Technology Services IT Governance
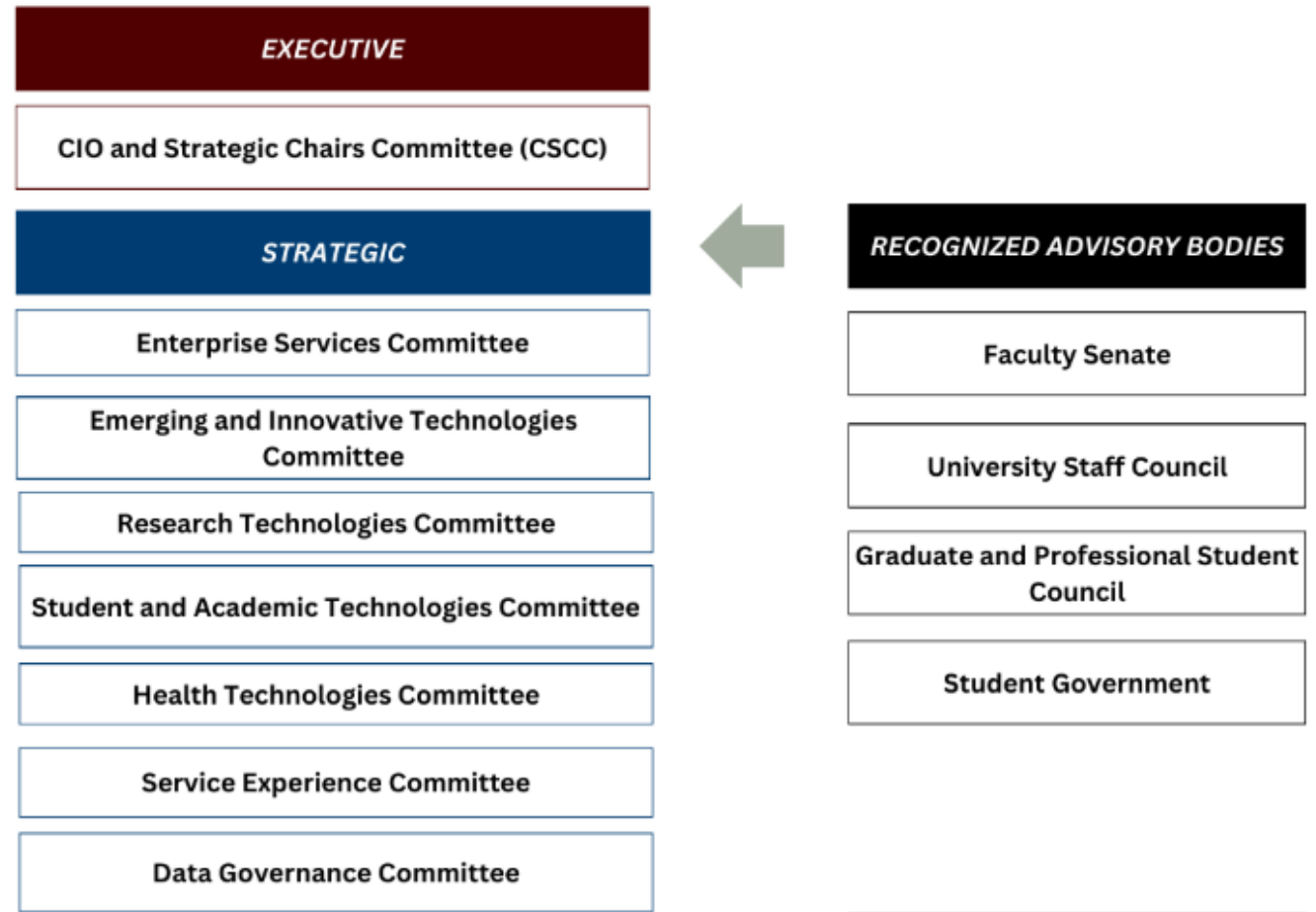
University-Wide IT Governance Framework

- Seven strategic committees provide input for the mission of the University by recommending IT solutions related to their focus.
- Each committee was created to balance input from university stakeholders and the mission of the university to make strategic IT decisions within a defined scope.

