Oregon State University
Information and Technology

IT ECOSYSTEM SECURITY

Protecting Oregon State University's digital assets and maintaining an agile IT ecosystem

Boad of Trustees // March 12, 2026

IT ECOSYSTEM

Data

OSU Community

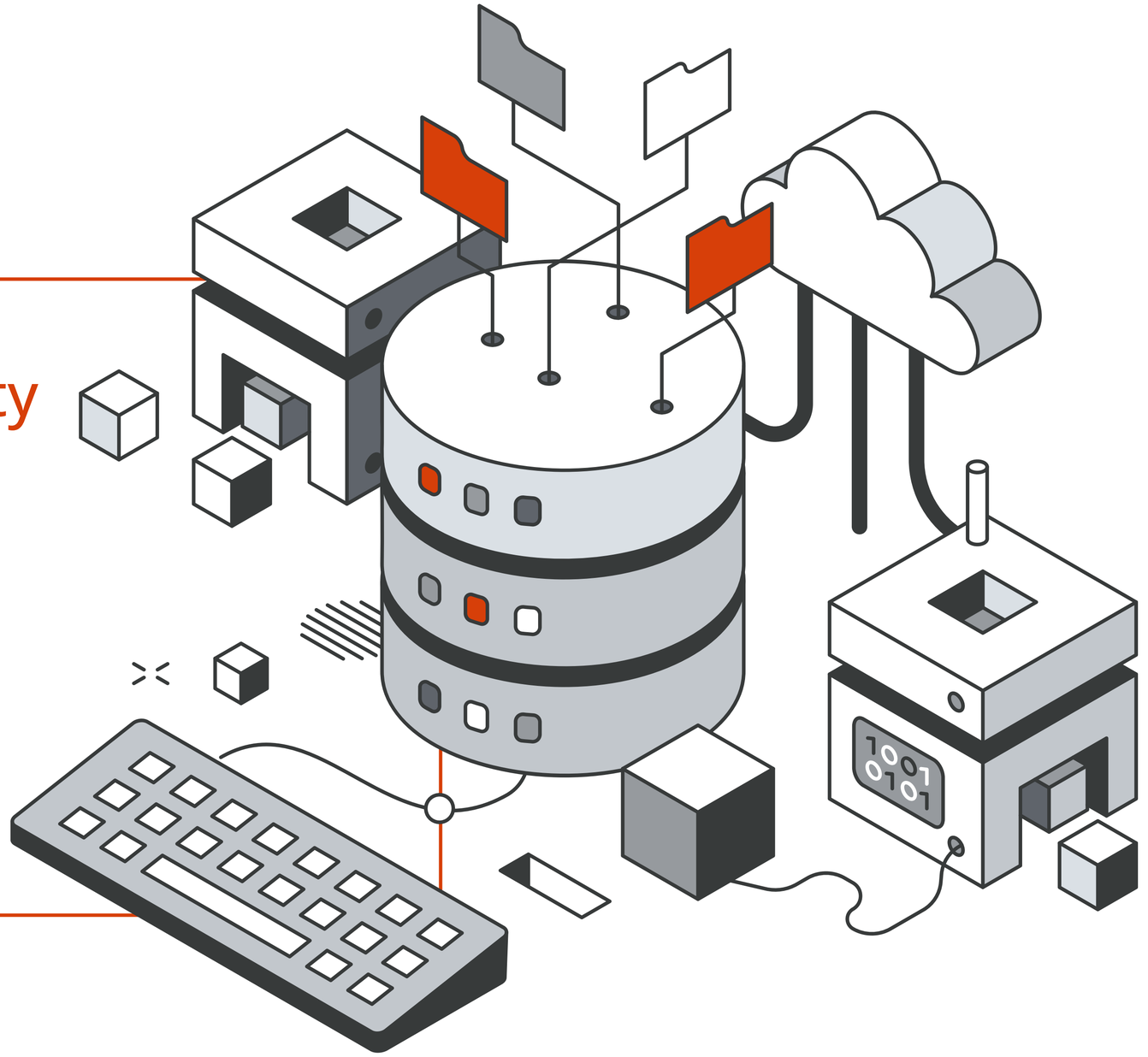
Research

