MINNESOTA IT SERVICES

One Minnesota IT – Building a Whole-of-State Technology Strategy

Jon Eichten | Deputy Commissioner

Minnesota IT Services (MNIT)

MNIT is the information technology agency for Minnesota's executive branch, but we also have a statewide role…

- **Executive branch:** agencies, boards, councils and commissions in the state (All IT Services)

- **Non-executive branch:** higher education, school districts, public libraries, legislative branch, judicial branch, constitutional offices, counties, cities, and other government organizations in the state. (Network Services, Security Services, Statewide Leadership)

MNIT has more than 2,800 staff members who:

Support over **41,000** end users for over **70** agencies/boards

Secure and manage over **2,700** agency applications and a statewide network connecting **3,000+** locations

Oversee and deliver over **490** projects with major IT components

Manage over **$470M** IT budget for project/program delivery

Resolve **38,000+** service desk tickets a month with a **4.7** (1-5 scale) satisfaction rating

Detect and resolve over **5,200** security incidents a year

Minnesota IT Services

Mission

We partner to deliver secure, reliable technology solutions to improve the lives of all Minnesotans.

Vision

An innovative digital government that works for all.

Customers/Partners

- Cabinet-level state agencies
- Non-cabinet boards, councils and commissions
- Higher education
- School districts
- Public libraries
- Legislative branch
- Judicial branch
- Constitutional offices
- Cities and Counties

What our work touches

My work helps keep maps and land data accurate, allowing communities in Minnesota to make informed decisions about property, land use, and development.

My work directly impacts the efficiency of state employees, allowing them to serve the public to the best of their ability.

Programs I work on help incarcerated persons find a path forward after prison and keep prisons safe and secure.

I help keep your data secure.

We help get critical info to Minnesotans through websites that we host and support.

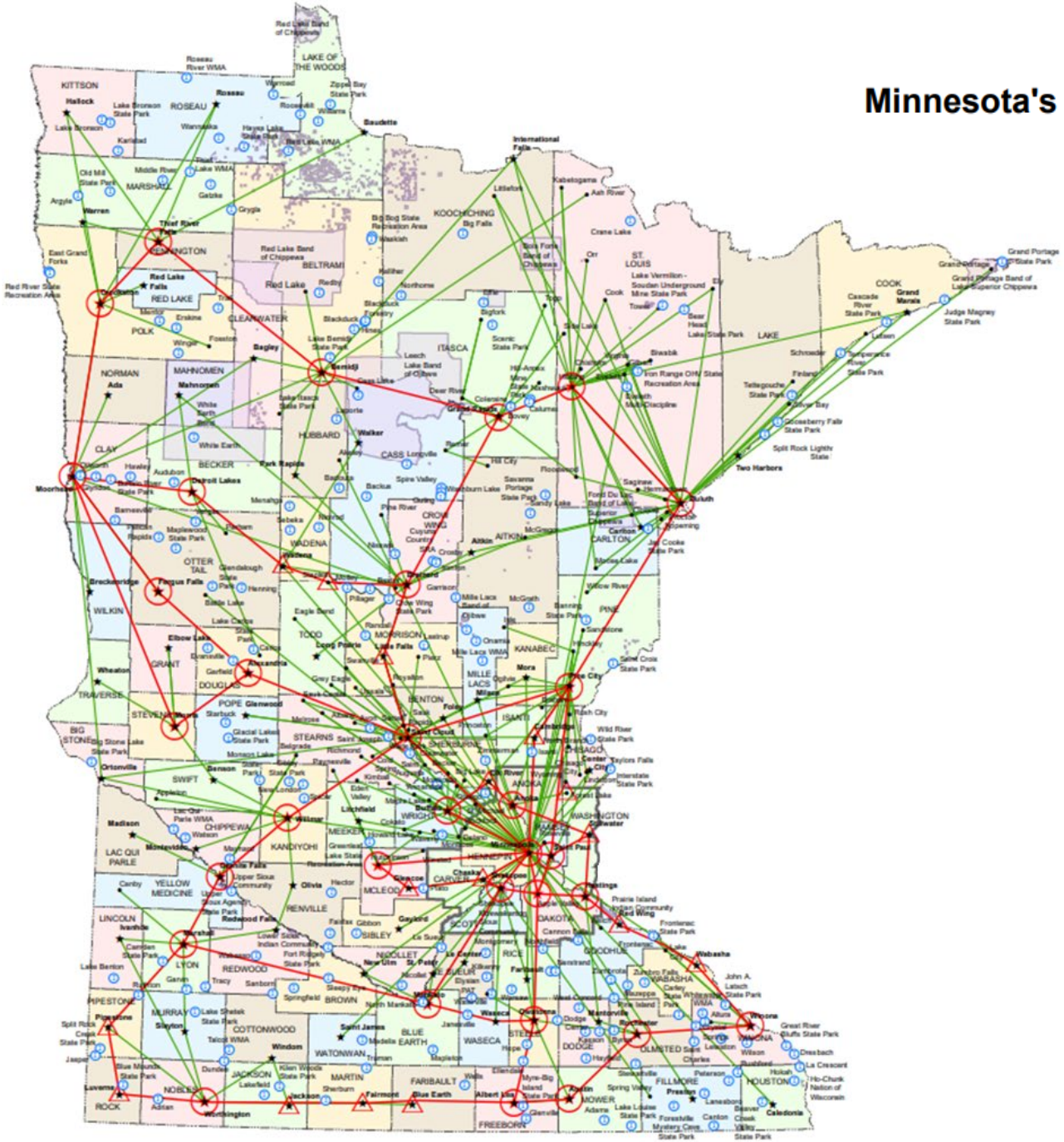
Getting people access to healthcare benefits.

