Lightstream Cyber Security

Flash Bulletin | May 2022

Mandatory 36-Hour Breach Reporting Window for U.S. Banks

In November of 2021, the Agencies, comprised of the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), and the Federal Reserve Board (FRB), passed a regulation that requires banks to notify regulators no more than 36 hours after they identify that a security incident (that rises to the level of a "notification event") has taken place. The regulation required full compliance by May 1, 2022. FDIC-supervised banks will report incidents to their case managers while banks that are regulated by the Board of Governors of the Federal Reserve System will need to inform the board. The Agencies explain though that not every data security incident is a notification event. According to the rule, a computer-security incident is "an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores or transmits. An incident requiring subsequent notification is defined as a 'computer-security incident' that has disrupted or degraded a banking organization's operations and its ability to deliver services to a material portion of its customer base and business lines"

Business Impact

While this requirement from the FDIC, OCC, and the FRB is new, most banks have already been using a 72-hour protocol for reporting. But with an even tighter timeline, banking corporations are going to have to ensure they're reporting accurate information. Roger Grimes of KnowBe4 explains that in the rush to report quickly, more corporations will probably report inaccurately, which increases the liability risk. Banks will need to first identify if a notification event has taken place, and if they determine that's the case, they have 36 hours from then to report.

Security Impact

Financial institutions are the backbone of the U.S. economy, according to Marcus Fowler, senior vice president of strategy engagements and threats at cybersecurity AI firm Darktrace, and are one of the most targeted sectors for cybersecurity threats. By establishing a tight window for breach reporting, banks can help restrict the scale of an attack and minimize the impact, protecting the "backbone" of our economy. Attackers try to harm as many victims as possible before defenders can address the issues, so the speed of reporting is vital in combating these cyber attacks.

Take Action

1. Review the FDIC's examples of notification events and set up parameters around what is and what isn't a notification event
2. Review incident response and business continuity plans to ensure compliance with the new reporting requirement

Recommendations

Lightstream recommends reviewing the new requirements and examining current policies and processes to ensure you're compliant. Prioritize security by identifying what is a security incident and if that incident is a notification event. Use a comprehensive vulnerability management program to protect your banking corporation. We can help. Our full-stack vulnerability management programs keep you ahead of emerging threats and attackers.

References

Gov Info Security
National Law Review
American Bar Association