The CISO Role at Penn

April 2026

Nick Falcone, University Chief Information Security Officer

Agenda

- Introductions
- CISO roles
- OIS Overview & Numbers
- Metrics

Introduction

- Nick Falcone
- University Chief Information Security Officer
- Prior:
  - CISO at Einstein Health
  - Enterprise Information Security Officer at Jefferson University and Hospitals
  - Security Engineer at Children's Hospital of Philadelphia
  - Manager at Protiviti Risk Consulting
  - Intern at Department of Defense

Introduction

- Specialized into low to medium maturity environments, culture change, and corporate politics
- Applied adversarial mindset/hacker mindset
  - Hacking computers
  - Hacking people
  - Hacking organizations
- Structured and planned soft skills
  - “People buy on emotion and justify with fact”
  - A learned skillset

CISO Roles Generally

Generic executive responsibilities:

- Set priorities
- Remove barriers
- Obtain resources

Generic CISO role:

- **Be right about risks** (set priorities)
- **Convince people you are right** (remove barriers; obtain resources)

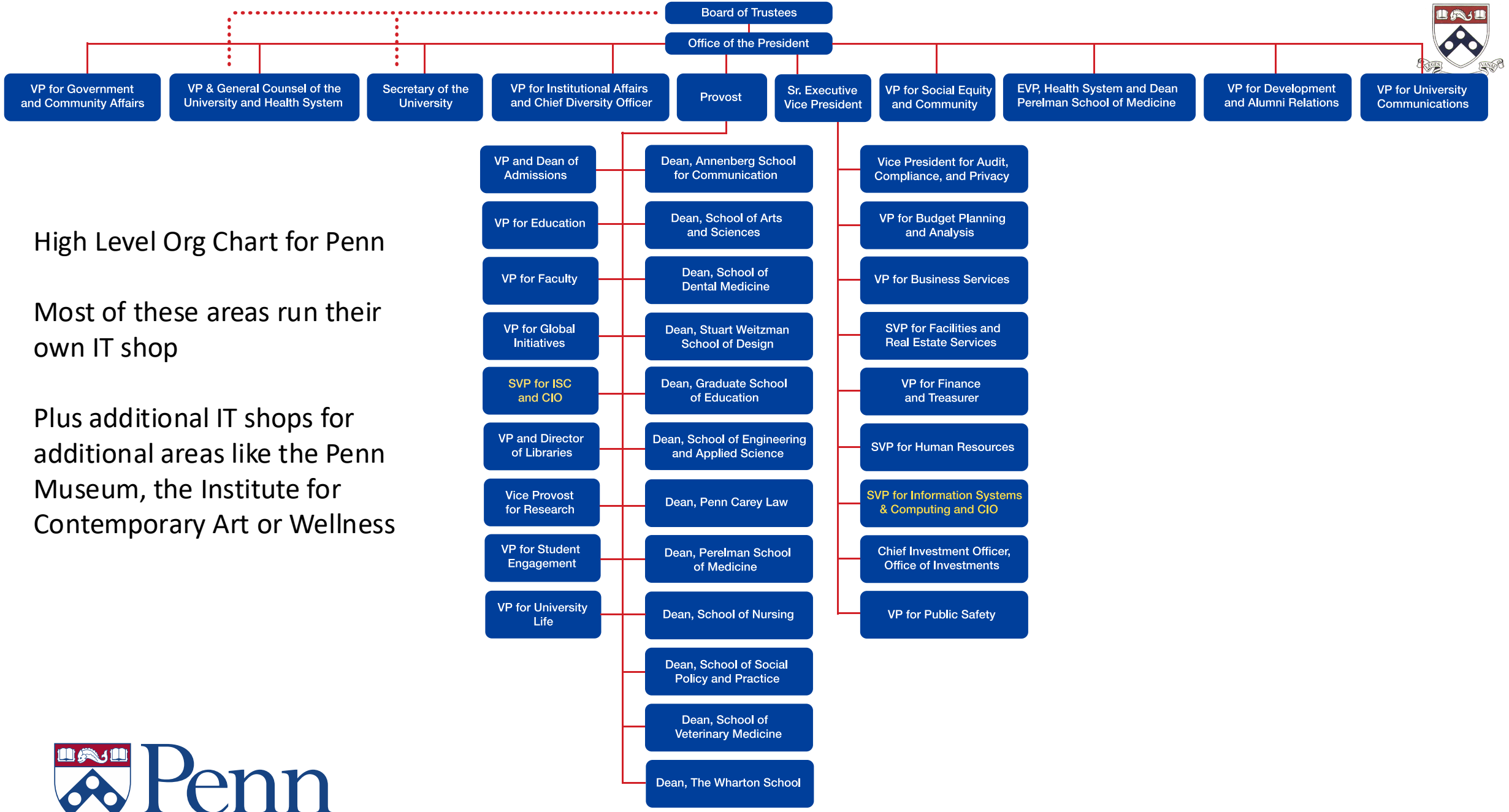
What does that look like day to day?

- **Building Relationships** (quick wins, solving problems, delivering on small promises, empathetic responses)
- **Assess Risks** (network with peers, keep up with media, technical and non-technical assessments, scans and metrics)
- **Manage the Team** (set direction, coach, paperwork)
- **Change Culture** (stakeholder analysis, presentations, one on one persuasion, shenanigans)
- **Hands on Activity** (smallest category, exec. communications during incident response, pinch hitting as needed)

What about during incident response?

