UNC GREENSBORO

# Information Security Transformation

Finding a new way to protect the university.

# The Role of Information Security @ UNCG

- Support Student Success
  - Ensure the **Confidentiality**, **Integrity**, and **Availability** of the systems and data that directly or indirectly aid in the delivery of knowledge to students.
- Protect the university's reputation
  - Data breaches make headlines, negatively affect public perceptions, and significantly increase costs in addition to creating operational disruption.
- Mitigate Risk
  - Security risks result in operational, financial, reputational, legal, regulatory, and other types of impacts.  Reducing security risks means reducing institutional risk in all these areas.
- Preserve the capability to function in key areas
  - Information Security controls play a critical role in complying with FERPA, HIPAA, PCI, and other regulatory requirements.
- Protect our research environments
  - Information Security technologies and practices help preserve the integrity of research data.
- Provide local solutions to global challenges
  - Information Security is a global concern, but local solutions are needed that meet the unique needs of UNCG's faculty, staff, administration, and students.

# Headlines

## Add Butler University to Breach List

Latest Incident Highlights Breach Vulnerabilities in Academia

A **data breach** affecting 163,000 students, faculty, staff and alumni at **Butler University** in Indianapolis, Ind., offers just the latest example of the risks facing educational institutions, which are seen as easy targets by cyber-attackers.

One month after the **University of Maryland** reported a breach that affected 288,000 students, faculty and staff, the institution has suffered a second cyber-intrusion.

## Indiana University Reports Breach

Information on 146,000 Students Potentially Exposed


## University Breach Exposes Employee Info

The **University of Central Oklahoma** is notifying 16,000 current and former employees about a breach involving unauthorized access to information stored on a server.


GARRETT M. GRAFF SECURITY 03.23.18 11:49 AM

## DOJ INDICTS 9 IRANIANS FOR BRAZEN CYBERATTACKS AGAINST 144 US UNIVERSITIES

a massive three-year campaign to penetrate and steal more than 31 terabytes of information—totaling more than $3 billion in intellectual property—from more than 300 American and foreign universities.

## Global University Provides Notice Of Data Breach

- Data on current and former students leaked

NEWS PROVIDED BY
**Global University →**
May 08, 2018, 06:00 ET

May 21, 2018

## 2,500 students, alumni and staffers affected by University at Buffalo data breach

## Yale University discloses old school data breach

"119,000 individuals affected"

The data breach was discovered a decade too late to do anything about it.

By Charlie Osborne for Zero Day | August 1, 2018 -- 09:30 GMT (02:30 PDT) | Topic: Security

UNC GREENSBORO

Source for data breach statistics: 2017 Ponemon Institute Cost of Data Breach Study: United States

# Current State of Information Security @ UNCG

- Current posture is strong, but needs to continue changing, adapting, and improving
  - As technologies continue to decentralize and migrate to the cloud, defenses need to adapt to the changing environment.
  - New areas include expanded mobile platforms, IoT, machine learning, AI, and Open Data initiatives
- Leveraging reactive capabilities, investing in proactive capabilities
  - Traditional reactive posture effectively helps us recover from compromises and protect against known threats
  - Next step in maturity is to start proactively assessing new and emerging threats prior to compromise
- What we think vs. What we know
  - Our history indicates but does not guarantee a strong posture of invulnerability.
  - A comprehensive program of internal and external assessments will help prove the strength of our defenses.
  - Measurable benefits of security tools/strategies needs to be shown via value-based metrics.
- Increasing Focus and Coordination at UNC System level
  - Complying with the February 2018 mandate for Information Security accountability from UNC System
  - Entering a new era of cooperative interactions with sister schools, with opportunities to lead the way

# The Challenge

- Deliver a transformative plan that shapes the future of Information Security at UNCG
  - Assess the current Information Security program to identify potential areas for improvement, and paths for the future.
  - Leverage industry and academic resources to identify desirable postures for the Information Security program and team.
  - Provide ITS and university leadership with value-based propositions and strategic plans for suggested improvements.
  - Translate the assessed needs for Information Security program improvements into outcomes that are aligned with the strategic goals of ITS and the university.
  - Pursue alignment with UNC System guidelines, industry standards and best practices, and regulatory requirements.

# The Plan

- Assess:
  - Work to identify the university's critical assets and systems, and how they are protected.
  - Assess the existing Information Security program and start building a plan for a new program focused on strategic risk mitigation.
  - Surface critical gaps and weaknesses that need immediate attention.
- Transform:
  - Deliver a multi-year strategic plan for critical information security program transformation and improvement.
  - Work closely with UNC System counterparts to leverage the combined resources of the system.
  - Pursue strategic partnerships that will measurably improve information security risk mitigation posture.
  - Transform the ITS organization and Information Security team to a new embedded security team model.
- Sustain:
  - Deliver on the goals of targets of the strategic plan for program transformation
  - Periodically reassess and adjust to changing conditions

# Intended Outcomes

- A new program-level definition for Information Security as part of the ITS portfolio of services
  - Aligned to strategic plans for the university and ITS
- A prioritized list of policy improvement initiatives, with suggested timelines and downstream dependencies
- A sustainable program of periodic assessments ensuring the viability and continuity of security and compliance activities
- Lists of identified security gaps and weaknesses, with impact statements and suggested improvements for each
- Prioritized and rationalized suggestions for process and workflow changes to support new program elements
- Key partnerships for sustaining security operations and prioritized risk management
- Proposed organizational changes needed to sustain new modes of operation