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.

Threat and Vulnerability Assessments

Threat & Vulnerability Assessments Introduction

Regular and systematic testing enables us to identify and rectify potential weaknesses in our system before they are exploited. It's an integral part of our cybersecurity strategy as it helps us anticipate and mitigate threats.

What is a Threat Assessment?

A threat assessment is the process of identifying potential security risks or threats to an individual, organization, or community. This involves:

1. Identifying the potential threat.
2. Assessing the credibility of the threat.
3. Developing a threat management plan.
4. Ongoing monitoring and review.

What is a Vulnerability Assessment?

A vulnerability assessment systematically identifies and evaluates security weaknesses in an organization's infrastructure, systems, and operations. It involves:

1. Identifying assets to be protected.
2. Assessing the vulnerabilities of those assets.
3. Prioritizing vulnerabilities based on risk.
4. Developing a remediation plan.

What is a Risk Assessment?

Risk assessment identifies and analyzes potential risks to determine their likelihood and impact on people, property, or the environment. It is an essential component of risk management and includes:

1. Identifying hazards.
2. Assessing the likelihood and consequences of those hazards.
3. Evaluating existing risk mitigation measures.

Threat, Vulnerability, and Risk Assessments: Key Differences

While all three assessments are important, they focus on different aspects of security:

1. Threat Assessment: Identifies and evaluates potential threats and their impacts.
2. Vulnerability Assessment: Identifies weaknesses in an organization's systems and operations and assesses the impacts of these vulnerabilities.
3. Risk Assessment: Identifies potential risks, analyzes hazards and vulnerabilities, and assesses existing mitigation measures.

Steps in a Threat and Vulnerability Assessment

A threat and vulnerability assessment involves:

1. Defining the scope.
2. Identifying potential threats.
3. Assessing vulnerabilities.
4. Analyzing risks.
5. Prioritizing risks.
6. Developing a risk management plan.
7. Monitoring and updating.

Tools for Threat and Vulnerability Assessment

To perform these assessments at The Knowledge House, we utilize several tools including NMAP, Burp Suite, Metasploit, and Wireshark. Each tool offers unique capabilities and collectively, they provide a comprehensive security evaluation.

Using NMAP for Network Exploration and Security Auditing

NMAP is a free, open-source tool used for network exploration and security auditing. It helps identify hosts and services on a network and potential security vulnerabilities that can be exploited by attackers.

Burp Suite for Web Application Security Testing

Burp Suite is a tool for testing web application security. It identifies potential security vulnerabilities by simulating attacks and providing detailed feedback on application behavior.

Metasploit: Penetration Testing and Exploitation Framework

Metasploit is a powerful tool used for penetration testing and exploitation. It simulates real-world attacks and identifies potential security vulnerabilities.

Wireshark: Network Protocol Analyzer

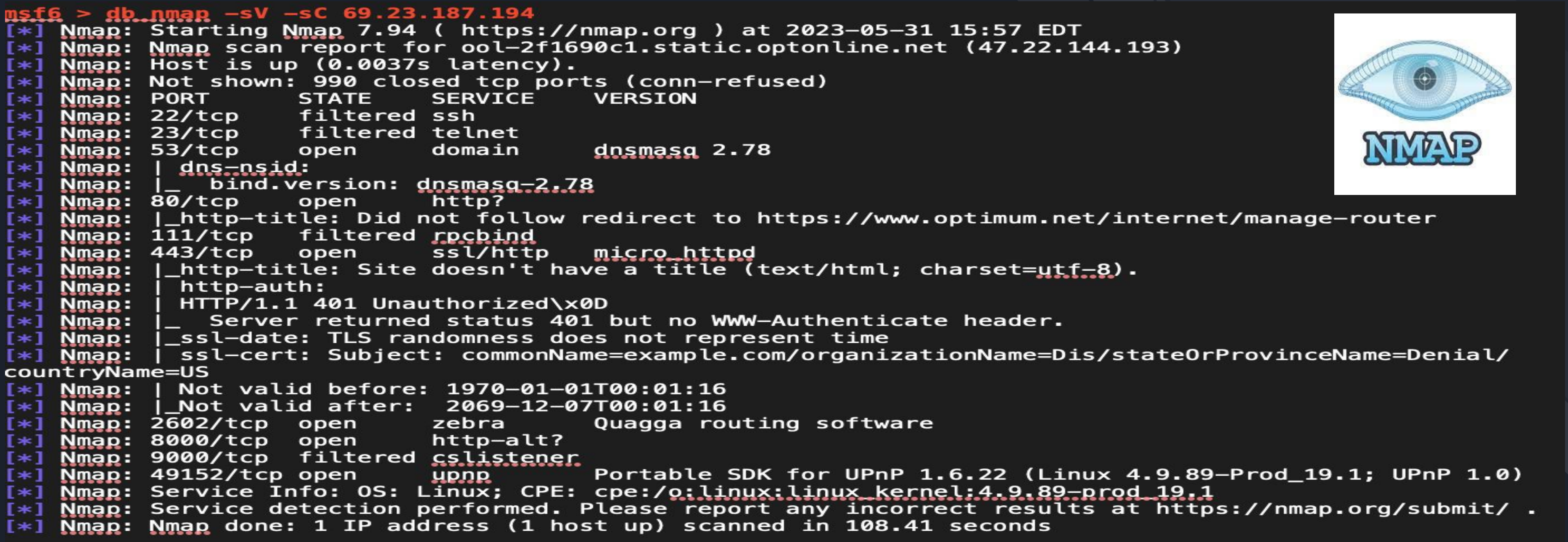
Wireshark is a network protocol analyzer that captures and analyzes network traffic in real time to identify potential security vulnerabilities and diagnose network issues.

