Keeping Competitive in an Increasingly Risky Industry

Retail Industry

RETAIL COMES UNDER ATTACK

CUSTOMER PROFILE

A retail chain in North America, with approximately 250 locations.

CHALLENGES:

- ✓ Ensure and maintain regulatory compliance.
- ✓ Protect and preserve the brand.
- ✓ Maintain customer loyalty and trust.
- ✓ Safeguard customer privacy while providing an amazing customer on-line and in store experience.
- ✓ Concerns over resurgence of ransomware
- ✓ Monitor a variety of disparate systems across multiple locations with minimal resources.

RESULTS:

- ✓ PCI-DSS – Payment Card Industry Data Security Standard compliance.
- ✓ Educate employees with Security Awareness Training.
- ✓ Consolidate security solutions to minimize vulnerabilities across the business.
- ✓ Actively monitor and alert 24 x 7 x 365.
- ✓ Streamline and automate backup processes to ensure business continuity and combat cyberattacks.

THE PROBLEM

The Retail chain was required by regulation to adhere to **PCI-DSS** Payment Card Industry Data Security Standards. PCI-DSS mandates how credit card data is stored and transmitted after accepting and processing it. This standard also carries anywhere from $5,000 to $100,000 per month fines for non-compliance.

Retailers, regardless of their size, care about their business and their clients. Preserving their brand and maintaining customer loyalty are fundamental to their success. Providing clients with a great customer experience often requires technologies that, at times not only provide competitive advantages, but may also introduce vulnerabilities into the environment.

Our customer was concerned about remaining competitive, maintaining compliance and protecting their customers as well as their brand. Protecting themselves against malicious insiders, spear phishing campaigns, ransomware, DDoS and supply chain attacks were their top concerns.

SCOPE & SELECTION CRITERIA

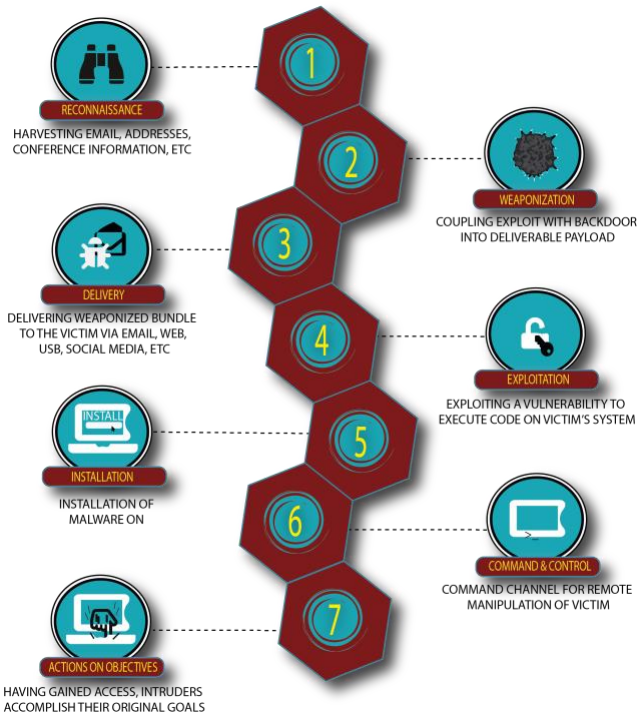
The stakes were high for our client and their IT Team. The project included a variety of testing to determine the organizations risk and to close any gaps found. iPRESIDIUM performed the following:

- In-depth assessment of the organization's cyber security vulnerabilities and potential threats.
- Perform a detailed Penetration test to level set the current controls and test against them in order to identify potential security risks to the network.
- Perform phishing attacks to gauge the security awareness of employees within the organization.

ENGAGEMENT

iPRESIDIUM performed a vulnerability assessment of the organization's internet accessible systems. Key steps involved system identification and vulnerability scanning. In addition, we conducted a network forensic scan and an email campaign to evaluate security awareness against social engineering attacks and any unauthorized activity on the network.

Our Penetration Testing simulated Advance Persistent Threats (APT) and Ransomware by leveraging Cyber Security Threat Monitoring Services to detect, analyze and respond to stealthier attacks in real-time. Our solution provided the ability to monitor all network ports and protocols along with custom sandboxing to identify command-and-control (C&C) communications, and/or other evasive techniques. iPRESIDIUM provided 45 days of full monitoring and remote management of anomalous activity.



THE SOLUTION

The entire project took 3 months to complete, providing the retailer with a comprehensive evaluation of their current Cyber Security practices in comparison with industry peers. iPRESIDIUM'S

Managed Security Services provided the organization with PCI-DSS compliance and the 24x7x365 monitoring the retailer needed.

Following iPRESIDIUM'S engagement, the retail chain quickly realized a number of benefits to their previous security risk management processes:

- 24x7x365 monitoring of their PCI environment on an ongoing basis by leading cyber security analysts. Providing real-time notifications of potential intrusions on their payment systems so the retailer can stop it before it has the potential to escalate.
- Conduct regular pen tests and security audits quarterly to identify any new risks or potential security concerns before they can wreak havoc on the network.
- Employ regular security awareness training for employees to identify potential digital threats to the business and how to properly respond.

While there is no such thing as perfect security, our client is now able to keep management up-to-speed on the business' security posture and compliance. They continue to enhance and provide their customers with better consumer experience while protecting their privacy and data.

About iPRESIDIUM

iPRESIDIUM is a cyber security and risk advisory firm. We provide end-to-end enterprise security services for private and public entities of all sizes. iPRESIDIUM helps customers protect their business, employees, data, and their reputations. We succeed by offering our clients cutting edge technologies with best-in-class security solutions, experienced industry professionals proficient in cyber security and managed service platforms. Our goal, to deliver our clients' the peace of mind they need so that they can focus on their business.

Since its inception in 2002, iPRESIDIUM has successfully exceeded the security needs of numerous organizations, across the following sectors: Healthcare, Retail, Education, Government and Public Sector, Financial, Technology, Hospitality, Insurance, Transportation and Manufacturing as well as over 50 US federal agencies and the intelligence communities.

www.ipresidium.com | info@ipresidium.com | 949-721-6612