Securing State Payment Card Data for Minnesotans

State of Minnesota — Minnesota IT Services

CATEGORY:
Cybersecurity

CONTACT:
Emily Shimkus
Director of Communications
emily.shimkus@state.mn.us
(O) 651-201-1011
(C) 651-485-1354

INITIATION DATE:
September 2019

END DATE:
June 2020

MINNESOTA IT SERVICES

Information Technology for Minnesota Government

Executive Summary

While state government is not typically perceived as a merchant, ongoing system modernization efforts mean more digital government financial transactions are made with debit and credit cards. That raises our vulnerability risks. Merchants are the main target for financial fraud, enabling criminals to easily steal and use personal consumer financial information from payment card transactions and processing systems. When a merchant is affected by security breaches, it also affects consumers; more than 11,733,087,704 records with sensitive information have been breached since 2005, according to PrivacyRights.org.

Minnesota IT Services commitment to securing our state is a key tactical priority to 1) better protect applications and citizen data and 2) to mature risk management and communication.

As the state of Minnesota is a key participant in payment card transactions, the state of Minnesota must use standard security procedures and technologies to thwart theft of cardholder data.

To achieve the MNIT 2020 Tactical Plan Secure the State goal, this project established a new payment card industry (PCI) program to monitor state compliance and secure cardholder data environments (CDE). The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL entities that accept, process, store or transmit credit card information maintain a secure environment. Compliance with the PCI DSS helps to alleviate these vulnerabilities and protect cardholder data. It also helps to minimize the potential impacts of a breach of cardholder information.

The project included the development and implementation of a new MNIT PCI Program, including new processes, people, and technologies to assess, manage, and report PCI compliance. The program includes a team with PCI expertise to assist agencies.

Merchant-based vulnerabilities may appear almost anywhere in the card-processing ecosystem including point-of-sale devices; mobile devices, personal computers or servers; wireless hotspots; web shopping applications; paper-based storage systems; the transmission of cardholder data to service providers, and in remote access connections. Vulnerabilities may also extend to systems operated by service providers and acquirers, which are the financial institutions that initiate and maintain the relationships with merchants that accept payment cards.

Idea

What problem or opportunity does the project address?

This PCI Program aligns with MNIT's strategies to bolster successful state cybersecurity efforts:

- Embed a security mindset into everything we do by building expertise across MNIT and the executive branch through training, communications, and engagement
- Prioritize security, mature risk management practices, and provide agency-specific recommendations around high-value investments through active collaboration with agency partners
- Use a layered approach to continually improve the defense of state infrastructure to address gaps that could lead to service outages or data breaches

- Prioritize, test, and implement application security to protect citizen data and the delivery of state services

The PCI Program provides a proactive approach to securing and monitoring the IT and business processes used for delivering state of Minnesota government services through compliant digital payment methods.

As the state of Minnesota is a key participant in payment card transactions, the state of Minnesota must use standard security procedures and technologies to thwart theft of cardholder data. For some context, in 2020 the state of Minnesota processed 30,150,390 credit/debit card transactions totaling $2,575,870,601.11.

Every Minnesotan that interacts with the state online or in person and pays for goods or services (day at the Zoo, or a state park, purchasing license tabs, fishing licenses, etc.) with a credit/debit card is impacted. Executive Branch agencies, which are now part of the MNIT PCI program, have 104 merchant accounts and in 2020 processed 4,702,963 credit/debit card transactions totaling $397,702,432.88. These merchant accounts are used for a variety of business processes that accept credit/debit card payments including online tab renewal, professional license fees, park and recreation registrations, fishing and hunting licenses, taxes, etc.

Why does it matter?

One of Minnesota's greatest challenges is the cybersecurity threat facing its IT infrastructure, data, and systems that citizens depend on. Although MNIT's cybersecurity strategy has refined over the years, **no organization is immune from these kinds of attacks.**

PCI card compliance protects cardholder data and applies to any organization that accepts, transmits, or stores that data. Being PCI compliant puts the safety of consumer data first and ensures positive brand reputation.