- **Prepare** (prep execs not to panic, guide playbooks, maintain access and visibility)
- **Response Scale** (24x7 vs business hours, making the call on when to bring in third party responders, legal support, insurance, etc.)
- **Communications** (keep execs away from team so they can work, message to campus & media with support from University Communications)
- **Manage Team Emotional State** (avoid panic and apathy, ensure no off the cuff actions/communications)
- **Accountability** (make and own most major decisions, protect staff from misdirected consequences)

Penn's IT Overview



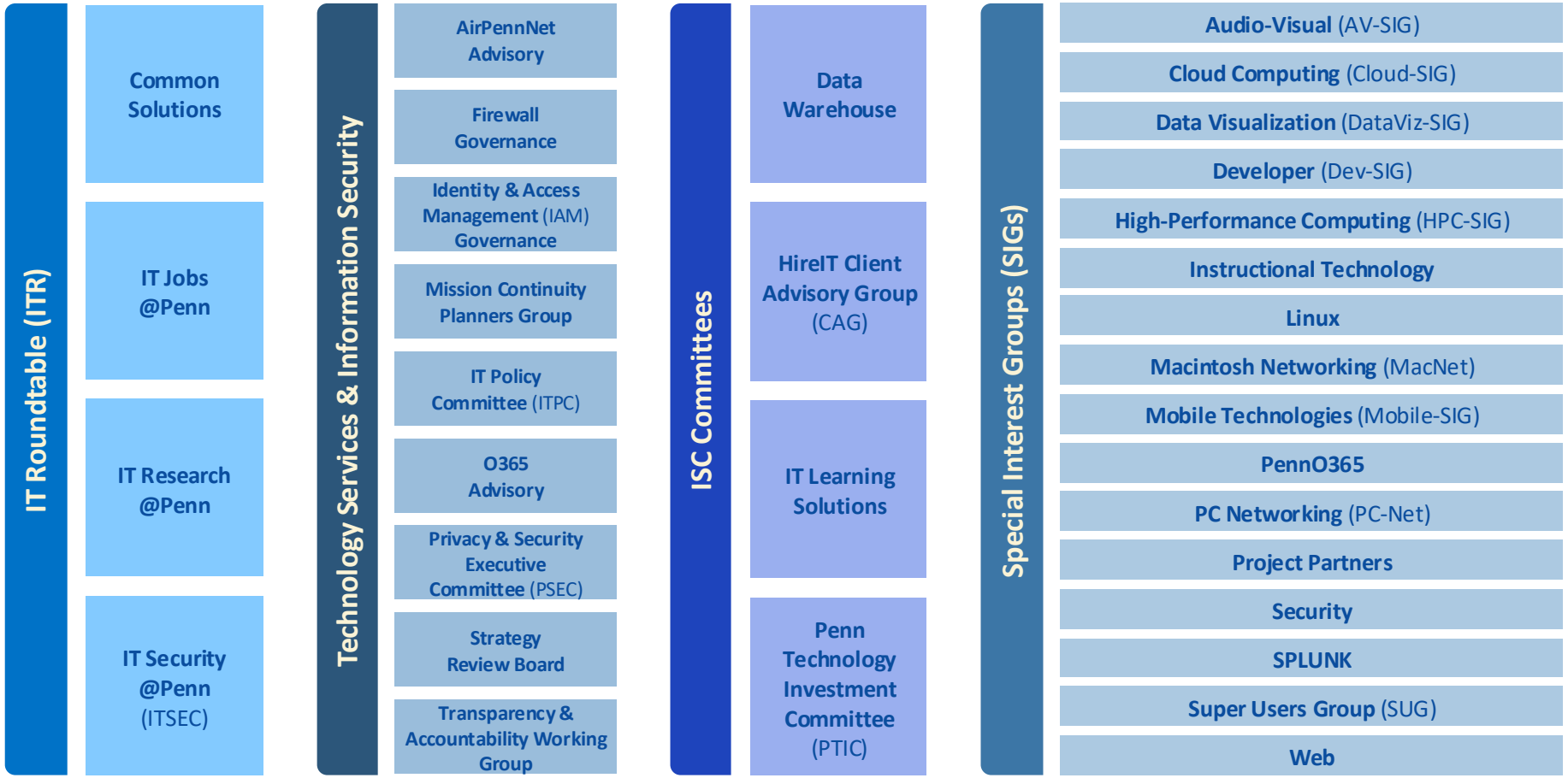
High Level Org Chart for Penn

Most of these areas run their own IT shop

Plus additional IT shops for additional areas like the Penn Museum, the Institute for Contemporary Art or Wellness