How we connect the state

- Minnesota's Network for Enterprise Telecommunications: MNIT's wide area network (WAN) service that connects sites to the state network.
  - Enables secure, reliable connectivity and support for data communications between agency sites, MNIT Enterprise data centers, external party sites, and to the internet.
  - Backbone speeds are up to 100Gbps, with up to 1Gbps wire speed to the desktop in most location.
  - Connects all 87 counties, 300 cities, and 200 public higher education campuses.
- MNIT and its predecessor agencies have been serving K-12 education with network services since the early 2000s.

MNET
Minnesota's Network for Enterprise Telecommunications

A Public-Private Partnership Delivering an Integrated Statewide Network



MINNESOTA IT SERVICES

How we serve state agencies

- **Hybrid Service Model**
  - **Enterprise services.** Network, hosting, data center, email, laptop/desktop, service desk, cybersecurity, etc.
  - **Agency-based services.** Dedicated MNIT team embedded in agencies to support their unique applications and data needs.
- **IT Strategy/Leadership**
  - **Policies and Standards.** Security, accessibility, responsible use of AI
  - **IT Strategy.** Cloud strategy, build vs. buy, IT procurement, modernization, maximizing value of data

Goal: Unify MNIT and Agency Strategies

Improve our data collection processes to:

- Better connect information across systems.
- Make data more accessible.
- Ensure MDE and our partners use valid and reliable data to evaluate the success of programs and initiatives.

- Shift from program-based data collection to integrated data exchange.
- Advocate for modern data strategies.
- Reduce compliance burden and provide valuable insights.

The role of the Technology Advisory Council (TAC)

- Advisory body for technology services including private-sector IT experts, public sector leaders, and legislators.
- Recommendations for MNIT and state agencies on modernizing technology and improving service delivery.
- BRC-IT reports (TAC predecessor): 2020 and 2021
- TAC reports: 2023 and 2024

TAC Recommendations

- Sustainable Funding
- Project to Product
- Customer Experience
- Agile Adoption
- Business Process Redesign
- Artificial Intelligence
- Data Sharing

Investing in the future of IT in Minnesota

Cybersecurity

Cloud migration

Technology Modernization Fund

Technology Modernization Fund highlights

Drinking water sampling

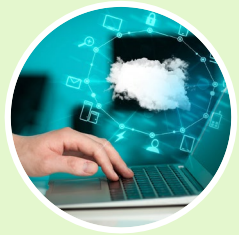
Help Minnesotans access safe water

MNsure easy enrollment

Connect uninsured Minnesotans to insurance

MDE county auditor data

Provide online data submission for county auditors, data access for school districts



