CASE STUDY

FPS Forges New Defenses with Cybersecurity Assessment

BUSINESS OVERVIEW

Fire Protection Services, LLC (FPS), is a leader in the Fire and Life Protection Industry in the Southeast. CEO Christian Dodder was confronted with managing aggressive growth targets in the business and providing new IT systems to improve customer service, drive new revenue, and improve efficiency, all at the same time.

As company growth accelerated, FPS needed to assess their current operations and develop a strategic approach to maturing their cybersecurity posture. The objective of this cybersecurity assessment was to identify vulnerabilities, proactively address issues, and make Fire Protection Services a 'hard target' that was unattractive to hackers.

KEY CHALLENGES

LACK OF GOVERNANCE – The assessment revealed that FPS had no documented cybersecurity policies or procedures and that it needed a formal approach to Risk Management.

UNVERIFIED RECOVERY – FPS had been running regularly scheduled backups, however, it did not have a formal disaster recovery plan and had not validated that it could successfully restore its systems from backup if needed.

PRODUCTIVITY LOSS – Limited budgets for IT security led to piecemeal solutions instead of a comprehensive strategy to prevent, detect, and resolve incidents.

LIMITED STAFF – Internal resources called upon to support IT security did not have the time or skillsets necessary to fully support the security program on top of daily operations.

FPS engaged Idenhaus to conduct a cybersecurity assessment to identify and address cybersecurity vulnerabilities, including verifying the ability to restore from backup. Shortly after the project ended, someone inadvertently ran a command that deleted months of invoices and financial data that was critical to the business. Fortunately, FPS was able to restore the data quickly from its verified backups. A crisis was averted and the business was not impacted.

The truth is, human error is a frequent cause of disaster. One wrong keystroke can result in significant data loss and downtime. Similarly, one wrong email open can let ransomware wreak havoc on all your files. No matter the company, a Cybersecurity Assessment should be priority to ensure your data is verified, safe, and secure at all times. If your business doesn't have a solid security program with defined policies or a data backup protocol in place, contact Idenhaus Consulting by email at **info@idenhaus.com** or give us a call at **404.919.6167**.

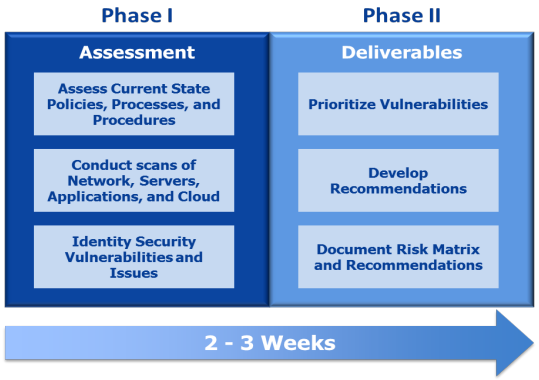
IDENHAUS Cybersecurity Assessment

IDENHAUS METHODOLOGY OVERVIEW

- **Interview** major IT and Business stakeholders to understand the current state environment
- **Evaluate** complexities of business and technical environments and identify security gaps
- **Run Security Scans** of network, servers, and Cloud platforms to detect vulnerabilities
- **Develop Recommendations** to improve FPS's security posture and strengthen its systems

ASSESSMENT PROCESS

Idenhaus reviewed FPS's processes and technology to develop recommendations to mature its security program. Our process delivered a clear understanding of FPS's strengths and struggles and laid out the roadmap to move forward. This drove executive support to proceed with enhancements to the FPS network, systems, and underlying security policies.



SUCCESSFUL DELIVERY

Idenhaus has years of experience working with customers from diverse industries. We understand that recommendations are not valuable if they are not actionable.

Based on a Strong Analysis
Recommendations are based on a solid understanding of the real problem as a result of the detailed analysis.

Incorporates Best Practices
Our recommended courses of action are based on lessons learned and industry best practices.

Consistent with the Project Objectives
Recommendations are aligned to the business strategy and goals of the organization.

TAKEAWAYS

The Cybersecurity Assessment provided strong evidence that FPS's systems and processes were due for an overhaul. By prioritizing and presenting the cybersecurity risks identified during staff interviews and security scans, Idenhaus was able to address key vulnerabilities and improve FPS's cybersecurity posture.

Key results:

- **Verified data backup technology and avoided a costly loss of financial information**
- **Identified "Quick Wins" that fixed key problems and maximized time to value**
- **Minimized vulnerability to cyber events**
- **Reduced impact and shortened recovery time of an incident**
- **Implemented formal security policies, new IT processes, and awareness training to mitigate insider threats**
- **Identified approaches to remediate cybersecurity issues on core systems**
- **Devised effective control techniques based on defense in-depth to mitigate the impact of the identified risks**

404.919.6167 @idenhaus info@idenhaus.com