Before the PCI Program, the intangible consequence was the **loss of Minnesotan's trust, and damage to our reputation as a state**. There are also **tangible consequences**. Non-compliance with the PCI DSS may result in:

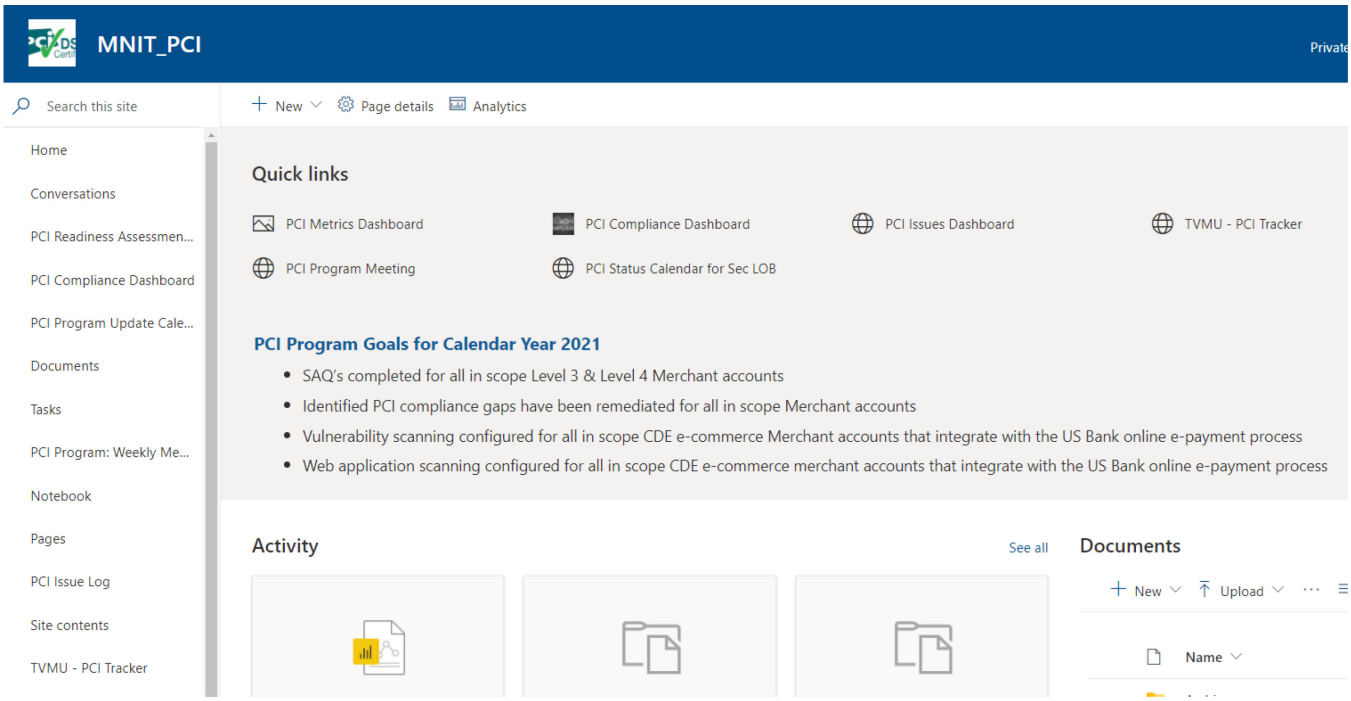
- Fines
- Increase in transaction fees
- Ending ability to accept payment from payment cards

Breach of card data may result in:

- Costs for mandatory forensic investigation by a PCI certified third party
- Costs for mandatory compliance assessments by a PCI certified third party and remediation of findings
- Fines and/or increased transaction fees
- Ending ability for the state to accept payment from payment cards
- Costs for credit monitoring and breach notification
- Card re-issuance penalties

What makes it different?

The state now has a centralized approach to managing requirements for agency merchant account holders. Everything is tracked and managed digitally and is available to agency end users through a SharePoint site, as shown below.



Implementation

What was the roadmap?