PELSB upgraded scanning

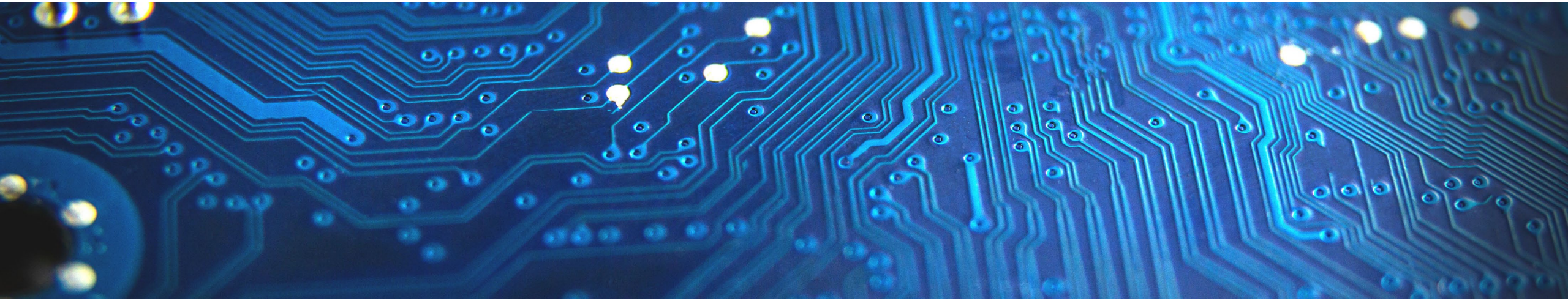
Update technology to support educator licenses and electronic documents

Veterans healthcare

Upgrade data use to improve care and operational efficiency

Cybersecurity investments

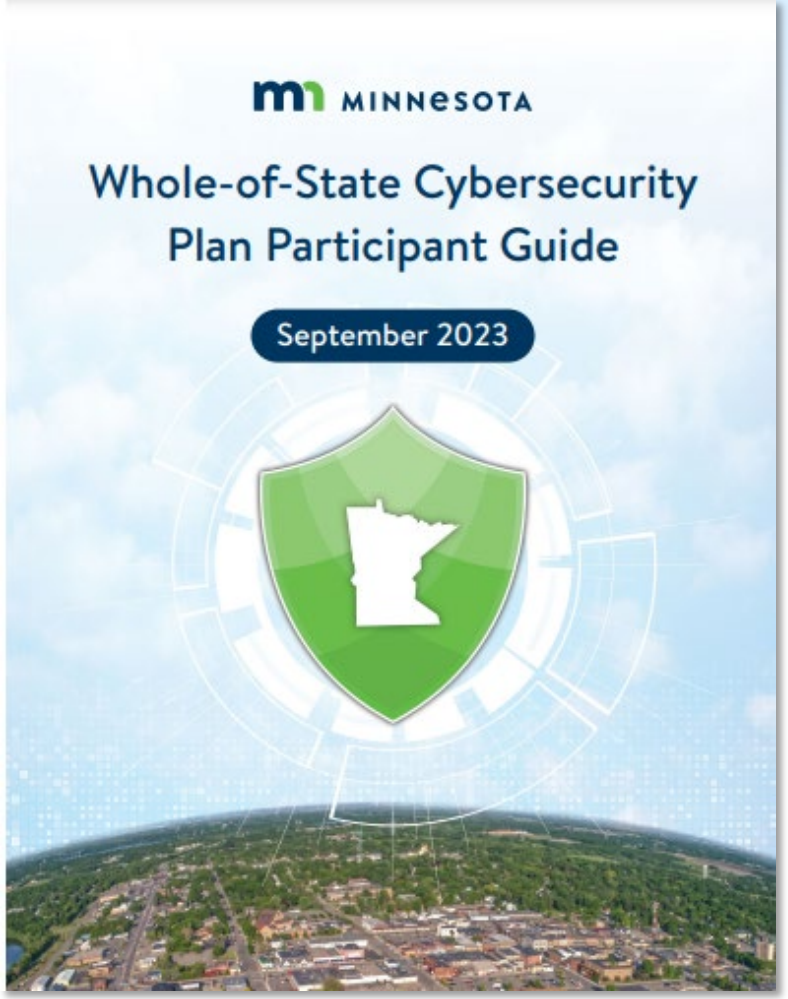
- **Security infrastructure**
  - Modernize Security Operation Center
  - Expand implementation of web application firewalls
  - Implement autonomous threat prevention
- **Balancing security, fraud protection, and better experiences**
  - LoginMN enterprise-wide identity service.
  - Mature governance, risk, and compliance program.
  - Advance vendor risk management program.
- **Whole-of-state approach**
  - New grant-subsidized services for local governments and school districts.
  - Mandatory cybersecurity incident reporting.
  - Partner with local and federal entities to deliver services.



