CyberSecure Campus: Enhancing Cybersecurity Infrastructure for Oakland University

Wasiu Abiodun Bello

Lake Erie College

Date:

May 02, 2025

1. Executive Summary

Cybersecurity is no longer optional but essential in today's digital-first academic landscape. Like many higher education institutions, Oakland University faces increasing cyberattack threats, including phishing scams, ransomware, and data breaches that compromise sensitive student, faculty, and research data. Despite existing IT infrastructure, vulnerabilities persist due to outdated systems, inconsistent security practices, and limited awareness across the campus community.

The **CyberSecure Campus** project proposes a university-wide initiative to modernize and fortify the cybersecurity infrastructure at Oakland University. The project will combine cutting-edge technological upgrades, such as enhanced firewalls, endpoint protection, multi-factor authentication (MFA), and real-time threat monitoring, with comprehensive cybersecurity training for all university members. Additionally, it will establish a structured incident response protocol aligned with national standards.

Oakland University will address existing vulnerabilities through this initiative and build a proactive, secure, and resilient digital environment that safeguards academic operations and supports the university's commitment to innovation and student success. The project will position Oakland University as a leader in cybersecurity readiness among peer institutions, ensuring compliance with federal regulations and building stakeholder confidence.

2. Project Background

Higher education institutions are increasingly attractive targets for cybercriminals due to the vast amount of sensitive personal, academic, and research data they store and manage. According to a 2022 EDUCAUSE report, over 70% of universities experienced at least one significant cyber incident within the past 12 months. These incidents ranged from ransomware

attacks to large-scale phishing campaigns, resulting in data theft, financial losses, and reputational damage.

Oakland University is not immune to these threats. While functional, the university's IT infrastructure includes legacy systems and decentralized security protocols that leave critical gaps in protection. The attack surface has expanded significantly with the proliferation of remote learning, BYOD (bring your own device) environments, and increased reliance on cloud-based platforms. These vulnerabilities expose the university to potential breaches that could disrupt operations, compromise privacy, and erode trust among students, faculty, and external partners.

Despite previous efforts to improve security, such as basic firewall protection and limited multi-factor authentication, Oakland University lacks a holistic, future-ready cybersecurity framework. Past investments have focused primarily on short-term solutions and reactive responses rather than building a strategic, campus-wide defense system.

Several institutions, including the University of Michigan and Michigan State University, have launched similar cybersecurity transformation initiatives with measurable success, including reduced incident rates and improved regulatory compliance. However, such models often rely on significant upfront investment and tailored implementation plans that address each campus's unique academic culture and resource constraints.

This project is designed to meet Oakland University's needs by aligning cybersecurity with its strategic goals of digital transformation, student success, and institutional resilience.

By modernizing infrastructure, training users, and implementing real-time monitoring and response systems, this initiative fills a critical gap that prior approaches have not adequately addressed.

3. Proposed Solution

The **CyberSecure Campus** initiative aims to transform Oakland University into a model of cybersecurity resilience in higher education. This project envisions a unified digital ecosystem where robust infrastructure, proactive monitoring, and informed campus stakeholders work together to mitigate threats, ensure data privacy, and support uninterrupted academic and research operations.

a. Project Schedule (18 Months)

Phase	Timeline	Key Milestones
Phase 1: Security Audit	Months 1–2	Complete full system vulnerability and risk assessment
Phase 2: Infrastructure Upgrade	Months 3–8	Deploy an advanced firewall, MFA, and endpoint protection
Phase 3: Training & Awareness	Months 6–12	Launch a campus-wide cybersecurity education program
Phase 4: Policy & Response Plan	Months 10–14	Establish a formal incident response framework
Phase 5: Evaluation & Handoff	Months 15–18	Independent audit, final report, transition to the IT team

b. Project Team Roles and Responsibilities

Role	Responsibilities
Project Manager	Oversee planning, execution, stakeholder reporting, budget, and team coordination
Chief Information Security Officer (CISO)	Define security protocols, lead threat modeling, and oversee compliance
IT Infrastructure Lead	Manage system upgrades, integrations, and technical implementation
Cybersecurity Analyst	Monitor threats, analyze data, and respond to incidents in real-time
Training Coordinator	Develop and deliver cybersecurity awareness content for staff and students.
External Security Consultant	Provide expert advice, third-party assessments, and compliance benchmarking

c. Risk Matrix

Risk	Probability	Impact	Mitigation Strategy
Data breach during transition	Medium	High	Run parallel systems with full backups; limit access
Low user adoption of new security protocols	High	Medium	Mandatory onboarding, incentives, and

			consistent communication
Resistance to training or policy changes	Medium	Medium	Departmental champions, gamified learning modules
Vendor delays in hardware/software delivery	Medium	High	Pre-qualification of vendors, buffer time in the timeline
Budget overruns	Low	High	Built-in contingency (5%); monthly budget review

d. Project Deliverables

1. **Full-System Security Audit Report**
2. **Modernized Infrastructure**
    - Next-generation firewalls
    - Endpoint Detection & Response (EDR) systems
    - Institution-wide Multi-Factor Authentication (MFA)
3. **Cybersecurity Awareness Program**
    - Online modules, workshops, and simulated phishing tests
4. **Incident Response Plan**
    - Custom-built for OU, aligned with NIST 800-171 standards

5. **Final Evaluation Report & Compliance Checklist**

e. **Communication Matrix**

Audience	**Communication Method**	**Frequency**	**Purpose**
Executive Stakeholders	Monthly reports & review meetings	Monthly	Budget, progress, risk, and key decisions
Project Team	Agile standups & weekly updates	Weekly	Status tracking and blocker resolution
University Community	Email updates, website, and town halls	Monthly to Quarterly	Awareness, updates, and engagement
IT Staff	Technical briefs, documentation	Bi-weekly	System implementation and transition support

