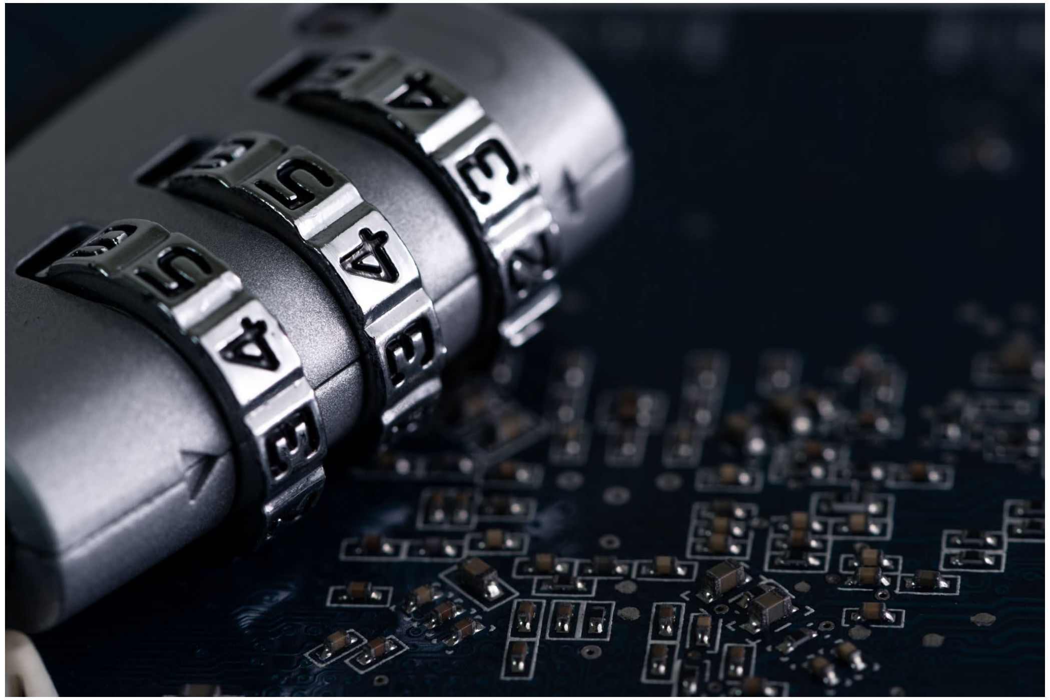
Information Services Security Overview

Joint Committee on Information Management and Technology

May 2025



Shane Walker
Chief Information Officer

Current State of Global Cybersecurity

Rising Cyber Attacks

The frequency of cyber attacks and data breaches is on the rise, posing significant challenges for organizations worldwide. Between 2021 and 2023, data breaches rose by 72%. In Q2 2024, there was a 30% year-over-year increase in cyber attacks globally, reaching 1,636 attacks per organization per week.

Increased Security Investments

Organizations are allocating more resources towards cybersecurity measures to protect sensitive data and systems from breaches.

