Creating an Incident Response Team (IRT) for your secure program is an important step in establishing an effective incident management plan. Including members from various departments ensures that you have a well-rounded team capable of handling different aspects of incident response. Here's a suggested approach for identifying individuals and their responsibilities within the IRT for a medium-sized nonprofit organization (NPO) that collects donations online and has 50-75 employees, the structure of the Incident Response Team (IRT) can be tailored to the organization's specific needs. Here's a suggested approach:

1. **IT Department:**
    - IT Manager/Network Administrator: will be responsible for managing the organization's IT infrastructure, including incident response coordination and technical support.
    - IT Security Specialist: Responsible for monitoring and analyzing security events, implementing security measures, and assisting with incident containment and resolution.
2. Legal Department:
    - Legal Counsel or Legal Advisor: Responsible for providing legal guidance during incidents, ensuring compliance with relevant regulations, and handling any legal aspects related to incidents, such as data breaches or privacy concerns.
3. Communications/Marketing Department:
    - Communications Manager: Responsible for managing external communications, such as issuing public statements, handling media relations, and communicating with donors and stakeholders.
    - Marketing/PR Assistant: Supports the Communications Manager in disseminating incident-related information to external audiences.
4. Management/Executive Team:
    - Executive Director/CEO: Involved in the incident response process to provide strategic direction, allocate necessary resources, and communicate with the board of directors.
5. Additional Roles:
    - Incident Coordinator/Manager: Responsible for overall incident response coordination, ensuring timely and effective communication among team members, and documenting incident response activities.
    - Donation Processing Representative: Handles incidents related to the online donation system, ensuring the integrity and security of donor information.

- Data Protection Officer (if applicable): Oversees data protection and privacy matters, ensuring compliance with relevant regulations and managing incident response from a privacy perspective.
- External Consultants or Vendors: Depending on the organization's resources and requirements, external consultants or vendors may be engaged for specialized incident response support, such as forensic analysis or technical assistance.

Given the size of the organization, some team members may have multiple responsibilities, and individuals with relevant skills and knowledge can contribute to the IRT. It's essential to provide proper training, clearly define roles and responsibilities, and establish effective communication channels within the team. Regular drills and exercises can also help ensure the team is prepared to respond to incidents effectively.

What Is an Incident Response Team? (*Incident response team: A blueprint for success* 2022)

An incident response team, also called an incident response unit, is a group responsible for planning for and responding to IT incidents, including cyber attacks, systems failures, and data breaches. These teams can be also responsible for developing incident response plans, searching for and resolving system vulnerabilities, enforcing security policies, and evaluating security best practices.

Incident response teams may be referred to by several names, often used interchangeably. In general, these teams perform similar tasks although there are differences. Some forms that incident response teams can take include:

- Computer Security Incident Response Team (CSIRT)—an assorted team of professionals that is responsible for preventing, detecting, and responding to incident response cyber security events or incidents.
- Computer Emergency Response Team (CERT)—can operate the same as a CSIRT but with a focus on partnerships with government, law enforcement, academia, and industry. These teams prioritize developing threat intelligence and best practices based on security responses. This is a trademarked designation that is controlled by Carnegie Mellon University.
- Security Operations Center (SOC)—generally includes a CSIRT or CERT but covers a broader scope of cyber security. SOCs are responsible for directing incident response in addition to monitoring and defending systems, configuring controls, and overseeing general operations.

How To Build An Effective Incident Response Team

To build an incident response team, you need to start with the right people and skill sets. The most effective teams include a wide variety of professionals to help manage all aspects of an incident and provide a broad range of expertise. Incident response team roles often include:

- Team leader—responsible for coordinating team activities and reporting to upper-level management.
- Communications—responsible for managing communications throughout the team and organization. These members are also responsible for ensuring that stakeholders, customers, and public authorities are properly informed about incidents.
- Lead Investigator—responsible for performing primary investigation of events, guiding the efforts of other analysts, and providing in-depth evaluation of cyber security incidents.
- Analysts and researchers—responsible for supporting the lead investigator and providing threat intelligence and context for an incident. These members are also often responsible for carrying out the incident response process.
- Legal representation—responsible for providing legal guidance in terms of compliance, interactions with law enforcement, and standards of integrity for forensic evidence.

When creating and managing your team, you can use an incident response template. These templates are not complete incident response plans, but can serve as a good starting point.

Considerations for Creating an Incident Response Team

When creating your team, there are a few considerations you should keep in mind. These considerations can help you ensure that your team is able to collaborate effectively and can help reduce gaps in expertise and functioning.

