SecureWorks

NATIONAL RESTAURANT FRANCHISOR SYSTEMATICALLY ELIMINATES VULNERABILITIES

With hundreds of millions of dollars a year being invested in advertising plus food and beverage R&D, this restaurant chain wasn't about to take any chances

Industry: Food Service | **Country:** United States

BUSINESS NEED

Facing growing cyber threats and successful attacks in the industry, the company sought to assess its cyber risk profile, vendor management practices, technical controls and business continuity practices.

SOLUTION

The client has systematically eliminated vulnerabilities, increased security awareness among employees and executives, and improved the company's overall cybersecurity posture, after a thorough security assessment by the SecureWorks Security and Risk Consulting team.

BENEFITS

› Reviewed policies and vendor management practices

› Assessed technical controls and business continuity practices

› Eliminated high-risk security vulnerabilities

› Accelerated the maturity of its information security program

› Boosted security awareness among employees and executives

› Increased trust in cyber safeguards among franchisees

PRODUCTS | SecureWorks Security Architecture Assessment | SecureWorks Incident Management Retainer | SecureWorks Vulnerability Management Assessment | SecureWorks Advanced Penetration Testing | SecureWorks Security Risk Assessment

THIS RESTAURANT CHAIN WASN'T ABOUT TO TAKE ANY CHANCES OF LETTING A SECURITY BREACH AFFECT ITS CURRENT MOMENTUM AND BRAND.

With thousands of outlets in almost every state in the U.S., mostly owned by franchisees, plus hundreds of millions of dollars a year being invested in advertising as well as food and beverage R&D, too much is at stake.

RAMPING UP SECURITY

In the face of growing cyberthreats over the years, the company had already taken steps to ramp up its information security programs, but largely in response to the compliance requirements of the Health Insurance Portability and Accountability Act of 1996 and the Sarbanes-Oxley Act of 2002. These mandates required it to develop a more mature information security program and tighter security controls around its infrastructure and data.

In addition to those regulations, 2004's first release of the Payment Card Industry Data Security Standard (PCI DSS) by the Payment Card Industry Security Standards Council was issued to help protect customer credit card data. At that time, the company hired a consulting company to evaluate the cardholder data environment, which resulted in additional tightening of its data security controls.

NEEDING MORE SAFEGUARDS

Until 2014, the company complemented these compliance-mandated security measures with standard enterprise security safeguards such as firewalls and antivirus software. Early that year, however, it decided that the growing number of cyberthreats and successful attacks warranted the development of an enterprise-wide cybersecurity framework based on a model suggested by the National Institute of Standards and Technology (NIST). It also hired its first dedicated IT security staff and kicked off a security awareness program.

Even with those initiatives underway, the company realized it needed outside expertise to take its security defenses to higher levels. After issuing a detailed RFP and a careful evaluation of responding vendors, it selected SecureWorks to conduct an extensive, stem-to-stern assessment of its overall risk profile and key components: networks, security policies and practices, and incident response plan. The scope included select franchisees and vendors. SecureWorks would then provide detailed recommendations for remediation and improvements.

ASSESSING THE FULL SPECTRUM

Spanning three months in 2015, SecureWorks Security and Risk Consulting experts conducted in-depth examinations of the company's entire security posture, using a six-step evaluation methodology recommended by NIST.

Among the many activities were physical security checks, internal and external penetration testing, critical device health checks, reviews of policies and vendor management practices, and assessments of technical controls and business continuity practices. Subsets of these evaluations were conducted at two corporate and two franchisee-owned stores.

In a detailed report to the executive and IT management teams, SecureWorks commended the company on the range of security initiatives taken up to that point, but shared significant concerns:

- Putting more importance on new products and services than protecting sensitive data about employees, financials and internal secrets
- Ad hoc security practices that needed more formal definition, documentation and consistent execution
- Lack of an enterprise-wide security framework and associated governance model, leaving too much responsibility for security policies, controls and execution to individual departments and personnel
- Insufficient IT security staffing and focus on the risks facing the company
- High-risk vulnerabilities in outdated technologies, as well as inadequate protocols for patch management, vulnerability management, risk management, vendor management and network segmentation

TAKING SECURITY TO HIGHER LEVELS

Based on the findings in the report, the company asked SecureWorks to provide specific recommendations for how SecureWorks services could help to remediate the security gaps, improve its overall security posture and accelerate the maturity of its information security program.

SecureWorks provided the company with a specific scope of work that suggested strategically focused offerings from its Managed Security Services portfolio. In late 2015 and early 2016, the company signed an agreement to implement them, recognizing that SecureWorks tools and expertise could support and supplement its own security staff.

PEACE OF MIND

Since deploying the services, SecureWorks has systematically eliminated vulnerabilities and improved the company's overall cybersecurity risk posture. Doing so has helped increase security awareness among employees and executives, while increasing its franchisees' trust in the stronger safeguards.

Today, the data of employees and customers is secured behind a layered, defense-in-depth model. This puts it as far from cyberthreats as possible, with 24x7 monitoring that provides deep-packet vigilance of all network traffic, whether inbound, outbound or across the company's internal networks.

Ultimately, SecureWorks Managed Security Services will help protect the company's brand — with millions of dollars of marketing investments behind it — from being sabotaged by a successful cyberattack. For the company's customers, executives, IT staff and even investors, that can provide peace of mind.

View all SecureWorks case studies at SecureWorks.com/Resources

SecureWorks is a global provider of intelligence-driven information security solutions exclusively focused on protecting its clients from cyber attacks. SecureWorks' solutions enable organizations to fortify their cyber defenses to prevent ecurity breaches, detect malicious activity in real time, prioritize and respond rapidly to security breaches and predict emerging threats.

SecureWorks®