AMP

AI

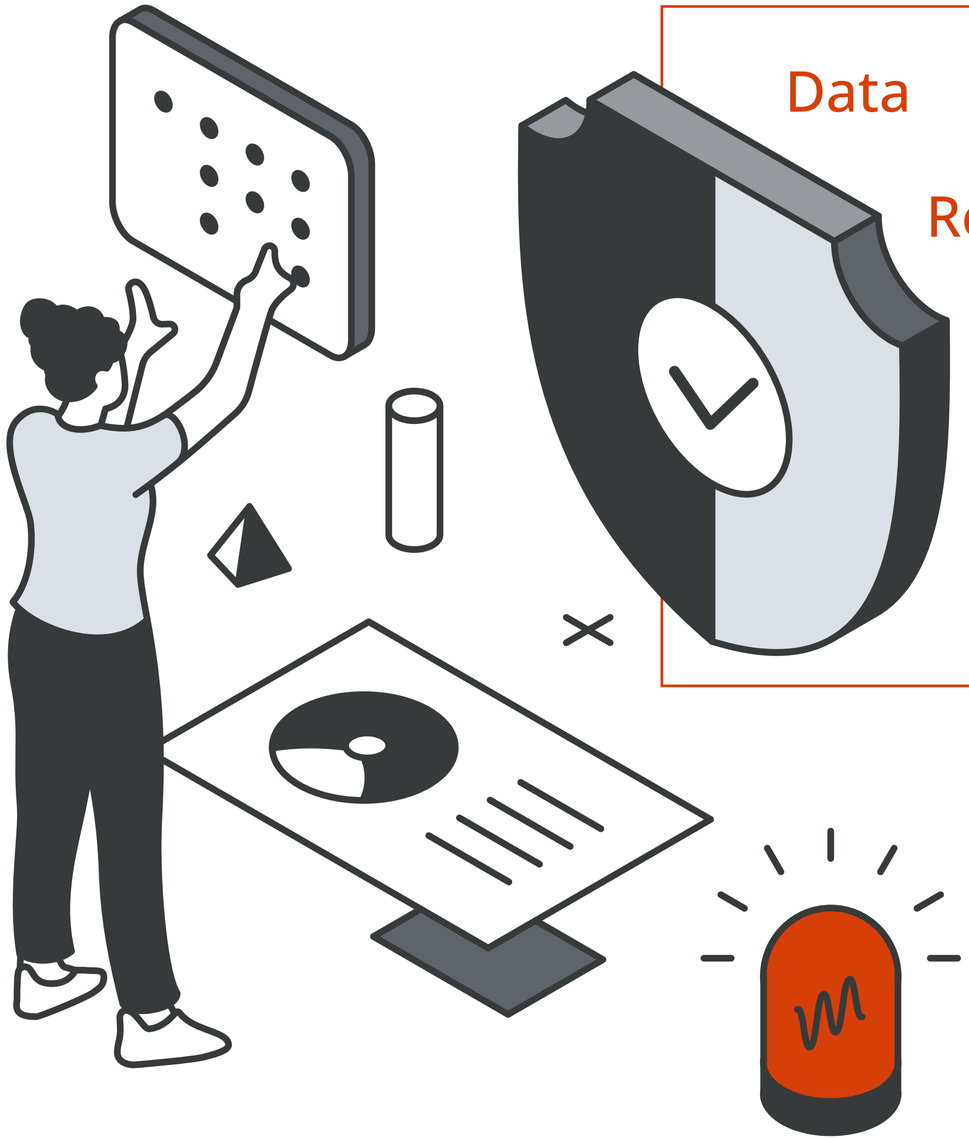
Facilities

Microsoft, Workday, ServiceNow



OSU SECURITY PROGRAM

OSU’s Security Program, based on the industry-standard NIST Framework, supports realization of Prosperity Widely Shared, enhancing security, privacy, and compliance.



