Foundational Cybersecurity for Application Preservation

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:
December 2017

END DATE:
December 2019

MINNESOTA IT SERVICES

EXECUTIVE SUMMARY

The Application Preservation Program is a cybersecurity initiative driven by the Minnesota IT Services (MNIT) team that partners with the Minnesota Department of Transportation (MnDOT). The objective is to keep applications in good technical health, and protect them by resolving issues proactively before they become obsolete and unsupported. Cyber attacks on government have increased significantly in the past several years, often targeting unsupported vulnerable systems—CNN reported in October 2019, that in the previous 10 months, 140 local governments, police stations and hospitals have been held hostage by ransomware attacks. Minnesota is making cybersecurity awareness, prevention and security best practices a part of our culture with programs like Application Preservation.

Application Preservation mapped out an ongoing strategy to identify technical health issues and prioritize resolution, to engage business partners in investment decisions, and assemble teams to complete the technical work needed. MNIT's greatest hurdle in this effort was helping the business understand the cybersecurity importance, priority, and resourcing needed to protect their applications. In the past, application components were renovated on an as-needed basis, nearly always in crisis mode which is inefficient and disruptive. Most of these efforts involved small armies of expensive consultants who spent time learning the applications and environments, then at the end of the project left without sharing valuable knowledge.

MNIT's Application Preservation program for MnDOT is based on a three-year cycle. Every application has similar components—operating systems, databases, middleware—although there are many flavors (Windows, Linux, Oracle, Microsoft) with different cycles of support. Our three-year program puts each application on a "stack" with three years of life left in it. This approach helps us standardize server stacks, and avoids having to be on the "latest and greatest" cutting edge versions of products that are often buggy and problematic.

MnDOT fully understood the value of the increased efficacy and cost effectiveness of a planned, resourced program. The primary investment was hiring 16 permanent, full-time staff who would retain the knowledge acquired during preservation of these applications. Every application they work on is a great investment in the future, gaining in-depth knowledge of application technologies, business practices, and environments. Most importantly, instead of making individual updates that are disruptive to the business, now we renovate the entire application at once and do basic maintenance (patches/updates) until the next cycle.

This program integrates IT, security, and business practices to achieve a superior priority and resourcing level. Applications are ranked for Business Value and Technical Health. These rankings are considered when planning priorities and work schedules, so we are not doing preservation work on an application that will soon be retired, replaced, or get major upgrades. Whenever possible, we organize application preservation work by business function, so multiple business disruptions are consolidated and scheduled during non-peak seasons/times.

All of this contributes to MnDOT's overall cybersecurity profile, and we measure that using MNIT's Risk Scorecard process. In 2019, our cybersecurity Risk Scorecard rankings were at 5.0 on a scale where 5.0 is the highest achievable score. **By embedding Application Preservation into every service, we have improved our risk profile, and achieved an agency-wide cybersecurity focus.**

EXEMPLAR

In the past, systems were tools used to accomplish specific goals, and maintenance of those tools was obscure, often neglected, and not valued. With a focus on cybersecurity, that has changed. These systems are now stitched into all workflows and everything MnDOT does depends on a seamless suite of technology solutions. Keeping that entire machine working means treating maintenance as a planned, coordinated program.

The Application Preservation program promotes a process of planned maintenance which reduces downtime and consolidates maintenance efforts to provide more secure, available and useful systems.

Maintaining systems is not a new concept – but it is all too often not done. Business leaders (and even IT) will almost always invest in new functionality, new features or other deliverables with obvious positive aspect. MnDOT leadership showed commitment and foresight in this investment in ongoing application maintenance to protect against cyber threats and make sure the business can run uninterrupted.

