
Capstone Project Presentation:
A Secure Program for
The Knowledge House

Welcome to Our Presentation - A Secure Program for The Knowledge House

Cybersecurity is no longer just an IT concern, but a crucial business issue. Implementing a secure program at The Knowledge House is a proactive investment that provides several key benefits.

A Secure Program for The Knowledge House: Key Benefits

Protection of Valuable Data: A secure program helps protect data from theft or damage, ensuring the privacy and trust of our stakeholders.

Compliance with Regulations: A secure program helps The Knowledge House conform to regulatory requirements such as PCI DSS or CCPA.

Resilience Against Cyber Threats: A secure program aids in identifying, mitigating, and responding to cyber threats effectively, thus maintaining operational continuity.

Fostering Trust: By demonstrating our commitment to cybersecurity, we build trust with our students, donors, staff, and the wider community. This trust is invaluable in our mission to educate and empower.

The Cost of Cyber Incidents

According to a study by Cybersecurity Ventures, the global cost of cybercrime is predicted to reach $10.5 trillion annually by 2025. Data breaches are the most expensive, costing an average of $3.86 million per breach. Incidents involving business-critical systems can have even higher costs due to downtime and loss of productivity.

A Secure Program for The Knowledge House

Six Vital Components to a Secure Program

Cybersecurity Framework

Threat and Vulnerability Assessments

Penetration Testing

Legal, Regulatory and Compliance Considerations

Development of Policies, Standards and Procedures

Incident and Disaster Response and Recovery & Business Continuity Plans

Cybersecurity Frameworks

Presented by: Elizabeth Bond and Aaron Kaah

What is a Cybersecurity Framework?

A cybersecurity framework is a structure containing processes, guidelines, and best practices to manage cybersecurity risks. It serves as the blueprint for building effective cybersecurity programs and protecting digital infrastructure.

Why is Cybersecurity Framework Important?

Cybersecurity frameworks provide a structured approach to address vulnerabilities and threats, foster clear communication across stakeholders, and enable systematic risk management.

What is NIST CSF?

This is the National Institute of Standards and Technology Cybersecurity Framework .

It is a set of guidelines, standards, and best practices developed by the National Institute of Standards and Technology (NIST) to help organizations manage and reduce their cybersecurity risk ensuring a resilient and secure infrastructure.

NIST CSF and Non-Profit Organizations

NIST CSF offers non-profits like The Knowledge House a language and structure to address cybersecurity risk across the enterprise. It provides flexibility and adaptability, aiding in risk management and protection of our digital assets and online donation systems. It contains five core functions.

The Core Functions of the NIST Framework: Protect

The 'Protect' function involves developing safeguards to guard against cyber threats. It encompasses access controls, secure configurations, data security, and employee awareness programs.

The Core Functions of the NIST Framework: Protect Function and Managing Third-Party Risks

The 'Protect' function extends to managing risks from vendors and partners. This is integral to The Knowledge House, where partnerships are crucial. We ensure all partners align with our cybersecurity standards.

The Core Functions of the NIST Framework: Respond

The 'Respond' function involves effective action and post-incident analysis when a cybersecurity incident occurs. This aids in preventing similar future incidents, bolstering our cybersecurity posture at The Knowledge House.

The Core Functions of the NIST Framework: Recover

The 'Recover' function emphasizes restoring systems, conducting lessons-learned exercises, and enhancing cybersecurity based on incident insights. It's a crucial function ensuring The Knowledge House's resilience in the face of cyber threats.

Engaging Stakeholders in Recovery

As part of the 'Recover' function, we ensure clear communication with our stakeholders about any incidents and their impacts. This helps maintain trust and transparency at The Knowledge House.

NIST 800-171: Our Chosen Cybersecurity Framework

NIST 800-171, designed for protecting Controlled Unclassified Information in non-federal systems, is our chosen framework at The Knowledge House. Given our role in educating minority and lower-income students, the protection of their information is paramount.

NIST 800-171: Our Chosen Cybersecurity Framework

NIST 800-171 contains 14 categories encompassing various cybersecurity aspects. These include Access Control, Awareness Training, Configuration Management, and more. We adopt these practices to protect our data and maintain the trust of our students and donors.

Key Components of NIST 800-171

Access Control: We regulate who can access our systems and data, ensuring only authorized users get access.

Awareness and Training: We emphasize educating our team on security protocols, threats, and how to handle potential incidents.

Configuration Management: We manage the setup of our systems to keep them secure, following the principle of 'least functionality'.

Incident Response: We have processes in place to swiftly react to security incidents, minimizing impact and recovering effectively.

How would NIST 800-171 Work for The Knowledge House?

Adopting NIST 800-171 aligns with our commitment to data security. It helps us maintain best practices in Access Control, provide Awareness Training to our staff, and manage our systems effectively, thereby protecting our valuable digital assets.

NIST 800-171: Securing the Future

The NIST 800-171 is more than a framework – it's an essential part of The Knowledge House's responsibility to protect their students, employees and donors' data. By implementing these guidelines, we ensure the resilience of our organization against cyber threats.