Data

OSU Community

Research

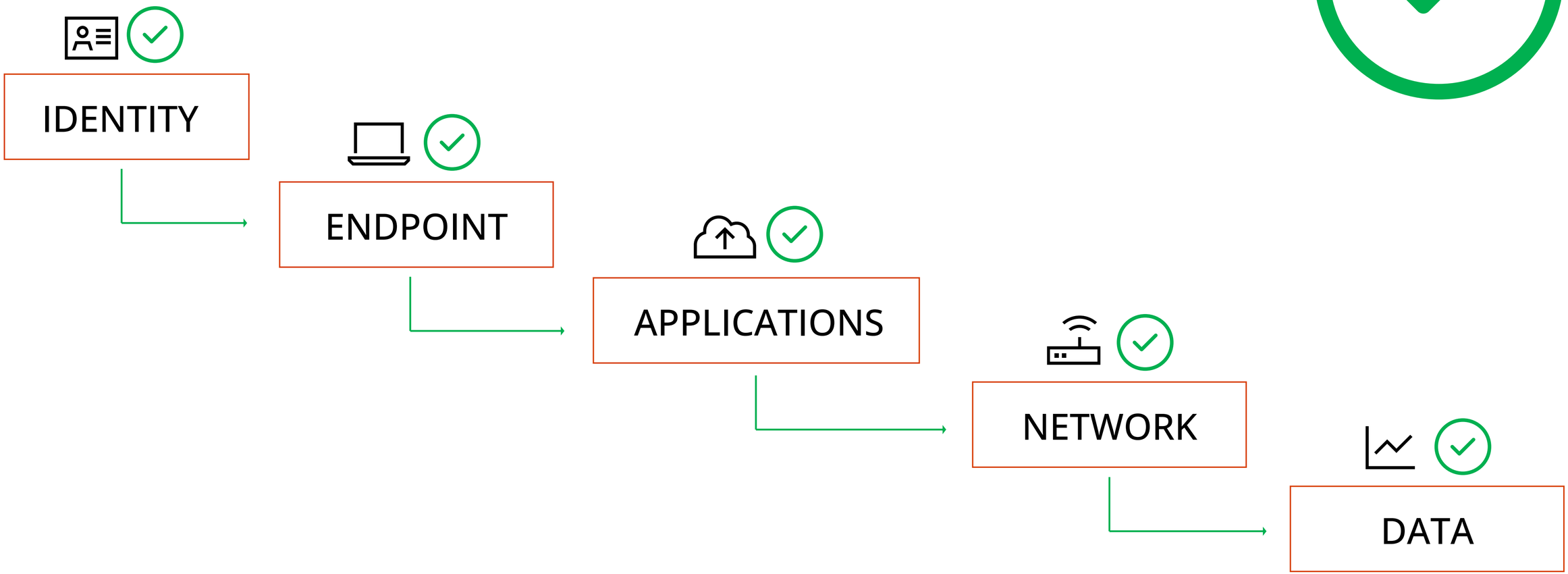
AMP

AI

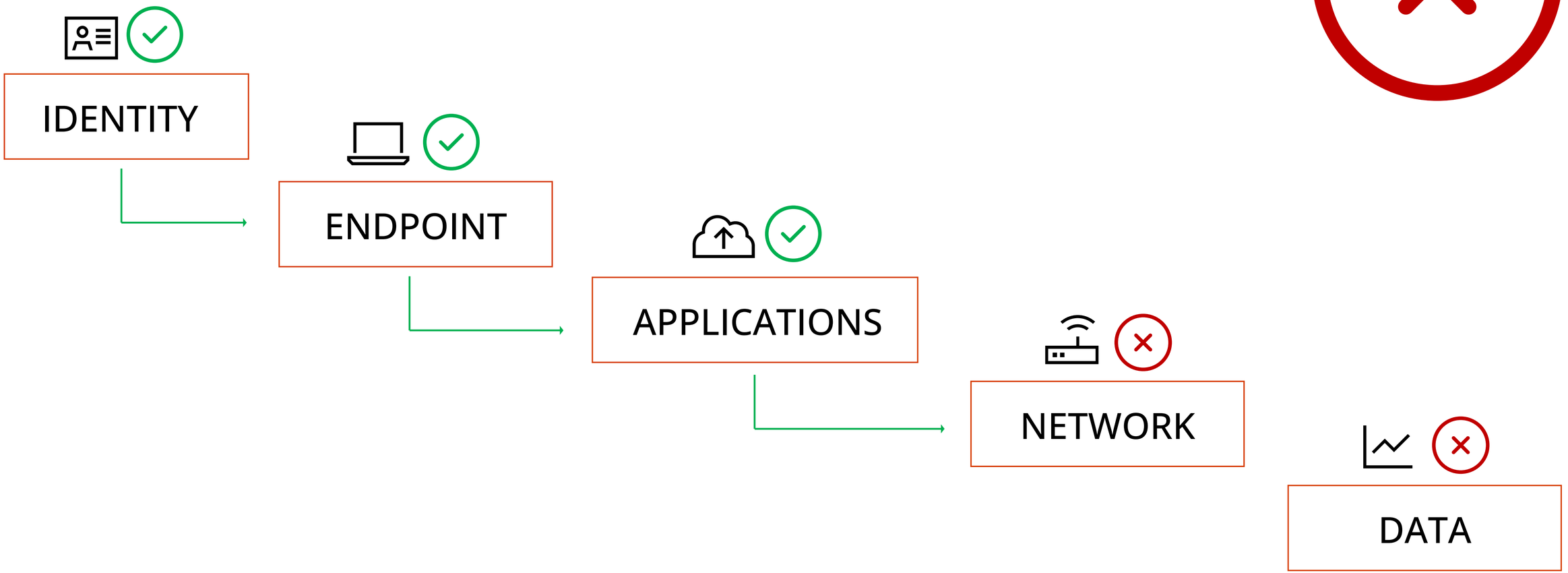
Facilities

Microsoft, Workday, ServiceNow

SMART ACCESS



SMART ACCESS (continued)



POWERED BY OSU IT

OSU INFORMATION SECURITY PROGRAM

Since committing to basing our foundation on the NIST Cybersecurity Framework in 2019, OSU's Information Security Program has steadily matured.

- ↑ Overall: 2%
- ↑ Govern: 4%
- ↑ Identity: 1%
- ↑ Protect: .3%
- ↑ Defend: 2%
- ↑ Respond: 2%
- Recover: 0%

POWERED BY OSU IT

GOVERNANCE:

