Implications of Cybercrime; Is Your Financial Institution Properly Covered?

By Kellie Lowder
Senior Advisor
Engage fi (Formerly CU Engage)

Cybercrime is on the rise and has completely disrupted the financial industry. *Forbes* recently reported that businesses suffer ransomware attacks every 40 seconds. Phishing emails cause two-thirds of ransomware infections, and every year, these attacks generate an estimated $1billion in revenue for cybercriminals.

While financial institutions have applied advanced security measures and devoted resources to protect all assets, including customer data, mitigating the risk cannot always eliminate a cyber-attack. The Coveware Quarterly Report estimates that more than 70 percent of attacks are on businesses with between 11 and 1,000 employees. These criminals aren't just after big business; they have found an easy way to target small to medium-sized businesses that are more vulnerable by demanding an average ransomware payment of $228,200 in Q2 of 2022. Add the fact that the average time to fully recover is 24 days, and these attacks can immobilize any financial institution.

One critical piece to a successful cybersecurity strategy is to have a proper insurance policy in place in the event something happens.

Cyber Liability Insurance
Cyber liability insurance coverage protects your financial institution against such cyber incidents. Risks covered can include:

- Cyber extortion
- Identity theft
- Business interruption
- Lost or corrupted data
- Reputation recovery
- Notification expenses

Cyber policies have been in existence for about a decade, but significant claims activity only began about three years ago. As a result, carriers are increasingly selective about who they will underwrite, policy limits have decreased, and loss deductibles have increased. Adding to the difficulty of

ensuring that your financial institution has adequate coverage, the overall cost of cyber liability insurance has soared year-over-year due to the increase in claims and unpredictability of the future. There is also a growing list of requirements to maintain coverage, such as providing extensive documentation and proof of Multi-factor Authentication (MFA). In some cases, a financial institution cannot obtain the proper insurance coverage without demonstrating the use of MFA's across the organization.

Don't Take Your Cyber Liability Policy for Granted

As with most insurance policies, financial institution cyber liability policies are unique to each insurance carrier and must be evaluated carefully. The following questions should be considered when talking about cyberbanking insurance:

- What is a sufficient limit of liability for my financial institution?
- What deductibles and rate increases are expected in today's market?
- How am I impacted under the Acts of War clause, given the current situation with Russia and Ukraine?
- What changes are on the horizon for how ransomware payments are handled? How is the new Cyber Information Sharing Act (CISA) legislation going to impact the decisions we make around paying ransoms and reporting them?
- What options are there for legal support and breach response available to my financial institution?

The stakes are high. Financial institutions are significant targets for cybercrime. According to global cybersecurity leader Trend Micro Incorporated, the banking industry experienced a 1,318% year-over-year increase in ransomware attacks.

In short, a proactive approach with a recovery plan in place is critical to protecting your financial institution against an attack. Cyber insurance will help to mitigate your risk but consider adding a third-party consultant to your strategy who can assist you in navigating the market alternatives and help prioritize coverage based on the specific needs of your financial institution.

As cybercrimes continue to increase in frequency and sophistication, financial institutions are working tirelessly to stay on top of quickly evolving situations. However, a consultant with experience and knowledge of your industry can work with your team to ensure you have the right protection in the unfortunate event that your systems or data are compromised.

Kellie Lowder brings almost three decades of experience working with FI's to help them achieve their goals. Prior to joining Engage fi, Kellie was functioning as a partner to our team while growing and managing her own consulting firm. Her passion for insurance comes from working with clients across the US as an executive at SWBC for almost fifteen years prior to starting her own firm. As senior advisor, Kellie is working with our team to build a new line of business to serve our clients' insurance needs. She will utilize her expertise to consult with financial institutions as they navigate key insurance decisions and negotiations.

To schedule a time to speak with Kellie or one of our other consultants about your financial institution's cyber security strategy, please call us at (844) 415-7962 or click here to book a call online.

Email
info@engagefi.com
www.engagefi.com

Phone
844.415.7962

Address
5550 W Executive Drive, Ste 540
Tampa, FL 33609