Threat and Vulnerability Assessment at The Knowledge House

Our team visited The Knowledge House headquarters to perform threat and vulnerability assessments using tools like NMAP, Wireshark, Metasploit Framework, Burp Suite, and assessments from PentestTools.com. We scanned their networks and website to identify vulnerabilities, particularly in their server-side software and security headers.

NMAP Demonstration

NMAP is a free, open-source tool used for network exploration and security auditing. It helps identify hosts and services on a network and potential security vulnerabilities that can be exploited by attackers.



```
msf6 > db_nmap -sV -sC 69.23.187.194
[*] Nmap: Starting Nmap 7.94 ( https://nmap.org ) at 2023-05-31 15:57 EDT
[*] Nmap: Nmap scan report for ool-2f1690c1.static.optonline.net (47.22.144.193)
[*] Nmap: Host is up (0.0037s latency).
[*] Nmap: Not shown: 990 closed tcp ports (conn-refused)
[*] Nmap: PORT      STATE    SERVICE    VERSION
[*] Nmap: 22/tcp    filtered ssh
[*] Nmap: 23/tcp    filtered telnet
[*] Nmap: 53/tcp    open     domain     dnsmasq 2.78
[*] Nmap: | dns-nsid:
[*] Nmap: |_  bind.version: dnsmasq-2.78
[*] Nmap: 80/tcp    open     http?
[*] Nmap: |_http-title: Did not follow redirect to https://www.optimum.net/internet/manage-router
[*] Nmap: 111/tcp   filtered rpcbind
[*] Nmap: 443/tcp   open     ssl/http   micro_httpd
[*] Nmap: |_http-title: Site doesn't have a title (text/html; charset=utf-8).
[*] Nmap: | http-auth:
[*] Nmap: | HTTP/1.1 401 Unauthorized\x0D
[*] Nmap: |_  Server returned status 401 but no WWW-Authenticate header.
[*] Nmap: |_ssl-date: TLS randomness does not represent time
[*] Nmap: | ssl-cert: Subject: commonName=example.com/organizationName=Dis/stateOrProvinceName=Denial/
countryName=US
[*] Nmap: | Not valid before: 1970-01-01T00:01:16
[*] Nmap: |_Not valid after:  2069-12-07T00:01:16
[*] Nmap: 2602/tcp  open     zebra      Quagga routing software
[*] Nmap: 8000/tcp  open     http-alt?
[*] Nmap: 9000/tcp  filtered cslistener
[*] Nmap: 49152/tcp open     upnp       Portable SDK for UPnP 1.6.22 (Linux 4.9.89-Prod_19.1; UPnP 1.0)
[*] Nmap: Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel:4.9.89-prod_19.1
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 108.41 seconds
```

NMAP Demonstration

Command Summary: `db_nmap -sV -sC 69.23.187.194`

- `-sV`: Probe open ports to determine service/version info
- `-sC`: Perform a script scan using the default set of scripts

Key Findings

- 10 open/filtered ports found on host 69.23.187.194*.
- Services running: SSH, Telnet, DNS, HTTP, HTTPS, Zebra (RIP), UPnP
- Server seems to be running Linux (4.9.89-Prod_19.1)
- SSL Cert info: commonName=example.com, organizationName=Dis, stateOrProvinceName=Denial, countryName=US

Potential Vulnerabilities

- Open ports can be entry points for attackers.
- SSL certificate seems to be self-signed and dated from 1970.
- http-title information indicates redirection and potential misconfiguration.

*Host IP Address changed for confidentiality purposes.