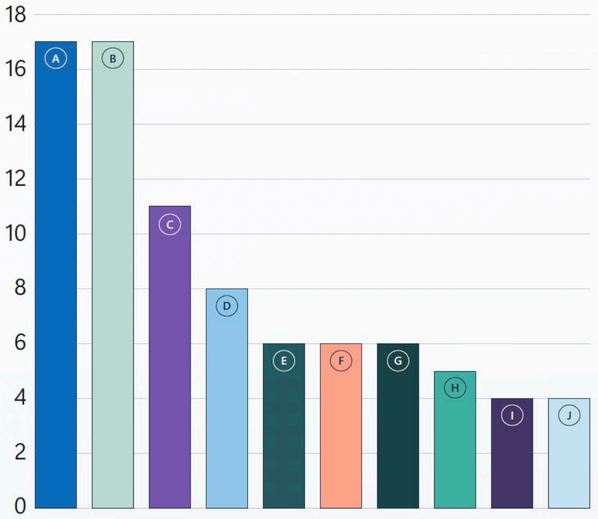
Information Security Advisory Committee

POWERED BY OSU IT

CYBER RISKS

Higher education and research continue to be a high target for cyber attack.

Ten global sectors most impacted by threat actors (January-June 2025)



	%
A. Government agencies & services	17
B. Information technology	17
C. Research and academia	11
D. Non-governmental organizations	8
E. Critical manufacturing	6
F. Transportation systems	6
G. Consumer retail	6
H. Communications infrastructure	5
I. Financial services	4
J. Healthcare and public health	4

