NEXT-GEN BANKING

Are You Viewing Cyber Risk Across the Enterprise?

From insider threats to third-party vulnerabilities, community banks must tackle the rising challenge and costs of protecting customer information.

In 2017, we have seen a wave of sophisticated cyber attacks and data breaches. September alone saw the Equifax breach of 145 million Americans' information, Deloitte's breach through an internal email platform and the SEC's disclosure of a hack that may have enabled illegal trades. Noting that intrusions will continue in both the public and private sectors, SEC Chairman Jay Clayton said, "A key component of cyber-risk management is resilience and recovery."

But how can you be resilient when attacks continuously evolve, compliance demands grow, digital ecosystems expand and resources for protecting data cannot keep pace? Community banks are increasingly looking for better, more cost-effective solutions. A first step is to view cyber risk as part of an Enterprise Risk Management (ERM) strategy. By doing so, banks elevate cybersecurity as a top concern for all departments, and can prioritize resources to those areas most in need.

REGULATORY FOCUS ON THIRD PARTIES

Regulators are increasing demands on banks, including greater board oversight, hiring of information security officers, and proof that the large number of third-party vendors now frequently involved in critical activities are being assessed, monitored and managed. There is an urgent need for economical solutions that answer crucial questions such as:

1) How do I know I'm assessing what's necessary to be compliant and managing the risk appropriately?
2) How do I ensure that vendors are assessed uniformly?
3) How do I risk-score vendors?
4) How do I monitor vendors' performance?

ENTERPRISE SECURITY PROGRAM

For community banks, vendor risk is compounded by substantial resource and budget constraints that hamper the implementation of a robust information security program, especially one that includes both defensive measures to protect non-public information and implements plans to recover from potential cybersecurity events.

"Managing cyber risk doesn't have to 'break the bank!' There are efficient, scalable solutions that help community banks understand and mitigate vulnerabilities."

– DAVID COTNEY,
ADVISOR, FORMER COMMISSIONER
OF BANKS, MASS

Allow CyberFortis-TSC, powered by its proprietary Secure Halo™ platform, to help provide a cost-effective and comprehensive suite of services to help community banks address these challenges now:

- Secure Halo™ enterprise security assessments that are mapped to NIST and international standards to improve cyber posture, mitigate vendor risk and qualify for cyber insurance.
- Advisory services that include compliance readiness, security program development and training.
- Professional and managed security services that utilize leading vulnerability management products.
- Founders with extensive financial services expertise who understand the needs of the community bank industry.

As you consider your security program development and management, CyberFortis-TSC can be a helpful resource. With more than a decade of experience protecting critical assets of the federal government and Fortune 500 companies, CyberFortis-TSC delivers mission-critical, economical solutions for community banks. Contact us. Free assessment of your cybersecurity maturity to first 20 respondents.

CYBER FORTIS

962 Wayne Ave, Suite 900, Silver Spring, MD 20902
617-429-1755 | www.cyberfortis.com