NCUA
National Credit Union Administration

Office of Examination & Insurance (E&I)

October 2020 Board Presentation

Cybersecurity Considerations for the Board of Directors During COVID-19

Presented by Johnny E. Davis Jr. (Special Advisory to the Chairman for Cybersecurity) and Division Director, Critical Infrastructure

COVID-19 Related Cyber-Attacks

Phishing and Malspam

Description: Digital forms of social engineering leveraging fake emails to acquire user information.

- **Quick Tips:** Exercise caution when opening emails about COVID-19, especially those from outside the organization. Exercise caution when entering credentials into a website, linked from an email, text message, or social media account, or when downloading attachments.

Credential Stuffing

Description: Automated injection of breached username/password pairs to fraudulently gain access to user accounts.

- **Quick Tips:** Utilize Multi-Factor Authentication (MFA) and/or make sure all passwords are secure and never reuse passwords on different accounts.

Ransomware

Description: A type of malware that attempts to deny access to a user's data usually by hackers encrypting the data until a ransom is paid.

- **Quick Tips:** Implemented, maintain and monitor cyber hygiene mitigation solutions to include training, test and exercise techniques; network segmentation; and sound backup, replication and recovery practices

RDP Targeting

Description: Within Port, Protocol and Service Management (PPSM), Remote Desktop Protocol allows an attack to remotely control another computer which makes it a great target for remote works hacks.

- **Quick Tips:** Even though your workforce needs to access systems remotely, limited and secure access by VPN can reduce the attack surface.

Unintentional DDoS Attacks

Description: Overwhelming networks, websites and online services with a goal of rendering the resource inoperable.

- **Quick Tips:** Have increased bandwidth allocations ready, temporarily disable unused services to allow for more bandwidth, and discourage your employees from streaming videos, music, or other streaming services through the VPN.

Common Root Causes: *Social Engineering (COVID-19 Themes) and Cyber Hygiene Exploitation*

Leveraged Source: Center for Internet Security

Business Continuity Questions

Have business impact and business process scenarios been reviewed and revised in the continuity plans based on the operating conditions of COVID-19?

How is the IT/cybersecurity function changing its priorities in the short, mid, and long-term to address the potential impacts to the critical business services and key assets?

Are resources (people, budget and technology/services) sufficient to achieve these priorities?

Have offsite data backup, replication and storage solutions been tested and verified in the event of a major impact to business operations, continuity and recovery strategies?

Cyber Hygiene Questions

How are policies and procedures related to remote access being strengthened to address the heightened risks created by employees working from home?

Have network port, protocol and application services been reviewed and limited to only those capabilities required to meet business and operational requirements?

Have policies and procedures been updated and communicated to ensure standard, normal and emergency configuration and change management practices are properly vetted and approved?

What actions have been taken to educate employees—the first line of defense—about how to identify and react to the latest social engineering schemes?

Incident/Breach Management Questions

Has the incident management plan been updated for leadership and employees in a remote working environment?

What actions have been taken to increase detection and monitoring controls for identifying malicious activity on networks, systems and endpoints?

How secure are the emerging utilized communications and collaboration capabilities?

Digital Strategy Questions

How is business changing its strategic priorities in the short, mid, and long-term to address the potential change to norms?

Have secure data management strategies been reviewed to reflect the potential normalization of a predominant remote workforce?

Have consumer experience via increased remote services delivery models been reviewed for secure operational efficiencies?

Cybersecurity Considerations for the Board of Directors During COVID-19

THANK YOU