Building relationships: Cybersecurity in E-12

Brandon Hirsch | Director of Government Relations

First steps in cybersecurity



Whole-of-State Cybersecurity Plan: Allows leaders at every level of government to work together, share resources and information, and leverage federal and state funding. They work collaboratively on cybersecurity issues to create a united front against threat actors.

- Focus on fundamentals
- Keep governance top-of-mind
- Coordinate early and often
- Stress communication and relationship building
- Low- and no-cost options
- Remove barriers to compliance

Minnesota Whole-of-State cybersecurity goals

1. Mature cyber capabilities throughout the state

2. Increase participation in programs and services known to work

3. Collaborate and share information throughout the state

4. Strengthen the cyber-resiliency of critical infrastructure

Cyber Navigator program

- Three cyber navigators and a supervisor supporting E-12 cybersecurity.
- Assists schools in risk assessments, policy development, and response planning.
- Helps districts implement security best practices and access resources.
- Connects schools with CISA's cyber hygiene services.
- Contact Cyber Navigator Team at CN.MNIT@state.mn.us

Risk assessments

Metro State University

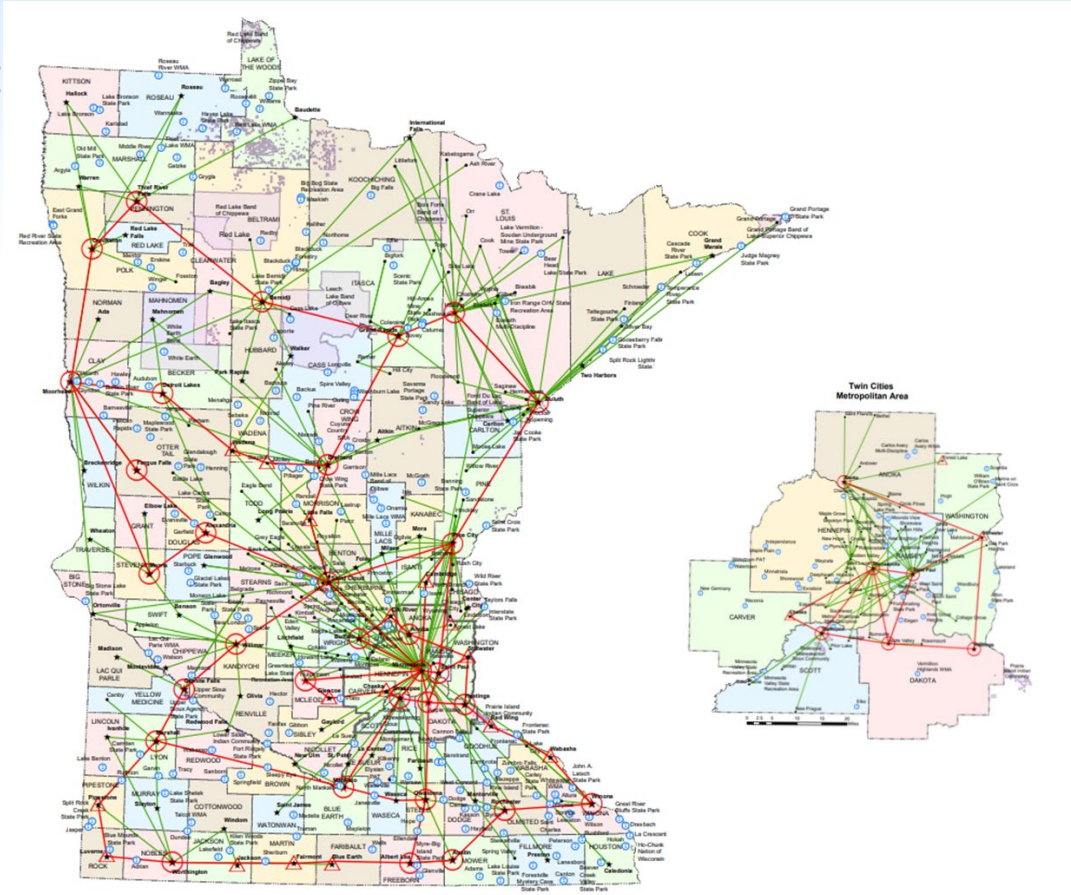
- Center for Internet Security's Critical Security Controls
- Implementation Group 1 Essential Cyber Hygiene
- Risk Assessment Methodology Continued collaboration
- https://www.metrostate.edu/mncyber/clinic