Findings and Next Steps

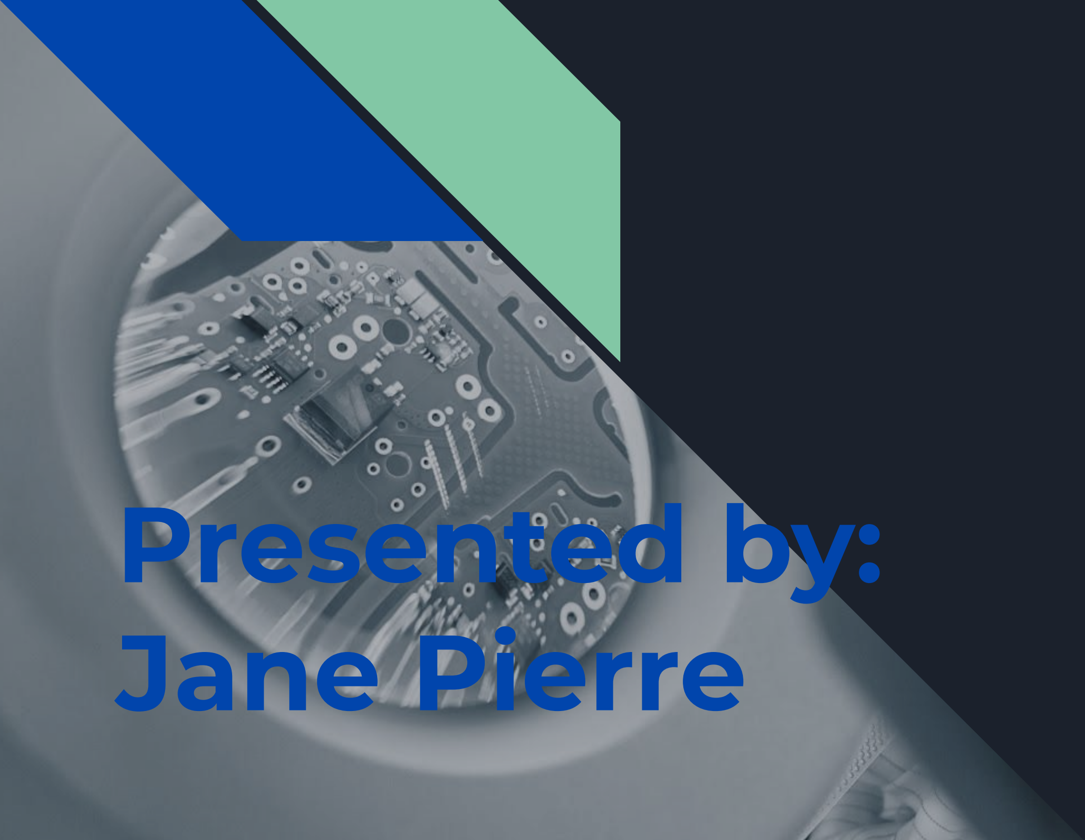
While the specifics of our findings are confidential, we found vulnerabilities in their server-side software and security headers. These findings were discussed further in a separate confidential report, which also includes the steps needed to mitigate these vulnerabilities and bolster The Knowledge House's security posture.

The Necessity of Ongoing Assessments

Threat and vulnerability assessments are not one-off exercises. To maintain a robust and up-to-date defense, regular monitoring and assessments are crucial. This enables us to stay ahead of emerging threats and continually refine our security strategies.

Threat, Vulnerability and Penetration Testing: An Integral Trio

Threat and vulnerability testing and penetration testing are interconnected stages of a comprehensive security strategy. While threat and vulnerability testing identifies and assesses potential weaknesses, penetration testing goes one step further by actively trying to exploit those weaknesses. This combined approach provides a complete picture of an organization's security posture, allowing it to understand both its potential vulnerabilities and how those vulnerabilities could be exploited by an attacker.



Presented by:
Jane Pierre

Penetration Testing

What is Penetration Testing?

Penetration testing or ethical hacking, simulates a real-world attack on a computer system or network to identify vulnerabilities and weaknesses that could be exploited by malicious actors.

Is Penetration Testing Important?

Penetration testing is vital to a secure program for numerous reasons. It helps identify vulnerabilities - with a report by Trustwave indicating that 98% of tested applications have at least one vulnerability. Moreover, compliance regulations like the PCI DSS or NIST often mandate penetration testing. Lastly, penetration testing assists in risk mitigation, reducing the risk of data breaches by 28% as per a study by the Ponemon Institute.

Penetration Testing for Non-Profit Organizations: Preserving Donor Trust

For non-profits, maintaining a secure program is crucial to establish and retain donor trust. According to a survey by Edelman, 81% of respondents consider trust in an organization a decisive factor in their donation decisions. Regular penetration testing demonstrates a non-profit's commitment to security, enhancing their reputation and boosting donor confidence.

Types of Penetration Testing

There are three main types of penetration testing:

1. White Box Testing: Tests the internal structure and code of the product with complete system knowledge.

2. Black Box Testing: Involves a real-world attack scenario without any prior knowledge of the system.

3. Gray Box Testing: Combines white and black box testing techniques with partial knowledge of the system.

Stages of Penetration Testing

Penetration testing involves several stages:

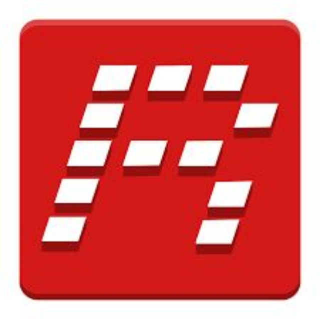
1. Reconnaissance and Planning
2. Scanning
3. Obtaining Entry
4. Maintaining Access
5. Analysis
6. Cleanup and Remediation

Social Engineering in Penetration Testing

Social engineering is a non-technical approach to penetration testing that exploits human psychology to gain access to sensitive information. It includes techniques such as phishing, pretexting, and physical impersonation, and helps identify weaknesses in an organization's security culture and employee training.

Tools for Social Engineering

Several tools aid in social engineering attacks, such as the Social-Engineer Toolkit (SET), BeEF, Maltego, and Recon-ng. These tools facilitate the creation of various social engineering attacks and the gathering of valuable information for the same.



Network Scanning in Penetration Testing

Network scanning identifies open ports, active hosts, and other network infrastructure details to find vulnerabilities that an attacker could exploit. It involves various types of scans like port scans, operating system detection, service discovery, and vulnerability scans.

Nmap: A Versatile Network Scanning Tool

Nmap, or Network Mapper, is a powerful tool for functionality and penetration testing, including port scanning and vulnerability detection. Its scripting engine allows hackers to examine known vulnerabilities, aiding in detecting system security flaws.

