Cyber Security: Four critical steps to take now

It's no secret that the financial services industry is a prime target for cyber criminals. According to the NetDiligence Cyber Claims Study, which surveyed cyber liability insurance providers, hacks of financial data are second only to healthcare at 17% (of all data hacks) vs. 21% respectively. Credit unions of all asset sizes are at risk and that same survey found that 71% of all submitted claims came from organizations with annual revenues under $2 billion.[i]

What should credit unions be doing now to protect themselves? The following steps are critical.

Conduct a thorough risk assessment—then update it as needed based on changes to the threat environment and when offering new products and services. In fulfilling their responsibility to develop a written information security program under NCUA rules, credit unions should perform a thorough risk assessment designed to:

- Identify internal and external threats that could result in unauthorized access to member information systems and member information;
- Assess the likelihood and potential damage of these threats; and
- Evaluate if existing protection measures are sufficient to mitigate these risks.

Use the FFIEC tool to gauge and improve preparedness. To help assess their cyber risks and gauge their level of cybersecurity preparedness, credit unions should use the Cybersecurity Assessment Tool (Tool) from the Federal Financial Institutions Examination Council (FFIEC). The Tool incorporates concepts and principles contained in the FFIEC IT Examination Handbook, the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, and industry-accepted cybersecurity practices. Although the Tool is considered voluntary at present, the NCUA has said its examiners are being trained on the Tool and will start using it when examining credit unions in the summer of 2016.

Completing the Tool is a two-step process:

- Credit unions first determine their *Inherent Risk Profile* before implementing controls across five categories: technologies and connection types, delivery channels, online/mobile products, organizational characteristics, and external threats.
- Credit unions then assess their *Cybersecurity Maturity Level* within five domains: cyber risk management and oversight, threat intelligence and collaboration, cybersecurity controls, external dependency management, and cyber incidence and resilience.

After completing these steps, credit unions should ensure their Cybersecurity Maturity Level is properly aligned with their Inherent Risk Profile.

Investigate insurance. It's impossible to entirely eliminate the risk of a cyber–attack. Credit unions should ensure they have adequate insurance coverage to address cyber exposures. Cyber policies are typically designed to protect the credit union in two areas: third-party claims (lawsuits against the credit union that may arise as a result of a data breach) and first-party claims (credit union expenses to cover the costs to recover from a breach, such as forensics, notifications, public relations expenses, and credit monitoring).

Connect with other financial institutions. Information sharing and collaboration are critical strategies to improve data security. Financial services firms that participate in information sharing forums have been shown to be better prepared to identify vulnerabilities and attack methods and have successfully mitigated cyber attacks on their systems.[ii] One great resource to investigate is the Financial Services Information Sharing and Analysis Center (FS-ISAC).

For more information on addressing your cyber security challenges, contact your CUNA Mutual Group Sales Executive at 1-800-356-2644

Resources:

- Please visit NCUA's Cyber Security Resources page for a wealth of helpful information on this topic.

[i] NetDiligence 2015 Cyber Claims Study

[ii] Federal Financial Institutions Examination Council "Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement" https://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Statement.pdf