Technological Vulnerabilities

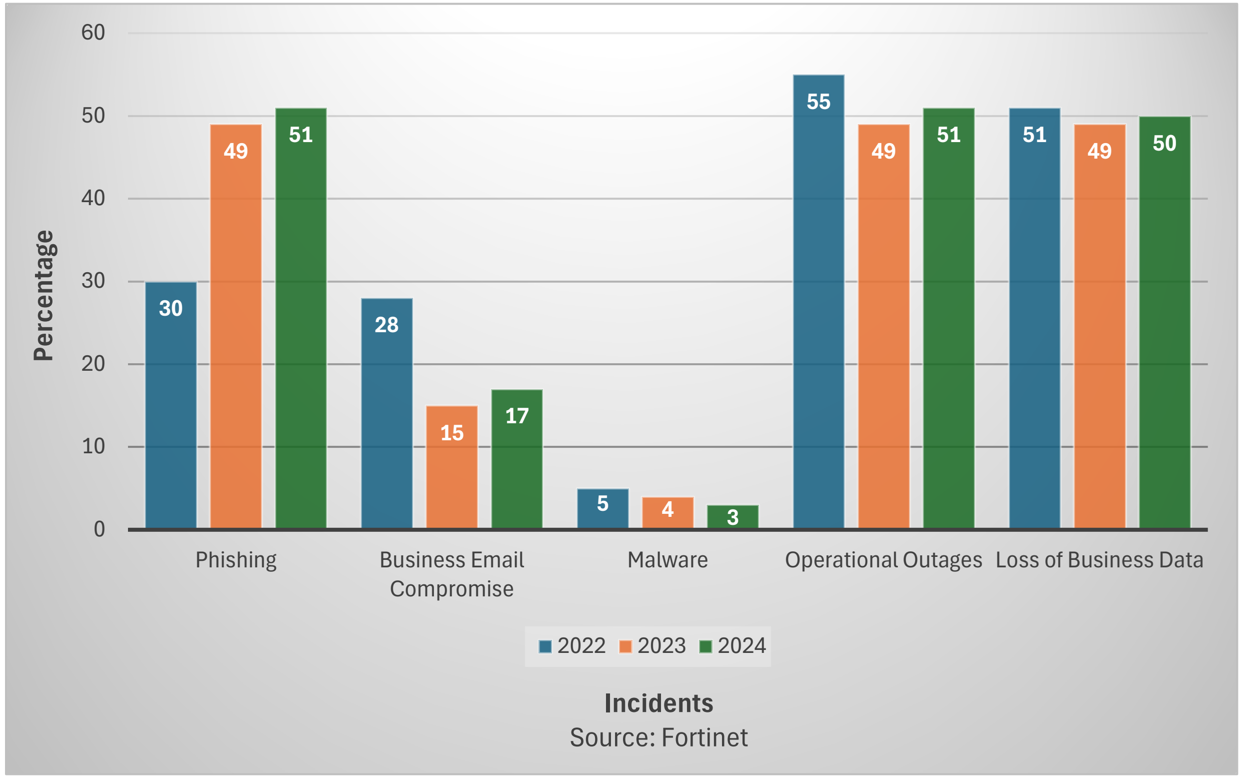
The rapid advancement of technology creates new vulnerabilities, making it essential for organizations to adapt their security strategies continuously.

Current & Emerging Global Threats

Common Crimes and Risks Online

Threat	Example
Business email compromise (BEC)	Scams exploit our reliance on email for business and personal communication, making them one of the most financially damaging online crimes
Identity theft	When someone steals your personal information, such as your Social Security number, to commit theft or fraud
Ransomware/Malware	Malicious software that blocks access to your files, systems, or networks and demands a ransom for their return
Spoofing/Phishing	Schemes aimed at tricking you into providing sensitive information to scammers

The advancements in AI have greatly improved the skills of hackers, allowing them to carry out complex and adaptive attacks with remarkable speed and accuracy. Nowadays, phishing emails often appear flawless, featuring impeccable grammar and formatting that enhance their believability.



Source: Fortinet

Cost of cybercrime:

- In 2022, globally around $6 trillion
- In 2023, estimated to be $8 trillion
- In 2024, estimated to be $9.5 trillion
- Global estimated in 2025 is projected to reach $10.5 trillion

Preventive Measures

FBI Recommended Countermeasures

✓ Cybersecurity Awareness Training	✓ Data Backup and Recovery
✓ Implement Spam Filters	✓ Software Restriction Policies
✓ Email Threat Scanning	✓ Use Least Privilege Access Controls
✓ Frequent Patching of Infrastructure	✓ Implement Server Virtualization
✓ Anti-Virus / Anti-Malware with frequent scanning	✓ Conduct Annual Penetration & Vulnerability Testing
✓ Segment IT and OT networks	✓ Secure Remote Access
✓ Limit Internet Exposure	✓ Monitor all assets
✓ Use Strong Passwords and Multi-Factor Authentication	✓ Use Passkeys