Cybersecurity and Infrastructure Security Agency

- Cybersecurity Advisors
- Cybersecurity Performance Goals
- Ransomware Readiness Assessment
- Onsite

What it means to be on MNET

- Baseline cybersecurity capabilities, including:
  - Incident response
  - DDoS & Radware
  - Cyber threat intelligence
- 24/7 service desk
- 24/7 network monitoring
- Network hardware lifecycle management



MNIT's Managed Detection and Response (MDR)

Grant-subsidized cybersecurity service available to K-12 school districts

- Fully managed, anti-virus tool to detect security risks and malicious activity
- 24/7/365 monitoring
- Rapid detection and containment
- Average response time ~ 7 minutes
- MNIT's Security Operations Center support and visibility
- MNIT and law enforcement collaboration
- Full remediation support, incident warranty

Value of MNIT's MDR Program

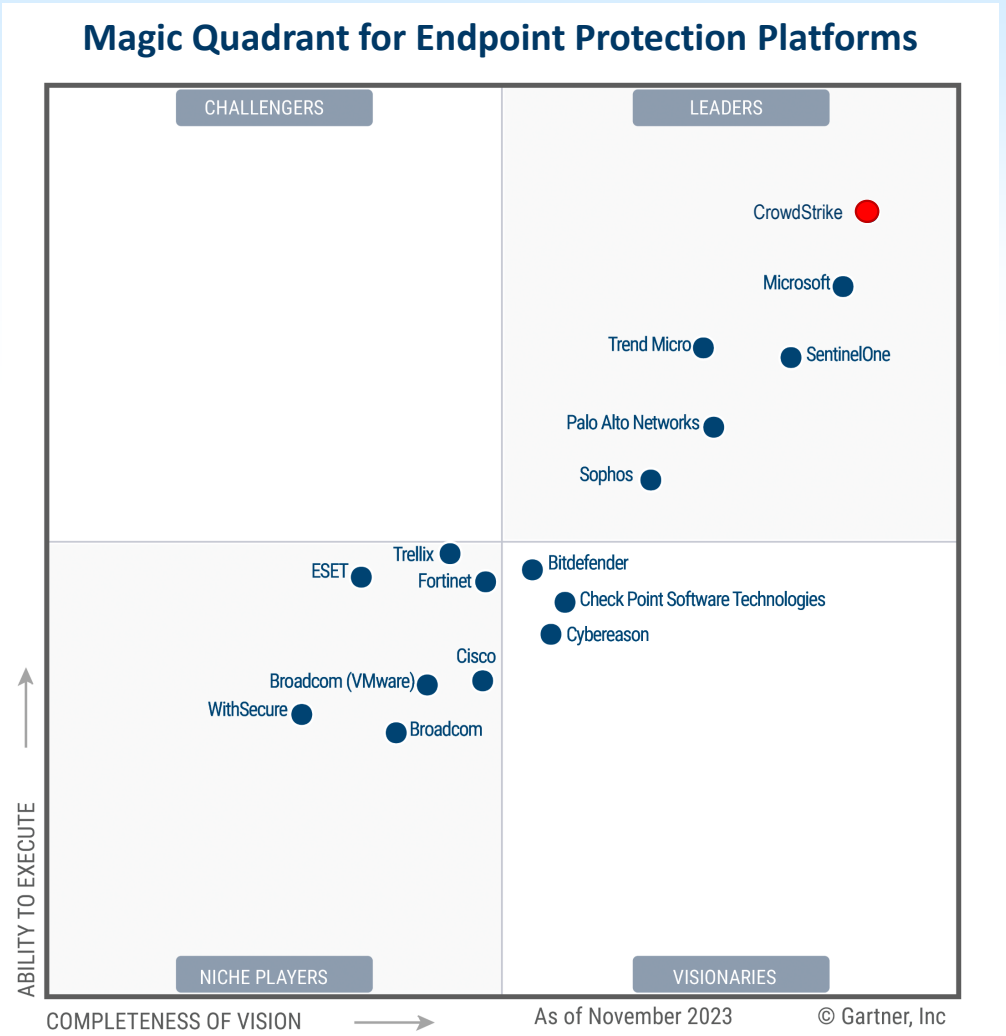
MDR looks for and blocks the types of attacks that could lead to data breaches, ransomware.