- Availability—you want members that can respond to incidents 24/7 and as quickly as possible. To ensure this response, you need to select members that are capable of accessing your systems on short notice and that are able to respond during a wide variety of hours. This often means supplementing teams with third-party resources during off hours or holidays to ensure constant coverage.
- Virtual or on-call team members—if you have limited employee resources, you may want to boost your team with virtual or as-needed members. These members may be full or part-time staff in another capacity but you can call them in as needed should an incident occur. This is a good option for members with very specific expertise that aren’t always needed but can still provide valuable support in certain situations.
- Effective advocate or executive sponsor—it is very helpful to have a person on your team that can serve as a team advocate or sponsor, such as a CISO. This person can help manage communications between your team and C-level executives to ensure that

the importance of cyber security response is understood. This person can also help ensure that you receive the budget you need to effectively operate.
- Team communication and morale—incident response teams are required to manage highly stressful situations that require clear communication and collaboration. To avoid team burnout, it's important that you encourage the strengthening of team relationships and the professional growth of team members.
- Diversity—technically diverse teams are able to handle a wider variety of situations than limited teams. Greater diversity can also help teams more quickly identify threats and develop more innovative solutions for minimizing damage and preventing future attacks.

Tips For Incident Response Team Members

Once your team is assembled, they're ready to start preparing for and handling IT incidents. Unfortunately, even with extensive preparation, incident response can feel overwhelming, especially for immature teams. To help develop your team's skills, you can start by training them to implement the following practices.

Supplement tools with insight

While technology is a great help in detecting incidents, it can't detect all suspicious events and is most effective when assisted by the insight of cyber security teams. In particular, teams may be better at investigating:

- Traffic anomalies—including sudden increases or decreases in traffic, traffic from inconsistent addresses, or unexpected traffic. These signs can indicate abuse of credentials, reconnaissance attacks, or issues with connectivity.
- Suspicious access—including attempts to or successful access of restricted files or system areas. For example, you may have superusers with permissions to access specific components but who typically have no reason to do so. If these users suddenly start accessing sensitive areas, it may indicate an incident.
- Excessive consumption—including sudden drops in performance, increases in resource demand, or large exports of data. These signs could indicate malware infections, data exfiltration, or abuse of resources, such as for crypto mining.

In assessing these issues, teams may find tools such as user and entity behavioral analytics (UEBA) solutions helpful. These tools can create or be fed baselines of "acceptable" behavior and alert teams when a deviant event occurs. Teams can then use the information provided by these tools to evaluate the event. They can also try to improve future tool responses by using the results to refine functioning.

Use a centralized approach

Centralizing your efforts makes most aspects of incident response easier. In particular, this includes monitoring and logging information, and cyber security or management tooling.

Centralizing information makes analysis of data easier and increases the accuracy of results by providing context for the events being evaluated. The most common way to achieve this type of centralization is with system information and event management (SIEM) solutions. These solutions can ingest data from across your systems and aggregate it into a single source.

Centralization of tooling makes it easier for teams to manage configurations and maintain systems. It also enables teams to respond more efficiently since they don't have to constantly switch between tools to accomplish a task. One way of achieving this is with cyber security orchestration, automation, and response (SOAR) solutions. These solutions enable you to ingest alert information, automate protective measures, and standardize responses system wide.

Base your actions on evidence

When you receive a cyber security alert you may be quick to jump to conclusions about whether the alert is important, what caused it, or how to address it. However, teams should avoid acting on these gut reactions and instead take the time to investigate events properly.

Casually dismissing an event can lead to oversight that later leads to a more significant attack, such as an advanced persistent threat. Likewise, following an assumption about what caused an alert or how to remediate it without first confirming your suspicions can end up causing damage or result in an insufficient response.

By taking the time to carefully investigate events can better ensure that your incident identification is accurate. Then you can respond effectively and efficiently without wasting effort or putting systems or workloads at risk.

On-Demand Incident Response Team: CyOps by Cynet

Cynet understands that building and managing an incident response team is not a viable option for all organizations. This is why, in addition to providing incident response automation, Cynet offers on-demand incident response services.

