Bank Regulators Dial Up Concerns About Cyber-Attacks

By Thomas A. Brooks / Nov 06, 2015

Because of the concern from banking regulators about the risk to financial institutions from the increasing frequency and severity of cyber-attacks involving extortion, the Federal Financial Institutions Examination Council (FFIEC)[1], on behalf of its members, has advised institutions that they should develop and implement effective programs to ensure that they are able to identify, protect, detect, respond to, and recover from these types of attacks.

The statement from the FFIEC, and subsequently repeated by its members to institutions they regulate, does not establish new regulations or guidance relating to protection against cyber-attacks. Rather, it is a strong reminder of the regulators' heightened concerns about cyber-attacks relating to extortion resulting from ransomware, denial of service and theft of sensitive business and customer information to extort payment or other concessions from victims.

The FFIEC reminds financial institutions that they face a variety of risks from cyber-attacks involving extortion, including liquidity, capital, operational, compliance and reputation risks, resulting from fraud, data loss, and disruption of customer service. It advises that financial institutions should ensure that their risk management processes and business continuity planning address the risks from these types of cyber-attacks.

To protect against the increased frequency and severity of potential cyber-attacks involving extortion, the FFIEC recommends that financial institutions consider taking the following steps:

- Conduct ongoing information security risk assessments.
- Securely configure systems and services.
- Protect against unauthorized access.
- Perform security monitoring, prevention and risk mitigation.
- Update information security awareness and training programs, as necessary, to include cyber-attacks involving extortion.
- Implement and regularly test controls around critical systems.
- Review, update and test incident response and business continuity plans periodically.
- Participate in industry information-sharing programs.

If a financial institution is a victim of a cyber-attack involving extortion, whether or not it results in unauthorized access to sensitive customer information, the FFIEC advises that the institution should report the event to law enforcement authorities as well as its primary regulator. Whether or not a suspicious activity report is required to be filed, the institution should consider doing so in order to aid law enforcement authorities in protecting the financial sector.

For more information regarding this issue, please contact Tom Brooks at tbrooks@clarkhill.com.