Preventive Measure Strategy

People

- An educated & proactive user community
- Subject matter experts on staff
- Vendor & peer partnerships

Process

- Frequent & established patching process for all infrastructure
- Outside audits & penetration testing
- Threat detection & remediation
- End user training
- Enhanced authentication

Technology

- Firewall protection
- Email filters
- Anti-virus / Anti-malware software
- Storage backup
- Server virtualization
- Disaster recovery
- 3rd party vendor services

More Legislative Statistics

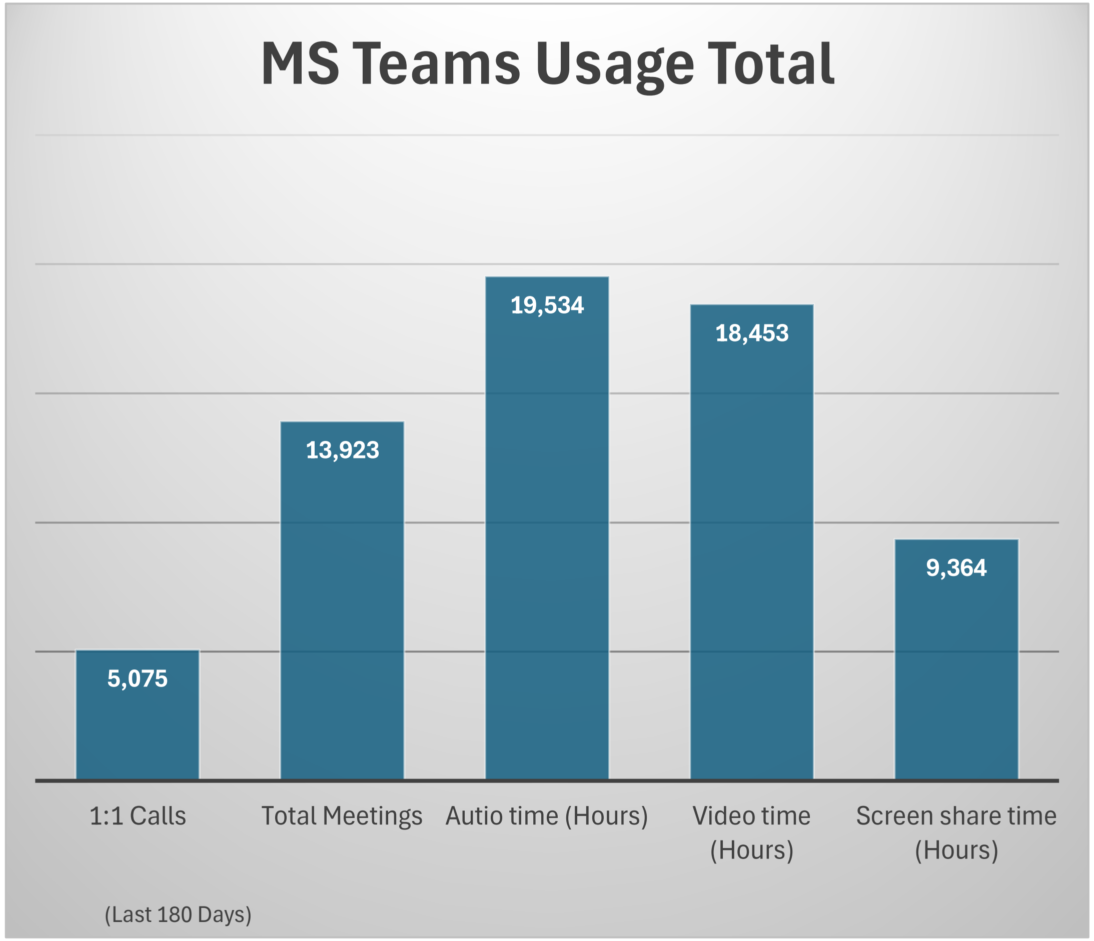
Video Usage Feb 13th – May 20th

- Total views of Committee meetings, floor sessions: 897,978
    - Live: 579,095
    - Video on Demand: 278,267
    - 85% of videos are fully watched

