IGI

Solve. Simplify. Secure.

CASE STUDY

Financial Industry

For a trusted Federal Credit Union that has been in business for more than 80 years, cybersecurity has to be a top priority. That's why this Upstate New York credit union chose IGI to help evaluate its security state, identify security gaps, and improve overall security posture. This IGI customer is dedicated to not only meeting the necessary cybersecurity requirements for compliance, but also taking extra steps to protect client information in an industry where data breaches are all too common.

The Challenge

Security breaches are a growing threat for all businesses, but the financial sector has been affected the most according to a 2016 study from IBM's X-Force Research team. Additionally, Federal Credit Unions are strictly monitored for compliance with state and federal security standards such as GLBA, NIST, COSO/COBIT, FFIEC, and ISACA. This means that financial institutions need to be more diligent in not only meeting compliance requirements, but also taking every possible measure to keep financial records safe.

The customer's main challenges centered around compliance and staying up to speed on its risk management practices. The customer, like all regional banks and credit unions, have the challenge of working with limited resources compared to their larger, national counterparts, while still facing the same security challenges. This customer had also fallen behind on its compliance audits due to lack of clear policies and procedures set by senior management and its outsourced IT organization.

The Solution

IGI is experienced in working closely with outsourced IT organizations to enhance their offerings, which made IGI a good fit to help the customer get back on track with its security. IGI knows that it's much less painful for customers to keep up with security compliance regularly than trying to catch up when you're due for audit.

IGI applied its holistic approach to cybersecurity, working with our customer to evaluate internal and external IT management; organization and operations; policies and procedures; physical and logical security access and controls; information security tools and applications; network security; and audit compliance. IGI also worked with the customer to conduct internal and external penetration testing to assess the security and readiness of the site, including its systems, networks, and applications. By simulating real-world attacks, IGI could identify the weaknesses in the customer's security measures and recommend the steps to lower its risk level.

IGI will continue to perform these critical security services, including regular penetration tests and compliance audits, through a multi-year engagement with the customer.

The Result

After in-depth evaluation and testing of the customer's existing security posture, including penetration testing, IGI helped help build a more comprehensive security program for the customer. This program involves more frequent risk assessment, automated vulnerability management, and security training for employees.

The customer now has the peace of mind knowing that its regulatory requirements are being met and its overall security posture is continuously improving. The customer network is now monitored for critical vulnerabilities around the clock with Nodeware™—IGI's own security solution. Additionally, employees are empowered to be security assets, rather than a liabilities, through IGI's comprehensive security awareness training program. Throughout the length of the multi-year engagement, IGI will continue to work with the customer to deliver additional services and refine its security plan as new needs arise.

175 Sully's Trail, Suite 202
Pittsford, NY 14534

585.385.0610
855.385.0610

www.nodeware.com
www.igius.com