Burp Suite: Web Application Security

Burp Suite is widely used for identifying and exploiting vulnerabilities in web applications. Its features include Intruder, Repeater, Sequencer, Decoder and Comparer which are useful for everything from mapping out a web application's attack surface to automating custom attacks. Burp Suite allows penetration testers to intercept, replay and manipulate HTTP/HTTPS requests to analyze and tamper with web applications for security testing.

Wireless Network Testing: Aircrack-ng

Aircrack-ng is a suite of tools for monitoring and testing wireless network security. It can crack keys, capture packets, analyze them, and perform attacks like deauthentication.

The Penetration Testing Report

The final deliverable of a penetration test is the report. This report typically includes details of the tests carried out, the vulnerabilities discovered, their severity, potential impact, and recommended remediation steps.

Remediation Process

Remediation is the process of fixing the vulnerabilities found during the penetration test. It involves addressing each vulnerability in order of its severity and potential impact. Periodic re-testing is necessary to ensure that the fixes have been effective and that no new vulnerabilities have been introduced.

Penetration Testing – Facing Forward

Penetration testing is a critical component of any cybersecurity strategy. For nonprofit organizations, this practice helps identify vulnerabilities, maintain compliance with regulations, and build donor trust. The insights and vulnerabilities identified through penetration testing are not only vital for maintaining our technical defenses but also for ensuring our compliance with various laws and regulations.

Presented by: Tianna Green

Legal, Regulatory and Compliance Considerations

Legal, Regulatory and Compliance: The Real

According to IBM's 2020 Cost of a Data Breach Report, the average total cost of a data breach is $3.86 million. This increases to an average of $8.64 million for breaches in the United States.

A Cybersecurity and Data Privacy Study by NTEN reported that over 70% of donors are concerned about how nonprofits manage and use their personal data. Failure to comply with data protection regulations can lead to a loss of donor trust, which can directly impact donations and funding.

Legal, Regulatory and Compliance: The Truth

According to a study by Rapid7, organizations that have implemented a comprehensive compliance program, including regular audits and updates, have seen a reduction in data breaches by up to 50%.

According to a study by Deloitte, nonprofits that comply with cybersecurity regulations have increased operational resilience, enabling them to recover up to 30% faster from cyberattacks.

Legal, Regulatory and Compliance Considerations

Legal, regulatory, and compliance aspects are crucial to any cybersecurity program. The Knowledge House must comply with regulations such as PCI DSS, FERPA, COPPA, the NY SHIELD Act and GLBA, even though some of these regulations are not designed specifically for non-profits. Complying with these regulations will ensure the security and privacy of the donor, student, and other sensitive information.

Payment Card Industry Data Security Standard (PCI DSS)

The PCI DSS is a set of security standards to ensure secure handling of payment card information. It provides a comprehensive framework of requirements and best practices for organizations that handle, process, store, or transmit payment card data. Compliance with the PCI DSS demonstrates an organization's commitment to protecting sensitive cardholder data and reducing the risk of data breaches. It helps maintain customer trust, avoid financial penalties, and ensures a secure payment card environment.

Satisfying PCI DSS Regulatory Requirements and The Knowledge House

The Knowledge House, as an educational nonprofit, actively engages in online donation collections, often accepting credit card donations. Due to the nature of these transactions, compliance with the PCI DSS is crucial. To satisfy the regulatory requirements of the PCI DSS, The Knowledge House should focus on key areas including: scope identification, compliance assessment, data encryption, secure network infrastructure, access controls, and vulnerability management.

PCI DSS Violations: Examples and Consequences

PCI DSS violations can occur in various ways such as storing sensitive cardholder data unnecessarily, allowing weak passwords, not implementing robust network security measures, and failing to restrict access to cardholder data. Violating the PCI DSS can lead to fines, up to $100,000 per month, increased transaction fees, reputational damage, legal consequences, and termination of card processing privileges. Remediation costs are also a significant consequence of non-compliance.

The Family Educational Rights and Privacy Act (FERPA)

FERPA is a federal law that protects the privacy of student education records. While it isn't specifically designed for non-profit organizations, compliance with FERPA encourages such organizations to implement measures for the protection of student education records. FERPA's key components include Data Security, Monitoring and Auditing, and Training and Education, which are crucial for securing student information and protecting the organization against data breaches.

Children's Online Privacy Protection Act (COPPA)

COPPA is a law that places parents in control over what information is collected from their young children online. Though The Knowledge House, as a non-profit, is not subjected to COPPA, it's recommended to protect COPPA's protections to potential child visitors. Violation of COPPA can lead to significant penalties, with a court potentially holding operators who violate the Rule liable for civil penalties of up to $50.120 per violation.

Stop Hacks and Improve Electronic Data Security (SHIELD Act)

The SHIELD Act strengthens New York’s data security laws, and as The Knowledge House's main office is in New York, it is subject to this act. Penalties for violating this act include a civil penalty of up to $20 per instance of failed notification, not exceeding $250,000, and up to $5,000 per violation for failing to maintain reasonable safeguards.

Gramm-Leach-Bliley Act (GLBA)

The GLBA regulates how financial institutions deal with private information of individuals. It includes the Financial Privacy Rule, Safeguards Rule, and Pretexting provisions, designed to protect personally identifiable information, prevent false pretenses for information collection, and control how private financial data is collected and disclosed.

Gramm-Leach-Bliley Act (GLBA)

The GLBA primarily applies to financial institutions, but non-profit organizations like the The Knowledge House should implement appropriate data protection practices, maintain confidentiality, obtain consent where required, and ensure compliance with applicable data protection laws.

