Board of Trustees

Audit Committee

December 9, 2024
Minutes
2:30 PM – 3:30 PM
Loughman Living Room, Scanlon Hall

A live stream of the meeting for public viewing will also take place at the following link: https://www.westfield.ma.edu/live

---

Committee Members Present: Committee Chair Theresa Jasmin, Vice Chair William Reichelt, Secretary Michael O'Rourke, Members: Melissa Alvarado, Tessa Lucey, and Dr. Gloria Williams.

Also present were Westfield State University President, Dr. Linda Thompson; Vice President for Administration and Finance, Stephen Taksar; Associate Vice President Financial Accounting Lisa Freeman; Associate Vice President Administration and Finance, Maria Feuerstein; Vice President of Institutional Advancement, Lisa MacMahon; Assistant Vice President Information and Instructional Technology, Alan Blair and Director of Dining Services, Melissa Sikes.

Committee Chair Theresa Jasmin called the meeting to order at 2:30 p.m., conducted a roll call of committee members, and stated the meeting was being livestreamed and recorded.

MOTION made by Trustee Lucey second by Trustee Alvarado to approve the meeting minutes of October 21, 2024. A roll call was completed, O'Rourke and Jasmin abstained. **Motion passed.**

Cybersecurity Discussion

- Importance of cybersecurity
  - Identified as a top risk in enterprise risk management
- Agenda items flipped to prioritize information on campus cyber update
- Vice President for Administration and Finance, Steve Taksar and Assistant Vice President Information and Instructional Technology, Alan Blair providing updates

PCI Assessment Update

- Engagement date for 2025 received
- Clean audit reported for several consecutive years
- Compliance with new PCI 4.0 standards ahead of schedule
  - Reduced cyber footprint for credit card payments
  - No storage of credit card data on local environment

Cybersecurity Awareness Audit

- Audit conducted by the state
  - Focus on training
- Response to auditors
  - Clarification on definitions of personnel
  - Still working on full compliance.

- Key cybersecurity measures discussed
    - Administrative privileges reduction
    - Multi-factor authentication
    - Training completion within 30 days

Future Actions
- Incorporating training requirements into acceptable use policy
- Current training completion rate at 72%
- Plans for improvement through collaboration with departments and human resources

Cybersecurity Training Requirement
- Discussion on requiring all students to complete cybersecurity training.
    - Some state colleges currently have voluntary training.
    - Conversations ongoing among CIO council and Higher Education Cyber Security Coordinating Committee about making it a requirement.
- Current training compliance rates.
    - 72% compliance noted, but the standard is 100%.
    - Previous phishing incidents reduced significantly after implementing multi-factor authentication.

Cybersecurity Initiatives
- Formation of a dedicated cybersecurity group.
    - Aimed at improving collaboration and communication across state colleges and universities.
    - Includes various departments such as EOS and the secretary's office.
- Creation of a cyber dashboard.
    - Intended to provide a holistic view of cybersecurity progress across all 24 state colleges.
    - Will compare current status against industry standards and previous years.

Cyber Defense and Compliance
- Adoption of CIS Critical Controls.
    - All 24 state colleges accepted it as the standard for cybersecurity practices.
    - Progress from version 5.5 to 8.0 of the information security policy.
- Internal audits and external assessments.
    - Regular self-audits conducted to ensure compliance.
    - External audits performed every three to four years for verification.

Financial Investments in Cybersecurity
- Last year saw significant financial investments in cybersecurity for higher education.
    - $1.6 million allocated, with Westfield State receiving $67,000.
- Local operating capital budget directed $185,000 towards endpoint management.
    - Focus on antivirus and managed detection response services.

Cybersecurity Enhancements
- Implemented centralized security training through "KnowB4."
    - First in the state to adopt this training program.
    - 23 out of 24 institutions are now participating.
- Transitioned to a new contract with the Commonwealth, reducing costs by 60%.
    - Savings redirected towards enhancing cyber defenses.