The PCI program was identified as a key priority to achieve the MNIT Security Strategic Plan strategies to 1) better protect applications and citizen data and 2) to mature risk management and communication. Breaches in security and non-compliance with the PCI DSS result in fines, increased transaction fees, or the removal of the ability to take credit/debit cards altogether. This widely impacts Minnesotans, as the fines or increased transactional costs will be added as increased fees to the citizens. Along with increased fees, the citizens who had their personal information and card data breached now face the risk of identity theft, fraudulent charges, and other hardships.

This program is an excellent example of MNIT's strategic goal to promote people-centered digital government services. Understanding the needs of MNIT's business partners and stakeholders helped us choose the right framework. Extensive interviews with end users and innovative, iterative designs drove all our decisions.

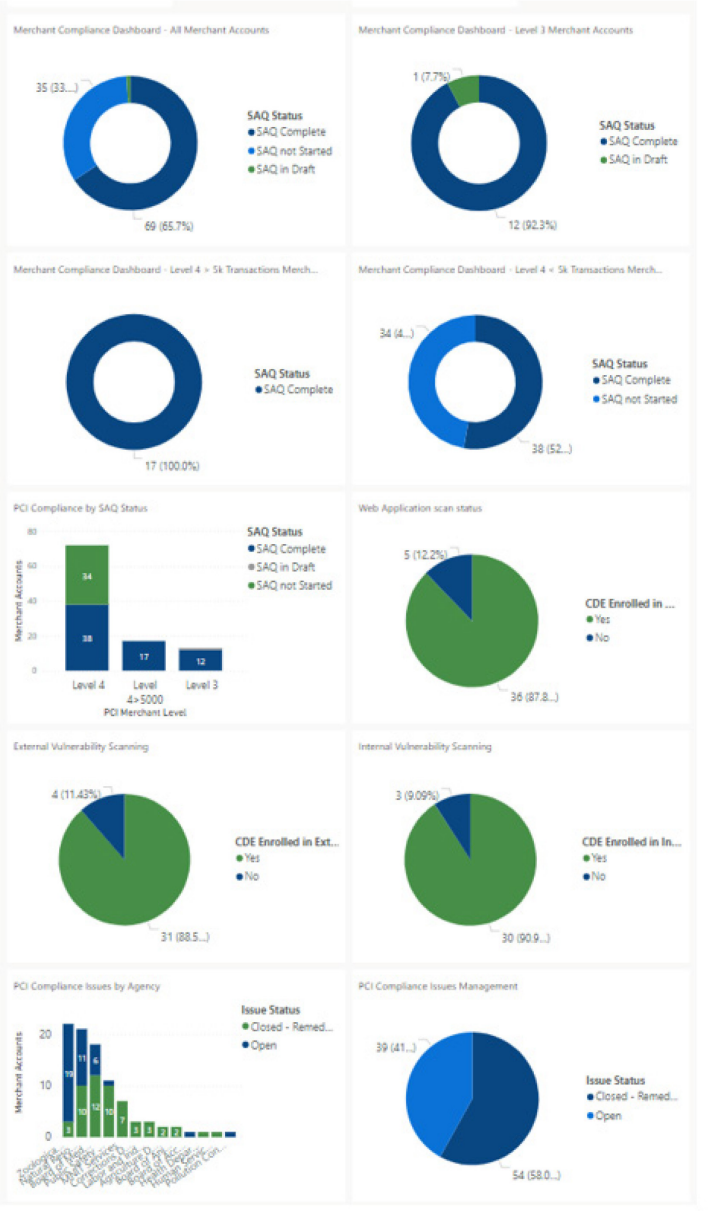
Project management approach

The project management approach for creating the PCI program followed Agile methodology, using end-user feedback and validation to provide iterative, continuous improvements. For example, compliance reporting started with spreadsheets and manual reporting, evolved to database manual reporting, and finally to real-time web-based reporting of data that actually matters to the stakeholders.

Metrics

Power BI provides built-in robust metrics dashboards that make it easy to track progress and success. PCI self-assessments and compliance reporting of agency cardholder data environments (CDE) are being completed per

requirements. PCI compliance gaps are identified, reported, and addressed. The PCI Program has dedicated staff available to address questions related to PCI.



