CYBERSECURITY UPDATE
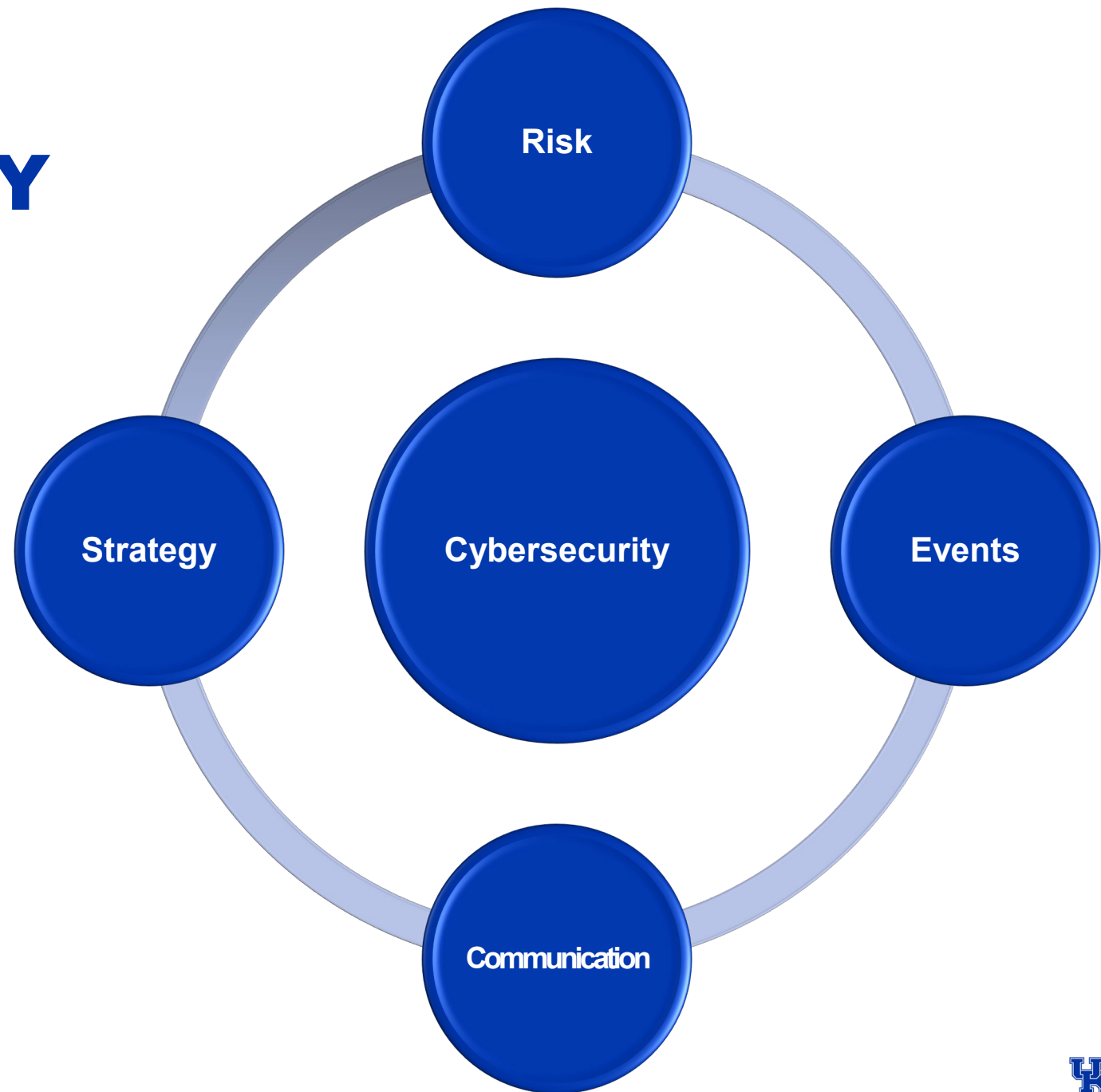
Marc Blevins, Analytics and Investigations Manager