Total Uploads Written Testimony: 91,758
Total Registration for Committee Meetings: 16,669

Legislative Internet traffic

- 1.3 Terabytes of Internet traffic has moved through the Legislative network



Information Traffic Since Start of Session

System Usage Feb 13th – May 20th

- Total OLIS page views: 6,290,502
- OregonLegislature.gov: 1,772,677

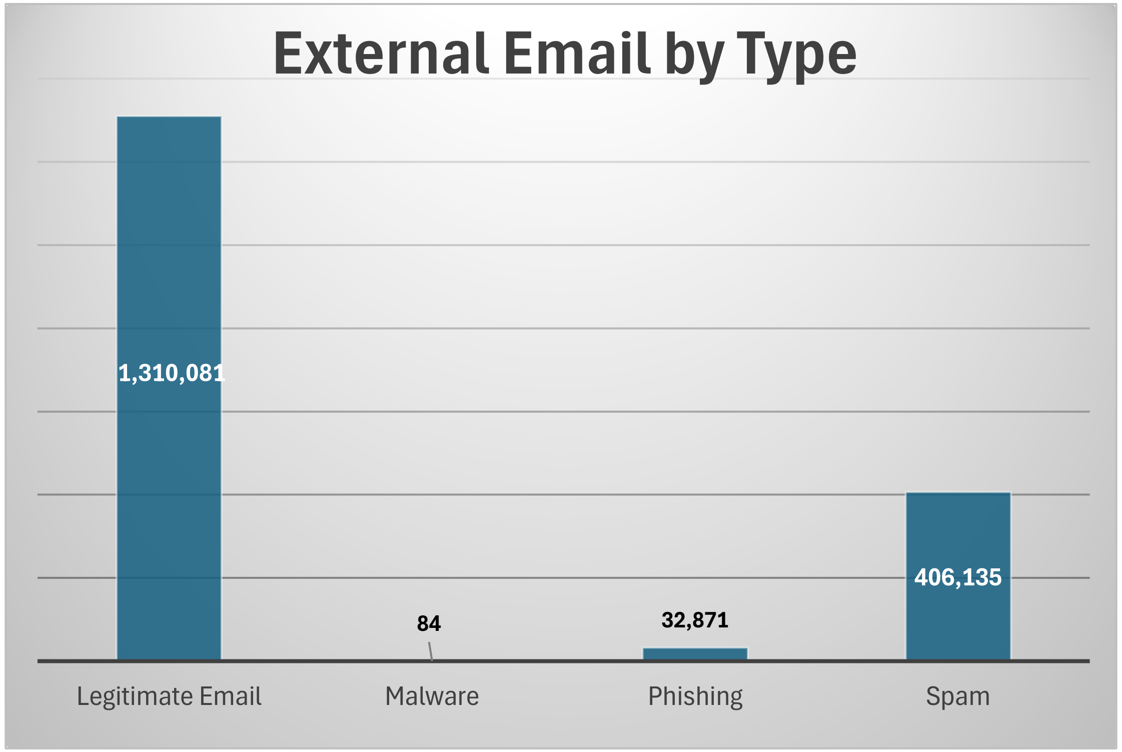
Capitol E-Subscribe

(People who have subscribed to bills, committees, Member press releases, etc.)