Penn
University of Pennsylvania

Campus Collaboration

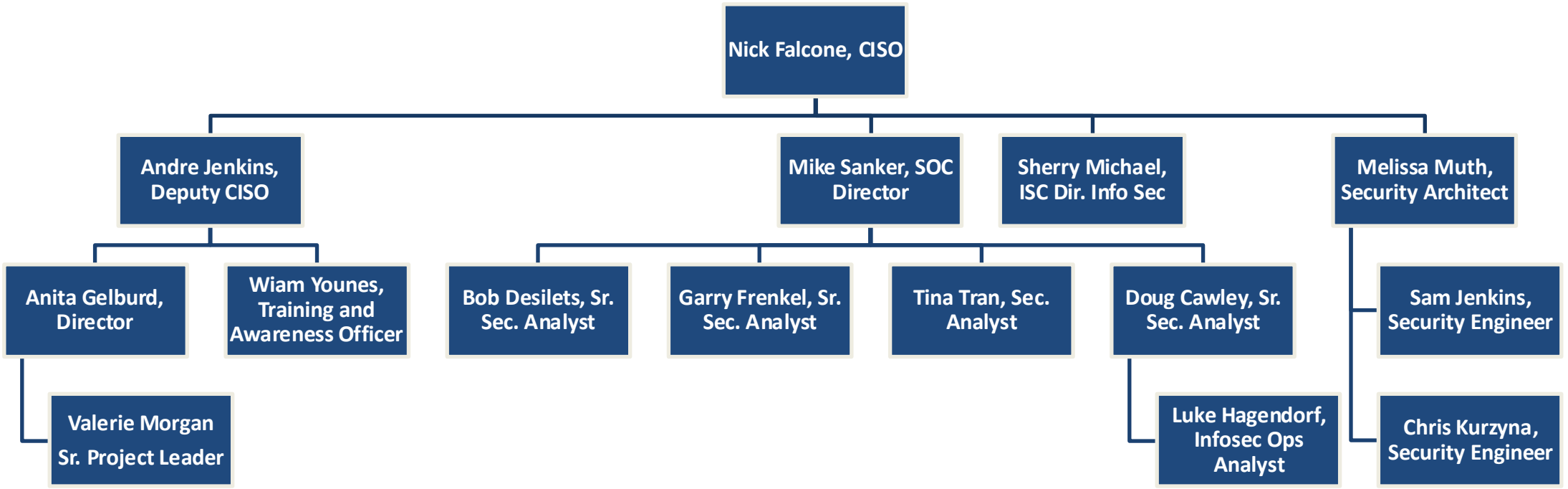


OIS Overview

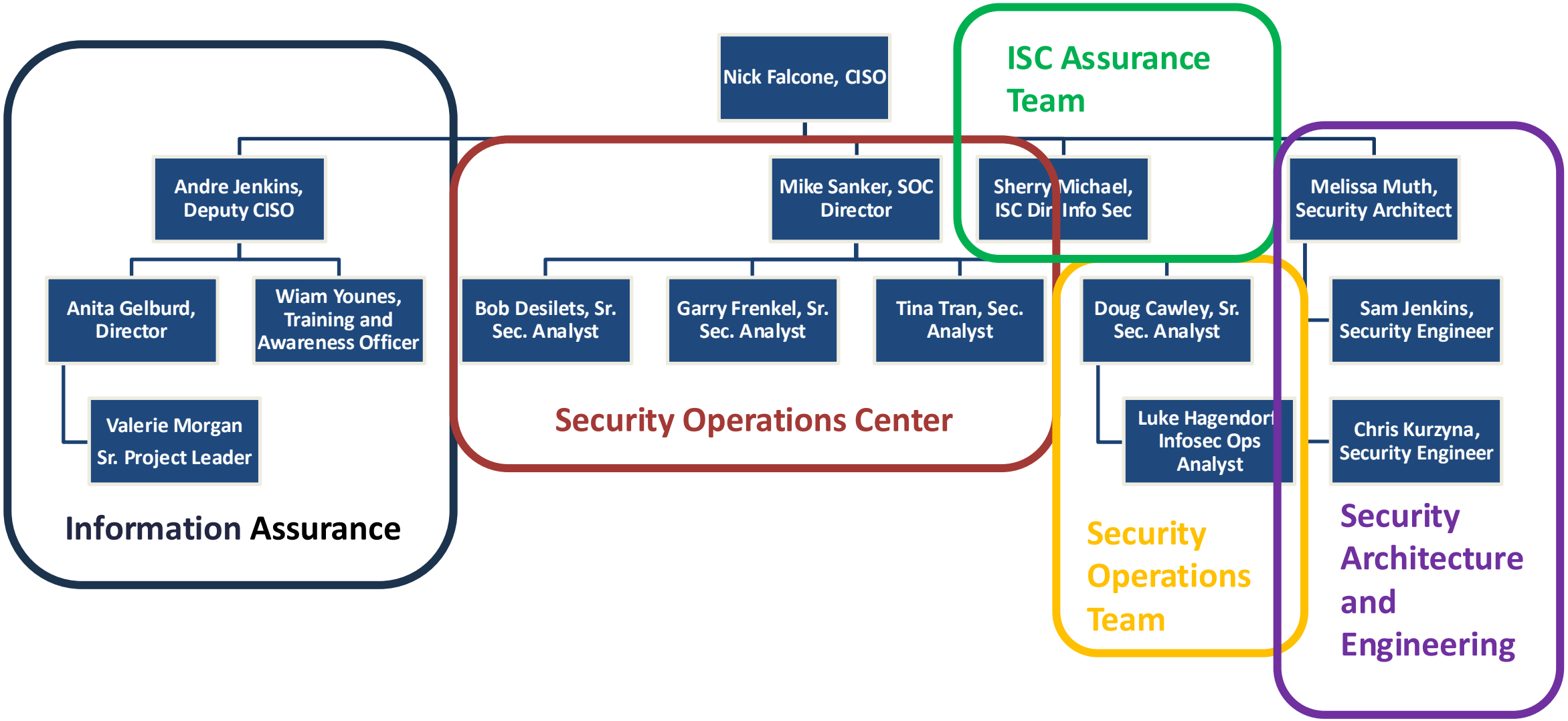
Goals

Security Operations	Consultations	Risks & Threats
Information Assurance	Awareness & Outreach	Point of Contact
Identity & Access	Mission Continuity	Major Incident Response

OIS Overview



OIS Overview



OIS Overview

Information Assurance: Governance, risk and compliance, policy, mission continuity, training and awareness

Security Operations Center: Tier 2/3 incident response, alert response, consulting