Compliance Monitoring and Auditing

Regular monitoring and auditing are essential to maintaining legal and regulatory compliance and ensuring that security controls remain effective. Internal audits should be carried out regularly to identify any vulnerabilities and assess the effectiveness of existing controls. External audits can be utilized to provide an independent assessment of the organization's security posture and compliance with laws and regulations.

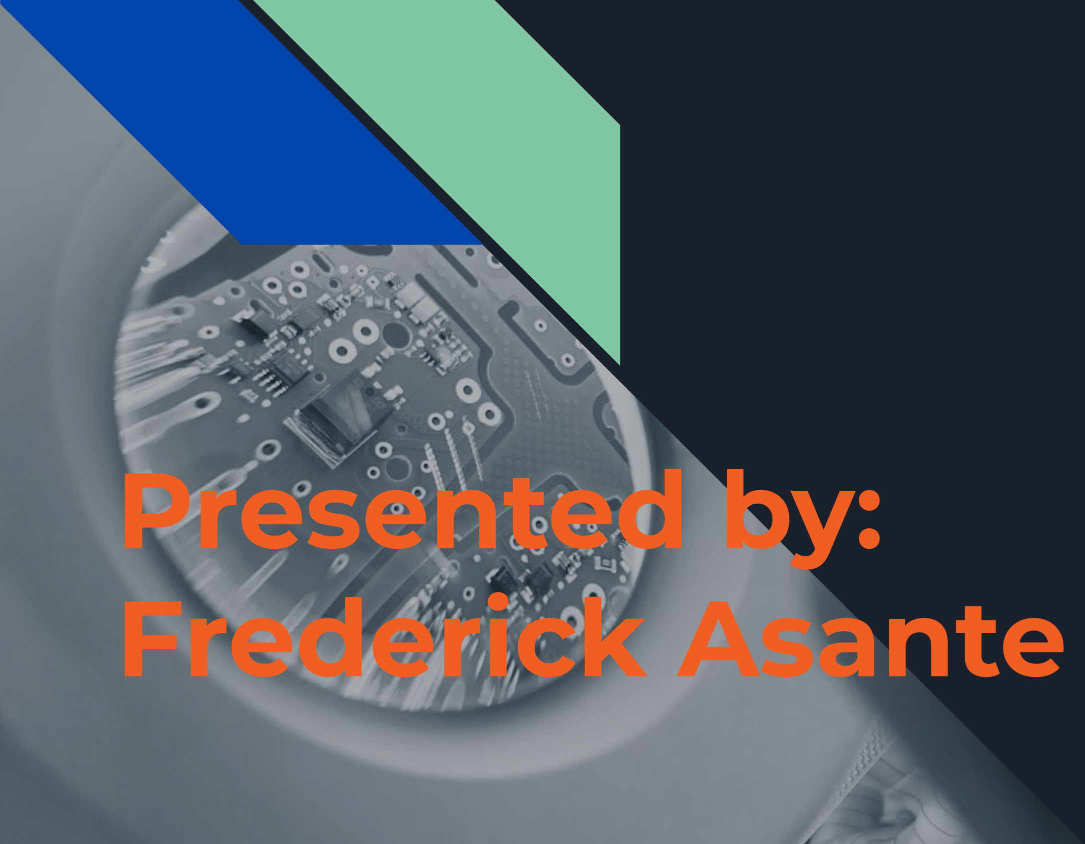
Staff Training and Education

Staff training and education play a significant role in an organization's cybersecurity efforts. Training programs should cover all necessary security practices and legal requirements, ensuring that staff are well-versed in the laws and regulations applicable to The Knowledge House. Regular training updates can ensure that staff are informed about the latest threats and how to respond appropriately.

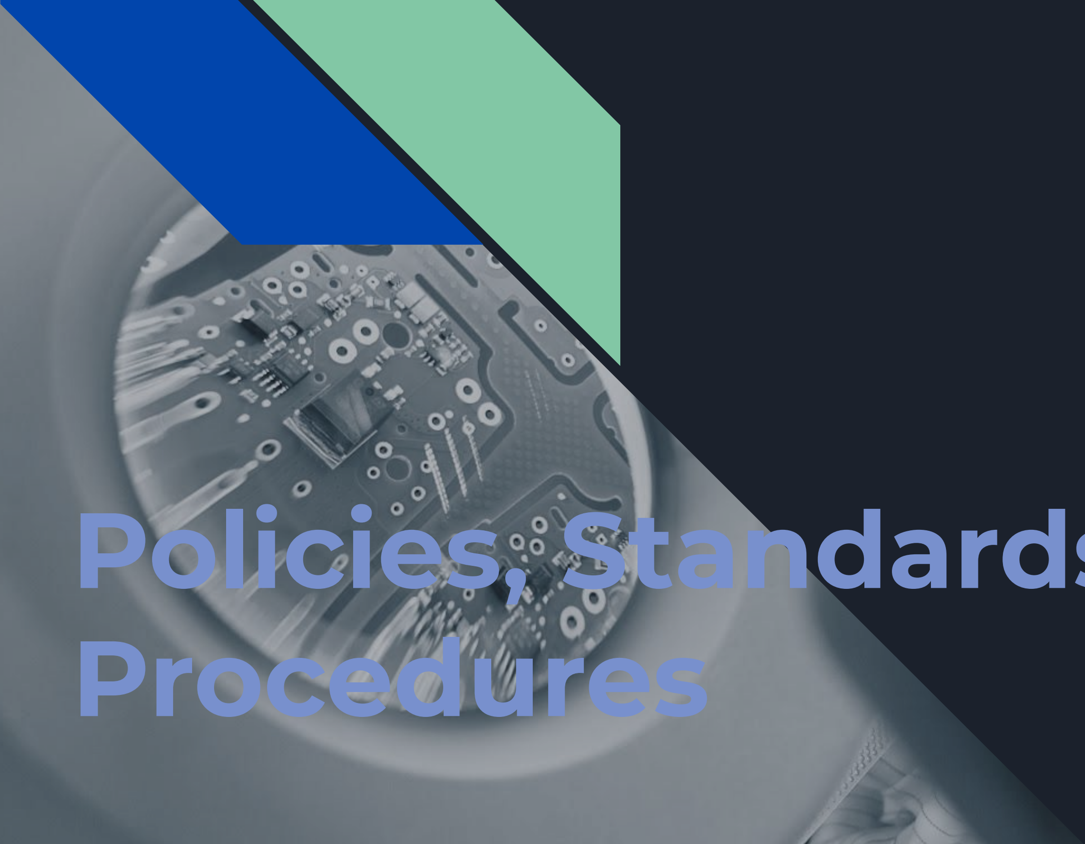
Legal, Regulatory and Compliance Considerations: The Next Steps