- Total emails sent to subscribers: 13,804,351
- Total number of people currently subscribed: 688,590

ODATA Usage

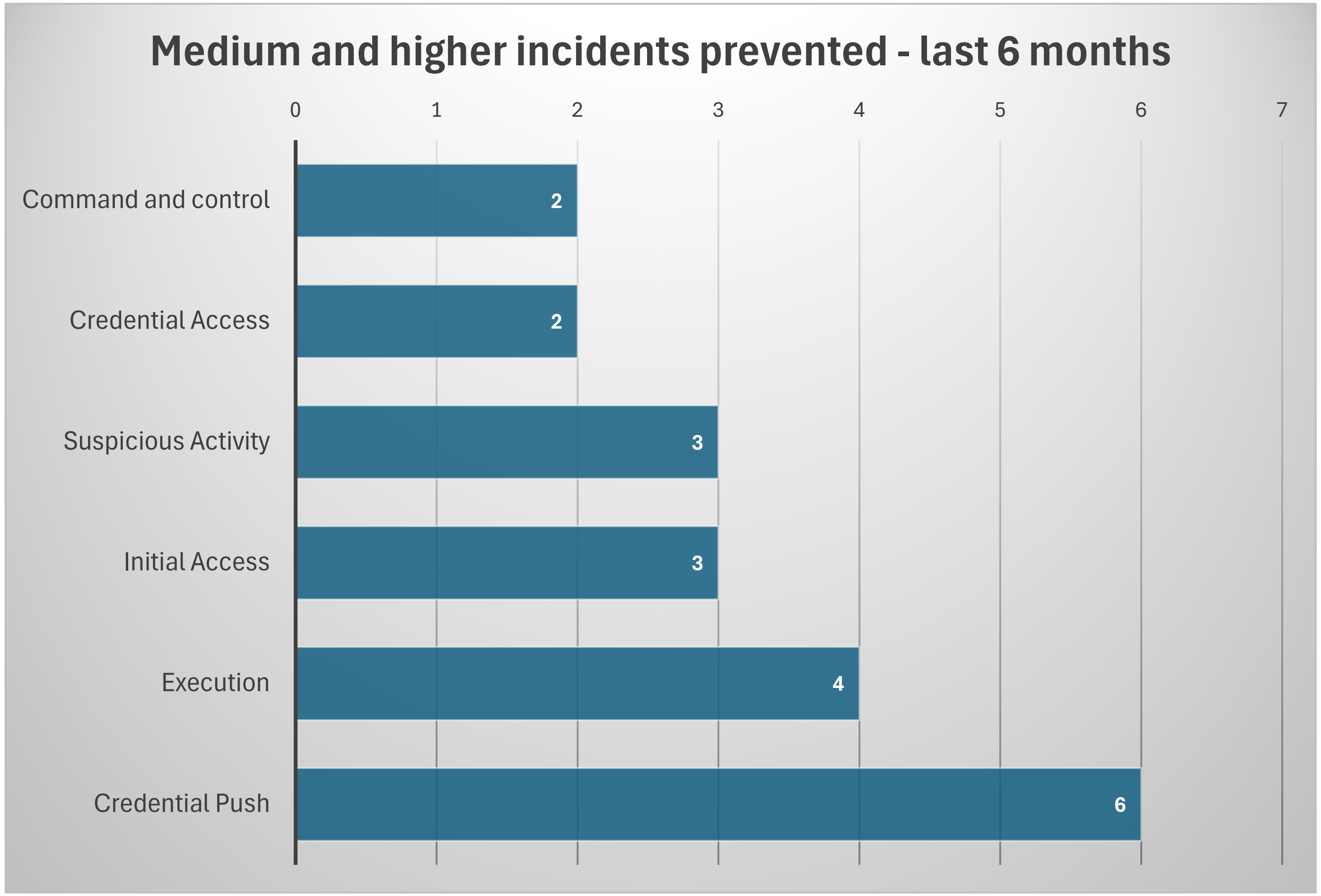
- Total requests for data to the Odata service: 106,208,610
- Industries of users include:
  - Legal
  - Universities
  - Media
  - High Tech
  - Government
  - Lobbying



Legislative Email Traffic

- Total email traffic: 1,749,171
- 77% is legitimate email
- 5000+ email messages are analyzed every day for SPAM, malware attachments, or phishing links.

