2025 CYBERSECURITY INCIDENT REPORT

January 2026

Minnesota IT Services
600 North Robert Street
St. Paul, MN 55146

TABLE OF CONTENTS

Minnesota Statutes, Chapter 3.197, requires the disclosure of the cost to prepare this report.
The estimated cost of preparing this report is $7,465.

EXECUTIVE SUMMARY

Cyberattacks against federal, state, and local governments continue to rise in both frequency and sophistication. These threats have disrupted critical services across the country and in Minnesota, and responding to these ever-evolving threats requires new strategies and tactics. To strengthen its cyber resiliency, Minnesota adopted a coordinated, whole-of-state approach. Minnesota IT Services (MNIT) leads this effort by aligning partners, applying industry best practices, and expanding access to advanced tools that prevent, detect, and respond to cyber threats.

In the past year alone, MNIT's managed detection and response (MDR) service analyzed more than 222 million security events and initiated 650,000 automated investigations — evidence of both the scale of threats and the value of enhanced monitoring.

The Cybersecurity Incident Reporting (CIR) law further strengthens cyber resilience by creating a secure, centralized system for collecting cyber threat reports from public entities. This information allows MNIT to deliver timely advisories, support rapid response, and share insights that help Minnesota governments defend against evolving threats.

This data gives MNIT and its partners a clearer picture of who is being targeted, which threats are emerging, and how attacks impact operations — providing the insight needed to strengthen defenses across the state.

This report examines Minnesota's:

- **CIR key findings:** Incident types, reporting volume, and who submitted reports.
- **CIR impact:** Improvements in reporting practices and interagency collaboration.
- **Data and trends:** Cyber threat patterns in Minnesota and nationwide.
- **Current resources:** Effectiveness of existing cybersecurity tools and support.
- **Opportunities to strengthen Minnesota's cyber posture:** Areas to further enhance Minnesota's cyber resilience.

As the cyber threat landscape continues to evolve, the CIR law has proven to be a critical tool for reporting, documenting, responding to, and mitigating incidents. It also provides essential information that MNIT shares with local governments to increase awareness and help prevent similar attacks. Working alongside federal, state, and local partners, Minnesota remains committed to protecting public data and strengthening our shared infrastructure.

BACKGROUND

The Minnesota Legislature amended Minnesota Statutes 16E.36 in 2024 to require MNIT and the Minnesota Bureau of Criminal Apprehension (BCA) to establish a cybersecurity incident reporting system that accepts the submission of timely, secure, and confidential cybersecurity reports from public agencies, government contractors, and private entities. Beginning Dec. 1, 2024, the law requires public agencies and government contractors to report cybersecurity incidents that impact the public agency.

MNIT partnered with the BCA in 2024 to create an online reporting form now available on MNIT's website to report cybersecurity incidents that impact services, systems, or people.

July 2024: MNIT began proactive outreach to more than 500 contacts across public entities to raise awareness about the new law, clarify who is affected, outline what to expect, and share the timeline for implementation. As part of this engagement, MNIT invited feedback on the CIR form and its instructions to ensure the process was straightforward and that the information collected was both relevant and complete. Based on this input, MNIT, working in partnership with the BCA, refined the form and guidance materials to better support agencies in meeting their reporting responsibilities.

Sept. 30, 2024: In accordance with the law, MNIT posted instructions on the CIR webpage for submitting cybersecurity incident reports and opened the form to optional reporting. Some entities began using the CIR form to report cyber incidents. The website includes the reporting form, instructions for how to report, a list of entities required to report, descriptions of the types of incidents to report, when reports must be made, and alternative ways to report if access to the form is limited. In addition, the website includes answers to frequently asked questions, a glossary of terms, and an outreach toolkit.

October 2024: MNIT again sought input from the 500+ contacts on the reporting form and instructions. MNIT used that feedback to finalize the form and instructions.

November 2024: In the weeks leading up to the effective date of the CIR law, MNIT conducted targeted outreach to over 600 contacts within public entities statewide to reinforce awareness of the law and its applicability. MNIT extended invitations to two informational CIR webinars and provided recommended actions to help agencies educate internal stakeholders about the new requirements. One week prior to the law's implementation, MNIT followed up with the same group, sharing access to the recorded webinars along with detailed guidance on the law and its reporting obligations.

Dec. 1, 2024: Effective date of the CIR law. Public entities began reporting.

Jan. 31, 2026: Beginning this date, and annually thereafter, the CIR law requires MNIT to submit a report on its CIR collection and resolution activities to the Governor and to the Legislative Commission on Cybersecurity. The report must include, at a minimum: information on the number of notifications received and a description of the cybersecurity incident types during the one-year period preceding the publication of the report; the categories of reporting entities that submitted cybersecurity reports; and any other information required in the submission of a cybersecurity incident report, noting any changes from the report published in the previous year.

Reporting guidelines

A cybersecurity incident is defined by law as an action taken using an information system or network that results in an actual or potentially adverse effect on an information system, network, or the information it contains.

Entities required to report: Under Minnesota Statutes 16E.36, the following public agencies and government contractors must report to MNIT and the BCA: cities; counties; townships; higher education (post-secondary); kindergarten-12th grade (K-12) school districts, charter schools, intermediate districts, and cooperative school units; law enforcement agencies; state agencies; and government contractors or vendors that perform work for or on behalf of a public agency with access to or hosting the public agency's network, systems, applications, or information if impacting data belonging to a public entity. Note: Reporting a cybersecurity incident is not a new requirement for state agencies. Under state security policies, state agencies are required to report security incidents to MNIT's Enterprise Service Desk and should continue this practice to be compliant with the CIR law.

