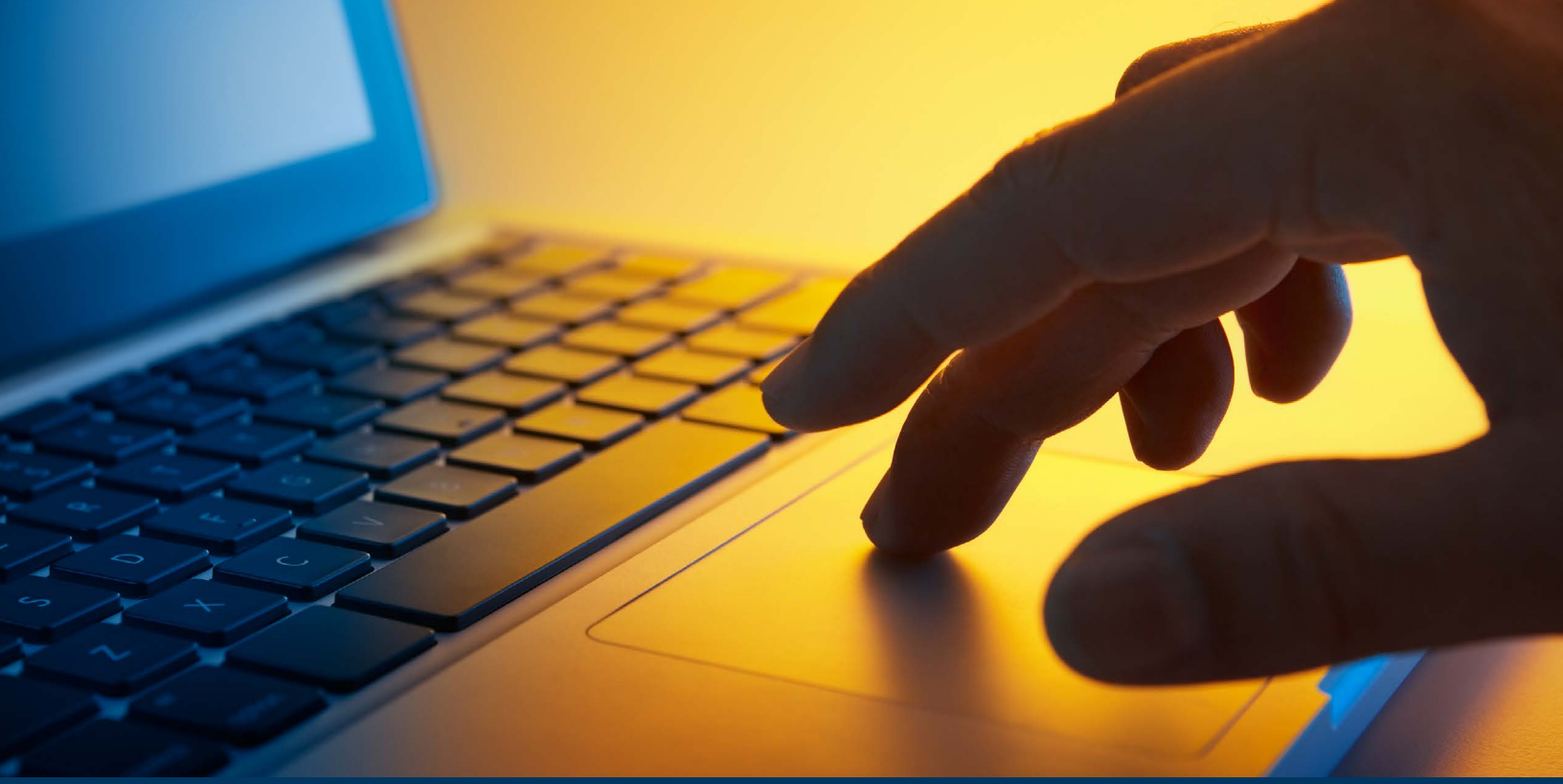

Security Risk Scorecards

State of Minnesota — Minnesota IT Services

CATEGORY:
Cybersecurity

CONTACT:
Cambray Crozier
Director of Communications
cambray.crozier@state.mn.us
(O) 651-201-1063
(C) 651-367-4616

INITIATION DATE:
October 2015

END DATE:
September 2016

MINNESOTA IT SERVICES

EXECUTIVE SUMMARY

Minnesota IT Services (MNIT) Security Risk Scorecards project sprung from this haunting question: "How can we protect what we have, if we don't know what we have?"

