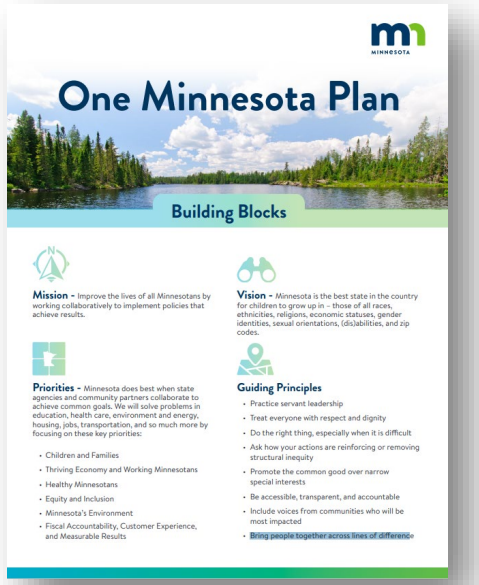
Minnesota IT Services

Tarek Tomes | Commissioner and State Chief Information Officer

MINNESOTA IT SERVICES

MNIT's Strategic Plan

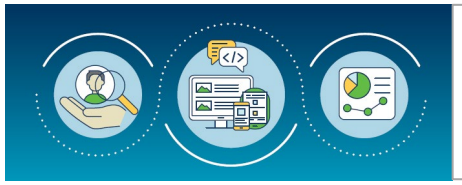
The One Minnesota Plan is part of the foundation of MNIT's Strategic Plan



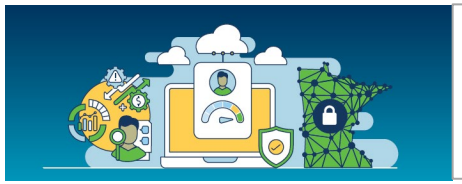
One MN Plan
Building Blocks

Strategic Plan
Public Facing

Strategic Themes



Customer Experience



Operational and Cybersecurity Excellence

Connected Culture

Legislative Investments in MNIT

MNIT

- **Advance Cybersecurity Statewide: $33 million**
  - $5.5 million in state matching appropriated funds for the State and Local Cybersecurity Grant Program (+$18M Fed.).
  - Investments in additional cybersecurity tools for the executive branch.
- **Enterprise Cloud Transformation: $34 million**
  - Funding to accelerate cloud adoption to enhance security and resiliency.
- **Targeted Application Modernization: $40 million**
  - Flexible multi-year appropriation to address outdated user-focused applications (both public and state staff) that pose cybersecurity risk or hinder modern user experience.

State of Cybersecurity - Global

The recently released 2023 Verizon Data Breach Investigations Report (DBIR) analyzed 16,312 cyber incidents & 5,199 confirmed breaches from last year.

Key takeaways:

- 95% of ransomware incidents cost orgs between $1-$2.25 million.
- 95% of all breaches were financially motivated.
- 83% were perpetrated by external actors.
- 74% involved human error (misconfigurations, phishing clicks, etc.).
- 24% involved ransomware.
- 19% were insider attacks.
- 17% were caused by social-engineering attacks.

Recent Global Cyber Incidents

T-Mobile

- Threat actor stole customer account data
- Application Programming Interface (API) exploited
- 37 million accounts compromised

Cloudflare

- 54% higher than previous DDoS attacks
- 71 million requests per second
- Impacted customer website availability globally

MOVEit

- 3,000+ organizations impacted (and growing)
- Zero-day vulnerability exploited
- Perpetrated by cyber-criminal organization

Zero-Day Vulnerabilities

VULNERABILITY

- A vulnerability in software, a system, or a service is found by a person who decides to keep it secret

EXPLOIT

- Knowledge of this vulnerability is used to develop ‘exploit code’ that is able to leverage the vulnerability to attack systems

ATTACK

- The Exploit is then used to perform one or more attacks on systems that are vulnerable

DAY ZERO

- ‘Day Zero’ is the day the vendor learns of the vulnerability and starts working to fix it