Wes Justice, Information Technology Audit Manager
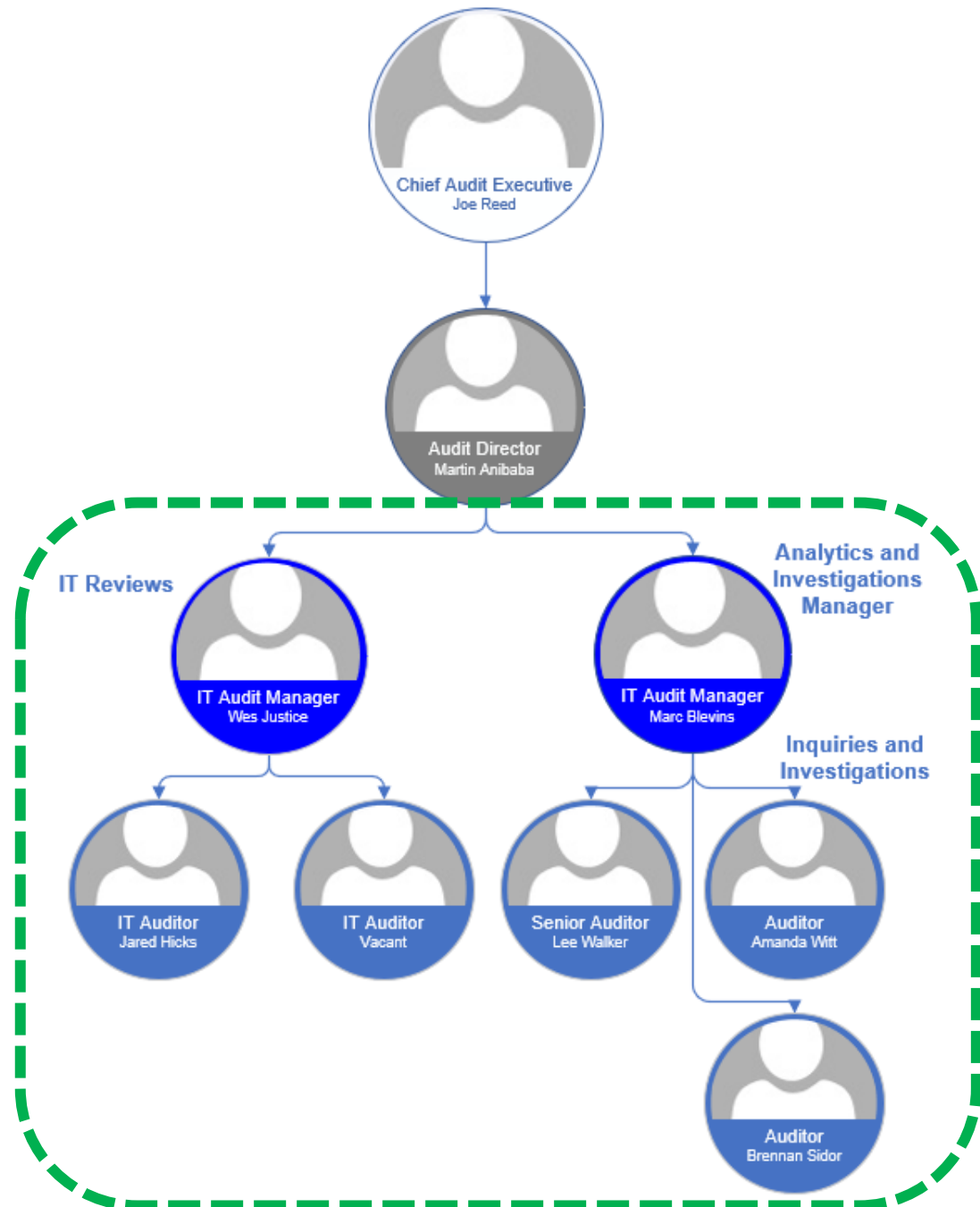
University of Kentucky

AN EQUAL OPPORTUNITY UNIVERSITY

Information Technology Team Structure

- Analytics & Investigations Manager: Marc Blevins
  - IT Audit Manager: Wes Justice
    - Jared Hicks
    - New hire starting June 2021
  - Analytics and Investigations Team
    - Brennan Sidor
    - Lee Walker
    - Amanda Witt

Cybersecurity is the art of protecting networks, devices and data from unauthorized access or criminal use and the practice of ensuring **confidentiality, integrity and availability** of information.