Cybersecurity is a top priority for MNIT and for Minnesota's Governor Dayton. MNIT's leadership knew that government business leaders needed to know what technology they had, and the risks involved in order to make informed decisions about IT spending and security. That meant MNIT needed a complete picture of Minnesota's security risk posture, including a complete inventory of the state's information technology assets, and an accurate risk profile of those assets.

MNIT initiated the Security Risk Scorecard project to design a method of presenting a picture of agency information technology in a way that made sense to business leaders and to create an accurate inventory of their IT assets.

MNIT used a foundational framework, common business software, color coding, and plain business language to bridge the gap of understanding between business and information security. Now business leaders know exactly what information and technology they have, what the security risks are, and how their business decisions and investments impact those risks.

This project aligns with the priorities of Minnesota Governor Mark Dayton, who recently signed onto "A Compact to Improve State Cybersecurity," an effort by 38 governors to improve state cybersecurity. The compact covers three main areas of cybersecurity, which Minnesota is already leading on: (1) build cybersecurity governance; (2) prepare for and defend against cybersecurity threats; and (3) develop a cybersecurity workforce.

It also aligns with the continuing top priority of MNIT's Commissioner and State Chief Information Officer Johanna Clyborne for the management, control, and protection of state systems and data to safeguard the privacy and security of all Minnesotans.

Our Scorecards are now baked into operations, and they are improving the security of information and information technology systems for State of Minnesota government. Staff in our six Line of Business teams schedule individual semiannual meetings with business leaders from each agency to review their Scorecards. Knowing agency business needs and constraints allows MNIT to reprioritize, escalate or postpone IT projects, making us more effective and efficient business partners.

EXEMPLAR

Security Risk Scorecards give business leaders a picture of the risks they accept by default. What makes this effort unique is that using common terms and format opens the way for frank conversations that could not occur before.

MNIT's technology leaders are now able to effectively communicate technology and cybersecurity risks to agency business leaders, who are accountable for that risk. Ensuring agency leaders have an understanding of their risk posture fosters a better partnership with MNIT to safeguard state systems and data. In addition, if we know about agency business needs in advance, we can reprioritize, escalate or postpone IT projects, making us more effective and efficient business partners.

Innovations stem first from choosing a holistic approach that covers all potential information at risk, not just technology systems and applications, but information in any form, such as sensitive information shared over the phone.

We chose a nationally recognized framework and business standards from the National Institute of Standards and Technology (NIST). This aligned Scorecards with state and national standard business practices so government leaders are using a common language that doesn't use IT jargon. The categories (identify, protect, detect, respond, recover) are intuitive to those with no IT background, so leaders understand the consequences of risks and posture.

MNIT's Security Risk Scorecard project used:

- The NIST Cybersecurity Framework to create, implement, and review our program, with organizational guidelines and benchmarks for critical infrastructure.
- The International Standards Organization (ISO) Cybersecurity Standard framework, a certifiable standard for securing all information and information technology systems.
- Microsoft Excel to display the Scorecards, software that is readily available and low-to-no cost because we already use it for other purposes.

Lastly, MNIT took this effort personally and proactively by leading the way. Staff in MNIT's six Line of Business teams meet semiannually with business leaders from each agency to review their Scorecard dashboards and analyze risks. Business leaders can then factor that knowledge into their decisions about IT projects.

CONCEPT

MNIT designed the Security Risk Scorecards to establish a consistent, repeatable method of informing government business leaders about the technology they had and the risks involved. With this knowledge presented in a way that made sense to them—in business terminology, not IT terms—they could make informed decisions about IT spending and security.

In order to do that, MNIT first needed a current picture of Minnesota's security risk posture, but a complete inventory of the state's information technology assets didn't exist, nor did we have an accurate risk profile of those assets. That initial work was required to form the foundation for the Scorecards.

MNIT developed a foundational framework that would be the core of our semiannual reviews with government business leaders. We used common business software, color coding, and plain business language to bridge the gap of understanding between business and information security.

The Security Risk Scorecard is actually a spreadsheet in Microsoft Excel that displays like an application, so there was no additional cost for custom software or development. Behind the scenes, a dataset generates detailed dashboards with numeric risk/maturity scores that roll up into a business-friendly main dashboard.