Types of incidents to report: Required entities should report cybersecurity incidents that impact services, systems, or people. This includes successful cyber events that compromise agency accounts, systems, data, or events that bypass security controls and target government systems. Incidents where Criminal Justice Information (CJI) and systems may have been impacted are always reportable. Types of incidents entities were asked to report in 2024-2025 (these are defined at the end of the report):

- Compromised account/password
- Defacement
- Denial of Service (DoS)
- Malware
- Network attack
- Operational Technology/Industrial Control System/Supervisory Control and Data Acquisition (OT/ICS/SCADA)
- Potential data exposure
- Ransomware
- Social engineering
- Unauthorized access
- Web application attack

When to report: A report must be made within 24 hours if CJI and systems are impacted; or within 72 hours of the government entity or the public agency or the contractor discovering the incident or reasonably identifies or believes that a cybersecurity incident has occurred. MNIT and the BCA understand some incidents may take longer to fully investigate. However, we encourage entities to submit an initial report within this timeframe to document the event and capture key indicators for sharing through state threat channels. The required cybersecurity incident reporting is in addition to other reporting requirements, like those for the Office of the Legislative Auditor (OLA) and data breach reports required by Minnesota law. Entities are expected to submit reports more than once if needed.

CIR DATA AND KEY FINDINGS

Minnesota has long recognized the importance of cybersecurity incident reporting as a foundation for strong statewide defenses. Executive branch agencies have reported cyber events to MNIT through the MNIT Security Operations Center (SOC) for years, providing consistent visibility into threats affecting state systems.

The CIR law significantly expanded that approach. For the first time, the law requires local governments and public education entities to report cybersecurity incidents that affect their operations. It also requires contractors and vendors to notify the public entities they serve when an incident could impact government systems or services. Together, these requirements strengthen Minnesota's ability to understand emerging threats and coordinate a more unified response across the public sector.

This inaugural report reflects the first full year of CIR data collection, covering the period from Dec. 1, 2024, when the law took effect, through Nov. 30, 2025. During this timeframe, Minnesota received 334 reports through the CIR form.

- 283 of the 334 reports were in-scope, meaning they were confirmed cyber events or potential cyber events that affected public agencies or personnel during the reporting period.
- 269 of the 283 in-scope reports were from non-executive branch entities such as counties, cities and K-12 schools.

Additional activity during this period included:

- 25 incidents were reported directly to the BCA and not captured by the CIR form.
- Additional events were identified through open-source data and not reported as required by the CIR law.

Reported incidents included a range of cybersecurity events:

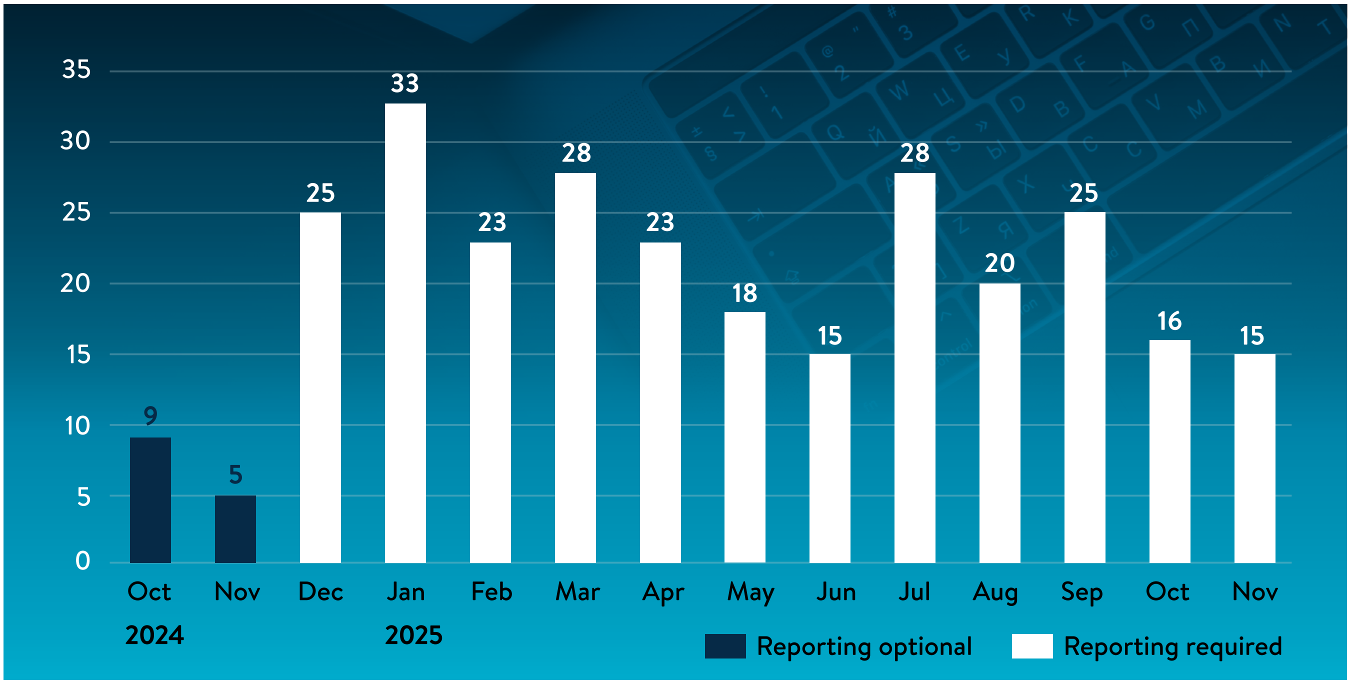
- Compromised account/password
- Potential data exposure
- Unauthorized access
- Malware
- Social engineering

Reporting entities represented a broad cross-section of Minnesota's public sector and local government partners, and include:

- K-12 public schools
- Counties
- Cities/townships
- Higher education
- Law enforcement

Because this is the first full year of data, we anticipate clearer and more defined trendlines in 2026.

CIR reports submitted



Optional reporting began Sept. 30, 2024. Required reporting began Dec. 1, 2024. From Dec. 1, 2024, through Nov. 30, 2025, entities reported 269 in-scope cybersecurity incidents via the CIR form.