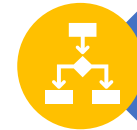- U.S. Cybersecurity and Infrastructure Security Agency

Risks of Insufficient Cybersecurity Practices

Data Compromise

Regulatory Noncompliance

Operational Disruption

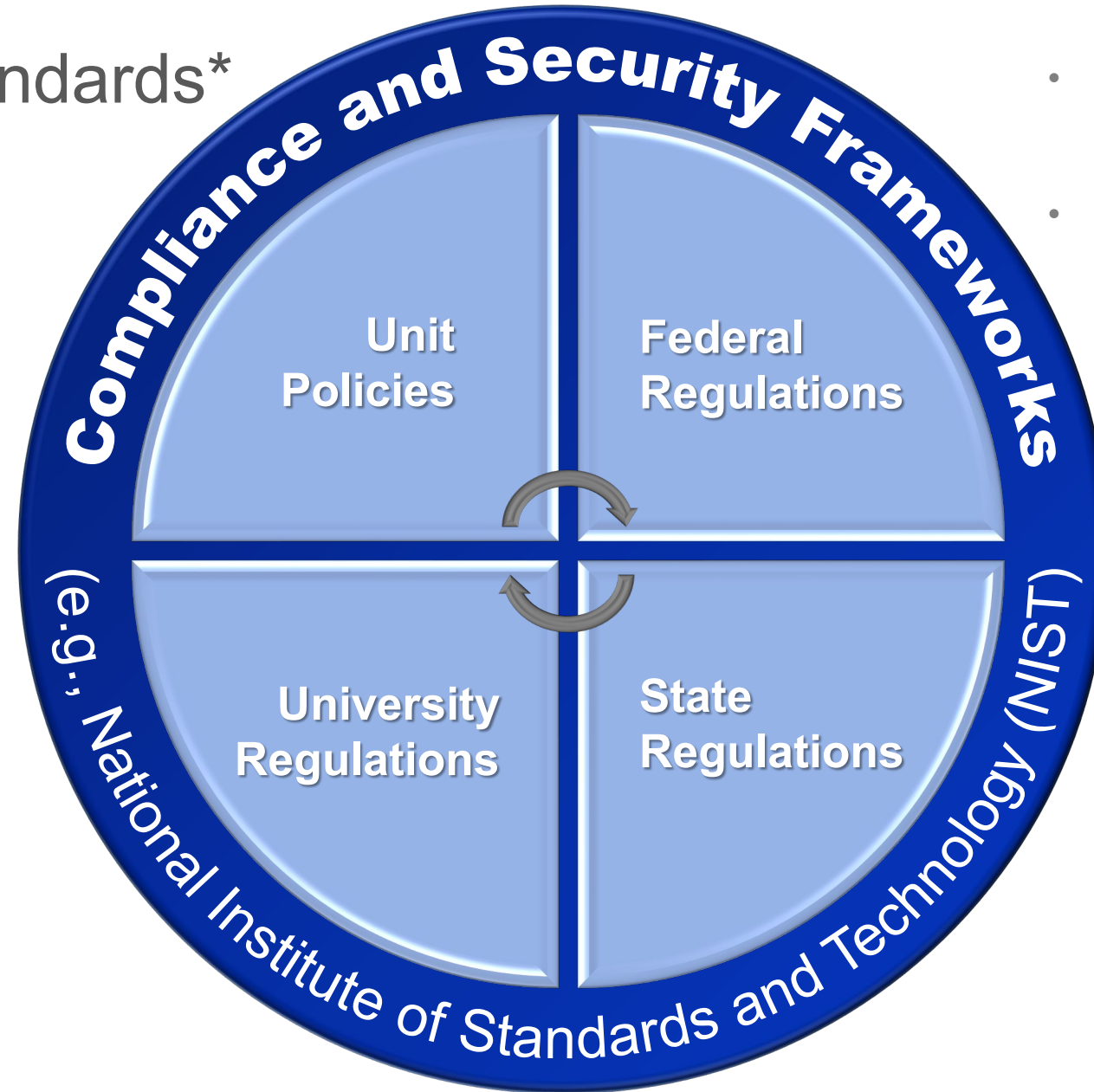Financial Loss (fines, recovery costs and revenue loss)