CONCEPT

State and local governments are notorious for being under-staffed and behind on application maintenance. This is a huge cybersecurity risk, and a historical lack of investment at the business level only compounds the problem. The Application Preservation program changed that, focusing on applications that are important to our business partners, **drawing a direct connection between the investment in staff, and the health, longevity, and security of their applications.**

In the past, most application maintenance was done only when there were significant security or operational risks to specific individual components of the application. This maintenance was often done on tight schedules, and was costly and disruptive to the business. By approaching maintenance from a proactive application preservation perspective, we highlighted the high cost of doing work in crisis mode, and demonstrated that a business investment in IT staff would result in much less disruption, and lower ongoing costs.

The investment made by our business partners is almost exclusively in staff costs. We hired 16 full-time personnel, placed in all areas of the MNIT operation at MnDOT—the largest single increase in MNIT staffing for our business partners at MnDOT.

Even with our staffing investment, there are still challenges. We need to communicate clearly and frequently with the business to ensure continued funding support. We meet regularly with MnDOT senior management and individual executives to review successes, challenges, and status. In addition, we lobby the MnDOT Technology Investment Management (TIM) Office to let the business partners know in advance that we will be working with their applications. The TIM Office also helps our business partners understand the process and need for testing and engagement. **Approaching our business partners from two angles affords an improved rate of successful business engagement.**

SIGNIFICANCE

Our Application Preservation program is primarily a multi-dimensional security and risk management effort. In addition to providing measurable progress in our cybersecurity profile, the Application Preservation program implementation also addressed customer relationship management. This was an opportunity to truly engage with our business partners on many levels—building awareness of the problem, and of the solution. Most importantly, it was an opportunity to build agency confidence and unprecedented long-term investment.

The Application Preservation program addresses almost 600 applications in the MnDOT Application Portfolio. These applications serve 5,000 employees, contractors and business partners in 30 office buildings, 200 rural truck stations, dozens of construction sites, and 100 unmanned instrumentation sites. These applications do everything from managing billions of dollars of state and federal investment in transportation, to measuring the depth of frost under our roads. The scope and scale of applications is vast, and extremely distributed in nature.

The holistic approach to application maintenance in relation to cybersecurity is the first of its kind for MnDOT. Not only are we striving to consolidate and minimize disruptive maintenance, but we are also working toward a regular cycle that keeps applications healthy and prevents vulnerabilities. In the past, a few applications had some maintenance cycles, but they were rare and followed inconsistently. **The Application Preservation program treats the entire portfolio of applications, tracking and managing maintenance activities to produce a regular, predictable cycle of maintenance with increased cybersecurity and risk management.**

IMPACT

Impact of this program is real and measurable. To measure effectiveness, we now are able to produce regular reports showing our progress in working through the portfolio of applications at MnDOT.

Most importantly, we have also been able to demonstrate that the Application Preservation project improved our cybersecurity risk profile. **In 2019, our MNIT cybersecurity Risk Scorecard rating was 5.0 — on a scale where 5.0 is a perfect score**; 70% of that was due to the application preservation work of eliminating old servers. We achieved this in the following ways:

- In one year, we have worked over 165 applications.
- The number of servers running current operating systems have increased from 60% to 95% as a direct result of this effort.
- During this project, 797 servers were built, none using unsupported operating systems.
- By the end of the project, only 6% were built with Windows Server 2012, which was still supported, but not the most current.

We have also reduced impact to the Minnesota Department of Transportation by consolidating maintenance activities for servers, middleware and database all at the same time. One of the most valuable qualitative impacts we are already seeing is that now knowledge is retained by permanent staff, which makes them more efficient going forward. Previously, when consultants were hired, they spent valuable expensive time learning

the environment and business practices before they could start working. Permanent staff continue to learn and build the essential business-related knowledge that makes their work more efficient and more impactful.

Rather than forming a dedicated team, most new hires were merged into existing service teams (Quality Assurance, Infrastructure, Database, Middleware, etc.). Adding entry level staff takes the load off more seasoned MNIT staff who work on Application Preservation efforts, so we get more skill level out than we put in. In addition, adding entry level staff creates career succession paths—someday these new, entry level hires will be the seasoned veterans.

By embedding Application Preservation into every service, we achieve an agency-wide cybersecurity focus where everyone is part of the solution.