Stakeholders

- Advocate and oversight role:
    - Minnesota Management and Budget: Assistant Commissioner of Accounting Services
    - MNIT: Assistant Commissioner and Chief Information Security Officer
- Implementation role:
    - MNIT Enterprise Services Teams
    - MNIT Line of Business Security Leaders and Teams
- End-user role:
    - Agency staff and leadership

How did you do it?

MNIT's Architecture and Secure Engineering leader developed the program and management processes. The project was approved through the Enterprise Project Management Office (ePMO). Communications were managed with bi-monthly meetings to discuss project and program status.

One of the biggest issues for state government is choosing the right tools and applications to enable the processes of a new program. A human-centered design approach was key to selecting tools that were already available, widely used, and familiar to state employees. Microsoft SharePoint and Power BI are part of Minnesota's M365 Government Community Cloud, available to all Minnesota Executive Branch agencies, and **align with stringent security and authentication standards**. We leveraged and evolved an existing framework developed by MNIT's Architecture and Secure Engineering team. This ensured security, end user buy-in and adoption, with little to no learning curve, and no additional costs or fees to agencies. These two applications provided an excellent platform to track PCI assessments and manage PCI issues. In addition, the Power BI Dashboard delivers real-time, meaningful agency-specific metrics to agency, security, and executive leadership.

Impact

What did the project make better?

Before the establishment of the PCI Program, the state of Minnesota lacked visibility into its ability to securely provide credit/debit card services to meet the PCI data security standards. This lack of visibility resulted in past security breaches of credit card systems and data and failure to comply with the merchant acquiring banks compliance requirements. The PCI Program improved government digital transaction security by establishing assessment and reporting processes, issue/remediation tracking, and providing expert guidance. Each merchant account is associated with a cardholder data environment (CDE) that is made up of technology and processes. The PCI Program is responsible for assessing and reporting to ensure compliance and that government services can continue to be cost effective and available for credit/debit card purchases.

This security and protection impacts the following groups:

- Executive Branch agencies that hold 104 merchant accounts to process, store, or transmit credit/debit card payments
- Potentially all 5.5M Minnesotans that provide their private data and credit card information to the State of Minnesota for government-run services

Metrics

Metrics for period of PCI Program initiation through 5/26/2021:

- All 104 merchant accounts are enrolled in the program
- In 2020, 4,702,963 credit/debit card transactions were processed, totaling $397,702,432
- Zero breaches
- Zero fines
- 93 security/PCI non-compliance issues identified to date: remediation complete or underway

- 92.3% of level 3 Merchant accounts compliance assessment complete for reporting year
- 100% of level 4>5k transactions Merchant accounts compliance assessment complete for reporting year
- 52.8% of level 4 Merchant accounts compliance assessment complete for reporting year

Benefits

- As partner agencies fulfill their missions, they are assured they are meeting PCI compliance and regulations
- Minnesotans can trust in our state to safeguard and protect their data securely
- MNIT is able to validate alignment with our strategic and tactical plans to secure the state as we continue to modernize, reduce risks and vulnerabilities, and serve Minnesotans

How do you know?

The following testimonial from Cindy Farrell, Assistant Commissioner of Accounting Services, Minnesota Management & Budget, is one example of the stakeholder responses to the PCI program overall:

"The MNIT PCI Team has done a fabulous job implementing the program. In the past, the state's response to PCI was very reactive, with little insight into agency compliance status at the statewide level. Now the team works proactively with state agencies to identify and resolve issues before they become real problems. And I love the dashboard that provides me with overall status reporting. Minnesotans can sleep well knowing their credit card information is secure with the state."

What now?

This project closed in June 2020 and has been fully operationalized, funded and staffed by MNIT. In its second year, the program seeks to deliver on the following PCI Program Goals:

- Self-Assessment Questionnaires (SAQ) completed for all in scope Level 3 & Level 4 merchant accounts
- Identified compliance gaps have been remediated for all in scope merchant accounts
- Vulnerability scanning will be configured for all in-scope CDE e-commerce merchant accounts that integrate with the online e-payment process
- Web application scanning will be configured for all in-scope CDE e-commerce merchant accounts that integrate with the online e-payment process