LIONFISH CYBER SECURITY™

A USE CASE SCENARIO

Comprehensive Cyber Security Readiness and Protection for Small & Mid-Sized Businesses

Banks Especially Vulnerable During COVID-19 Pandemic

Threat actors will continue to target banks into the future. Paul Benda, SVP for risk and cybersecurity policy at the American Banker's Association, says phishing has increased more than 400 percent since COVID-19 hit, according to a January 2021 report in the ABA Banking Journal.

And, according to the Deloitte Center for Financial Services Global Outlook Survey 2020, 71% of bank leaders expect their organizations to increase cybersecurity spending, with cloud computing/storage and data privacy rounding out the top three areas of needed improvement to combat the risk of data breaches. That's why Lionfish Cyber Security exists as a managed security services provider (MSSP) to be your partner in fighting cybercrime.

Security research data suggests that malicious intent can be captured with solid cybersecurity awareness, prevention and security best practices a part of your banking culture. Lionfish provides task management and expertise when you need it, to augment your team and set your planning up to be regular and consistent.

A Banker's Goal: Increased Risk Management, Compliance, & To Protect Essential Operations

Our Company Mission:

To provide best-in-class cyber security protection for small and medium-sized businesses by strategically aligning our By With and Through Platform™ as a force multiplier to navigate today's cyber threat landscape.

The Financial Industry's Dilemma:

*The financial services industry takes in the highest cost from cybercrime at an average of $18.3 million per company surveyed, reported Accenture recently. Various reports indicate that breaches to financial service firms can take an average of 98 to 233 days to detect.

*Common breaches occur because of phishing, third-party file-sharing services, manipulated data, and ransomware—all leading to financial loss. Financial firms are 300 times more likely than other institutions to experience cyber breaches, according to the Boston Consulting Group.

*Banking applications for the paycheck protection program were even hacked at Charlotte-based Bank of America in 2020, during this pandemic.

What is needed is additional employee training, cybersecurity risk assessment, proper vendor due diligence, and cybersecurity monitoring on an ongoing basis.

In the banking sector, even manipulated data can result in non-compliance with data standards and incur large fines.

Web, mobile and IoT access for banking clients creates more vulnerability, and without regular surveillance and outside cybersecurity support for a high level of cyber hygiene, breaches will continue to impact the bottom line.

Solution:

Lionfish Cyber Security offers a subscription model at a reasonable fee to provide your cyber leaders with hands-on support, levelling up as the systems grow, and a managed security services provider (MSSP) they can depend on.

Our vCIO will go beyond traditional security steps. He or she will define & implement our employee engagement BWT Platform™ and standardize your best cyber practices. There will be a technology risk assessment leading to further planning and even budgeting for ongoing cyber support. Our policies and procedure development can make a difference in our organization.

There's no time like the present to begin a cybersecurity task management approach and bring in a partner that can support you on a weekly basis with real-time monitoring and threat management.

That's why Lionfish has 24/7 support available, in addition to a robust engagement channel tailored to your needs, upon an initial assessment. The company has knowledge from implementing CMMC certification principles in all its levels of service.

The company's key personnel operate in the ocean of change as the diver, the lionfish hunter, seeking and destroying hackers with a 6-pointed triton – the By-With-Through Platform™ for cyber security protection. The Lionfish crew teaches its customers, like you, to help chart their course forward.

Managed Security. Cyber Support. Security Training. Lionfish Cyber Security technical teams know when to act, and how to bring a knowledgebase, with video and archived checklists.

Core Benefits

- Supplement your staffing needs with our seasoned security professionals and apprenticeships
- Management of routine I.T. Security tasks to save you time and focus on your business
- Affordable enterprise level managed security services designed specifically for small businesses
- Cyber awareness training to achieve data care best practices that protect your most valuable assets - customer and employee data.
- As a CMMC registered provider organization, Lionfish is certified by the Department of Defense to help you qualify for and maintain government contracts
- Proactive Technology Management to mitigate malicious activity
- Rapid remediation and set up of appropriate disaster recovery mechanisms to keep your business running smoothly

The Lionfish BWT platform presents opportunities for collaboration, training, information sharing, and even highly trained apprentices ready to enter your company and be a part of your cyber team. All interactions are preserved in a variety of user access levels, based on your desired requirements. The Lionfish BWT platform™ is continually updated based on US cyber landscape threats and utilizes expert customer service with reporting and purchasing options that go above and beyond your necessary operational needs.

To learn more, contact us at 877-732-6772, or info@lionfishcybersecurity.com

LIONFISH CYBER SECURITY™

Lionfish Cyber Security
3815 River Crossing Pkwy, Suite 100
Indianapolis, IN, 46240
877-732-6772

info@LionfishCyberSecurity.com
LionfishCyberSecurity.com

CYBERSECURITY MATURITY MODEL CERTIFICATION · CMMC-AB · RPO · REGISTERED

CMMC-AB Registered Provider Organization™