UNIVERSITY of NORTH CAROLINA WILMINGTON

TO: UNCW Board of Trustees
FROM: Dr. Sharyne A. Miller, Chief Information Officer & Associate Vice Chancellor for Information Technology Services
DATE: April 8, 2025
SUBJECT: Annual IT Governance & Risk Update

Trustees,

This report provides a brief overview of the Information Technology Services (ITS) offices whose primary responsibilities include managing and supporting daily operations related to information security, governance, risk, and compliance. Details on the activities conducted by these offices are included to highlight the threats and risks the University faces on an on-going basis.

Key Offices and Leadership

- Office of Information Security: Led by Aaron Culler, Director of Information Security, with a team of four staff members and four apprentices.
- Office of Governance, Risk, and Compliance: Led by Steve Perry, IT Assessment, Policy, and Governance Officer, with three additional staff members.

Information Security Highlights

- Firewall: Blocked nearly 97 million malicious connections in one day.
- Security Events: Over 850 cybersecurity investigations in the last 30 days.
- Vulnerabilities: Resolved 53 vulnerability tickets since January 2025.
- Phishing: Over 100 phishing emails reported in the last 30 days.
- Security Awareness Training: 53% completion rate among university employees.
    - This number continues to rise as reminder notices are sent across campus.

Emerging Risks

- **Expansion of CUI and NIST Compliance:** The Federal Government is expanding the scope of Controlled Unclassified Information (CUI) to include more data types, impacting research and institutional administration. UNCW must become compliant with National Institution for Standards and Technology (NIST) 800-171, which mandates 110 security controls. Establishing and maintaining compliance with NIST 800-171 will require additional staff, technological resources, and third-party audits.
- **Artificial Intelligence:** AI tools pose risks such as training with sensitive data, invalidating data use agreements, and AI-generated cyber-attacks. The advanced capabilities and rapid implementation of AI tools pose a considerable risk to the

University. The main concerns include the retention of sensitive user inputs by AI models for training, the risk of invalidating previous data use practices as integrated into services, and the use of AI tools to efficiently create phishing emails, cyber-attack scripts, and gather open-source intelligence.

Planning and Risk Mitigation Strategies

- **Security Baseline (Windows):** The ISO 27002 security framework guides cybersecurity strategies at UNCW. As we look towards broader NIST compliance for campus, ITS has adopted the Center for Internet Security (CIS) Benchmarks for Windows Endpoints to enhance protection and align additional controls with the NIST framework.
- **Vulnerability & Patch Management:** ITS is refining its process with a unified console for rapid deployment and monitoring and inclusion of threat intelligence in priority remediation.
- **2FA Changes:** Enhancements to multi-factor authentication have been implemented to reduce compromised accounts.
- **National Guard Penetration Test and Incident Response Planning:** UNCW partnered with the North Carolina National Guard for a penetration test and is reviewing/updating its incident response plan. The test was a success with minimal findings.
- **Theat Intelligence Hub:** ITS developed a cyber intelligence hub to centralize cyber threat information. Providing the ability to manage various intelligence sources, submitting indicators of compromise, and providing an intrusion analysis workflow. ITS plans to present our Cyber Intelligence solution to the broader UNC system to aid our sister schools in threat intelligence and risk management.

Operation Tobacco Road

- **National Cybersecurity Exercise:** Operation Tobacco Road is a comprehensive cybersecurity exercise where multiple teams collaborate to defend attacks using real-world tools and techniques over several days. The UNCW IT Security team placed second last year, just behind the North Carolina National Guard, earning recognition for their technical skills from event sponsors and the UNC System.

Recent Threats

- **PowerSchool Breach:** Thousands of student information records were exfiltrated and auctioned on the dark web.
- **National Student Clearinghouse:** Student information data breach affecting 890 schools.
- **Lumma Stealer Campaign:** Malware targeting U.S. state, local, tribal, and territorial government organizations. Targeted UNCW, defeated by IT Security.

UNIVERSITY of NORTH CAROLINA WILMINGTON

Governance Programs

IT Governance: UNCW's IT Governance Program is overseen by the Chief Information Officer and supported by the IT Governance Steering Committee and subcommittees has recently focused on mitigating risks associated with technology proliferation and outsourcing services. Efforts include integrating governance principles into existing processes, identifying duplicative services, and creating an inventory of reviewed software for campus use.

Data Governance: UNCW's Data Governance Program has established an enterprise data warehouse (EDW) to support data-driven decision-making. The EDW enhances efficiency, consistency, security, and scalability for strategic initiatives. The Seahawk Insights Portal provides access to dashboards visualizing data such as strategic metrics, admissions trends, and student lifecycle information. Security measures include "FERPA 101" training and access control tickets to ensure data protection.

Third-Party Risk Management

The IT Vendor Risk Management (VRM) Program addresses risks associated with third-party software. Improvements in the software review process have reduced approval times from over 30 days to around 5 days. The program conducts formal third-party risk assessments to ensure data protection, collaborating with the Office of the General Counsel to negotiate data protection terms in contracts. Assessments are conducted for third-party solutions and systems that access, process, store, or otherwise utilize sensitive University data. In FY25, 40 third-party risk assessments have been completed, with an additional 10 pending. These assessments cover various data scopes, including student records, human resources, finance, and more.

Compliance

As the University expands its research efforts into new areas, handling research data compliance will require increased resources in ITS and other departments. Non-compliance can result in loss of future opportunities with research sponsors, fines, potential criminal charges, and damage to the University's reputation. The primary concern for ITS is the new use of CUI data and identifiable health information. These emerging compliance requirements will need new resources for implementation and support for policy alignment, training, dedicated software and hardware, and IT security monitoring and reporting