Building the foundational dataset was the most labor-intensive part of the project. Over the past three years, MNIT's enterprise security and IT staff gathered information about and from applications, infrastructure, computers, facilities and other business processes. The sheer volume of data was enormous. MNIT secures and manages systems at over 1,300 locations, supports and secures over 2,800 agency applications, oversees and delivers over 350 projects with major IT components, and maintains 4,368 virtual and 1,598 physical servers. MNIT delivers over 3,000,000 emails per week; and supports over 28,000 enterprise IP telephony stations. Some agencies also had specific federal and state compliance and data privacy regulations that factored into the process.

The dashboard for Scorecards allows business leaders to see at a glance exactly what information and technology they have, what the security risks are, and how their business decisions and investments impact those risks. The dashboard includes NIST's key framework areas: Identify (assets, information and technology), Protect, Detect, Respond, and Recover. The words use straightforward plain language, and they make sense to those who are unfamiliar with IT terminology. The language is endorsed by the National Association of Board of Directors and Business Associates. The NIST framework leverages business language to bridge the gap between non-IT business people and IT.

One of the best features of the project is that once the dataset and the Excel framework were created, the Risk Scorecards can be used forever. Updates are loaded semi-annually, so there is always a current snapshot of the risk and health of IT for the entire state. The concept and implementation are completely repeatable by anyone. The only cost is staff time to gather information and input it into the Scorecard.

The first pilots were tested in the summer of 2016, and Security Risk Scorecard reviews with agency business leaders were completed by the end of 2016. The reviews for the first half of 2017 were completed in June 2017 (except three agencies that will complete by the end of 2017).

SIGNIFICANCE

The scope of the initiative was to establish a consistent, repeatable method of informing government business leaders about the technology they had and the risks involved. The goal was to help them to make business decisions about IT projects.

To do this, the scope included gathering data about information technology and assets from each agency in the executive branch of Minnesota government, and creating a database that would generate an inventory and a dashboard for each agency.

There are no similar projects to MNIT's knowledge in state government, so this project was unique from the start. In a letter to the State CIO, Department of Human Services' business leaders called the Scorecard review meeting "the most useful meeting of the year." All other agency leaders have expressed positive feedback on this initiative.

MNIT security staff have had significant interest from other states. Our staff have given nearly a dozen presentations about this project in the past year, including to the Minnesota Society of CPAs' Risk Management Conference and a recent MS-ISAC conference.

This project aligns with the priorities of Minnesota Governor Mark Dayton, who recently signed onto "A Compact to Improve State Cybersecurity," an effort by 38 governors to improve state cybersecurity. The compact covers three main areas of cybersecurity, which Minnesota is already leading on: (1) build cybersecurity governance; (2) prepare for and defend against cybersecurity threats; and (3) develop a cybersecurity workforce.

It also aligns with the continuing top priority of MNIT's Commissioner and State Chief Information Officer Johanna Clyborne for the management, control, and protection of state systems and data to safeguard the privacy and security of all Minnesotans.

IMPACT

For the first time ever, Minnesota has targets for each of the key Risk Scorecard areas. Security staff collaborated with each agency business to set a target for each area – where they think they need to be in terms of risk and maturity of their systems. This will always be different for each agency, for example the Department of Revenue may have greater risk, and need more maturity than systems at the Department of Agriculture.

Additionally, MNIT and our agency business partners have never before had a complete picture of all the information technology being used by Minnesota state government, and the risk posture of the state. We aren't aware of any other states that have similar efforts in place.

Before this project, government business leaders made decisions about IT spending without knowing or understanding the risks. Ultimately, risk is owned by the business. However, that risk, and the relative

business decisions around that risk, affect the service delivery, operations, and cost of the services MNIT provides to those agency businesses.

The real focus of the Scorecards was to show business leaders the health of the information systems and applications they rely on. That knowledge paved the way for hard conversations that many state governments are engaged in about modernizing outdated systems and applications. Knowing the risks involved helps business and IT leaders make informed decisions about when and how to invest in IT.

The benefits of using the framework to create the Scorecard is that it leverages business language to bridge the gap between non-IT business people and IT. It's easier to set benchmarks when there's a common language for leadership and their peers.