Increase in Cyber-Attacks Leads to Influx of New Reporting Obligations

Insights
3.31.22

In the wake of Russia's invasion of Ukraine, and amid growing concerns regarding the threat of increased cyberattacks targeting infrastructure and other critical industries, there has been a flurry of federal activity to implement new requirements for the reporting of cyber-attacks – including a new federal law that will introduce mandatory reporting obligations on many businesses. This activity impacts entities in both the public and private sector and furthers the federal government's efforts to improve the nation's cybersecurity, especially in light of the impending threat of increased cyberattacks. What do businesses need to know about the influx of legislation and regulatory activity that could soon impact your operations?

The Cyber Incident Reporting for Critical Infrastructure Act of 2022

Notably, the Cyber Incident Reporting for Critical Infrastructure Act of 2022, which was passed as part of the omnibus spending bill on March 15, requires mandatory reporting by critical infrastructure of substantial cyber incidents and ransomware payments. The Act imposes new mandatory reporting requirements for entities in the critical infrastructure sector – including those in the chemical, commercial facilities, communications, critical manufacturing, emergency services, energy, food and agriculture, healthcare and public health, and information technology areas. These reporting requirements will not be effective until the final rules are effective and published, which could take as long as 36 months.

Under the new law, these entities must report to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA):

- a covered cyber incident no later than 72 hours after the covered entity reasonably believes the incident occurred, and
- any ransom payment for a ransomware attack within 24 hours of making the payment as a result of a ransomware attack, even if the ransomware attack is not a covered cyber incident.

Reportable incidents under the Act include: (i) a substantial loss of confidentiality, integrity, or availability of a system or network; (ii) a serious impact on operational systems and processes; or (iii) a disruption of business or industrial operations.

A report of a covered cyber incident under the Act must include:

A report of a covered cyber incident under the Act must include:

- a description of the affected information systems, networks, or devices;
- a description of the unauthorized access;
- the estimated date range of the incident;
- the impact to the operations of the covered entity;
- a description of the vulnerabilities exploited and the security defenses that were in place;
- information related to each actor reasonably believed to be responsible for the cyber incident;
- the category or categories of information that were, or are reasonably believed to have been, accessed or acquired; and
- the name of the entity and its contact information.

Similar information is required for reports of ransom payments, such as:

- the type of virtual currency or other commodity requested;
- the ransom payment instructions, including information regarding where to send the payment, if applicable; and
- the amount of the ransom payment.

Supplemental reporting is also required if substantial new or different information becomes available and until the covered entity notifies CISA that the incident has concluded and has been fully mitigated and resolved. All reports will be treated as confidential and will not constitute a waiver of any applicable privilege or protection provided by law.

If CISA has reasonable grounds to believe that an entity has experienced a reportable cyber incident or made a reportable ransom payment, yet has failed to submit a required report, CISA may obtain information about the cyber incident or ransom payment by engaging the entity directly. The entity will have 72 hours to respond to CISA's request, after which time CISA may issue a subpoena. If the entity fails to comply with the subpoena, the Act allows for a referral of the matter to the U.S. Attorney General, who can then bring a regulatory enforcement action or criminal prosecution against the offending entity.

Other Cybersecurity Legislation and Regulations

The Transportation Security Administration (TSA) has also imposed mandatory reporting requirements on rail and pipeline sectors, which have been in effect since December 31, 2021. Under these reporting requirements, those entities are required to report to CISA within 24 hours of a cybersecurity incident certain information including, but not limited to: (i) the affected systems or facilities; (ii) a description of the incident; (iii) any known threat information, including information about the perpetrator, if available; (iv) a description of the impact or potential impact on operations or systems; and (v) a summary of planned or considered responses.

In addition, on March 9, the U.S. Securities and Exchange Commission (SEC) proposed new cybersecurity rules for publicly traded companies to enhance and standardize public cybersecurity disclosures. Under the SEC's proposed rule, public companies would be required to report to the agency within four business days of the determination of a material cybersecurity incident the following information: (i) when the incident was discovered and if it is ongoing; (ii) a brief description of its nature and scope; (iii) whether any data was stolen, altered, accessed, or used for unauthorized purposes; (iv) the effect of the incident on the company's operations; and (v) whether the incident has been remediated or is being remediated.

Takeaways

As noted above, the reporting requirements related to the Cyber Incident Reporting for Critical Act will not be effective until the final rules are effective and published, which could take as long as 36 months. However, the regulation of data privacy and security appears to be at the forefront of everyone's mind, and employers should act now to build effective practices to address these new and impending obligations. In light of these new laws, companies in sectors affected by the new reporting requirements should pay careful attention to the government's deadlines and reporting requirements. If you haven't already, the time is now to implement comprehensive cybersecurity risk management processes.

Conclusion

Fisher Phillips will continue to monitor any further developments in this area as they occur, so you should ensure you are subscribed to Fisher Phillips' Insight system to gather the most up-to-date information. If you have any questions regarding how cybersecurity threats could impact your organization, or best practices for mitigating the risk of those threats, please consult your Fisher Phillips attorney, the author of this Insight, or a member of Fisher Phillips' Privacy and Cyber Practice Group.

Related People

Monica Snyder Perl
Partner
617.532.9327
Email

Service Focus

Privacy and Cyber