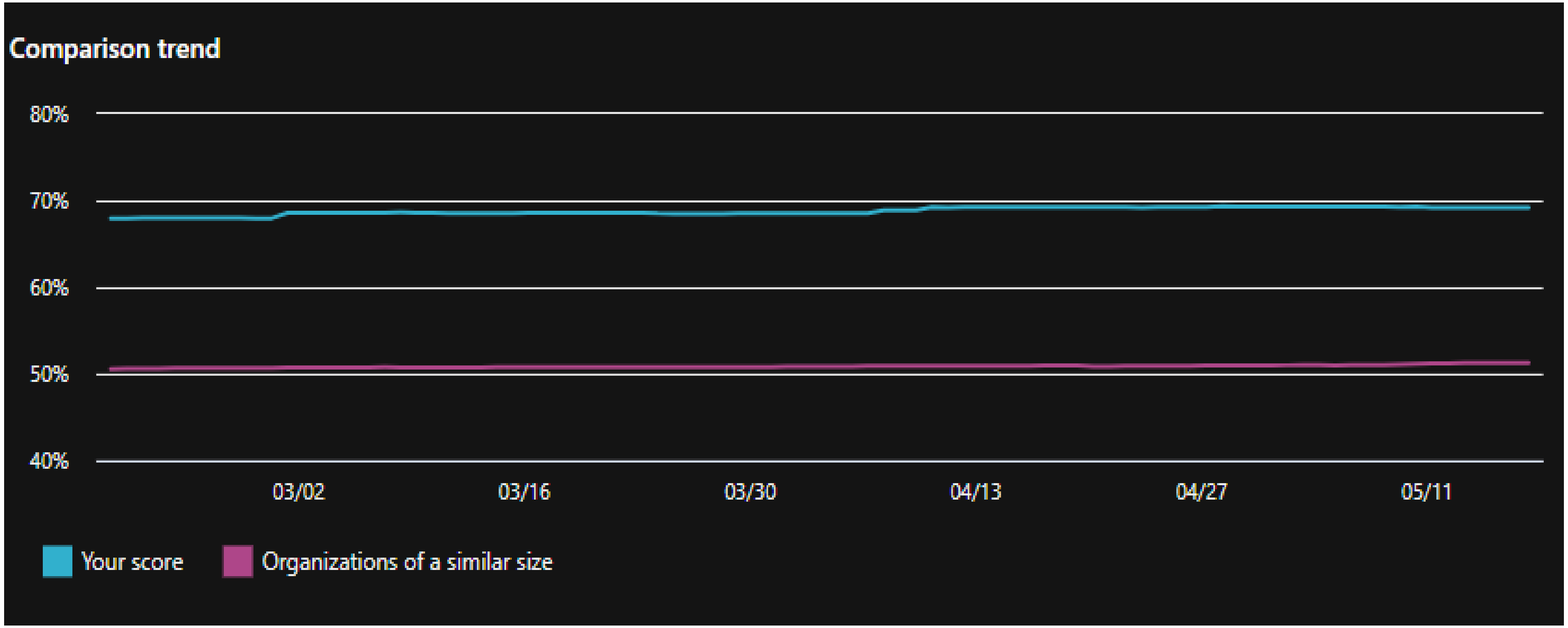
Incidents



- Digital safeguards play a vital role in preventing incidents from happening.
- Daily, there are approximately three automated investigations, triggered by users clicking on potentially harmful email links.
- Training users on awareness is essential for protecting the Legislative network.

Results...