EXECUTIVE

CIO and Strategic Chairs Committee (CSCC)

STRATEGIC

Enterprise Services Committee

Emerging and Innovative Technologies Committee

Research Technologies Committee

Student and Academic Technologies Committee

Health Technologies Committee

Service Experience Committee

Data Governance Committee

RECOGNIZED ADVISORY BODIES

Faculty Senate

University Staff Council

Graduate and Professional Student Council

Student Government

TEXAS A&M UNIVERSITY
Technology Services

IT Governance Membership

- Members are appointed by University leaders and groups from across the University such as:
  - CPI
  - Faculty Senate
  - President
  - Provost
  - Deans
  - Student Government

University-Wide IT Governance

- Committees meet 5 times a year
  - February
  - April
  - June
  - September
  - November

  * Sub-committees and task forces meet as needed to complete tasks

- Visit https://it.tamu.edu/about/it-governance/index.php for additional information

Benefits of University-Wide IT Governance

- **Strategic Alignment**
  - Ensures IT investments and initiatives are aligned with the organization's overall mission, vision, and objectives.
  - Helps prioritize IT projects based on their contribution to business value.
- **Improved Decision-Making**
  - Establishes clear roles, responsibilities, and processes for decision-making regarding IT resources.
  - Provides a framework for evaluating the impact of IT-related decisions on the organization.
- **Better Service Delivery**
  - Improves the quality, reliability, and timeliness of IT services delivered to internal and external stakeholders.
  - Aligns IT services with user needs and expectations.
- **Optimized IT Resource Utilization**
  - Ensures that IT resources (e.g., people, technology, data) are used effectively and support high-priority initiatives.
  - Reduces underutilization or overextension of IT capabilities.
- **Increased Stakeholder Confidence**
  - Builds trust among stakeholders (e.g., executives, customers, employees) by demonstrating that IT is managed effectively and responsibly.
  - Provides transparency into IT operations and their alignment with business goals.

TAMU System IT Governance

System-Wide IT Governance

- Ensure alignment with TAMUS mission and act as the definitive decision-making body for A&M System IT governance system-wide decisions

- 23 Members
  - Chair: A&M System CIO
  - Selected member CEOs/Presidents
  - Selected member CFOs
  - Selected member CAOs
  - Selected member CIOs

System-Wide IT Governance

Committees

- Executive IT Council (meets semi-annually)

- Academic Technology Council (meets quarterly)

- Enrollment Management IT Council (meets 3 times per year)

- CIO Council (meets 3 times per year)

- A&M System IT Shared Services (meets semi-annually)

Visit https://it.tamus.edu/governance/it-governance-framework/ for additional information

Benefits of A&M System IT Governance

- **Leverage Existing Solutions**
Reduce duplicative efforts and identify opportunities to leverage solutions that two or more members are using

- **Gain Access to Expertise & Lessons Learned**
Share insight, expertise and lessons learned from across the A&M System

- **Cut Costs**
Leverage economies of scale to cut project costs or set up a master contract with premium pricing

IT Security & Risk

TEXAS A&M UNIVERSITY
Technology Services

IT Risk & compliance team

- **Adam Mikeal** <adam@tamu.edu>
  - Chief Information Security Officer
- **Joe Mancha** <jmancha@tamu.edu>
  - Director — IT Risk & Compliance
- **Paul Wiggins** <paul.wiggins@tamu.edu>
  - Associate Director — Research Security & Compliance
- **Audit Field Team**
  - Team of policy and security analysts; perform audit readiness and assessment functions to help prepare groups for System Audit

Research Security & Compliance

- **Grants & contract review**

  ○ Work with RIO to ensure compliance with requirements in contract language

- **Export control, CMMC, and CUI compliance**

  ○ New regulations from federal partners around Controlled Unclassified information is trickling down to funding agencies