Data protection and security compliance are essential for any organization, whether in the educational sector, business sector, or non-profit sector like The Knowledge House.

Complying with relevant regulations like PCI DSS, FERPA and COPPA helps organizations to protect their reputation, maintain trust with stakeholders, and avoid costly penalties.



Presented by: Frederick Asante



Policies, Standards and Procedures

Why Should a Non-Profit Develop Policies, Standards and Procedures?

Policies, standards, and procedures serve as the foundational guidelines for The Knowledge House's cybersecurity posture. They provide a well-defined roadmap to help the organization navigate the complex landscape of cybersecurity, ensuring that everyone understands their responsibilities and what is expected of them.

Why Should a Non-Profit Develop Policies, Standards and Procedures?

As an educational non-profit organization, The Knowledge House is subject to various regulations, including FERPA, COPPA, and PCI DSS. These regulations often require organizations to have specific policies and procedures in place to protect sensitive data. By maintaining up-to-date policies, standards, and procedures, The Knowledge House can demonstrate its compliance with these regulatory requirements.

Why Should a Non-Profit Develop Policies, Standards and Procedures?

As an educational non-profit organization, The Knowledge House is subject to various regulations, including FERPA, COPPA, and PCI DSS. These regulations often require organizations to have specific policies and procedures in place to protect sensitive data. By maintaining up-to-date policies, standards, and procedures, The Knowledge House can demonstrate its compliance with these regulatory requirements. The policies, standards and procedures developed for The Knowledge House include Access Management, Password Policies, Remote Work Policies, Incident Reporting, and Data Handling & Classification.

Understanding Access Management at The Knowledge House

Access Management is a critical component of our security infrastructure at The Knowledge House. It ensures that only authorized individuals can access specific systems, data, and applications based on their role. Our Access Management policy defines roles, user authentication procedures, data access controls, and account management.

Access Management at The Knowledge House: Your Role and Permissions

Each role within The Knowledge House has predefined access permissions, based on job responsibilities. It is crucial for employees to understand the scope of their roles and the permissions associated with them. Accessing systems or data beyond one's authorization is strictly prohibited and can have serious consequences.

User Authentication Procedures

User Authentication Procedures are essential for verifying the identity of users trying to access our systems. This involves the use of strong passwords, two-factor authentication, and ensuring that credentials are kept secure.

Managing Your User Account

Be vigilant with your account settings and permissions. Regularly review and update your account security settings. Report any suspicious activity related to your account immediately to the IT department.

Password Policies and Procedures

Strong, unique passwords are a cornerstone of security. Passwords must be complex and not easily guessable. Regularly changing passwords and employing two-factor authentication are highly recommended.

Remote Work Policies and Procedures

The Knowledge House supports remote work while ensuring that data and systems remain secure. Our Remote Work Policy encompasses secure access procedures, employee training, securing devices and home networks.

Remote Access Procedures

Remote access to The Knowledge House systems is secured through VPNs and requires multi-factor authentication. Employees must ensure that they are connecting through a secure network and that their devices are free of malware.

Incident Reporting Procedures

Employees are required to report any security incidents immediately. Our Incident Response Team will then take the necessary steps to contain and mitigate the impact of the incident.

Data Handling and Classification Policies and Procedures

Data Handling and Classification Policies guide how different types of data are to be handled within The Knowledge House.
These policies categorize data based on sensitivity and specify the protocols for storing, sharing, and disposing of data.