4. Project Deliverables and Goals

The **CyberSecure Campus** project will result in a secure, modernized digital infrastructure for Oakland University, backed by real-time monitoring, policy-based access controls, and a campus-wide culture of cybersecurity awareness. The goal is to significantly reduce vulnerabilities and cyber incidents while ensuring compliance with federal standards and higher education best practices.

a. Project Deliverables

Deliverable	Description
Comprehensive Security Audit Report	A third-party and internal assessment detailing current vulnerabilities, gaps, and priority risks.
Advanced Security Infrastructure	Upgraded firewalls, MFA, endpoint detection, secure VPNs, and SIEM integration.
Cybersecurity Awareness Training Modules	Customized online learning modules and workshops for all students, faculty, and staff.
Simulated Cyberattack Drills	Controlled phishing and incident simulations to test response readiness.
Incident Response & Recovery Plan (IRRP)	A standardized protocol aligned with NIST 800-171 and CMMC compliance frameworks.
Final Impact Evaluation and Compliance Report	Documentation demonstrating risk mitigation, training completion rates, and audit outcomes.

b. Timeline for Deliverables

Deliverable	Expected Completion
Security Audit Report	Month 2

Infrastructure Upgrades	Month 8
Training Program Launch	Month 6 (continuous)
Simulated Cyberattack Drills	Months 10 and 16
Incident Response Plan	Month 14
Final Evaluation Report	Month 18

c. SMART Goals

Goal	**Target**
Increase network security score (internal audit benchmark)	From 68% to 90% by Month 18
Reduce phishing email click rate across campus	From 27% to below 10% within 6 months
Ensure cybersecurity training participation	100% of faculty, staff, and students within 12 months
Achieve compliance with NIST 800-171 security standards	By Month 18
Establish the average incident response time.	Under 4 hours per incident by Month 12

These goals ensure accountability and make the project outcomes highly visible and measurable to stakeholders. By aligning deliverables with SMART criteria—Specific, Measurable, Achievable, Relevant, and Time-bound—the CyberSecure Campus initiative demonstrates a strong return on investment and a clear pathway to institutional resilience.

5. Project Resources Required

A strong cybersecurity framework requires cutting-edge technology, skilled personnel, training programs, and ongoing monitoring. This section outlines the **financial investment**,

resource allocation, and **justification** necessary to successfully execute the CyberSecure Campus project at Oakland University.

a. Total Estimated Budget: $400,000

Category	Estimated Cost	Description
Infrastructure & Hardware	$200,000	Next-gen firewalls, network access control systems, secure servers, and MFA devices
Software Licenses	$50,000	SIEM platform, endpoint detection & response (EDR), secure VPNs
Personnel & Consultants	$100,000	Cybersecurity analyst(s), external consultant for audits, training developers
Training & Awareness Program	$30,000	Learning management system (LMS) modules, in-person workshops, and campaign material
Contingency Fund (5%)	$20,000	A buffer for unplanned costs, emergency fixes

b. Budget Justification

- **Infrastructure Investments** are crucial to modernize existing systems vulnerable to known threats. Investing in advanced firewalls, secure cloud access tools, and real-time monitoring provides long-term risk mitigation.

- **Software Licenses** ensure up-to-date, secure platforms for detecting and responding to cyber incidents quickly.
- **Expert Personnel** and consultants bring industry-standard knowledge to guide implementation and ensure compliance with NIST 800-171 and CMMC frameworks.
- **Training** is essential in creating a security-conscious culture and reducing human-error vulnerabilities, which are the leading cause of breaches in higher education.
- The **Contingency Fund** ensures flexibility to handle evolving cyber threats and potential project delays.

c. Resource Allocation Plan

Resource	Allocated Use
$200,000 (Hardware)	Secure servers, firewall appliances, and access control devices
$50,000 (Software)	Licensing for SIEM tools, MFA, and endpoint detection systems
$100,000 (Personnel)	Hiring cybersecurity contractors, part-time consultants
$30,000 (Training)	Program development, simulation tools, communications
$20,000 (Contingency)	Reserved for unforeseen expenses and incident mitigation

This allocation plan prioritizes **long-term stability**, **user education**, and **regulatory alignment**, ensuring that Oakland University strengthens its cybersecurity posture and builds institutional capacity for ongoing digital security management.

6. Conclusion

Oakland University stands at a critical juncture where proactive investment in cybersecurity is not just strategic—it's essential. The **CyberSecure Campus** project directly addresses growing threats to academic integrity, data privacy, and institutional reputation by modernizing digital infrastructure, building user awareness, and creating a culture of preparedness.

With cyberattacks on higher education institutions rising year after year, continued reliance on outdated systems and fragmented security protocols places the university at risk, not only of data breaches and financial losses but also of non-compliance with evolving federal standards. This proposal offers a practical, cost-effective, and scalable plan to mitigate those risks and future-proof the university's digital operations.

By securing the necessary resources and support for this initiative, Oakland University can:

- Reduce preventable cyber incidents
- Improve operational continuity
- Enhance trust among students, faculty, and external partners
- Demonstrate leadership in cybersecurity within the academic community

The **CyberSecure Campus** project is more than a technical upgrade—it is a strategic commitment to excellence, safety, and resilience in a rapidly evolving digital world. With timely action and stakeholder collaboration, this initiative will protect what matters today and lay the groundwork for a secure tomorrow.

We respectfully request your support and funding to bring this vision to life.