Reports submitted by entity

REPORTING ENTITY	REPORTS SUBMITTED
K-12	81
County	69
City/township	53
Higher education	19
Law enforcement	13
State	12
Critical infrastructure and key resources (CIKR)	9
Personal	8
Nonprofit	2
Other	2
Vendor	1
TOTAL	**269**

CIR reports by incident type

When using the CIR form to report an incident, entities can report one or more incident types occurring at one time. Below are types of incidents reported either individually or in combination with others at least six or more times.

INCIDENT TYPE	COUNT
Compromised account/password	95
Potential data exposure	20
Compromised account/password, potential data exposure, unauthorized access	18
Other	17
Social engineering	11
Unauthorized access	11
Compromised account/password, potential data exposure	9
Malware (general)	6

Additional data on incident types

- 72 additional combinations of incident types were reported five or fewer times.
- 156 of the 269 CIRs (58%) included compromised accounts/passwords as an incident type. (Meaning, in addition to the 122 listed in the table, 34 more incidents of compromised accounts/passwords were reported in combination with another incident.)
- 31 of the 269 (12%) CIRs included social engineering in combination with other incident types (eight of which also included compromised accounts/passwords).

Key takeaways

In the past year:

- The CIR law took effect Dec. 1, 2024.
- 269 in-scope cybersecurity incidents were reported via the CIR form.
- Compromised account/password were the most common type of incidents reported.

CIR IMPACT

With additional cyber threat information, MNIT and the BCA enhance their ability to track, document, respond to, and mitigate cybersecurity incidents, improving how Minnesota understands and manages cyber risk statewide. Moreover, the law enhanced the state's collective cyber defenses by allowing MNIT and the BCA to collect information about cybersecurity incidents and share information with appropriate organizations supporting a more-informed approach to cybersecurity defense across the state.

This inaugural year of the CIR implementation demonstrated clear value:

- **Delivered faster access** to state support when local entities experienced cybersecurity events.
- **Created a clearer statewide picture** of threats by improving how incident information is shared and analyzed.
- **Built durable partnerships** across agencies, local governments, education entities, and critical infrastructure, reinforcing Minnesota's collective security posture.
- **Enhanced communication** and outreach to entities across the state, through a shared channel with 474 state and local partners.
- **Helped public organizations** navigate available state and federal cybersecurity resources, making it easier to find the right support at the right time.

The CIR reporting guidance focuses on collecting the most meaningful incidents — those that had a clear impact on the affected entity. The information entities provide on the CIR form is private under state law. The state cannot give this information to others without the reporting entity's consent, except certain government entities may access this information if allowed by law.

The law requires MNIT and the BCA to anonymize and share cyber threat indicators, general cybersecurity guidance, and relevant defensive measures to help strengthen cyber threat intelligence and help Minnesota governments defend against cybersecurity threats and prevent further attacks. MNIT and the BCA use this lens to shape the reporting requirements.

MNIT's Cyber Navigator team triages each report an entity submits. Reports involving Criminal Justice Information Systems (CJIS) data are provided to the BCA for follow up. The MNIT SOC is alerted of all reports for situational awareness and support when needed. Due to resource constraints, not every submission is provided direct follow up; however, all reporting entities may request support. Reporting entities are connected to state, federal, and other resources when appropriate and with the reporting entities' approval. All incident data is maintained for potential links to broader cyber campaigns or emerging threats.

The findings emphasize the value of consistent, statewide reporting. They also set the stage for understanding the law's broader impact.

Key takeaways

In the past year:

- Information sharing improved statewide.
- MNIT provided information on a shared channel with 474 state and local partners.
- Trust deepened among partners.
- Knowledge of state resources broadened.

MITIGATING CYBER THREATS

Preventing, detecting, responding

In its first year, the CIR law strengthened Minnesota's cybersecurity ecosystem by improving the flow of incident information, building trust among partners, and expanding visibility into cyber risks across public sector organizations. This growing body of data now enables Minnesota to move beyond individual incident response and begin identifying patterns, trends, and systemic risks over time. Data collected through CIR provides a clearer view of the types of incidents impacting public entities and allows MNIT to track those trends alongside national threat intelligence, open-source reporting, and executive branch cyber events monitored by MNIT's SOC.

Beyond the CIR reporting requirements, MNIT also utilizes information received through its Whole-of-State program, specifically, the MDR tools to complement CIR data. MNIT currently works with 215 local government entities and K-12 partners across the state that use MNIT's MDR tool. MDR is a 24/7 solution that looks for and blocks the types of attacks that could lead to data breaches, ransomware, or other major events that local governments are required to report through the CIR form. As of Nov. 30, 2025, MNIT's MDR covered nearly 64,000 local government endpoints (workstations and servers) and 55,000 executive branch endpoints.

Cybersecurity events from the past 12 months

222M

Events detected by MNIT's MDR tool

650,000

Automated investigations triggered by events

107,000+

Threats that had the potential to impact government services

This data comes from both the MDR tools offered to local governments through MNIT's Whole-of-State program and executive branch systems that MNIT's SOC manages. Given the average cost of a data breach exceeds $2.8 million, those prevented incidents represent an estimated $300 million. With approximately 3,300 eligible Whole-of-State entities, MNIT continues to bring more local government and K-12 partners into the MDR program.

Among the 215 local government and K-12 partners using MNIT's MDR tool:

- Six confirmed critical incidents were prevented in 2025. Each involved compromised credentials — the theft of usernames and/or passwords, typically tied to social engineering or phishing emails that rely on end-user manipulation.
- Forty reported CIRs, representing 19% of MDR participants or 26% of all reporting entities. Most reports from entities participating in the MDR program involved compromised passwords or accounts, which target identity rather than endpoint processes — malware, command and control, exfiltration of data, anomalous behavior, and other event types.
- In other cases, endpoints were compromised that did not have MDR installed — the events were vendor-related, or MDR stopped the malicious actions.