- Reduces operational disruption
- Low-cost, high-value solution
- Cost-sharing model

Cost structure

2024	$18
2025	$22
2026	$32
2027	$38
Post-SLCGP	$46

**per device annually; current rates*



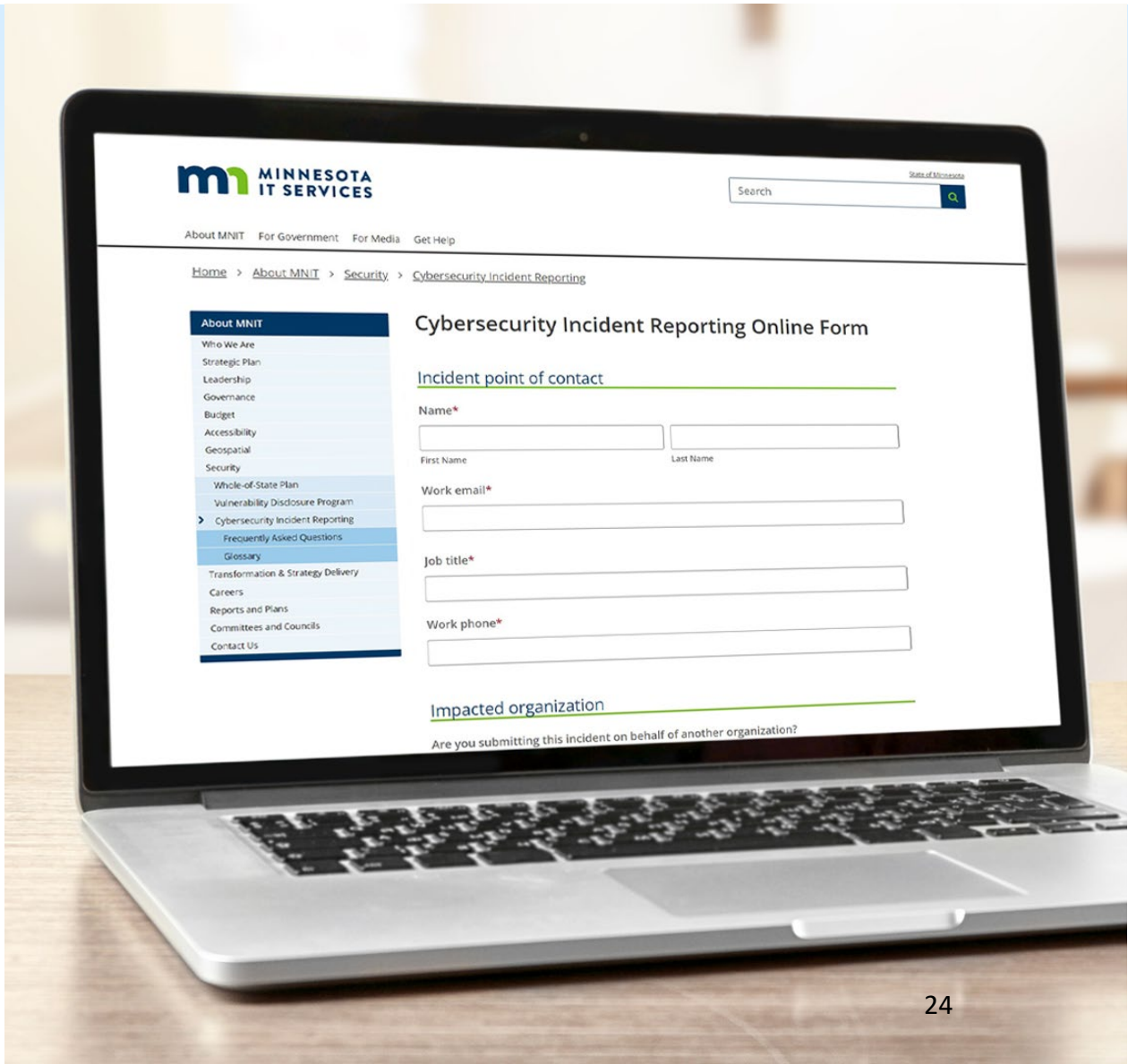
Cyber threat intelligence

- **Cyber navigators**
  - Connect school districts and local governments with resources and tools to bolster their cyber defenses
  - Collaborate with federal, state, and local government partners to identify the threat landscape in Minnesota
- Centralize feeds
- Dedicated resource
- Proactive intelligence gathering
- Processing event data (IOCs, TTPs, reporting)
- Collaboration & representation

Cybersecurity incident reporting

Reporting tool: mn.gov/mnit/cir

- Law took effect Dec. 1, 2024.
- Standardizes reporting protocols.
- State may collect information about cybersecurity incidents, anonymize it, and share it with appropriate organizations to strengthen cyber defenses statewide.



Cybersecurity incident reporting requirements

Who must report

- State agencies, political subdivisions; **school districts, charter schools, intermediate districts, cooperative units, and public post-secondary (higher education) institutions**.
- *Government contractors or vendors* that provide goods or services to a public agency must report an incident to the public agency.

When to report

- Within 24 hours if Criminal Justice Information is impacted.
- Within 72 hours of when incident was identified or occurred.

Reporting tool: mn.gov/mnit/cir

Cybersecurity incidents to report

What to report:
Cybersecurity incidents that impact services, systems, or people.