Microsoft Secure Score: 69%



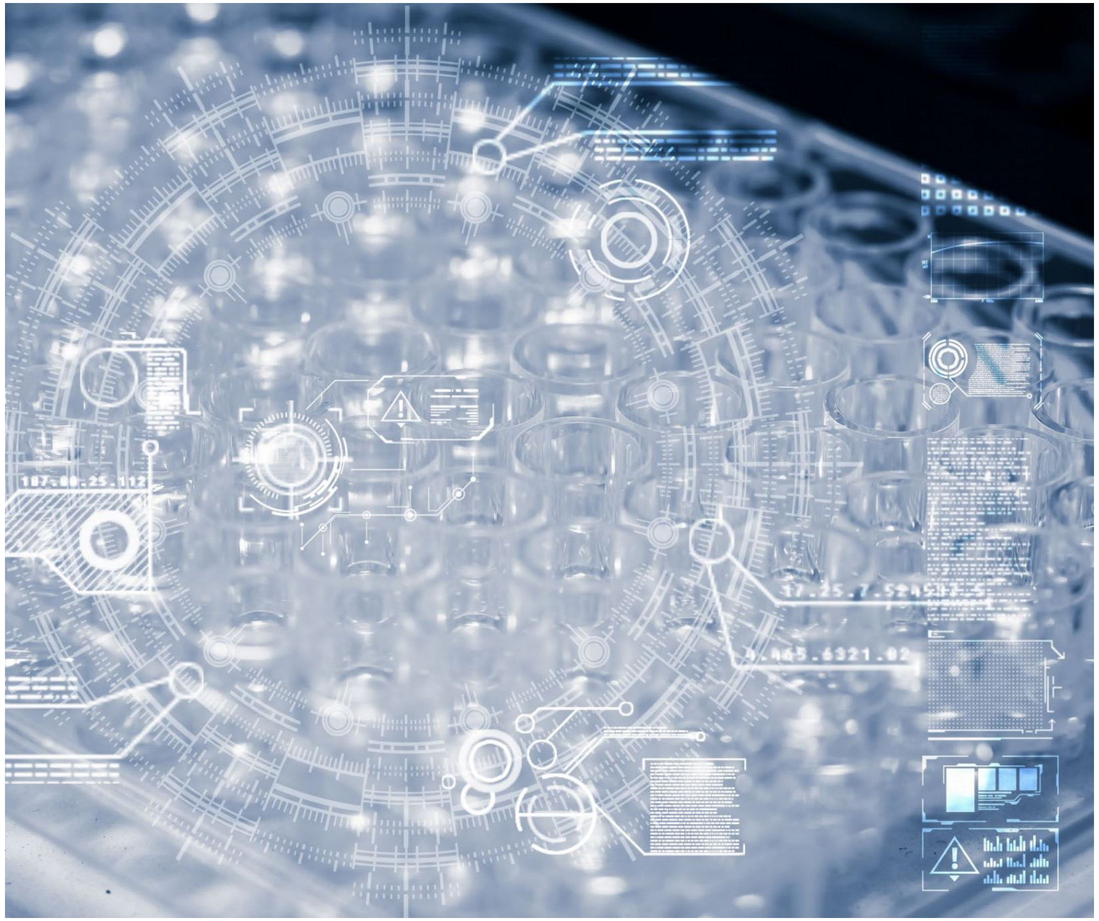
- The team's added security measures have made our Legislative security stronger than that of similar-sized organizations.

What we do….

- Proactively review logs and dashboards daily to find anomalies.
- Respond to any incidents per the Legislative Incident Response Policy.
- Follow industry best practices and frameworks regarding writing software and deploying physical assets to the Legislative network.
- Implement automated runtime books that initiate protective or remediation actions as cyber attacks increase or new zero-day attacks emerge.
- Patch software applications on a regular cadence, or as zero-days arise.
- Frequently review in place protections for updates to or modifications of by a vendor.
- Conduct security penetration testing with external partners such as CISA.
- Keep current on emerging threats and technologies to prevent them by subscribing to industry newsletters, forums, self-paced and virtual classroom training.

Appendix

Artificial Intelligence and Machine Learning in Cybersecurity



Faster Threat Detection

AI technologies enhance the speed of threat detection, allowing security teams to respond more quickly to incidents.

