

Cybersecurity Overview for the Advisory Committee on Capitol Area Security

Brandon Hirsch, Director of Government Relations
Peter Alsis, Cybersecurity Navigator

MNIT has more than 2,400 staff members who:



Support over **35,000** end users for over **70** agencies/boards



Secure and manage over **2,500** agency applications and a statewide network connecting **3,000+** locations



Oversee and deliver over **400** projects with major IT components



Manage over **$400M** IT budget for project/program delivery



Resolve **35,000+** service desk tickets a month with a **4.7** (1-5 scale) satisfaction rating



Detect and resolve over **1,000** security incidents a year

MNIT Mission and Values

Mission

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

Vision

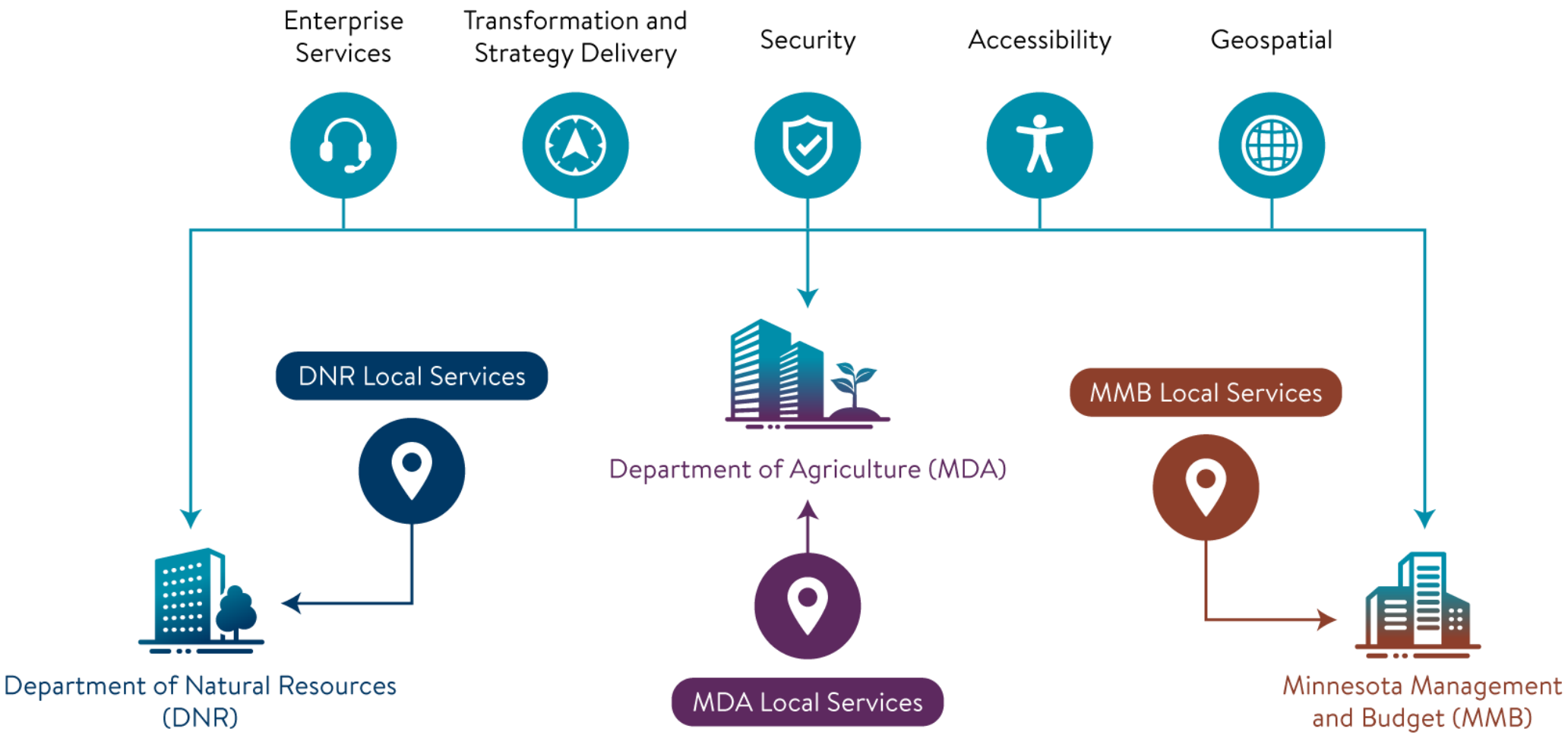
An innovative digital government that works for all.

Guiding Principles

- Practice servant leadership.
- Treat everyone with respect and dignity.
- Do the right thing, especially when it is difficult.
- Ask how your actions are reinforcing or removing structural inequity.
- Promote the common good over narrow special interests.
- Be accessible, transparent, and accountable.
- Include voices from communities who will be most impacted.
- Embrace change.
- Measure when you can.
- Engage with empathy.



How We Operate



Local agency services are largely unique to lines of government business and involve support of agency-specific applications and projects.

