Published on *The National Law Review* https://natlawreview.com

Privacy Monday – March 2, 2015: How is Your Cyber Resilience?

Article By:

Cynthia J. Larose

Welcome to March (and in the Northeast, the arrival of meterological spring is welcome indeed……)

We start this month with a question: Have you looked at your cyber resilience?

The ***Federal Financial Institutions Examination Council (FFIEC)*** recently described "cyber resilience" as an organization's ability to recover critical IT systems and resume normal business operations in the event of a cyberattack. On February 6, the FFIEC added a new Appendix J to its Business Continuity Planning booklet titled Strengthening the Resilience of Outsourced Technology Services(Guidance) which discusses the importance of cyber resilience in light of the increasing sophistication and volume of cyber threats and their ability to disrupt operations and challenge business continuity preparedness and provides recommendations for financial institutions and their services providers for addressing and mitigating cyber resilience risks and strengthening business resilience. Published in 2003, the Business Continuity Planning booklet is one of a series of booklets that comprise the FFIEC Information Technology (IT) Examination Handbook and provides guidance to assist field examiners from the FFIEC member agencies in evaluating financial institution and service provider risk management processes to ensure the availability of critical financial services. The FFIEC has also set up a cybersecurity awareness website and in the past year piloted a cybersecurity assessment program at a number of financial institutions across the country. Although these most directly apply to financial institutions and their service providers, the question of cyber resilience is critical to every organization.

So what are cyber resilience risks?

The Guidance identifies the following five (5) cyber resilience risks and recommends that financial institutions and their services providers address these risks in their respective business continuity plans to ensure that appropriate resilience capabilities are in place:

1. **Malware Attacks**: to strengthen resilience against malware threats, the FFIEC recommends, in addition to the traditional signature-based anti-malware systems, implementing a layered anti-malware strategy, including integrity checks, anomaly detection, system behavior monitoring, and security awareness training for employees;

2. **Insider Threats**: to strengthen resilience against insider threats, the FFIEC recommends controls such as employee screening, segregation of duties, and dual controls.

3. **Communications Infrastructure Disruptions**: to strengthen resilience against cyber attacks that target underlying infrastructure directly and disrupt communications, such as denial of service (DDoS) attacks the FFIEC recommends that financial institutions plan for alternate communications infrastructure via an independent redundant infrastructure, however the FFIEC member agencies acknowledge that complete data communications resilience may be difficult to achieve;

4. **Data or Systems Destruction and Corruption**: to strengthen resilience against data destruction (e., data is erased or rendered unusable) and data corruption (i.e., data is altered without authorization), the FFIEC recommends using measures such as data replication (to be effective, this strategy requires appropriate redundancy controls and segregation of replicated data files to ensure that replicated data cannot be destroyed or corrupted in an attack on production data), an air-gapped data back-up architecture (i.e., physically separating a computer, system, or network from other computers, systems, or networks), and periodic read-only data back-ups (i.e., transmission of data to a physically and logically separate read-only backup location); and

5. **Simultaneous Attacks on Financial Institutions and Service Providers**: to strengthen resilience against a cyber attack targeting both a financial institution and its service provider(s), the FFIEC recommends that financial institutions and their service providers consider the possibility of such an attack in their business resilience planning, including their recovery and testing procedures.

How can you achieve cyber resilience or improve your cyber resilience?

In addition to the controls discussed above, the Guidance lists the following mitigating controls that should be considered and implemented by financial institutions and their service providers to achieve and/or improve cyber resilience:

1. Data backup architectures and technology that minimize the potential for data destruction and corruption;

2. Data integrity controls, such as check sums;

3. Independent, redundant alternative communications providers;

4. Layered anti-malware strategy;

5. Enhanced disaster recovery planning to include the possibility of simultaneous attacks;

6. Increased awareness of potential insider threats;

7. Enhanced incident response plans reflecting the current threat landscape; and

8. Prearranged third-party forensic and incident management services.

In addition to cyber resilience, the Guidance discusses three (3) other key elements of business continuity planning that financial institution should address to ensure they are contracting with service providers that are strengthening the resilience of outsourced technology services:

1. Third-Party Management: this element addresses a financial institution management's responsibility to control the business continuity risks associated with its service providers and their subcontractors and involves due diligence procedures, regular monitoring, and strategic, integrative considerations with service providers;

2. Third-Party Capacity: this element addresses service provider's abilities to deliver essential services under adverse scenarios and considers the potential impact of a significant disruption on a service provider's ability to restore services to multiple clients; and

3. Testing with Service Providers: this element addresses the importance of validating business continuity plans with service providers and involves testing the business continuity resilience among the financial institution and service providers, in addition to the review of test results and remediation of any observed weaknesses; and

A financial institution's and its service providers' ability to respond effectively to a cyber attack is critical to operational resilience and preparedness is key. Financial institutions should consider the cyber resilience risks and controls discussed above, incorporate them into their business continuity plans, as appropriate, and periodically test their ability to resume normal operations after a cyber attack. It is equally critical that financial institutions impose these requirements on their third-party service providers, since, as noted in the Guidance, "regardless of whether the systems and resilience capabilities are managed by the financial institution or TSP, the financial institution's management and board are responsible for the oversight and assurance of continuing operations in a timely manner."

National Law Review, Volume V, Number 61