INFORMATION
TECHNOLOGY SERVICES
EAST TENNESSEE STATE UNIVERSITY

Nicks Hall, Room 425
Johnson City, TN 37614
P (423) 439-7000
F (423) 439-5770

INFORMATION SECURITY STRATEGIC PLAN 2017-2022

INTRODUCTION

Information security is essential to the mission and institutional strategic goals of East Tennessee State University. ETSU supports a comprehensive campus–wide information security program and recognizes that information security is a shared responsibility; as a result, the university is set to establishing its first formalized information security program. The purpose of this information security plan is to develop a comprehensive information security program to adequately protect the confidentiality, integrity and availability of information, and reduce risk to an acceptable level.

MISSION STATEMENT

The Chief Information Security Officer (CISO) is committed to engaging and working with ETSU to identify, develop, seek approval for, and promote a comprehensive University information security and risk management program. The program will focus on attack prediction, exposure prevention, breach detection and incident response through continuous monitoring and data analytics (Figure 1). It is the mission of the CISO to utilize user education, Governance, Risk Management, and Compliance (GRC) to meets the needs of ETSU and supports its mission, while protecting the University's assets against unauthorized use, disclosure, modification, damage and loss.

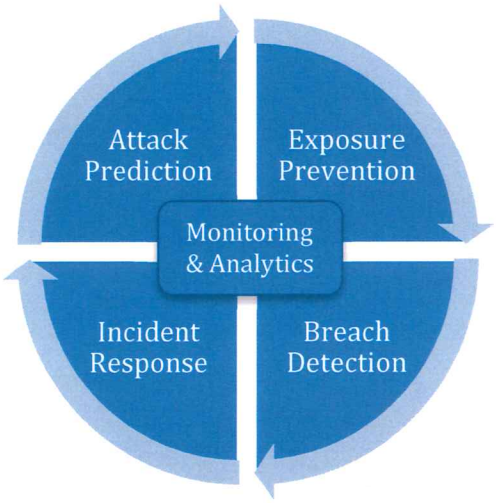

Figure 1 – Measureable continuous cyber improvement process

STRATEGIC OBJECTIVES

Implement an information technology security program for East Tennessee State University to effectively manage security risk to its information technology assets. Assuming that there will be

Nicks Hall, Room 425
Johnson City, TN 37614
P (423) 439-7000
F (423) 439-5770

sufficient resources for people, processes and tools, it will take one to five years to completely implement the following strategic goals.

STRATEGIC GOALS

PLAN

Goal 1: Identify, approve and promote a best practice IT security standard.

The CISO, in partnership with all appropriate University constituents and committees, will guide ETSU in the selection of an appropriate information security standard that best serves the University's mission.

Key Benefits

- Provide a clear information security baseline for all University constituents.
- Serve as a catalyst for implementing secure business processes.
- Provide a security model for policy development.

Goal 2: Develop, approve and promote a comprehensive set of IT security policies.

The CISO, in partnership with all appropriate University constituents and committees, will guide ETSU in the development of a comprehensive set of information security policies. Policies will be based on the information security standard selected in Goal 1, will follow information security best practices, and will be tailored to best support the University's mission and risk appetite.

Key Benefits

- Consistent information security controls across all University constituents and processes.
- Topic specific and focused baseline for implementing information security controls.
- Foundation for implementing and measuring compliance.
- Clear security role responsibility and accountability.
- Consistent prevention and remediation processes.

ENHANCE

Goal 3: Implement a formal risk and contingency management program.

The CISO will drive the development and implementation of an IT centric business impact analysis and risk assessment, which will provide ETSU the necessary information and tools to identify its mission essential business functions, understand their relationships, and quantify the risk associated with their disruption. Subsequently, a business continuity and disaster recovery plan will be established to provide continuity of mission essential functions that are dependent upon IT

Nicks Hall, Room 425
Johnson City, TN 37614
P (423) 439-7000
F (423) 439-5770

systems, and provide for timely recovery of dependent IT systems. A schedule for periodic testing of these plans will be established.

Key Benefits

- A plan for ETSU's business units to provide continued service in the absence of IT systems.
- Continuous improvement through regular risk and maturity assessment testing.
- Recovery of IT systems and services according to critical business units' needs.
- Identification of university's mission critical functions related to IT systems.
- Improved visibility over business function dependencies.
- A risk based approach to information security.

Goal 4: Inventory and classify sensitive systems and data.

The CISO will initiate a campus-wide inventory process to identify and classify sensitive systems and data. Sensitive systems and data will be protected in accordance with the policies set forth by the University under Goal 2 and following guidance from the campus CISO, HIPAA officer, data owners, and business owners. Sensitive data no longer needed for business or archival purposes will be purged in accordance with University and applicable retention policies.

Key Benefits

- Reduced risk of exposure from unknown sensitive systems and data sets.
- Consistent classification, management, and protection of sensitive data.
- Improved compliance for HIPAA, PCI, FERPA and other requirements.
- Holistic view and inventory of sensitive systems and data.

Goal 5: Establish a broad information security educational and training program.

The CISO will establish a broad ongoing information security awareness program in support of Goal 2. The information security awareness program shall be well integrated into the University's Human Resources, on-boarding and off-boarding workflow, include relevant education material and training tailored to both board and specific audiences, and provide measurable results of effectiveness.

Key Benefits

- Improved employee recognition of and response potential and real security concerns.
- Improved awareness of security threats and their impact on information assets.
- Reduced number of incidents from social engineering and other attacks.

MONITOR

Goal 6: Align University governance and IT to support information security and risk reduction.

INFORMATION
TECHNOLOGY SERVICES
EAST TENNESSEE STATE UNIVERSITY

Nicks Hall, Room 425
Johnson City, TN 37614
P (423) 439-7000
F (423) 439-5770

ETSU will align and strengthen relevant current governance committees, and establish new governance committees as needed to infuse and drive information security across all aspects of the University life and business. The CISO and the CIO will assess IT requirements and align processes to enhance technical and management IT security controls, implement new controls where needed, and monitor controls' effectiveness.

Key Benefits

- Improved information flow among business units and between business units and ITS.
- Improved awareness of perceived risk, and risk appetite by the CISO.
- Ability to make more informed risk based decisions across the university.
- Support and implement the "security is a shared responsibility" model.

Goal 7: Establish a process for regular progress reporting.

The CISO will establish a vehicle and schedule for reporting on the progress of this information security strategic plan to various University constituents, and senior leadership.

Key Benefits

- Visibility over governance, risk and compliance status and progress.
- Ability to make informed risk based decisions.

Andrea Di Fabio
Chief Information Security Officer and Associate Chief Information Officer

Karen D. King
Chief Information Officer and Sr. Vice Provost for Information Technology Services

Brian E. Noland
President