Agenda

- Cybersecurity Threats & the Public Sector
- Cyber Attacks Impacting Physical Security
- MNIT’s Approach & the Capitol Complex

Cybersecurity Threats & Public Sector

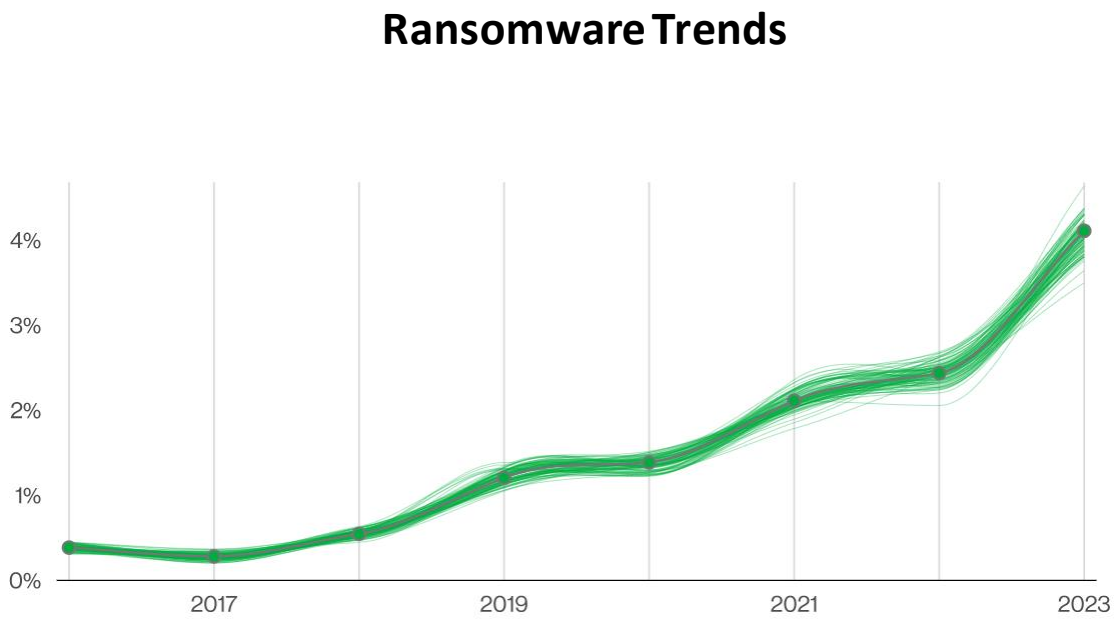
Persistent, Evolving Threats

- Nation-state/Advance Persistent Threats (APTs), as-a-service, hacktivists
- Impact on state, local, tribal, private sector, critical infrastructure
- Misconfigured devices, unpatched vulnerabilities, third-party vendors, compromised accounts, insider threat/phishing

THERE IS NO ZERO-RISK

Ransomware - Trends

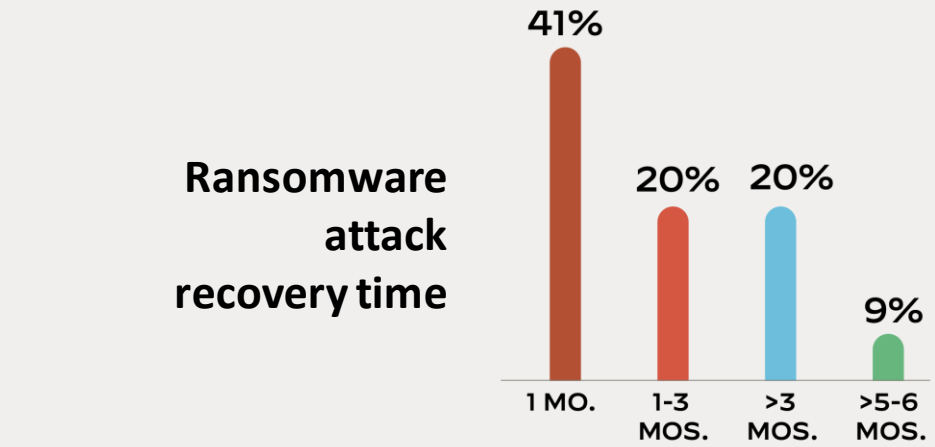
- Increased from 13% to a total of 25% of all cyber investigations
- 40% - Stolen remote access credentials
- 35% - Phishing through email
- 15% - Brute force of web applications