Collaborative Efforts and Training
- Collective bargaining with NSCA led to mandatory training for all members.
    - Training is educational and applicable to personal life.
- Shared services initiative faced challenges due to varying needs of institutions.
    - Participated in surveys to identify common services like security awareness training.

Incident Response and Future Focus

- Established a fusion center for immediate information sharing during incidents.
    - Aimed at improving communication and response among institutions.
- Identified key focus areas for the next 1-3 years.
    - Increasing data breaches, particularly from third parties.
    - Rise in phishing and social engineering attacks since 2020.

Insider Threats and Data Management
- Increase in insider threats due to personal device usage.
- Importance of leveraging legal counsel in procurement.
    - Emphasis on stronger contract language for cloud services.
    - Requirement for vendors storing sensitive data to fill out a questionnaire.

Network Security Measures
- Network segmentation referred to as the "moat effect."
    - Protects data by keeping it contained within specific areas.
    - Reduces the cost of mitigating breaches.
- Need for improved vendor risk management.
    - Regular follow-ups on contract renewals and updates.

Cyber Insurance and Incident Response
- Cyber insurance has evolved into a partnership.
    - Provides off-site response repositories for incident plans.
    - Offers free services for data storage and access during outages.
- Importance of building a comprehensive incident response plan.

Threat Detection and Response
- High volume of attacks detected at Westfield State.
    - Approximately 88 million attacks noted.
    - Use of automated systems and AI for threat detection.
- Implementation of a trust principle in network security.
    - Block everything and only open necessary ports for vendors.
    - Use of endpoint detection and response systems for local threat monitoring.

Incident Response and Training
- Conducting red table exercises to improve incident response.
    - Minor incidents used for training purposes.
- Focus on phishing and social engineering training.
    - Identifying red flags in suspicious emails.

Security Policies and Controls
- Aligning policies with the Center for Security Critical version 8.0.
    - Transitioning from 21 to 18 critical controls, categorized.
- Implementing access management and acceptable use policies.
    - Providing refresher training for users who fail phishing tests.

Authentication and Vulnerability Management
- Utilizing strong multifactor authentication.
    - Transition to 15-character passwords without frequent changes.
- Ensuring timely patch management for vulnerabilities.
    - Critical patches addressed within 24 hours.

AI and Cybersecurity Initiatives
- Engaging in discussions about AI's role in academia.
    - Concerns about generative AI and its security challenges.
- Continuing investment in cybersecurity initiatives.

- Collaboration with state and university resources for future planning.

Cybersecurity Initiatives

- Implementing defenses around educational rooms to support STEM programs.
- Approximately 2.5 million cybersecurity jobs are currently vacant in the U.S.
  - The required skill set for these jobs is specific and not easily acquired.
- Funding is necessary for educational institutions to enhance cybersecurity training.
  - Example: Bridgewater's funding model is mentioned.

Backup and Data Security

- Priority for leadership this year is to achieve encrypted immutable backups.
  - Current backups are encrypted and stored in two different locations.
- Moving backups off-site to improve security.
  - The process involves a site mass to ensure data accessibility.
- Challenges with initial encryption costs for system databases.
  - Importance of having backups that are secure from ransomware attacks.

Community and Collaboration

- Emphasis on statewide communities and organizations implementing best practices.
- Acknowledgment of the importance of support systems in cybersecurity.
  - Example: Reliable communication at all hours is crucial for operations.

There being no further business, **MOTION** made by Trustee Williams and seconded by Trustee O'Rourke to adjourn the meeting. There being no discussion, **motion passed unanimously**. Meeting adjourned at 3:25 p.m.

Attachment(s):

a. Minutes 10/21/24 (Draft)
b. Campus Cyber Update
c. Cyber Security Awareness Audit (State Auditor)
d. Payment Card Industry Data Security Standards (PCI-DSS)

Secretary's Certificate

I hereby certify that the foregoing is a true and correct copy of the approved minutes of the Westfield State University Board of Trustees, Audit Committee meeting held on December 9, 2024.

_____ _____

Michael O'Rourke, Secretary Date