CASE STUDY

Payment Card Industry Compliance Remediation

Durham College

THE CHALLENGE

Durham College recently contracted MNP to evaluate and remediate their Payment Card Industry Data Security Standard (PCI DSS) compliance. Citing concern about a recent successful phishing scheme at another Canadian college, they also noted increased pressure from their current and potential future banking partners to meet industry requirements.

From the outset, the project faced several key challenges.

First, the college in question is situated on a shared campus with the University of Ontario Institute of Technology. Although both schools manage their affairs independently, the structure of their relationship and nature of the shared network and PCI framework would require extensive coordination to ensure both institutions achieve full compliance.

Moreover, a teachers' strike threatened to interrupt the original project timeline. The steering committee indicated a need for minimal downtime to accommodate the compressed school year. They requested a delay of remediation activities until the end of the spring semester, requiring the team to reorganize the schedule in order to continue to meet the fall 2018 timeline.

MNP'S APPROACH

Alignment

MNP's Cyber Security team first secured buy-in, alignment and commitment from all stakeholders, business unit managers and front-line resources. This required consulting with the technical, finance, human resources and communications teams at both schools, along with more than 20 vendors and web service providers.

Gap Analysis

An MNP Qualified Security Assessor (QSA) then prepared the initial assessment and gap analysis in line with PCI standards. The process involved multiple interviews and a comprehensive review of existing technology assets and current procedures. The QSA detailed their findings in a comprehensive report, which included recommendations for the remediation team to follow. They remain closely connected to the project and continue to provide guidance and advice as required.

Project Management

Working with the remediation teams at both schools, MNP dispatched a project manager to develop a project plan and schedule, form a steering committee and coordinate teams, training, vendors and communications. They also helped to oversee the development of new policies and procedures, ensured all documentation was accurate and up-to-date and managed risks and issues arising through the course of the remediation project.

Training

MNP worked with management and frontline staff who process credit card transactions to provide comprehensive security awareness training. All developers also received secure coding training.

Vendor Management

MNP Cyber Security team coordinated directly with all vendor partners to demonstrate and strategize potential solutions which would help both institutions achieve their payment card and security requirements.

OUTCOME

While the project is still ongoing, both schools are on target to achieve full PCI compliance by Fall 2018.

Beyond the initial project scope, the clients have also demonstrated increased awareness of cyber security threats among staff and leadership and a more robust risk management culture. This will likely result in greater resilience against other threats including phishing and social engineering attacks moving forward.

For more information on how MNP can help your organization, contact:

Danny Timmins
National Cyber Security Leader
T: 905.607.9777
E: danny.timmins@mnp.ca

Eugene Ng
Cyber Security Leader, Eastern Canada
T: 905.607.9777
E: eugene.ng@mnp.ca

Tom Beaupre
Cyber Security Leader, Quebec
T: 514.228.7844
E: tom.beaupre@mnp.ca