establishing a crisis response nerve center, bringing in additional expertise, and having a plan for alternative support and services during an attack. During the remediation stage, companies could leverage lessons learned to consider developing cyber strategies and focusing on building cyber maturity and resilience. This could include creating a post-crisis cyber strategy and road map for undergoing a cyber transformation to boost maturity across the cybersecurity organization.

Companies that prepare to comply with new regulations may segment their preparation into three stages: (1) determining their baseline existing cybersecurity reporting capabilities, (2) identifying gaps to meet reporting requirements, and (3) developing a road map to fill existing gaps.

Ultimately, companies could consider a mix of short- and long-term actions to increase preparedness for impending regulatory requirements. Short-term actions may include the following:

— Set up a cyber-reporting cross-functional team to strategize and drive near-term actions. This team could be composed of one or two compliance/regulatory and legal experts, one or two technology/cybersecurity experts, key business leaders, and corporate-strategy experts.

— Proactively evaluate and examine the baseline for current cybersecurity reporting capabilities. Include reporting capabilities for incidents as well as cyber-defense posture (for example, board cyber expertise, governance, and oversight).

— Determine which capabilities need to be built. Define gaps in current capabilities and processes. Then establish a road map for filling those gaps within the regulatory timelines (for example, establishing processes for tracking,

This article constitutes general business information, not legal, regulatory, or cybersecurity advice.

reporting, and involving the board in the event of cyberincidents).

Longer-term actions may include these efforts:

- Establish a long-term cyber-reporting and disclosure group. This group could engage in tracking ongoing legislative CISA and SEC rulemaking processes and coordinate reporting across the business. Ensure that resources from compliance/legal, technology, key product groups, and public relations are pulled into the process and team.

- Optimize reporting processes and hire new talent as needed. Adjust processes as regulation is refined. Continue to attract talent within the company and on the board.

Along with governments, regulatory agencies, and companies around the world, the US government has joined efforts to increase oversight of cybersecurity incidents. Congress recently passed the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) to require reporting of cyberincidents, and the SEC has proposed a rule requiring publicly listed companies to report such incidents to the SEC and disclose them to investors. These new requirements have important implications for risk management and legal compliance. Companies should consider preparing for these changing requirements and adopting a framework for readiness, response, and remediation. They can do this with a three-stage approach of determining baseline capabilities, identifying gaps to meet reporting requirements, and developing a road map to fill existing gaps.

Tucker Bailey is a partner in McKinsey's Washington, DC, office; **Justin Greis** is a partner in the Chicago office; and **Matt Watters** is an associate partner in the New Jersey office, where **Josh Welle** is an engagement manager.

The authors wish to thank Peter Bacon, Marci Lacy, and Songyue Xu for their contributions to this article.

Designed by McKinsey Global Publishing

This article constitutes general business information, not legal, regulatory, or cybersecurity advice.