In contrast, the MNIT SOC's recording of cyber events greatly exceeds the volume of what is required to report via the CIR law. MNIT tracks every possible executive branch event, not just the ones that rise to reporting under the CIR. MNIT's visibility into state agency cyber events means that significantly higher volumes of events are recorded — many of which may not reach the bar of reporting under CIR.

MNIT also has a broader responsibility to support the non-executive branch sites on Minnesota's Network for Enterprise Telecommunications (MNET). One of the major advantages that MNET provides is greater visibility of activity and threats impacting local government and education, and provides MNIT the ability to detect and take action on malicious activity at a statewide level.

Key takeaways

In the past year:

- More than 200 local government partners use MNIT's MDR tool.
- Several entities joined MNIT's MDR program after experiencing a cybersecurity event.
- MNIT's MDR tool provided to local partners and executive branch agencies detected over 222 million cyber events.
- Of those, over 107,000 had the potential to impact government services.

IDENTIFYING AND TRACKING TRENDS

Cyber incidents do not occur in isolation. The CIR law gives Minnesota the visibility needed to move from one-off response to trend-based risk management by analyzing incident data alongside national threat trends, open-source reporting, and executive branch cyber activity monitored by MNIT's SOC.

Cyberattacks targeting state, local, and private sector entities in Minnesota happen regularly. Many are handled quietly because organizations respond and contain the incidents quickly, protect sensitive information, and maintain operational continuity. However, an unknown — though likely meaningful — number of incidents still go unreported. This is reinforced through incidents discovered through open-source reports, dark web monitoring, and reports submitted to the BCA. A cyber incident involving law enforcement data must be reported to the BCA within 24 hours of event discovery. In total, the BCA captured 46 of these events.

Entities may hesitate to report incidents for several reasons, including limited awareness of the law, staffing constraints, uncertainty about what qualifies as reportable, or concerns about reputational impact. The CIR law helps address these barriers by offering a clear, confidential reporting process that strengthens Minnesota's understanding of statewide cyber threats, and the support public organizations need.

MNIT and its Cyber Navigator team advocate for and continue outreach to in-scope entities regarding reporting a cyber incident. Early reporting supports entities with the best potential path to reducing risk. MNIT accepts reports at any point during an incident and continues to encourage in-scope entities to report early and to partner with Cyber Navigators on response.

When entities report cybersecurity incidents through the CIR form, they bolster MNIT's information sharing efforts with the local government community. Through reporting, entities learn from peers and stay current on threats and trends. When sharing CIR information across agencies and partners, we collectively reduce data silos that create opportunities for attackers.

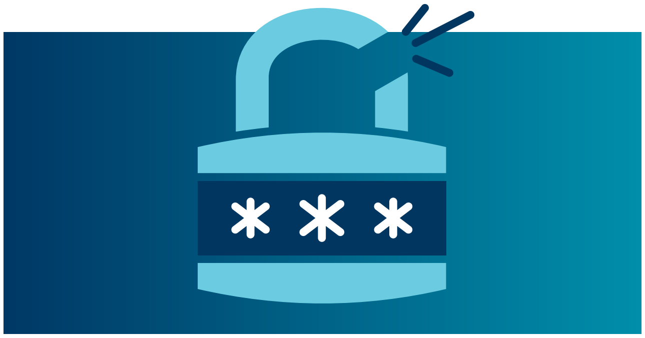
Common types of cyberattacks

Minnesota's CIR data shows that most reported cyber events involved phishing campaigns, compromised account/password, accessing malicious links/domains, and compromised email accounts. Early detection and quick response helped limit impacts and prevent additional attacks. Minnesota's experience with cyber events aligns with what is occurring nationally.

Phishing

Nationally, the FBI Internet Crime Compliant Center (IC3) National Threat Report shows phishing incidents account for the most reported incidents in 2024.[1]

- Financial gain was the top motive in more than half of cyberattacks with known motives, according to Microsoft, primarily through extortion or ransom.[2]
- According to Microsoft, identity-based attacks rose 32% in the first half of 2025 as adversaries increasingly used social engineering to compromise user identities and access sensitive data.[3]
- Adversaries have adopted generative artificial intelligence (AI) to improve the speed, scale, and realism of cyber operations, especially social engineering and influence campaigns, using large language models (LLMs) that require little skill or customization.[4]
- National and local government organizations face heightened cyber risk due to older infrastructure, constrained budgets, and sensitive data holdings. These factors make them attractive targets for both nation-state and financially motivated adversaries.[5]

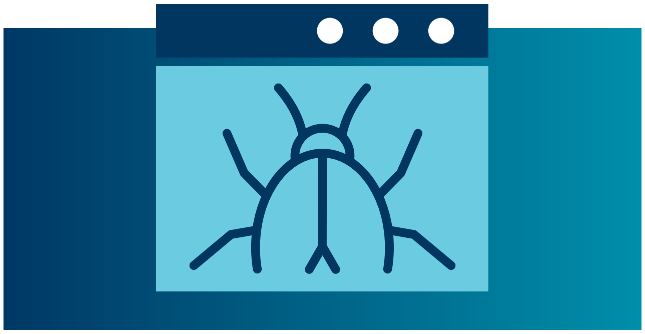


Compromised account/password

MNIT's SOC data shows similar trends impacting Minnesota's executive branch agencies, where compromised passwords (535), compromised accounts (146), and social engineering (133) account for nearly 40% of all incidents. When comparing only the events reportable under the CIR law that percentage increases to 80%.

However, these types of events do not necessarily indicate serious concerns, as the MNIT SOC utilizes risk-based identity management tools for alerting and forced password changes that identify and react to risks before deeper access occurs.

CIR reporting requirements emphasize incidents that impact data or involve novel techniques. To strengthen oversight, MNIT also includes in its executive branch metrics any event that triggers automated or manual analysis of abnormal account activity, regardless of whether a data impact is confirmed.



