CONNECT | SOLUTIONS ISSUE | NEW FALL PROGRAMMING

GEORGIA

COMMUNITIES FIRST

SEPT/OCT 2022

Taking Charge!

Cyber Risk Pro's on Staying Ahead of Threats

Official Publication of the
CBA
COMMUNITY BANKERS
ASSOCIATION OF GEORGIA

Member:
ICBA
Independent Community Bankers of America

Cyber Risk: Are you Complacent or Proactive?

As your financial institution broadens the use of technology to become more competitive and efficient, you become increasingly more susceptible to cyberattacks. Hackers continuously exploit these new opportunities to breach your systems. This constantly changing environment makes it imperative that you operate with a proactive mindset instead of reacting when the attack happens. When a champion boxer steps into the ring, he isn't just walking into a fight. He's come primed for battle. He has spent months training, assessing his opponent, and devising a strategy in preparation to win. He doesn't just take the punches; he goes on the attack. It is essential for financial institutions to do the same in the face of cyberattacks. Organizations need to reevaluate their strategy for cybersecurity and move beyond mitigating a breach after it occurs.

How can financial institutions approach cybersecurity differently and more effectively?

At DefenseStorm, we encourage financial institutions to change their way of approaching risk management with a fresh perspective, putting readiness at the forefront. We use the 4 C's as a method for reevaluating how to manage cyber risk: Continuous, Consistent, Centralized and Clear. Identification and assessment of potential threats must be continuously exercised in real-time as they materialize. A one and done approach to risk assessment doesn't allow institutions to assess new risks as they emerge, leaving them vulnerable. Implementing a consistent means for evaluating risks as well as uniform application, scoring, and evidencing of internal controls within a centralized platform ensures data accuracy and integrity. Lastly, gain a clear picture of how the institution's risk profile has evolved over time by leveraging robust audit logs, dashboards, and reporting.

In a recent speech to the financial sector, Acting Comptroller of the Currency, Michael J. Hsu, raised his concern that what has been good enough will not be sufficient going forward, and that there is work to be done. Stating that "success can breed a false sense of security," he urged that financial institutions "cannot be complacent. In a world of constantly evolving threats, vigilance must be maintained," particularly with the "increasingly complex dependencies in the provision of financial services."

How can financial institutions fortify their cyber defenses proactively?

1. Understand that complacency is a risk in itself. Relying on a static method of security and believing that it is sufficient exposes financial infrastructures to threats. Ensure your program is evolving at a pace commensurate with the evolving threat landscape.
2. Establish awareness of where and why the majority of breaches occur. This will allow your cybersecurity team to create a more strategy for preventative controls. Leverage information sharing partnerships and open dialogue with contacts in the public and private sectors to collectively recognize, assess, share, and address cyber threats.
3. Employ ongoing assurance testing methods. Put ongoing monitoring and testing programs in place to identify and remediate deficiencies and gaps in your program in a timely manner.

Your Institution Can Achieve Cyber Risk Readiness

Many financial institutions now partner with cybersecurity companies who can assist with 24/7 monitoring for cyber threat detection and investigation. Outside Security Operation Centers (SOC) focus on maintaining security while lessening the burden on the financial institution so they can prioritize daily business functions. Partnering with a proficient credentialed resource to assess and evaluate threats gives financial institutions an advantage in the war against cyberattacks.

As technological advancements continue to revolutionize the financial industry, the threat of cyber attacks equally gain momentum. By altering perspective, implementing a proactive plan, and approaching cybersecurity with a collaborative effort, financial institutions are prepared to triumph against malicious acts.

Steve Soukup
Chief Executive Officer
DefenseStorm

DEFENSESTORM®

CBA COMMUNITY BANKERS ASSOCIATION OF GEORGIA GOLD PROVIDER