Reputational Harm

University of Kentucky

Cybersecurity Standards*

- UK Information Technology Services (ITS) Information Security Policy
- UK HealthCare Information Technology (UKHC IT) Information Security Policy
- College/Unit Information Security Policies

Administrative Regulation (AR) 10 Information Technology

Not an all-inclusive list

Compliance and Security Frameworks
(e.g., National Institute of Standards and Technology (NIST))

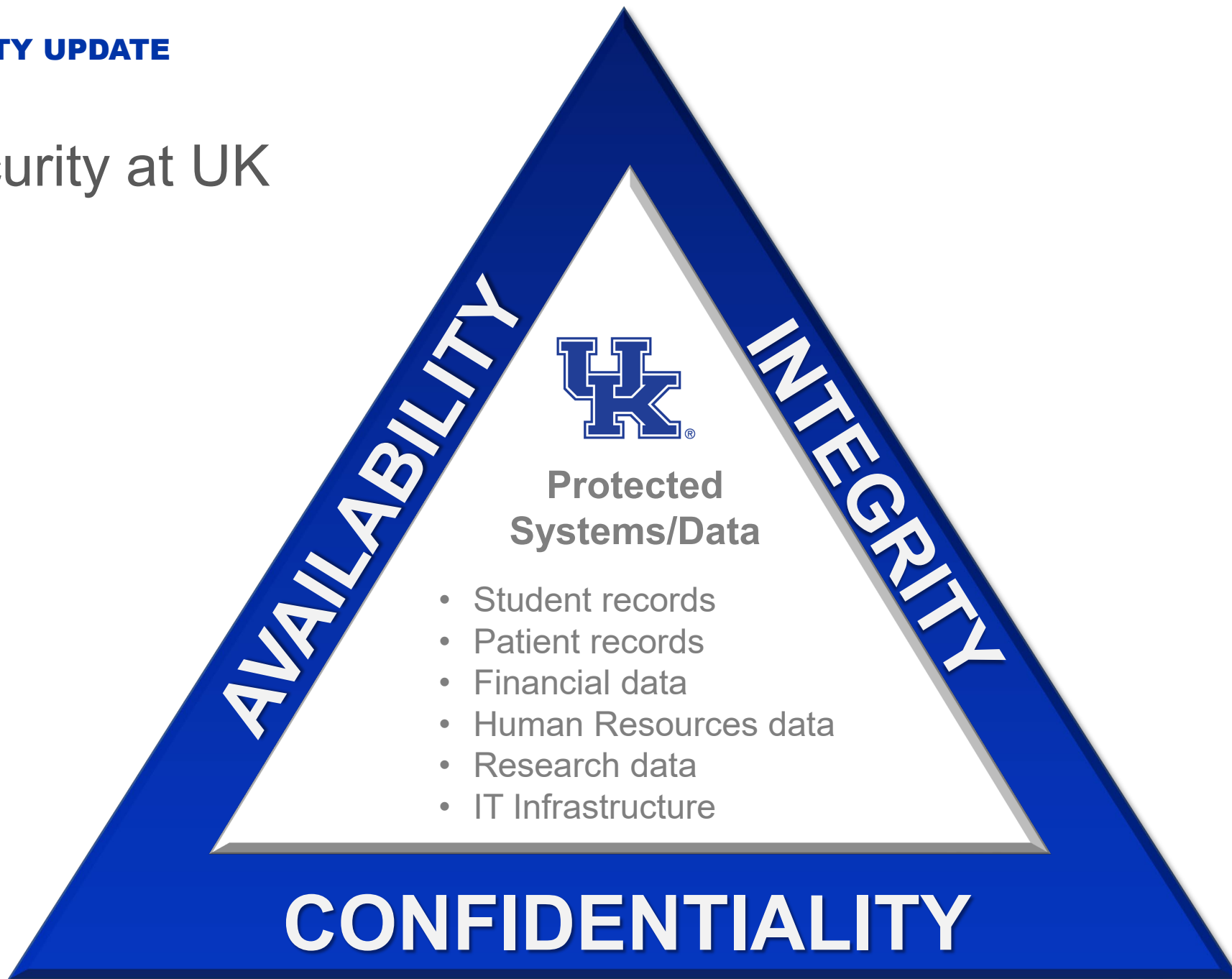**Unit Policies**

Federal Regulations

University Regulations

State Regulations

- Health Insurance Portability and Accountability Act (HIPAA)
- Family Educational Rights and Privacy Act (FERPA)

Personal Information Security and Breach Investigation Procedures and Practices Act

University of Kentucky

Cybersecurity at UK

AVAILABILITY

INTEGRITY

Protected Systems/Data

- Student records
- Patient records
- Financial data
- Human Resources data
- Research data
- IT Infrastructure

CONFIDENTIALITY

University of Kentucky

Recent Cybersecurity Events

NEWS
FBI, other agencies warn of 'imminent cybercrime threat' to U.S. hospitals

UKNOW
Blackbaud Data Security Incident Affects UK HealthCare

kentuckykernel
6,000 myUK accounts were found for sale on the dark web, UK IT officials say

LEXINGTON
HERALD LEADER
Computer systems at UK and UK HealthCare hobbled by massive, month-long cyber attack

NEWS
Major hospital system hit with cyberattack, potentially largest in U.S. history

INSIDE HIGHER ED
FBI Warns of Increased Ransomware Attacks Targeting Colleges

UKNOW
ITS Has Been Alerted to Ransomware Attacks

University of Kentucky

2020 Cybersecurity Incident

Key factors leading to incident:

Web application patch management	→	Exploited overprivileged accounts	→	Insufficient endpoint protection, incident detection, and virtual private network authentication (VPN) systems

University of Kentucky

Cybersecurity Information Tour: "Cybersecurity is Everyone's Job"

More than 20 virtual cybersecurity "information tour" sessions were conducted October - November 2020

Participants:
- Deans and administrators
- IT leadership personnel across the enterprise