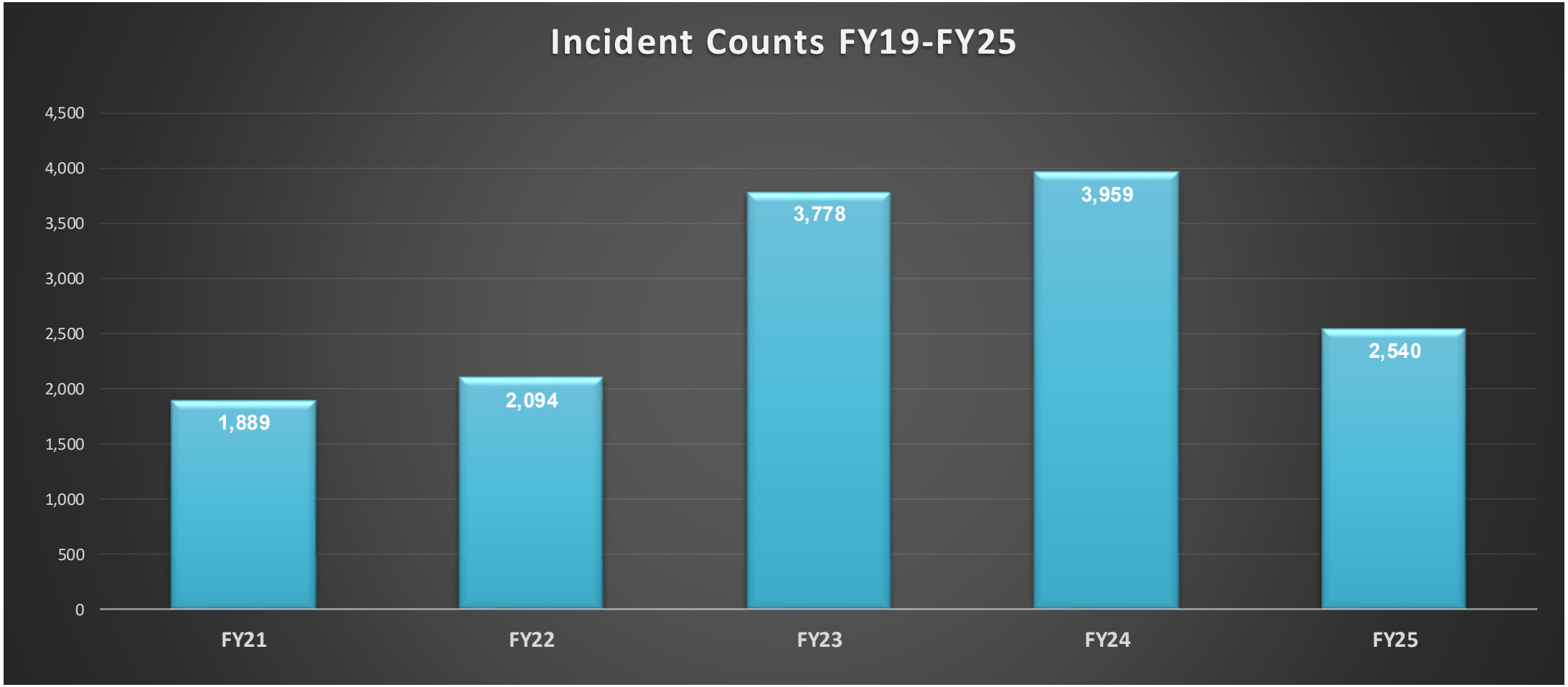
Security Architecture and Engineering: Tool builders and maintainers, automation

Security Operations Team: Tier 1/2/3 incident response, alerting, technical consulting

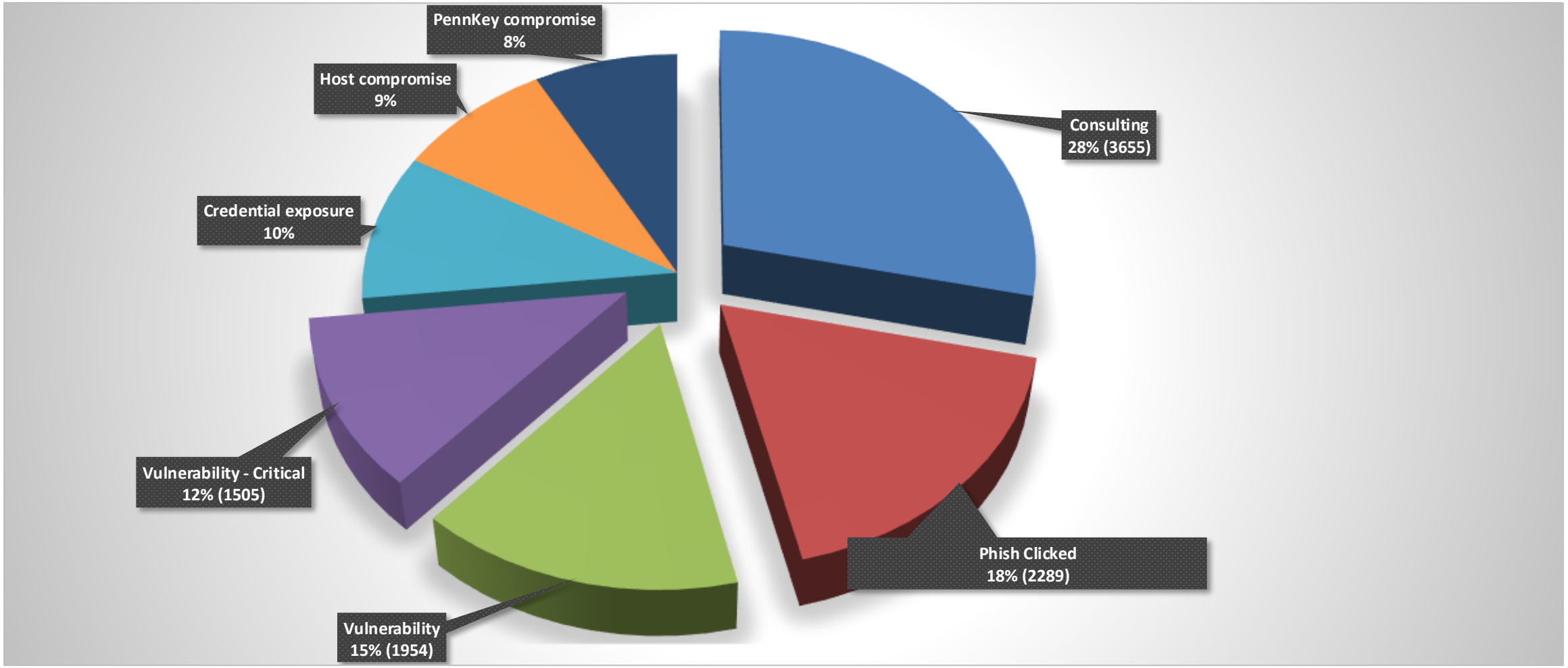
ISC Assurance Team: policy, projects, process, risk and compliance, mission continuity