- **Federal zero-trust cybersecurity requirements; NIST standards**

  ○ CISA and NIST continue to tighten regulations around data associated with any federal partner (including funding agencies)

IT compliance and regulatory landscape

Governance/compliance hierarchy

System Member

Texas A&M Rules and SAPs;
Texas A&M controls catalog
(local implementation)l

1

Texas A&M System Regulations

System Policies; System Regulations; System controls catalog

2

State of Texas Legislation and Administrative Rules

Texas Administrative Code §202; Texas Government Code §2054; DIR rules and policy; DIR controls catalog (NIST-53)

3

Federal Legislation and Administrative Rulemaking

US Code, Code of Federal Regulations, NIST 800-53, NIST 800-171, CMMC, CUI, NSPM-33

4

Georgia Tech lawsuit for cybersecurity fraud

- DOJ files lawsuit against Georgia Tech under False Claims Act

- Claims Georgia Tech and GTRC knowingly failed to comply with federal cybersecurity requirements related to DoD contracts

- Further alleges invoicing fraud related to billing under the contract

Key Allegations

- **Non-Enforcement of Cybersecurity Regulations**
  - University created a culture of neglect

- **Fraudulent Cybersecurity Assessment Score**
  - Used a model that was "fictitious" to boost score

- **Failing Basic Security Hygiene**
  - Lab PI refused to allow security agents on devices; university officials failed to enforce requirements

- **Fraudulent Invoicing**
  - University continued to submit invoices under DoD-funded grants

Security at scale

Operations at scale

- **Lots of people**
  - **30k** employees; **80k** students; **100k** affiliates

- **Lots of research activity**
  - **$1.3 billion** in research expenditures

- **Lots of things**
  - **187k** active NetIDs; **250k** managed identities
  - **250k** devices tracked; **90k** state assets

Results in lots of data

In the last month:

- **5.8 billion** log events collected *per day*

- **14PB** of network data scanned

- **130M** email messages scanned; **91M** blocked at gateway

- **10M** authentication events; **2.8M** Duo auth events

The cyber threat landscape

Threat landscape for Texas A&M University

- **Most common types of threats:**
  - Credential phishing / BEC (business email compromise)
  - Malware
  - Ransomware

- **APT (Advanced Persistent Threats)**
  - Nation-state actors; typically aligned with military or military-funded
  - TAMU saw multiple targeted attacks from nation-state-aligned actors in the past 24 months: Russia, Iran, DPRK, and China

