GEORGIA
COMMUNITIES FIRST

WINTER 2023

BANKING
IN THE LEGISLATURE

Official Publication of the
CBA
COMMUNITY BANKERS
ASSOCIATION OF GEORGIA

Member:
ICBA

LEGISLATIVE SESSION | PROFESSIONAL DEVELOPMENT PROGRAMS | 2023 SCHOLARSHIPS

The Cost of Cyberattacks:

How much should you spend in Cybersecurity?

As we embark on a new year, warnings about devastating cyber attacks on the financial sector are making headlines. The urgency for financial institutions (FIs) to strengthen their cybersecurity measures and safeguard assets is fueled by the increasingly brazen attacks by cyber criminals. Along with evolving cyber threats comes the rumor of a potential recession, and budget cuts are imminent in anticipation of a decline in the economy. However, where you shouldn't see cut backs is in the cybersecurity department. Instead, banks should be ready to evaluate and invest in fortifying their cyber defenses because the cost of an attack is just too great.

The cost of cyber attacks

According to IBM, in their report Cost of a Data Breach 2022, "Reaching an all-time high, the cost of a data breach averaged USD 4.35 million in 2022. This figure represents a 2.6% increase from last year, when the average cost of a breach was USD 4.24 million. The average cost has climbed 12.7% from USD 3.86 million in the 2020 report." Given those statistics, financial institutions need to ask themselves: How much risk am I willing to incur? With the rising threat of cyber attacks, banks must weigh the financial and reputational impact of breaches versus the investment in more effective protection methods. Consider this: banks that succumb to a cyber attack suffer monetary theft, disruptions to service, hefty non-compliance fines, and compromised sensitive client data resulting in damage to their reputation. When the collective impact is measured, banks are realizing that they can't afford to NOT invest in cybersecurity solutions.

How much should I spend on cybersecurity?

Budget is always the first question when it comes to bolstering cybersecurity. Before you start crunching numbers with the CFO, understand that setting a specific budget to spend on cyber risk management BEFORE deciphering your bank's needs is not the most efficient first step. Banks should first conduct a thorough cyber risk assessment to understand the financial investment needed to prevent, detect, and respond to cyberattacks. You wouldn't expect a mechanic to tell you how much it's going to cost to repair your car before he peeks under the hood, and the same process applies to cyber risk management. So, let's discuss how to identify the magic number.

Understanding your cyber risk to get the most bang for your buck.

Estimating a cybersecurity budget and throwing it into a one-size fits all security plan without proper guidance won't get you the tailored solutions necessary for your bank. Ultimately, it could result in paying more for products and services your bank doesn't need or will even use. Through a comprehensive risk assessment, your FI can identify the right combination of resources to address its precise security vulnerabilities. During this process you'll also gain valuable insight into existing capabilities and deficiencies that impact detection, response, recovery, and resilience when faced with a breach. Implementing an approach based on aggregated data about your bank's particular cyber risk landscape improves how you prevent a malicious attack or respond and reduce the impact of one.

Start by securing a partnership with a cybersecurity company well-versed in the unique challenges and regulations financial institutions face. Once you have an ally in the fight against cybercrime, the risk assessment is completed and evaluated. Your data will determine exactly what your bank needs to stay cyber risk ready. Then, an appropriate budget and allocation of funds is established so you can prioritize and invest in the most accurate, necessary, and effective solutions.

Cybersecurity planning can seem like a daunting financial burden. However, with guidance from an industry expert to create a strategic plan that is designed to address your bank's cyber risk needs, the value of your budget is maximized, and a powerful approach is created to stop attacks before they happen.

Steve Soukup
CEO
DefenseStorm

DefenseStorm®

CBA
COMMUNITY BANKERS ASSOCIATION OF GEORGIA
GOLD PROVIDER