CyOps, Cynet's Cyber SWAT team, is on call 24/7/365, allowing enterprises of all sizes to get access to the same expert security staff that protect the largest enterprises. Here's what you can expect from the CyOps incident response team:

- Alert monitoring—continuous management of incoming alerts: classify, prioritize and contact the customer upon validation of active threat.
- 24/7 availability—ongoing operations at all times, both proactively and on-demand per the customer's specific needs.
- On-demand file analysis—customers can send suspicious files to analysis directly from the Cynet 360 console and get an immediate verdict.
- One click away—CISOs can engage CyOps with a single click on the Cynet Dashboard App upon suspicion of an active breach.
- Remediation instructions—conclusion of investigated attacks entails concrete guidance to the customers on which endpoints, files, user and network traffic should be remediated.
- Exclusions, whitelisting, and tuning—adjusting Cynet 360 alerting mechanisms to the customers' IT environment to reduce false positives and increase accuracy.
- Threat hunting—proactive search for hidden threats leveraging Cynet 360 investigation tools and over 30 threat intelligence feeds.
- Attack investigation—deep-dive into validated attack bits and bytes to gain the full understanding of scope and impact, providing the customer with updated IoCs.

Resources:

- *Incident response team: A blueprint for success*. Cynet. (2022, December 1). https://www.cynet.com/incident-response/incident-response-team-a-blueprint-for-success/#:~:text=Incident%20response%20teams%20are%20composed,%2C%20researchers%2C%20and%20legal%20representatives.
    - (*Incident response team: A blueprint for success* 2022)

Creating a Disaster Recovery Plan

1. Identify Critical Assets and Operations: Identify the assets and operations that are crucial for the organization's functioning, such as your online course delivery system and the credit card payment processing system.
   Group Members: Lucas and Mishelly

Provide Training: Ensure that all staff members, not just the IRT, have a basic understanding of incident identification and reporting.
Group Member: Lucas

When providing training to a non-profit organization about incident identification and reporting, it's important to follow a structured approach that effectively conveys the necessary information. Here's a step-by-step guide on how you can conduct this training:

1. Understand the organization's context: Begin by familiarizing yourself with the specific activities, operations, and potential incidents relevant to the non-profit organization. Gain an understanding of their industry, the types of incidents they may encounter, and any regulatory requirements that apply.

2. Define key terms: Clarify important terms related to incident identification and reporting. Examples may include incidents, near misses, hazards, and reporting mechanisms. Ensure that all participants have a common understanding of these terms.

3. Establish training objectives: Determine the goals you want to achieve through the training session. These objectives could include educating participants about incident identification techniques, explaining the importance of prompt reporting, and outlining the reporting process.

4. Develop training materials: Create instructional materials that cover the relevant concepts and procedures. Consider using a variety of resources such as presentations, case studies, handouts, and practical exercises to make the training engaging and interactive. Tailor the materials to the organization's specific needs.

5. Start with the basics: Begin the training by introducing the concept of incident identification and why it is essential for the organization's safety and well-being. Explain the potential consequences of not identifying and reporting incidents promptly, such as increased risks and potential harm to employees or beneficiaries.

6. Identify common incidents: Discuss common incidents that the organization may encounter, such as workplace accidents, safety hazards, security breaches, or data breaches. Explain the importance of being vigilant and observant to spot such incidents.

7. Teach incident identification techniques: Provide practical guidance on how to identify and recognize incidents effectively. This may involve educating participants about signs, symptoms, and indicators of different types of incidents. Encourage them to maintain open communication and to actively report any observations.

8. Explain the reporting process: Walk participants through the organization's reporting procedures, including whom to report incidents to, how to document relevant information, and any specific forms or systems to use. Emphasize the importance of clear and concise reporting, along with any timelines or deadlines that should be followed.

9. Highlight confidentiality and non-retaliation: Discuss the importance of maintaining confidentiality when reporting incidents and assure participants that non-retaliation measures

are in place. Stress the organization's commitment to creating a safe reporting environment and protecting individuals who report incidents in good faith.

10. Provide examples and case studies: Use practical examples and case studies relevant to the organization's activities to illustrate incident identification and reporting processes. Encourage participants to analyze the scenarios and discuss the appropriate steps to take.

11. Facilitate discussions and Q&A sessions: Engage the participants by encouraging questions, facilitating discussions, and addressing any concerns they may have. This interaction can help clarify concepts and reinforce understanding.

12. Reinforce reporting culture: Emphasize the importance of fostering a strong reporting culture within the organization. Explain that reporting incidents is not about blame but rather about identifying areas for improvement and preventing future incidents.

13. Offer resources for ongoing support: Provide participants with additional resources and references that they can consult after the training session. These may include reporting templates, relevant policies and procedures, or contact information for designated incident management personnel.

