RGS GLOBAL ADVISORS
1441 Broadway, Suite 6057, New York, NY 10018
390 North Orange Avenue, Suite 2300, Orlando, FL 32801

The Cost of Managing Cybersecurity Risks and Related Incident Reporting

August 2022

Recently, the ABA Banking Journal reported that based on an IBM commissioned study, data breaches continue to grow costlier for financial institutions[1]. The study indicates that financial institutions on average incurred about $6 million in 2021 and 2022, and on average the direct cost of dealing with a breach increased by $250,000, compared to the cost per the prior study done in 2020-2021. In addition to the direct impact of dealing with a breach incident, is the increasing cost of implementing systems and internal controls to prevent a breach from occurring. This cost may not even include the embedded burden of complying with regulatory requirements and expectations which now requires incident determination and related reporting to regulatory authorities.

Recent Regulatory Perspective

On August 2nd, the acting Comptroller of the Currency addressed the joint meeting of the Financial and Banking Information Infrastructure Committee and the Financial Services Sector Coordinating Council. He noted that, based on the OCC's observations, most cybersecurity breaches resulted from control deficiencies, such as:

- Lack of strong authentication
- Ineffective systems configuration
- Poor patch management
- Inadequate cyber response and resilience capabilities

The acting Comptroller of the Currency also stressed the importance of reducing cyber risk by maintaining effective incident response processes and rapid recovery when preventative controls are insufficient to prevent a cyber incident from occurring. In addition, he appealed for a commitment to cooperation and collaboration for working together on streamlining the incident report and threat information sharing process, as this would contribute to strengthening collective defenses against the threats challenging the financial services sector.

[1] https://bankingjournal.aba.com/2022/07/data-breaches-grow-costlier-for-financial-institutions/

Concerns about cyber vulnerabilities continues to increase and be emphasized across all regulatory agencies. For example, in March of this year the Florida Office of Financial Regulation (OFR) issued a reminder to banks and other financial service entities about the critical importance cyber security measures are to their infrastructures and the need for responsible professionals at these institutions to stay updated on the latest cybersecurity measures and threats. This clearly signals ongoing regulatory concerns and a message of additional regulatory oversight and expectations concerning cyber controls and monitoring.

Other States such as New York, Texas and California, have separate cybersecurity regulations requiring incident reporting by the state regulated banks concerned. This is in addition to the incident identification and reporting requirements imposed by the federal regulatory agencies.

Computer-Security Incident Notification Requirements

Noted in the address by the acting Comptroller of the Currency is his appeal to collaborate around sharing of information concerning breaches and computer security incidents. The reference reinforces the incident reporting regulatory requirement rule for banking organizations and their bank service providers that became effective on April 1, 2022, with a compliance date of May 1, 2022. The final rule, issued on November 23, 2021[2], serves to provide regulatory agencies with early awareness of emerging threats to banking organizations and is intended to help in identifying potentially systemic cyber events. While this is a simple request, the actual implementation of processes and determining what constitutes an event, requires interpretation, and represents another burden distracting from core business considerations and increasing the risk of potential regulatory criticism. It also adds a responsibility to communicate with third-party service providers on this matter to address computer security incidents at these third-party vendors.

Let us review the rule reporting requirements and the definitions / guidance as to what criteria should be used in determining a reportable incident. The rule requires that, 'as soon as possible', but no later than 36 hours after a computer-security incident is identified the bank is required to notify its Federal Regulator. The agencies have specified the reporting channels, and the reporting may be done via email to incident@fdic.gov by FDIC regulated banks[3] or via email to

[2] https://www.fdic.gov/news/board-matters/2021/2021-11-17-notational-fr.pdf

[3] https://www.fdic.gov/news/financial-institution-letters/2022/fil22012.html

incident@frb.gov by banks regulated by FRB[4]. The OCC regulated banks are required to submit their reporting through BankNet[5]. As mentioned above, state-chartered banks may additionally be subject to a different incident identification and reporting requirement to their respective state regulators.

The federal rule defines a computer-security incident as an event that results in actual harm to the confidentiality, integrity, or availability of data that the systems processes, stores or transmits. As mentioned, this is a simple enough definition, however, to evaluate whether actual harm occurred is open to interpretation and judgment and there is no guidance that provides the parameters for such determinations. Therefore, there is potential for inconsistencies amongst banks in making such determinations, not to mention the cost associated with the effort. The rule continues to define an incident that would require notification without reference to a measurement of harm, stating that a 'Notification incident' is a computer-security incident that has materially disrupted or degraded, or *is reasonably likely* to materially disrupt or degrade, a banking organization's ability to continue its operations, activities, etc. The definition sets as a base-line consideration of whether the incident resulted in, or could have resulted in a material disruption or degrading of any of the following:

- Operations, activities, processes, or ability to deliver its products and services in the normal course of business
- Operations, process, or system failures that would result in a material loss of revenue, profit, or franchise value
- Any discontinuance or failure that would be a threat to the financial stability of the United States

Examples of a reportable incident provided in the rule guidance include, major computer-system failure, cyber-related interruption of services, denial of service or ransomware attack. However, these are only a few examples. In addition, third-party service providers are required to notify at least one 'bank-designated' point of contact at each of their banking organization customers. This notification is required as soon as possible after a computer security incident has occurred and meets the criteria that the incident has "materially disrupted or degraded, or is reasonably likely

[4] https://www.federalreserve.gov/supervisionreg/srletters/SR2204.htm
[5] https://www.occ.gov/news-issuances/bulletins/2022/bulletin-2022-8.html

to materially disrupt or degrade, covered services provided to such banking organization for four or more hours". While the regulation provides for notification requirements in case no 'bank-designated' point of contact exists, failure to designate a point of contact may create variance from bank's incident response plan and expose it to risks, including compliance and regulatory risks.

Noted is the vagueness of certain terms used by the rule such as, actual harm, and material which is likely to contribute to the over reporting of incidents in fear of regulatory repercussions, and therefore, could marginalize the effectiveness of this reporting, and result in underreporting by some institutions.

Recommendation Concerning Incident Reporting

We recommend that internal policies and parameters be established which defines and helps identify reportable incidents. In addition, we recommend forming a committee of key stakeholders to confirm mission critical operations, systems and a list of vendor supported systems or applications in use. Formal processes should record and evaluate all computer-security incidents for escalation as needed and consideration for reporting based on the rule criteria. Guidelines concerning materiality and measurements of harm to provide consistency in reporting should be part of the procedures developed. Policy and processes can also be measured against industry practices and be reviewed with industry experts to obtain broader insights and ideas that may be helpful.

Conclusion

Cybersecurity risk will continue to increase and as recommended above, to address incident reporting, the best way to keep costs under control is to have well formulated policies, procedures and reporting frameworks that meet regulatory requirements and align with bank's risk profile. Such efforts will provide a means for clarity and appropriate action steps when needed, saving time and having the benefit of mitigating cybersecurity related regulatory risks.

RGS Global Advisors is a leading cost-effective provider of Internal Audit, Technology Risk Management, Cybersecurity and BSA/AML/OFAC Compliance Consultancy services to Financial Institutions.

For further guidance or assistance contact us at: info@RGSGlobalAdvisors.com