Data Types and Handling Procedures

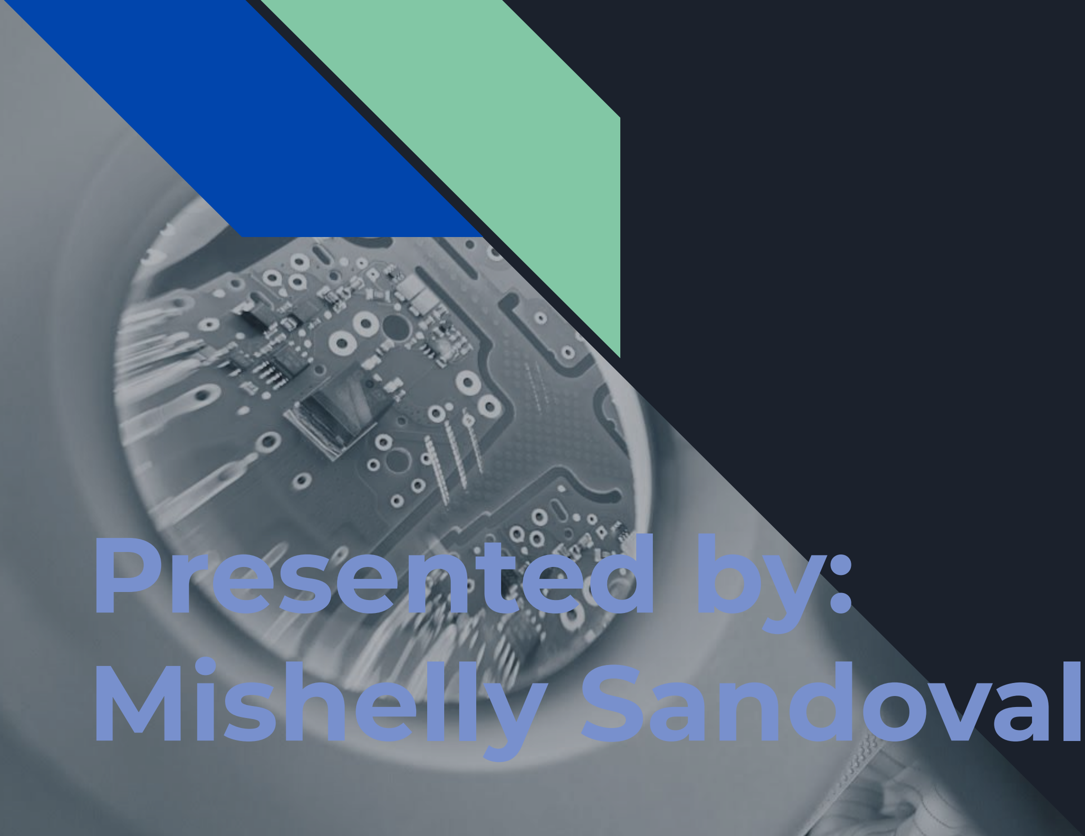
Data types include Personal Identifiable Information (PII), financial information, course materials, and more. Handling procedures encompass encryption, access controls, and proper disposal methods.

Compliance, Audit and Training

Regular audits are conducted to ensure compliance with our policies and external regulations. Training programs are in place for employees to stay updated on best practices and the importance of cybersecurity.

Policies, Standards and Procedures – Moving Forward

Policies, standards, and procedures are not static documents, but dynamic instructions that guide our daily operations. They establish The Knowledge House's commitment to incident and disaster preparedness, outlining the measures we take to mitigate potential threats and disruptions.



Presented by:
Mishelly Sandoval

Incident and Disaster Response and Recovery and Business Continuity Plans

Incident and Disaster Response & Recovery, Business Continuity Plans

The Knowledge House's commitment to cybersecurity is exemplified not just in the policies, standards, and procedures we've outlined, but also in our preparedness for potential incidents and disasters. This transition from policy to practice embodies the spirit of our secure program.

Why should The Knowledge House have Incident and Disaster Response and Recovery & Business Continuity Plans?

Minimizes Disruption: In the event of a cyber incident or disaster, the primary goal is to minimize disruption to our operations. For a non-profit like The Knowledge House, this is particularly vital. The incident and disaster response & recovery plan is designed to tackle this head-on, allowing us to swiftly isolate and address the issue to reduce operational downtime.

Preserves Stakeholder Trust: Trust is a vital currency in the non-profit sector. Our donors, students, and partners need to know that we're doing everything we can to protect the information they share with us. By having a robust business continuity plan, The Knowledge House demonstrate that they take this responsibility seriously and are prepared to navigate even severe disruptions.

Why should The Knowledge House have Incident and Disaster Response and Recovery & Business Continuity Plans?

Fulfilling Our Mission: The Knowledge House's mission is to radically change the way we approach education and career readiness. An integral part of fulfilling this mission is ensuring that their services are resilient and reliable. Implementing comprehensive incident response, disaster recovery, and business continuity plans is a critical part of this, enabling them to continue delivering our services even under challenging conditions.

Resource Optimization: Incidents and disasters can be costly, especially if not managed effectively. A well-executed response and recovery plan can help us optimize the use of resources during such events, minimizing financial impact and ensuring a swift return to normal operations.

What is an Incident Response and Recovery Plan?

An Incident Response Plan is a set of procedures to handle and manage a cybersecurity incident effectively. It involves multiple stages such as identification, containment, eradication, recovery, and post-incident analysis.

Initial Response: Identification and Confirmation

The first step in any response strategy is identification and confirmation. At The Knowledge House, systems and network traffic are actively monitored to detect and evaluate any unusual activities promptly.

Containment: Isolation and Preservation of Evidence

Post-identification, the incident is isolated to prevent further damage, and evidence is preserved for further analysis and potential legal actions.