By the Numbers

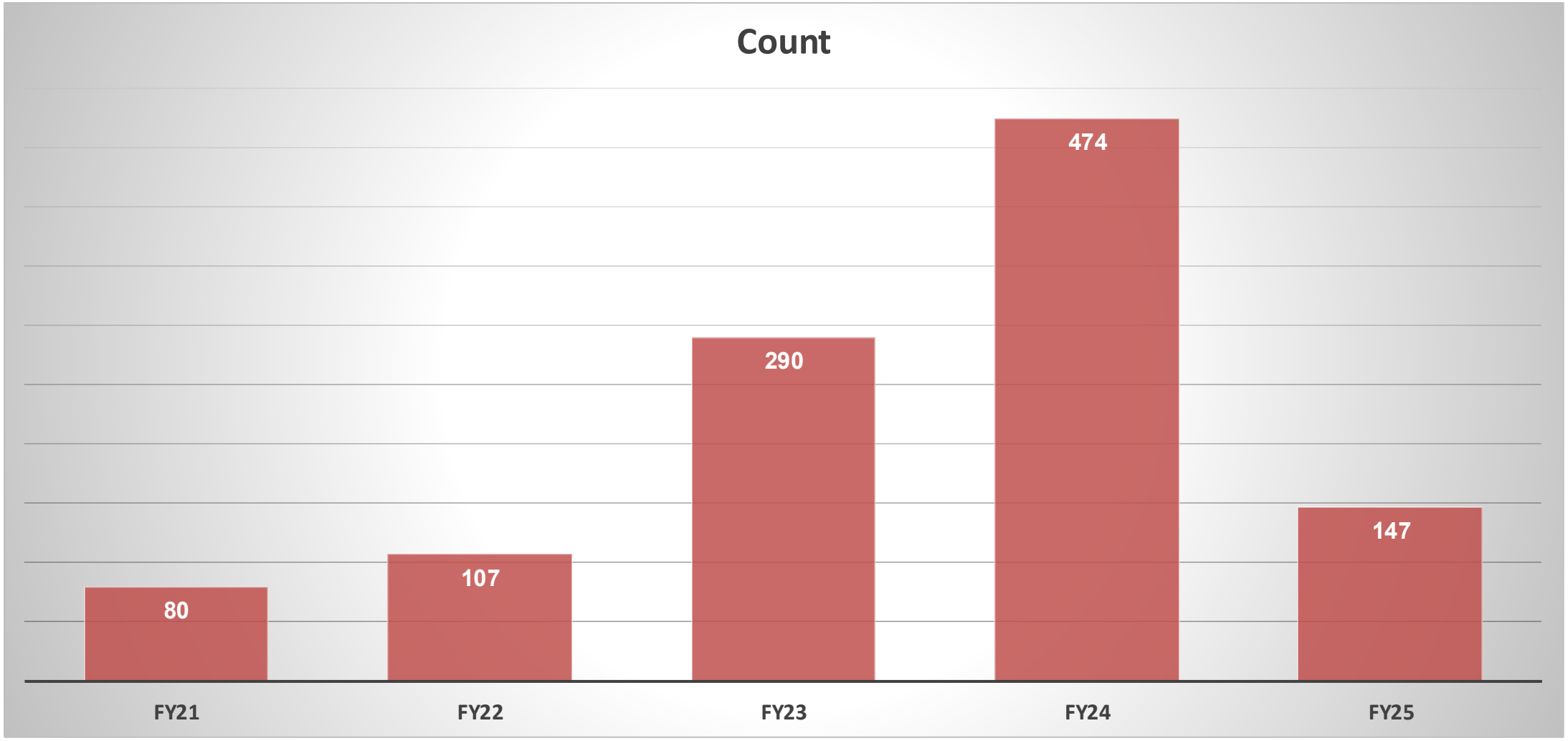
Incident Counts FY20-24



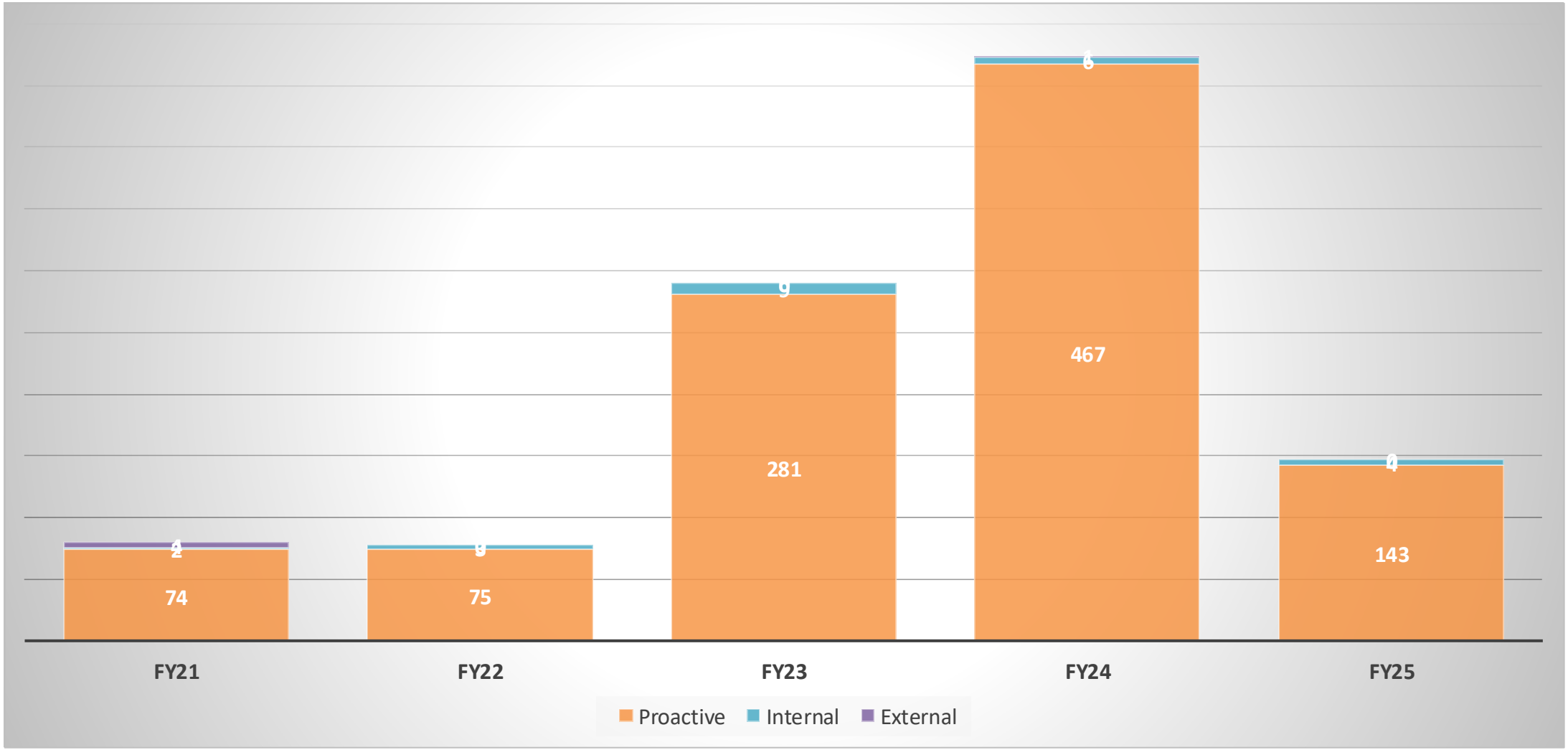
Incidents by Type FY20-24



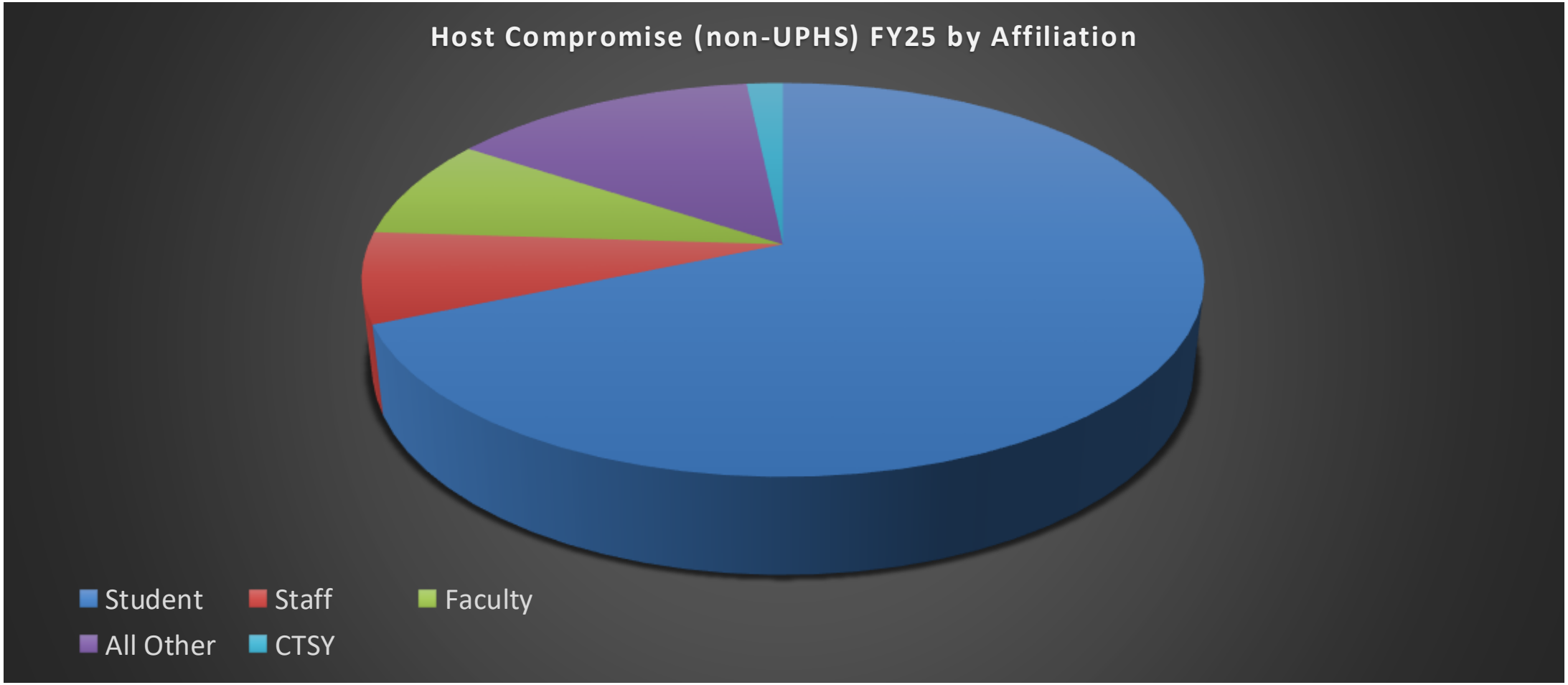
Host Compromise Incidents FY21-FY25



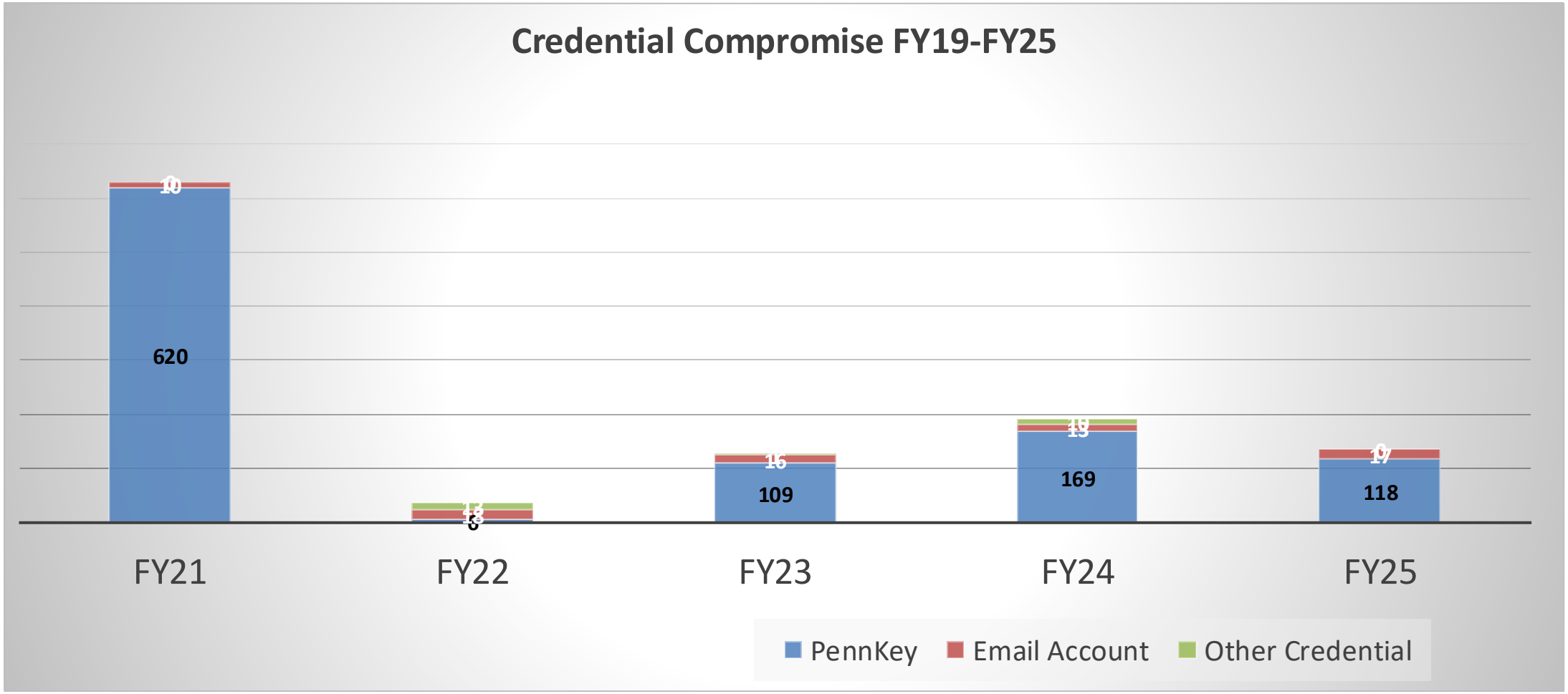