Malware

The MNIT SOC also manages endpoint detection tools, which record all event data as malware. Whether considering MNIT's Whole-of-State MDR program or the MNIT SOC's executive branch endpoint detection and response (EDR) tool, MDR does not detect compromised accounts or passwords, as those events involve identity compromise, rather than the system or endpoint.

MDR detects and responds to malicious activity — including abnormal processes, suspicious behaviors, malware, data exfiltration, and persistence techniques. By focusing on behavior, MDR helps identify serious threats earlier, reducing the risk of system and data compromises that can escalate into high-impact events like ransomware.

Ransomware

Ransomware and related attacks remain one of the most damaging cyber threats facing public and private organizations worldwide. Cybercriminals use malicious software to lock systems or encrypt data, then demand payment for its release. Ransomware often begins with a simple action — clicking a phishing email, opening a malicious link, or downloading an infected file — but can quickly disrupt critical services and compromise sensitive information.

According to national cybersecurity researchers, ransomware events are up 37% from 2024.[6] Data from public research indicates that the average cost of a data breach for a public sector entity exceeds $2.8 million per incident. Ransomware also disproportionately impacts small and medium sized organizations. Ransomware is present in 88% of data breaches in organizations with fewer than 1,000 employees.

A total of six ransomware events were reported via the CIR law. Only one of these events involved a MNIT Whole-of-State partner, and that event was prevented. In at least one other case, ransomware impacted a municipality before the threat actors pivoted to a network with MNIT MDR, where it was detected and prevented from spreading. Open-source, threat intelligence platforms, and dark web monitoring indicate nearly 70 ransomware events in Minnesota within the CIR law report timeline. Of these, over 40 involved local government or K-12 schools.

Preventing cyberattacks

State and national trends in cyber threats demonstrate that most cyber events can be avoided through basic measures:

- Providing regular security and phishing-awareness training for employees.
- Using security tools such as MDR — whether it's MNIT's MDR or a service with similar characteristics — to detect and block attacks that could result in data breaches, ransomware, or other major incidents.
- Implementing system security scans to identify unmet security controls and risk.
- Conducting regular external scans to identify areas malicious actors may exploit.

Key takeaways

In the past year:

- Six ransomware events were reported via the CIR law, and nearly 70 more ransomware events were identified through other means.
- In Minnesota's executive branch agencies, compromised passwords, compromised accounts, and social engineering account for nearly 40% of all incidents.
- Cyberattacks targeting public and private sector entities in Minnesota happen regularly.

CURRENT RESOURCES

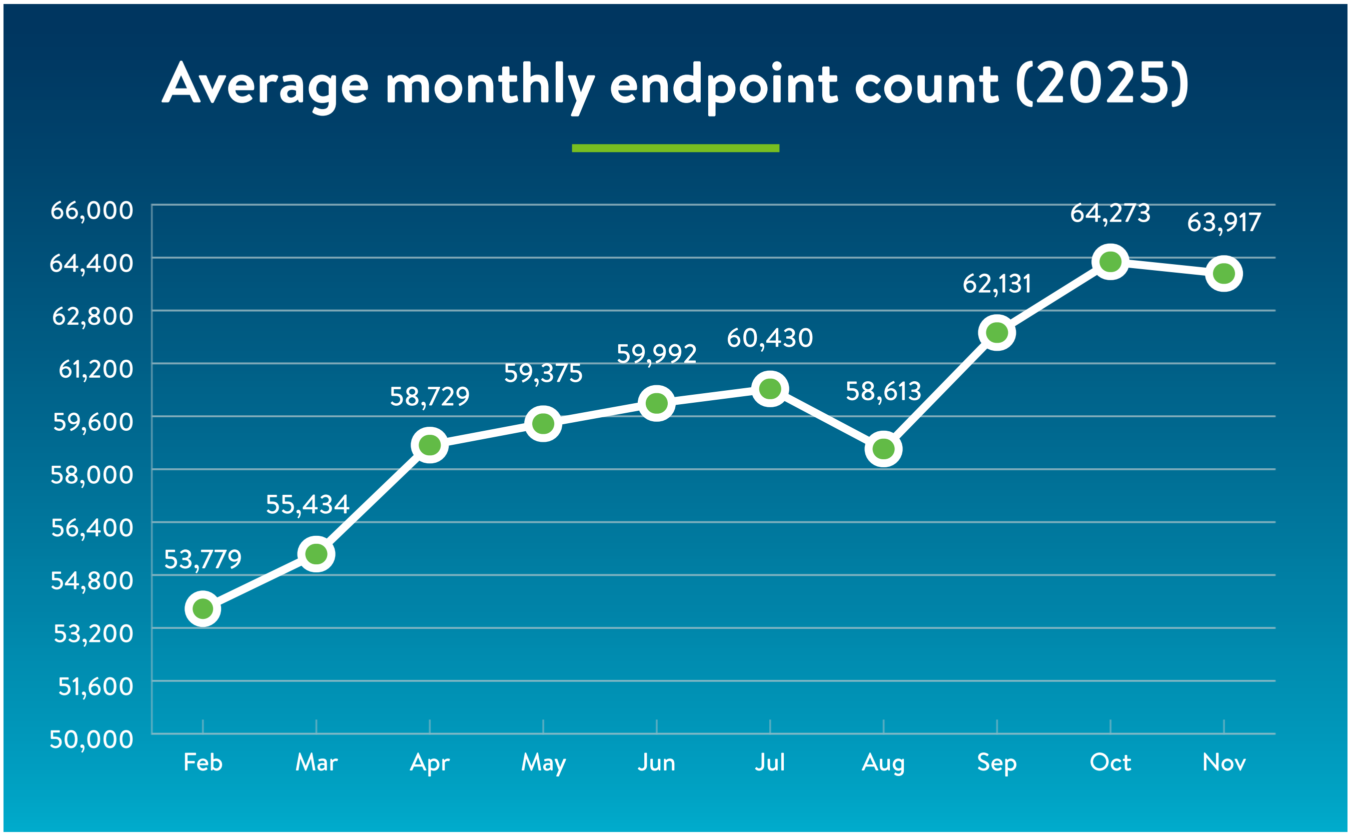
Taken together, these trends underscore the need for strong, accessible cybersecurity support across Minnesota. Through the Whole-of-State Cybersecurity Plan, MNIT offers enterprise-grade services to local government entities in Minnesota. These cybersecurity services help detect misconfigurations, prevent user errors, and protect against compromised credentials. This includes vulnerability scanning, endpoint detection, log collection, risk assessments, system security scans, malicious domain blocking, threat intelligence, and information sharing.