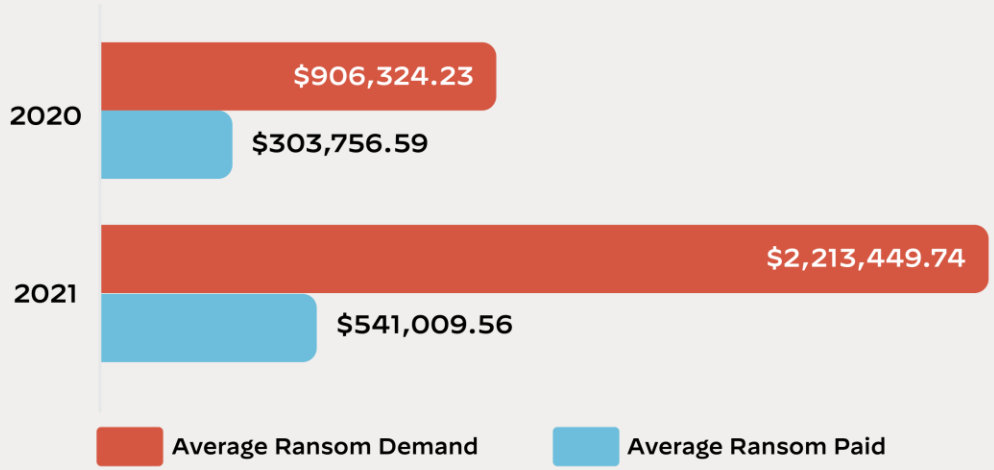


Source: Verizon Data Breach Investigation Report (DBIR) 2022 and M-Trends 2022

Ransomware - Impact

- Downtime & Disruption
  - 59% more than a month to recover
- Inaccessible Critical Systems
- Public Disclosure
  - Brand image & sensitive data
- Lack of backups to rebuild systems
- Extortion
  - 144% increase in average demand
  - 78% increase in average payments



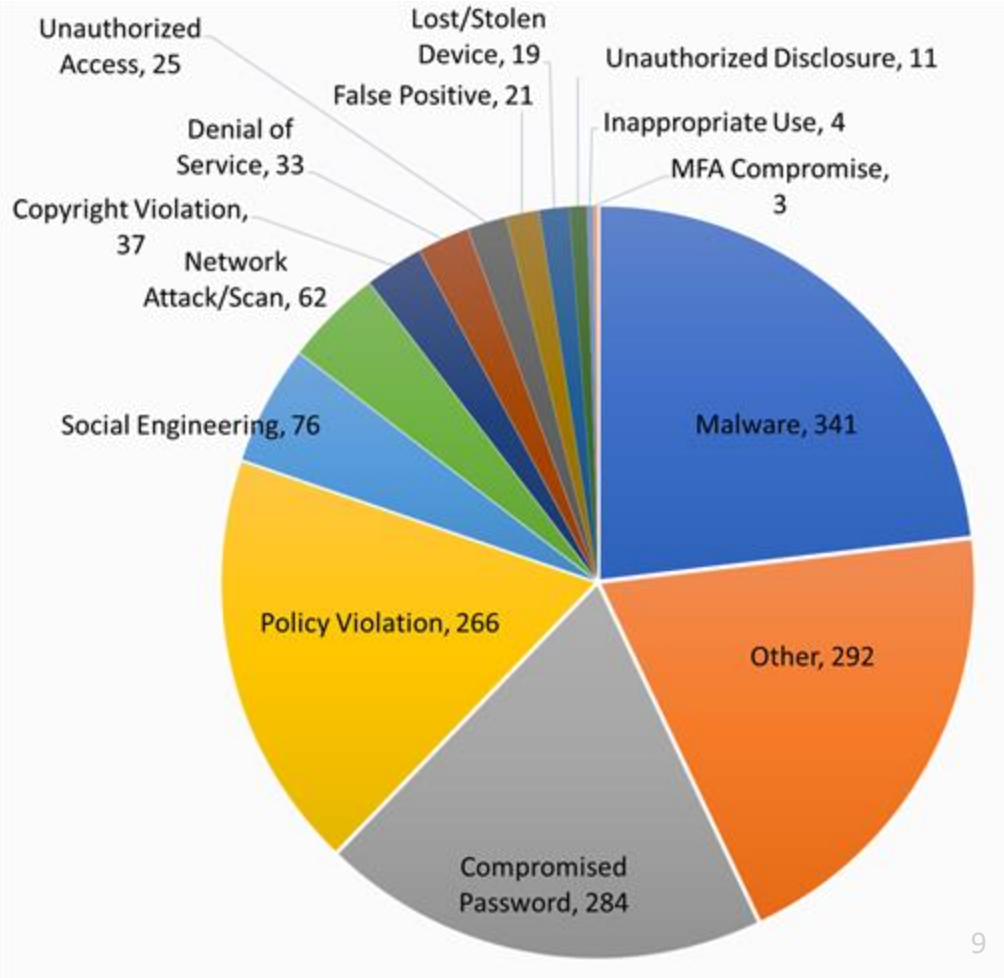


Source: Palo Alto Unit 42 Ransomware Threat Report 2022

Other Attacks

- Supply Chain
- Cyber Espionage
- DDoS
- Staging / Scanning
- AI impact

MNIT: Incident Response by Types, 2022-2023



Cyber Attacks Impacting Physical Security

- Critical Infrastructure
- Communications
- Third-party vendors and supply chain
- Law enforcement and Emergency Services

MNIT's Approach & the Capitol Complex

- Expanding Partnerships & Consolidating Efforts
- Communication & Collaboration
- Knowing broader threats and having actionable intelligence
- Service provider tools & services
- Learn & Adapt

Thank You!

Brandon Hirsch

Brandon.Hirsch@state.mn.us

Peter Alsis

Peter.Alsis@state.mn.us