Eradication: Investigation and Remediation

Once contained, a thorough investigation is carried out to understand the cause and impact of the incident. Remediation efforts are undertaken to remove the threats and vulnerabilities that led to the incident.

Recovery: Systems Restoration, Data Recovery, and Communication

The recovery phase includes restoring systems and recovering data. Effective communication to stakeholders about the incident and recovery efforts is critical during this phase.

Post-Incident Analysis

Post-incident analysis involves reviewing the incident, implementing improvements based on the learnings, and documenting everything for future reference.

Importance of Incident Response

An effective Incident Response Plan can significantly reduce the damage from a cyber incident and enable a faster recovery, thereby saving costs and preserving the organization's reputation.

Disaster Recovery & Business Continuity

Disaster Recovery involves restoring IT infrastructure and systems after a disaster, while Business Continuity is about ensuring that essential business functions can continue during and after a disaster.

Identifying Critical Assets and Operations

Critical assets like our online course delivery system and credit card payment processing systems need to be prioritized in the Disaster Recovery and Business Continuity Plans.

Disaster Recovery: Key Steps

Key steps include creating a disaster recovery team, assessing risks, developing a disaster recovery plan, implementing the plan, and regularly testing and updating the plan.

Business Continuity: Key Steps

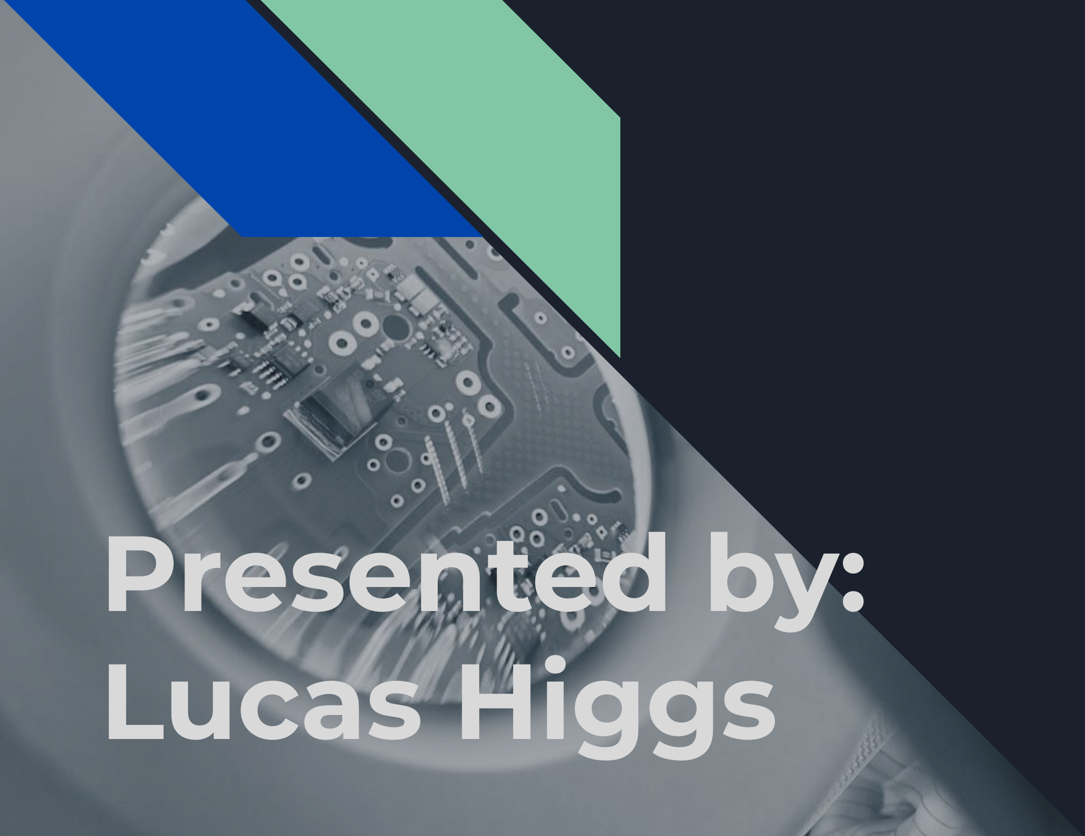
Business continuity planning involves identifying essential functions, performing a business impact analysis, creating a business continuity team, developing the plan, and regularly testing and updating the plan.

Business Continuity: Key Steps

Business continuity planning involves identifying essential functions, performing a business impact analysis, creating a business continuity team, developing the plan, and regularly testing and updating the plan.

Moving Forward in Incident and Disaster Response and Recovery & Business Continuity Plans

Everyone in The Knowledge House has a role to play in disaster recovery and business continuity. By understanding our plans and your role in them, you can help ensure that we recover from any incident as quickly and efficiently as possible.



Presented by: Lucas Higgs

Building a Stronger Cybersecurity Culture at The Knowledge House Together

A cybersecurity framework with a focus on NIST 800-171, threat and vulnerability testing, penetration testing, legal and compliance considerations, policy and procedure development, and incident and disaster response and recovery, along with business continuity planning are the foundations of a secure program.

Building a Stronger Cybersecurity Culture at The Knowledge House Together

Cybersecurity is a shared responsibility that requires a concerted effort from all of us at The Knowledge House. By implementing the practices discussed in this presentation, we can collectively enhance the security posture of The Knowledge House, ensuring the safety of our students', employees’ and donors' digital information.