Host Compromise Incidents by Source



Host Compromise (non-UPHS) FY24 by Affiliation



Credential Compromise FY21-25

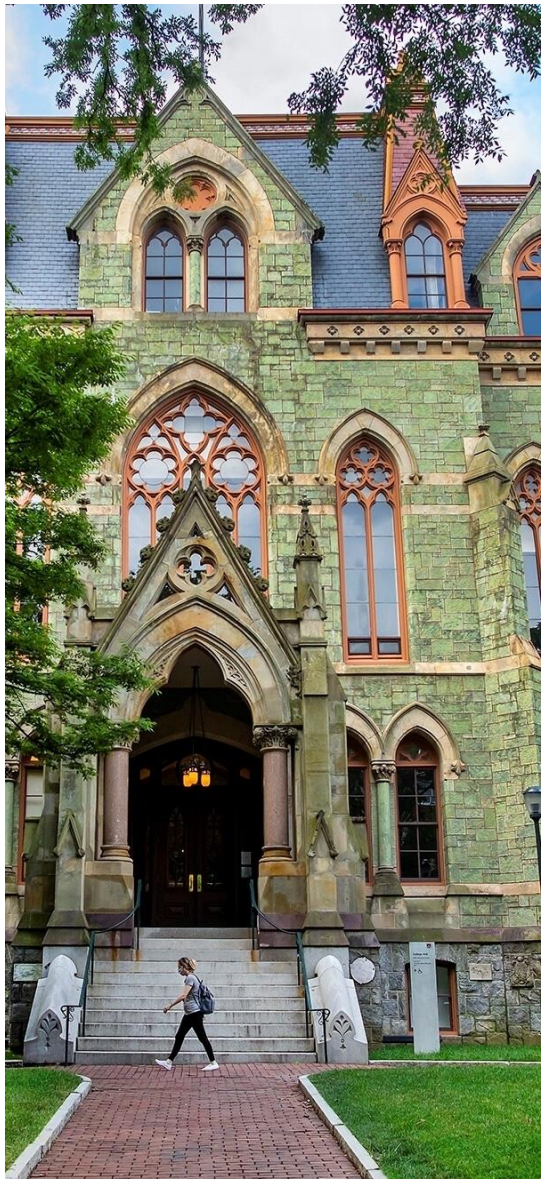


Board reporting

- Typically once or twice per year in person, with a written update for other quarters
- Semi-standardized approach:
  - Top risks and updates on how they are being addressed
  - Project updates for major efforts
  - Metrics – Penn wide and focused on top ten applications
  - Review of high impact incidents