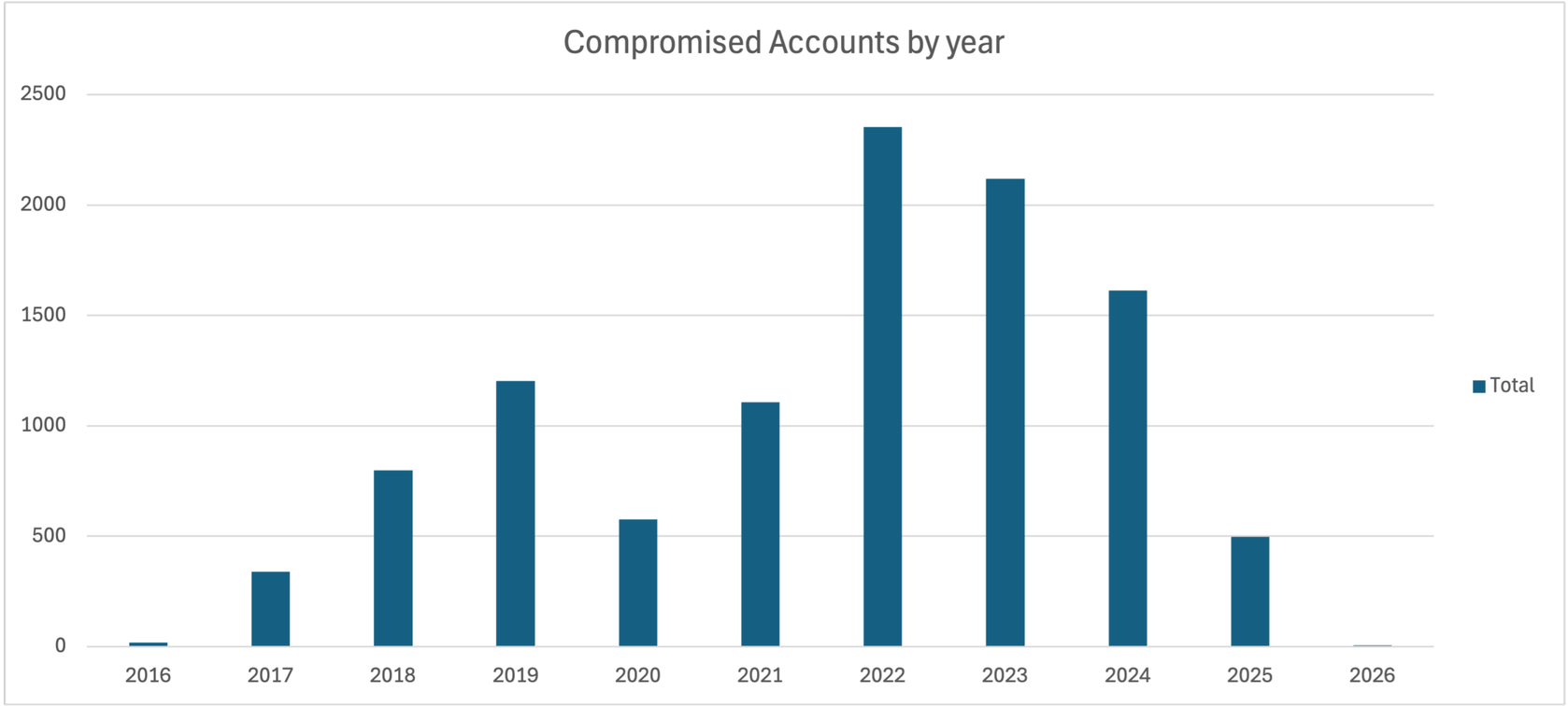
Source: Microsoft Threat Intelligence

IT and government bodies were the most impacted by cyber threats this year, from national to local entities. These organizations manage critical public services—for example, healthcare, research and academia, transportation, and public safety—and store vast amounts of sensitive data, including personally identifiable information (PII), tax records, and voting information. Additionally, many local governments operate on legacy systems that are difficult to patch and secure, and budget constraints and small IT teams often mean delayed updates, minimal threat monitoring, and limited incident response capabilities. This makes them high-value targets for both nation-state actors and financially motivated cybercriminals.

While attacks on IT, manufacturing, transportation, finance, energy, and healthcare can have both digital and physical consequences, attacks on industries like research and academia and telecommunications could additionally serve as a launchpad for attacks on other entities.

INCREASED PROTECTION + RESILIENCY

OSU continues to implement tools that increase visibility, enable faster response. and elevate institutional resiliency.



POWERED BY OSU IT

COLLABORATIVE RESILIENCY

OSU provides training and builds awareness in the community to bolster vigilance and improve resiliency.

OSU hosted the second annual Cyber Carnival in October to engage students with cybersecurity awareness

QUESTIONS?