Presenters:
- UK chief accountability officer and audit executive
- UK chief information officer
- UKHC chief information officer

Tour objectives:
- Increasing awareness of recent cybersecurity events
- Discussing policies, procedures and best practices for cybersecurity governance and operations
- Listening to concerns and suggestions from autonomous IT service areas for improving the university's overall cybersecurity posture
- Trending risk areas

University of Kentucky

Cybersecurity Information Tour

Key discussion topics

- Consistently evolving cybersecurity threat landscape

- Enterprise-wide cybersecurity incident response plan
  - Unit-level response plans to align with enterprise

- Establishment of minimum requirements and cybersecurity standards enterprise-wide.
  - Supplemented as necessary by unit-level policies, standards and processes

- Opportunities for enhanced training and cross-unit communications and collaboration

- Ongoing UKIA cybersecurity review activities

University of Kentucky

UKIA Cybersecurity Activity

Cybersecurity Follow-up

- Client check-in around 90 days from issuance of final report

- Follow-up based on target completion dates noted in the Management Action Plan

Unannounced Cybersecurity Reviews

- Conducted via unannounced site visits or virtually via same-day notifications

- Limited scope reviews with quick turnaround focused on trending, high risk cybersecurity threat areas

- Provides immediate value to colleges or units via short-term review and analysis

- Increases enterprise-wide awareness of cybersecurity risks and best practices

- Enhances preparedness for cybersecurity incidents

Current/Upcoming Process Reviews

- Endpoint vulnerability management

- **Web application security**

- Phishing awareness

- Account deprovisioning

- Server configuration

- Endpoint configuration

- IT asset management

- Cybersecurity incident response

University of Kentucky

UK INTERNAL AUDIT MISSION STATEMENT

To support UK in its pursuit of excellence by providing expert analyses and advice to champion the achievement of management objectives.

University of Kentucky