LIONFISH
CYBER SECURITY™

A USE CASE SCENARIO

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

A Manufacturer's Nightmare: Bracing for the Storm

Goal: Increased Risk Management, Compliance, & To Protect Essential Operations

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 Manufacturer's Dilemma:

Industrial facilities have traditionally spent more time in production and supply chain management than looking at IT and ICS cyber security issues. But the factors influencing cybersecurity issues within a manufacturing environment has rapidly evolved in the last 24 months. Since COVID-19, the US FBI reported a 300% increase in reported cybercrimes. However, with the advent of the Internet of Things, and new hackers interested in de-stabilizing our nation, the need for cyber diligence and deterrence rings true.

The Control System Cyber Security Association International (CS)2AI and KPMG showcased their first annual cybersecurity report focusing on industrial control systems (ICS) and operational technology (OT) in November 2020, finding that nearly 46% of cyber-attacks have been attributed to negligent insiders (i.e. individuals with trusted access who unwittingly facilitate or cause a breach). The balance includes hacks attributed to scammers (16%), cybercriminals (14%), nation-state actors (12%) and malicious insiders (11%).

The 2020 SolarWinds hack has exhibited just how vulnerable key industrial environments really are, with malware into a software update unknown for months.

The Cs2AI and KPMG report also showed the difference between those using a managed service provider for cybersecurity, and those who do not. 47% of organizations with a mature program use managed services for ICS cybersecurity, compared to only 5% of companies with a less mature program. Additionally, those with a mature program conduct end-to-end security assessments more frequently (53% vs 36%). The report also showed that companies with a mature program are much more likely to replace vulnerable hardware or software after an assessment (63% for mature programs vs 34% for less mature programs).

So, knowledge really is power—and the cyber security threatscape is expanding.

A typical manufacturer, like yours, can face internal issues with social engineering, malware, phishing, and exfiltrated data taken for financial gain.

Solution:

The solution for manufacturers involves staff support and expertise, using a cyber security managed service provider, and ongoing reviews of trusted access and internal capabilities for mitigation to make intelligent decisions for remediation, if a situation comes from a hack.

Cyber readiness is a term that has come to mean finding a trusted partner to support internal needs and battling the tide of unexplained network activity, plus regularly eliminating the root cause of problems that lead to breaches.

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.

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™ (RPO), 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™

This institution is regulated by the Office for Career and Technical Schools - 10 N Senate Avenue, Suite SE 308, Indianapolis 46204 - OCTS@dwd.in.gov http://www.in.gov/dwd/2731.htm