To help local governments strengthen and secure their cybersecurity defenses in an effort to present a united front against cyber threats, MNIT's services include:

- **Managed Detection and Response (MDR):** A 24/7 solution that looks for the types of attacks that can lead to data breaches, ransomware, or other major events and blocks those attacks.
- **Next-Generation Security Information and Event Management (Next-Gen SIEM):** This solution collects and aggregates log data from multiple sources, centralizing information for faster detection, analysis, and response.
- **Malicious Domain Blocking and Reporting (MDBR):** A cloud-based solution that uses technology to prevent IT systems from connecting to harmful web domains and limit infections related to malware, ransomware, phishing, and other cyber threats.

- **Internal Vulnerability Management Service (IVMS):** Enterprise-class vulnerability tools use scanning technology to identify, assess, prioritize, and remediate security vulnerabilities.
- **External Vulnerability Management Service (EVMS):** A combination of attack-surface management and vulnerability scanning tools perform external scans to assess an entity's threat and vulnerability posture from an outside perspective.

With the help of federal grant funds, including the State and Local Cybersecurity Grant Program (SLCGP) and the Statewide Security Monitoring Initiative (SSMI), MNIT provides these sophisticated cybersecurity tools for free or at a reduced cost to Minnesota's local entities. This has proven to be an effective method to help prevent, detect, and respond to cyberattacks.



Managed detection and response (MDR) is one tool MNIT offers to address potential cyber incidents. Over the past year, MNIT's MDR program increased to over 200 local governments and K-12 partners, covering more than 63,000 endpoints (workstations and servers).

Over the past year, MNIT broadened its free and low-cost cybersecurity services to include Next-Gen SIEM and MDBR to strengthen prevention, detection, and response capabilities. This expansion became essential as federal programs have reduced their previous support of state cybersecurity work.

The accelerated progress in combating cyber threats across the state is thanks, in large part, to federal cybersecurity grant funding. As of the writing of this report, there will be no additional federal investments after December 2026. This cessation of funds will put continued progress at risk.

Federal reductions have impacted coordination and decreased the availability of federal partners on the ground. With SLCGP and other key grants expiring soon, the long-term funding outlook remains uncertain. It is worth noting that the U.S. Congress is considering additional federal support for cybersecurity risk mitigation grant programs, but as of the publication date of this report, these negotiations are ongoing.

Key takeaways

In the past year:

- With the help of federal grant funds, MNIT provided free or low-cost services to hundreds of local government entities.
- These enterprise-grade cybersecurity services prevented and detected cyberattacks on state and local government partners.
- Providing resources statewide presents a strong, united front against cyber threats.

OPPORTUNITIES TO STRENGTHEN MINNESOTA'S CYBERSECURITY POSTURE

Minnesota's cybersecurity resources deliver the greatest impact when paired with strong, trusted partnerships. As federal conditions evolve, Minnesota continues to strengthen collaboration with state, local, and Tribal partners to share best practices, raise awareness of available tools, and improve coordination during cyber incidents.

MNIT works closely with the Minnesota National Guard Cyber Coordination Cell (C3), a unit established to strengthen cybersecurity support across all levels of government. The C3 played a critical role in the early response to the ransomware attack on the City of St. Paul in 2025, coordinating trusted expertise between city officials, private response firms, and the National Guard Cyber Protection Team (CPT). This activation marked the first time the CPT assisted any local entity with cyber incident response and recovery.

As cyber threats grow more complex and distributed, Minnesota must continue investing in local capacity building, information sharing, and interagency collaboration. Strong engagement closes long-standing gaps, improves early risk detection, and ensures that all public entities — especially smaller or under-resourced ones — have the tools and support needed to protect essential public services.

Opportunities for the state

Expand cybersecurity programs

Minnesota's state-supported services — such as MDR, Next-Gen SIEM, vulnerability scanning, threat intelligence, and information sharing — have proven effective and widely used. However, several federally funded programs face reductions or expiration, putting these and other programs at risk, including MDBR, risk assessments, community engagement, and tabletop exercises.

- **Opportunity:** Expand eligibility for state-supported services, increase deployment capacity, and help local governments transition away from expiring federal resources. Sustaining and scaling these services is critical for maintaining baseline defenses statewide.

Enhance training, policy guidance

Many public sector organizations lack updated cybersecurity policies, incident response plans, or clear governance structures. Partners frequently request policy templates, best-practice guidance, and support in implementing foundational security practices. The Minnesota Cybersecurity Task Force is currently developing many of these resources. Additionally, the Cyber Navigator team provides key updates on cyber incidents through the state, local and tribal (SLT) information-sharing site.

MNIT also conducts and participates in table-top exercises, including scenarios focused on critical infrastructure. Opportunities to integrate additional critical infrastructure sectors will help secure the state in the event of a major incident.

- **Opportunity:** Expand tabletop exercises, provide tailored policy-development guidance, and support entities in implementing and auditing critical security controls. Strengthening governance and preparedness will improve resilience across every sector.