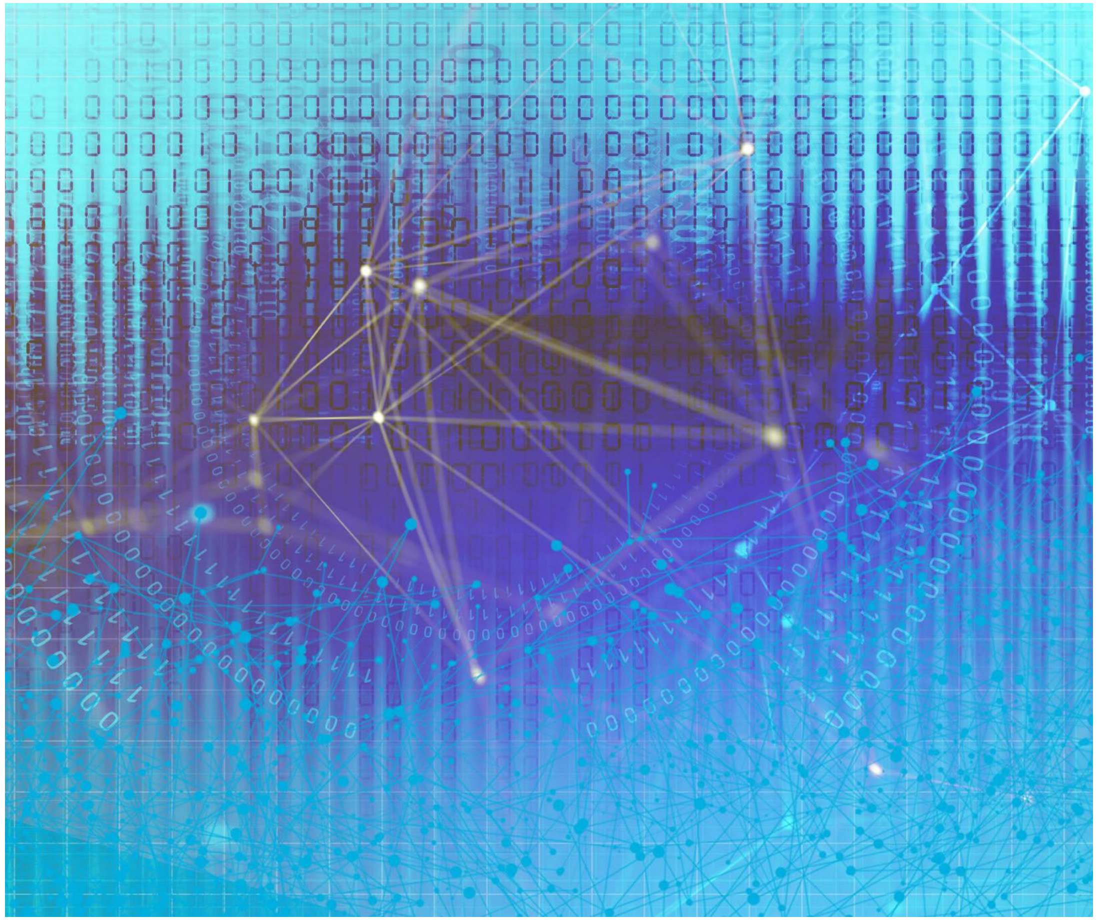
Data Analysis Capabilities

Machine learning algorithms analyze vast amounts of data to identify anomalies and improve overall security measures.

Predicting Potential Threats

AI models can predict potential security threats by recognizing patterns and trends in historical data.

Rise of Quantum Computing and Its Implications



Revolutionizing Computing

Quantum computing has the potential to transform various fields by performing complex calculations much faster than classical computers.

Impact on Cybersecurity

The rise of quantum computing poses significant challenges to current encryption methods, risking data security worldwide.

Addressing Encryption Risks

The cybersecurity community must develop new strategies and encryption methods to counteract potential threats from quantum computing.