SAFEGUARDING UND BY BUILDING BRIDGES

The University of North Dakota (UND) established the Safeguarding UND initiative by effectively integrating traditional physical security and public safety issues with cybersecurity concerns.

CHANGING LANDSCAPE OF THREATS

- According to the World Economic Forum, two of the top five risks over the next ten years for organizations are extreme weather events and cyber-related attacks.
- The Department of Public Safety (DPS) and the University Information Technology (UIT) at the University of North Dakota realized there was an ever-widening gap in crisis management and planning.
- The gap seemed to exist among physical and cybersecurity issues.
- No discussion was occurring within departments on how cyber issues affected public safety.

BREAKING DOWN PAST PROCEDURES AND SYSTEMS

- Proactive approach
  - Monitor the forces that drive change
  - Analyze relationship to risk
  - Adapt strategies required to manage risk flexibly
- Develop strategic partnership to build up physical and cyber security protection systems that enhance public safety.
- Implement and maintain systems aimed at preventive, detective and corrective measures while considering the existing architectural, operational and security system elements already integrated at UND.

PREVENTIVE MEASURES

- Enterprise Risk Management Committee
  - Cross-section of University stakeholders
  - Facilitates discussions of concerns across the institution related to the five areas of risk (i.e. financial, operational, strategic, compliance and reputational)
  - Conducts an annual risk and vulnerability assessment
- Technology initiatives
  - Update acceptable use of technology policies with mandatory annual training
  - Install endpoint protection in UND-owned devices
  - Implement multi-factor authentication
  - Block BitTorrent across UND network
  - Electronic signatures
  - Secure wireless
  - Secure file share
- Education
  - Cybersecurity training
  - Phishing awareness training
  - Acceptable use of technology training
  - Title IX reporting and support available
  - Sexual violence and discrimination prevention and awareness
  - Protecting minors on campus
- Addition of four new security related positions
DETECTIVE MEASURES

- Employ updated technology to provide proper situational awareness and detect threats before they occur
- Update and integrate legacy systems into a single platform to provide a common operating picture of the campus community, including
  - Electronic door access
  - Video surveillance
  - Alarms
  - Building automation systems
- Gain membership to the International Watch Foundation preventing the use of the University network to gain access to child pornography sites
- Instituted vulnerability assessments on servers to better understand how to keep the systems secure

CORRECTIVE MEASURES

- University emergency operations plan
  - Allows for immediate response and recovery from a critical incident
- Continuity of Operations Plan (COOP)
  - Each division completed a COOP to identify their critical functions
  - KualiReady (COOP planning tool)
- Strengthened the Information Security Incident Response Team
  - Consolidated functional areas within the network
  - Implemented a phishing awareness campaign
- Create culture where concerns are reported and University responds
  - Widespread communication to campus about initiatives, resources, and expectations
  - Additional cybersecurity, investigative and public safety staff added

STRATEGIC PARTNERSHIPS MAXIMIZE OUR EFFORTS

The items discussed are just a few systems this partnership has implemented and maintained. All departments are looking to incorporate future systems in the merging fields of physical and cybersecurity protection. All of these have been done to safeguard UND and move the institution forward as a leader in these emerging topics while allowing the University to become a risk agile organization.