Strengthen response support

Technical assistance during an active cyber incident remains one of the largest gaps, particularly for small, rural, or under-resourced entities. Current services focus primarily on preparation and post-incident recovery, leaving many organizations without timely support when an event occurs. This gap also contributes to reluctance among local entities to seek help or report incidents quickly.

- **Opportunity:** Coordinate services specifically for entities reporting under the CIR law. Expanding real-time response capacity would build trust, increase reporting, and reduce the severity of incidents across the state.

Strengthen CI, vendor oversight

Critical infrastructure (CI) tied to local government — such as health care, water/wastewater, and energy systems — often operates with limited cybersecurity resources. Heavy vendor outsourcing complicates visibility into security posture and incident reporting. Of the 400 CIR reports received, 10% involved critical infrastructure incidents. While Executive Order 22-20 improved communication between state agencies and CI sectors, many agencies still lack authority to require action or reporting.

In addition, some vendors fail to report incidents likely due to lack of understanding of reporting requirements. In at least one major incident impacting numerous Minnesota local entities, the impacted vendor failed to report after being notified of the CIR law.

- **Opportunity:** Clarify state authority for CI-related incident reporting, strengthen vendor oversight, and improve supply chain resilience through clearer expectations and standardized contract requirements.

Opportunities for local partners

Understanding Minnesota's opportunities requires examining the realities local partners experience. Across all levels of government in the public sector, cybersecurity measures are challenged by resources, capabilities, and competing priorities. Insufficient measures are maintained due to lack of awareness of available resources, or understanding of how available resources fit within a respective environment.

Building trusted relationships through expanded outreach is the initial step toward overcoming those barriers. Local partners can take steps to reduce common cybersecurity threats:

Strengthen their security posture

- Meet with MNIT's Cyber Navigator team to review their current security posture and discuss available tools. Compare their existing capabilities with free or low-cost services to identify immediate risk-reduction opportunities.
- Conduct a cybersecurity risk assessment — either independently or with assistance from MNIT or one of its partners.

Stay connected and informed

- Join MNIT's information-sharing community for local government. Use this forum to ask questions, learn from peers, and stay current on threats and trends.
- Attend the MNIT SOC Daily Brief and the Cyber Navigator monthly SLT meeting to maintain situational awareness and receive timely updates.
- Learn about the Minnesota Cybersecurity Task Force and track its work to direct funds toward shared cybersecurity challenges.

Improve communication and coordination

- Use secure communication channels when sharing sensitive information across agencies and partners. Reduce data silos that create opportunities for attackers.
- Build and maintain partnerships with state, local, Tribal, and federal entities to support coordinated response and shared defenses.
- Strengthen information sharing by participating consistently and helping mature statewide processes.

Expand local capacity

- Invest in capacity building through training, knowledge sharing, interagency collaboration, and participation in statewide initiatives.
- Expand their use of existing MNIT programs such as cyber navigators, MDR, and vulnerability scanning as resources allow.
- Prepare for changes in federal resources by planning for potential shifts in grant funding or the expiration of existing programs.

Enhance preparedness and response

- Define clear reporting expectations by engaging in efforts to clarify state authority for critical-infrastructure incident reporting.
- Develop or join incident response teams or services that support entities reporting under the CIR law.
- Participate in policy guidance, training sessions, and tabletop exercises to strengthen organizational readiness.
- Improve supply chain resilience by building stronger vendor and contractor oversight

Use data to target local risks

- Build tailored risk profiles using Minnesota sector-based data — such as trends observed across peer organizations — to understand threats most relevant to their environment.

Cybersecurity threats are damaging to government operations and an evolving public safety risk. By sharing information, we help provide a better understanding of the nature of and impacts from cybersecurity events to keep services available to Minnesotans and protect their data.

A MESSAGE FROM MINNESOTA'S CISO

This inaugural year of reporting provides Minnesota with clearer, more comprehensive insight into how cyber incidents are affecting public services across the state.

The findings in this report highlight the importance of a proactive defense, data tracking, and information sharing. The foresight of the Minnesota Legislature in passing the CIR law has enabled MNIT and executive branch partners to mature their ability to detect, prevent, respond to, and recover from cyber events.

With the CIR law in place, Minnesota now has stronger visibility into the threats facing public sector organizations and a clearer pathway for supporting them. The law builds a vital bridge between state and local partners — strengthening communication, improving information sharing, and fostering collaboration that is essential for defending Minnesota from cyber events

Data submitted through the CIR system shows that Minnesota's cyber threat landscape closely reflects national trends — both in the types of attacks occurring and in the increasing sophistication of threats targeting state, local, and private sector organizations.

MNIT uses this information to strengthen the state's overall cyber resilience. The data collected through CIR submissions helps MNIT and its partners better understand the impact of cyberattacks, identify patterns, and focus on the steps most effective in preventing future incidents.

The CIR law strengthens Minnesota's defenses by collecting cybersecurity incident information, anonymizing it, and sharing it with appropriate partners to improve readiness and response. In its first year, the law contributed to:

- Timely support for local organizations, connecting them with state resources that help prevent, detect, and respond to incidents.
- Improved intelligence sharing, creating stronger communication channels between state and local entities.
- Greater awareness of available cybersecurity tools and services, helping organizations build stronger defenses across all phases of cybersecurity.
- More trusted partnerships across Minnesota's public sector, supporting a coordinated approach to protecting state and local systems.

The CIR law marks another step forward in Minnesota's efforts to strengthen cyber resiliency. As federal conditions evolve, Minnesota continues to enhance communication and work with state, local, and Tribal partners to share best practices, raise awareness of available tools, and improve coordination during cyber incidents. Strong collaboration with state and local partners remains essential to building a layered, whole-of-state defense.

The cybersecurity resources and tools MNIT is able to provide at a subsidized cost — with the help of state funding and federal grants — have resulted in local governments being better positioned to protect Minnesotans' sensitive data. Collective, continued investment in people, processes, and technology will advance our cybersecurity maturity and help Minnesota prepare for and defend against emerging threats, including AI-enabled attacks.