Types of incidents to report:

- Compromised account/password
- Defacement
- Denial of service
- Malware
- Network attack
- OT/ICS/SCADA
- Potential data exposure
- Ransomware
- Social engineering
- Unauthorized access
- Web application attack

Protected information

Reported cybersecurity incidents are:

- Security information pursuant to section 13.37.
- Not discoverable in a civil or criminal action absent a court order or a search warrant.
- Not subject to subpoena.

MNIT or BCA may:

- Anonymize and share cyber threat indicators and relevant defensive measures to help prevent attacks.
- Share cybersecurity incident notifications with potentially impacted parties through cybersecurity threat bulletins or relevant law enforcement authorities.

Cybersecurity incident reporting benefits

Shared information can help prevent other cyber attacks from occurring or help other organizations better remediate attacks.

Minnesotans

- Gain a better understanding of the nature of and impacts from cybersecurity events.

MNIT and BCA

- Gain awareness of the scope of incidents.
- Assist organizations in defending their IT resources.
- Understand how bad actors bypass security controls.
- Track and identify trends in cybersecurity incidents.

Public entities

- May receive advisories or guidance from MNIT/BCA to help defend against cybersecurity threats.

Public leaders

- Gain improved quality of data related to cybersecurity risks.
- Able to better identify potential gaps that require resources to mitigate risk.

Questions?

Minnesota IT Services

jon.eichten@state.mn.us

brandon.hirsch@state.mn.us