- **Constantly evolving threats and techniques**
  - AI is enabling new types of attacks and malware; constant cat-and-mouse
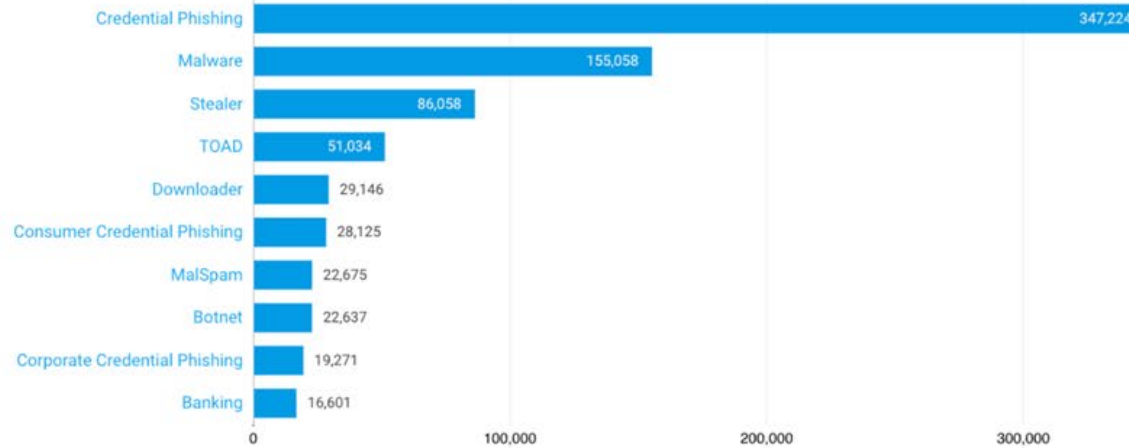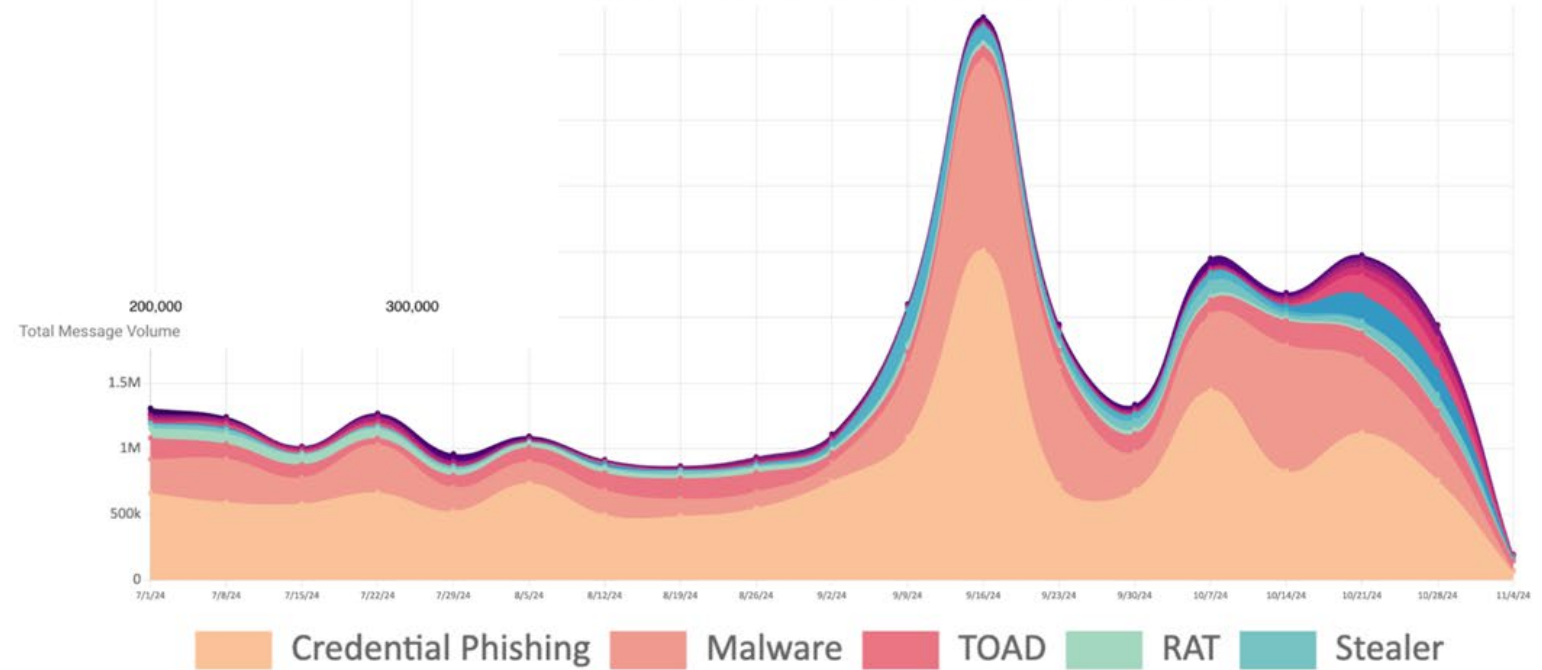
Threat landscape ~~industry~~ industry comparison (2024)
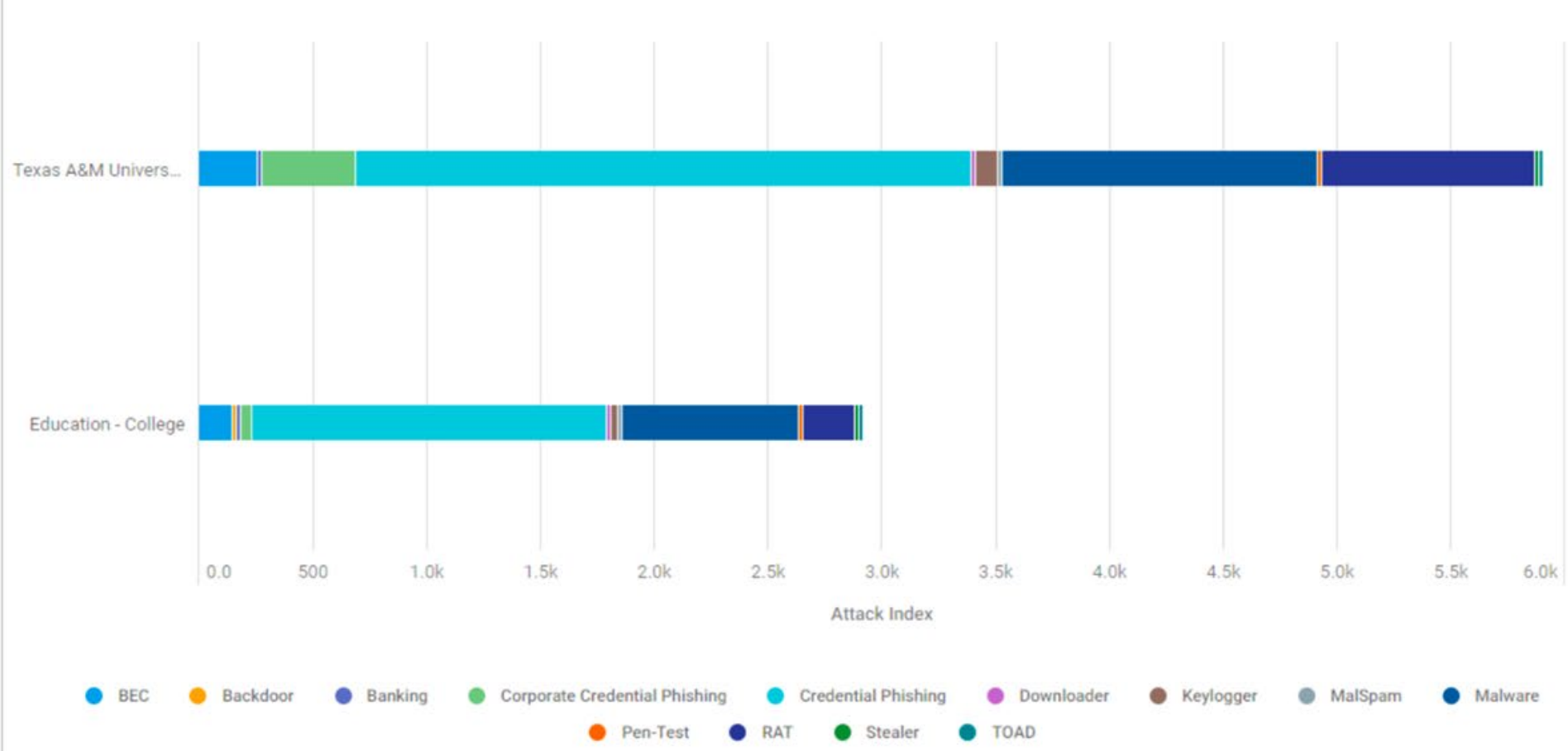
New Tools

TEXAS A&M UNIVERSITY
Technology Services

- Admin by request
  - Clients Deployed: 6,408 across system parts 02, 23 and 28
  - deployment to address audit findings
  - Agent deployment replacing existing PAM solutions – in progress through all Colleges and Units
    Working directly with research teams to ensure workflow and use of tool aligns with business need
- Network Segmentation
  - Part of the new Next Generation Aggie Network