Going forward, MNIT's ability to continue to provide subsidized cybersecurity services to local governments remains uncertain as select federal programs end and some grant funding is set to expire. MNIT's cost-sharing model ensures local governments have a vested interest in the cybersecurity services they choose to implement. However, with grant funding substantially offsetting the price of these critical services, some entities could struggle to maintain their level of cyber defense if they must fund the full cost with their local budget.

As cyber threats grow more complex and distributed, Minnesota must continue investing in local capacity building, information sharing, and interagency collaboration. Strong engagement closes long-standing gaps, improves early risk detection, and ensures that all public entities — especially smaller or under-resourced ones — have the tools and support needed to protect essential public services.

We thank the Minnesota Legislature for its continued investment in cybersecurity, along with federal support and grants that help protect Minnesotans' data. In 2026, MNIT will expand CIR analytics, strengthen partnerships, and further enhance statewide cyber protections. Sustained and strategic investment remains critical to advancing these efforts, funding future initiatives, and ensuring Minnesota's digital government remains resilient in the face of evolving threats.

John Israel

Chief Information Security Officer (CISO)
Minnesota IT Services

DEFINITIONS

Types of incidents public entities were asked to report in 2024-2025:

Compromised account/password

- **What it is:** When a bad actor gains access to someone's account by stealing credentials (passwords, usernames, etc.).
- **Reportable incidents:** When an employee's credentials are used to access accounts or data, regardless of whether a data breach occurs. Exposed employee credentials that were secured before a bad actor misuses them, if techniques were involved to gain access (optional if other defenses prevented access/misuse).

Defacement

- **What it is:** An attack where a bad actor alters the appearance of a website, usually to spread a message or cause embarrassment.
- **Reportable incidents:** Malicious changes or replacement of website or digital content, often involving social or political messaging, or meant to draw attention for other reasons. Redirection of website visitors to a different site, often containing malware or malicious content.

Denial of Service (DoS)

- **What it is:** A flood of traffic that overwhelms a website or online service, making it unavailable to users.
- **Reportable incidents:** Impactful DoS and Distributed Denial of Service (DDoS) events that disrupt services and evade defensive tools. Noteworthy DoS and DDoS events (even if mitigated or non-impactful) when the indicators, methods, or volume of attacks could help defend other entities.

Malware

- **What it is:** Malicious software that can damage or disrupt computers or networks, or steal information.
- **Reportable incidents:** Malware that bypasses security controls and executes without detection by existing defenses.

Network attack

- **What it is:** Unauthorized access to a computer network, often with the intent to steal data or cause harm.
- **Reportable incidents:** Malicious activity aimed at disrupting, damaging, or gaining unauthorized access to computer networks. Common network attacks include Denial of Service (DoS), Distributed Denial of Service (DDoS), Man-in-the-Middle (MITM), phishing, Structured Query Language (SQL) injections, malware, and insider threats.

Operational Technology/Industrial Control System/Supervisory Control and Data Acquisition (OT/ICS/SCADA)

- **What it is:** Attacks targeting systems that control industrial processes, such as factories or utilities.
- **Reportable incidents:** Successful attacks on OT networks, controllers, or human-machine-interfaces that result in physical damage or disruption.

Potential data exposure

- **What it is:** Unauthorized access of data maintained by a public entity that compromises the security and classification of data.
- **Reportable incidents:** Phishing attacks that lead to account compromise, unauthorized access, or data exfiltration. Any instance where personal data are obtained by deception or accessed, altered, deleted, and/or disclosed by the attacker. Exposed data on public sites, servers, or third-party applications where protected data may have been exposed publicly.

Ransomware

- **What it is:** Malware that encrypts (locks) users out of their data or systems until a ransom is paid to the attacker.
- **Reportable incidents:** Any instance of ransomware software that encrypts or locks data maliciously by a bad actor, even if encryption did not occur.

Social engineering

- **What it is:** When a bad actor tricks, manipulates, influences, or deceives people into sharing information they shouldn't share, downloading software that they shouldn't download, or performing actions that compromise security to gain control over a computer system or to steal information. Phishing is a type of social engineering where a bad actor sends fraudulent messages, often via email, to trick individuals into selecting links, revealing personal information, or installing malware.
- **Reportable incidents:** Novel phishing events that successfully bypass security controls and result in account or system compromise. Other emails, texts, or content that successfully trick employees into revealing information or taking other action not authorized by their employer

Unauthorized access

- **What it is:** Gaining access to a system, network, or data without permission.
- **Reportable incidents:** When cybersecurity tools are defeated, or cybersecurity controls are ineffective, and a bad actor gains unauthorized access to a system, network, or data.

Web application attack

- **What it is:** An attack targeting a website or online service to steal data, disrupt services, or gain unauthorized access.
- **Reportable incidents:** Impactful attacks that exploit vulnerabilities in web applications, leading to unauthorized data access or application modifications.

APPENDIX

The report is based on data collected from the Cyber Incident Reporting Law, open-source reporting, the MNIT SOC, and various other state, federal, and private sector partners.

1 Internet Crime Complaint Center (IC3). https://www.ic3.gov/annualreport/reports

2 Microsoft. 2025. *Microsoft Digital Defense Report 2025: Lighting the Path to a Secure Future*. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf#page=17

3 Microsoft. 2025. *Microsoft Digital Defense Report 2025: Lighting the Path to a Secure Future*. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf#page=11

4 CrowdStrike. 2025. *2025 Global Threat Report*. https://fusion.vsp.virginia.gov/wp-content/uploads/2025/07/CrowdStrikeGlobalThreatReport2025.pdf#page=19

5 Microsoft. 2025. *Microsoft Digital Defense Report 2025: Lighting the Path to a Secure Future*. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf#page=11

6 Verizon. 2025. *2025 Data Breach Investigations Report.* https://www.verizon.com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf#page=10