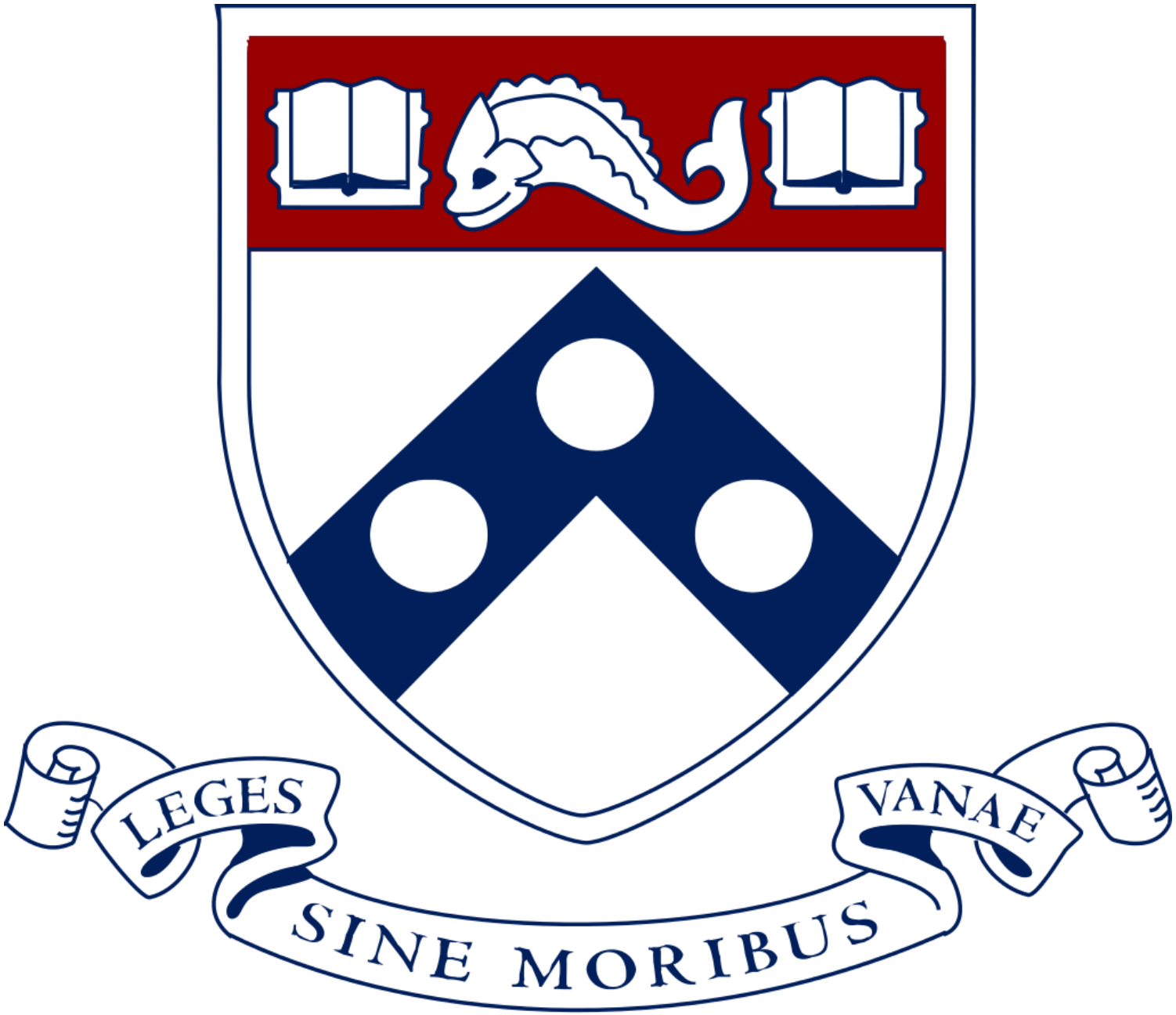
University-Wide Information Security Metrics

Metric	Previous	Current
Patching (Target: less than 30 days) Measure adjusted to quarterly vs annual.	12.3 days average (Q1 FY26)	13.6 days average (Q1 FY26)
Serious Incident Detection Time (Target: less than 3 days)	30 Days (2 serious events)	NA (0 serious events)
Phishing Simulation Outcomes (Target: less than 15%)	32% (Fiscal YTD)	28% (Fiscal YTD)
Security Budget as a Percent of IT Budget	xxx (FY24)	xxx (FY25)



Security Risks & Projects Update

Risks	Actions	Action Status
Identities and Accounts	IAM Project	Removed hundreds of thousands of stale accounts from Kite Active Directory. Upgraded password reset support implemented for most PennKeys.
Decentralization	Penn SecureIT	Penn SecureIT project to consolidate SEVP IT functions in progress.
Ransomware	ISC CrowdStrike Complete pilot	Pilot success; expanding to SEVP centers as part of the above effort.
State Sponsored Hackers		
<location specific>	<improvement plan>	<progress>
Program Maturity/Scale	Accepted risk	See Penn SecureIT slides
Unmanaged Devices	Accepted risk	Accepted risk


LEGES
SINE MORIBUS
VANAE