14. Evaluate the training: Seek feedback from the participants to evaluate the effectiveness of the training session. Use their input to make improvements for future training initiatives.

Remember that the specific content and delivery methods may vary depending on the organization's needs, culture, and industry. By following this structured approach, you can provide valuable training on incident identification and reporting to the non-profit organization.

Outside research: (*How to write an effective incident report* 2023)
What is Incident Reporting:

- As part of Incident Management, the purpose of incident reporting is to record an incident, determine its possible cause, document any actions taken, and make it known to stakeholders. An incident report can be used in the investigation and analysis of an event. It includes the root cause and corrective actions to eliminate the risks involved and prevent similar future occurrences. Incident reports can also be used as safety documents that indicate potential risks and uncontrolled hazards found on the work site for future assessments
- An incident report can be used by:
    - an authority to create a report of an incident;
    - a worker to report an incident he/ she has witnessed;
    - any member of the organization to raise awareness about an incident that has occurred in the worksite.

- Incident reporting is the process of documenting all worksite injuries, near misses, and accidents. An incident report should be completed at the time an incident occurs no matter how minor an injury is. This article covers an in-depth explanation of the incident reporting procedure and the types of events you should report.

Benefits to incident reporting: (*How to write an effective incident report* 2023)

- Immediate reinforcement of Actions
- Hazards and Threats Communication and Awareness
    - Possible threats could be:
        - High-risk jobs
        - Equipment and machine damage
        - Bad employee behavior (alcoholism, violence, sexual aggravation, bullying, etc.)
        - Infectious diseases
        - Absence of proper PPE and controls
        - Non-compliance
- Continuous improvement of processes

Incident Training: (*How to write an effective incident report* 2023)

- Incident report training is a series of practical lessons to help employees develop skills for proper incident reporting. Adequate Training can empower workers to report and respond to all incidents immediately, aiding in their quick resolution and subsequent investigation. Typical incident reporting training includes what is considered a reportable event, how to create a good incident report, and what details need to be documented.

Example:

- Why accident and incidents should be investigated and the parties who need to know when they happen
- Things that an investigator should consider or avoid for effective investigations
- What to do after witnessing or being involved in workplace incidents and the specific information to remember

- Best practices for gathering statements from witnesses or related parties during an incident investigation
- Accident causation, the different stages of evaluating incidents, and deeper investigation to identify the root cause
- Meaningful recommendations and actions to prevent incidents from recurring
- A refresher lesson to gauge learners' understanding of investigating accidents and incidents

When to Write a Report:(*How to write an effective incident report* 2023)

The rule of thumb is that as soon as an incident occurs, an incident report should be completed. Minor injuries should be reported and taken as equally important as major injuries are. These injuries may get worse and lead to more serious injuries or health issues. Employers, managers, and safety officials should be aware of the different situations and events that should be reported.

Here are 4 types of incidents you should report:

1. Sentinel events – these are unexpected occurrences that resulted in serious physical or psychological injury or death (e.g., slips, trips and falls, natural disasters, vehicle accidents, disease outbreak, etc.).
    - Worker injury incident
    - Environmental incident
    - Property damage incident
    - Vehicle incident
    - Fire incident
2. Near misses – these are situations where the people involved had no injuries but could have been potentially harmed by the risks detected.
3. Adverse events – related to medicine, vaccines, and medical devices (in compliance with ISO 14971). These events occur when an act of commission or omission harmed a patient rather than from the existing disease or condition.
4. No harm events – these are incidents that need to be communicated across an organization to raise awareness of any harm that may happen.

How to Write a Report:

- Be Accurate
- Be Factual
- Be complete
    - Ensure that all essential questions (what, where, when, why, and how) are covered in the incident report. Record not only the people who were injured and what caused the accident to happen, but also include details such as people who witnessed and reported the incident or those who will conduct an investigation. Anticipate what other significant details will be needed for any future study and investigation
- Be Valid
    - Upon completion, those who are involved in the incident (e.g. victim, witnesses, manager, reporter, etc.) should sign off to testify and validate all the information that was mentioned in the incident report. This confirms that the incident report is truthful and unquestionable.
- Graphic
    - Photos, diagrams, and illustrations should be included as supporting evidence. Take many photos of the injury, damage, and surrounding environment. This supplements the facts stated and provides more clarity to be easily understood by the recipient.

Resources:

- *How to write an effective incident report*. SafetyCulture. (2023, May 26). https://safetyculture.com/topics/incident-report/
    - (*How to write an effective incident report* 2023)

Creating a Disaster Recovery Plan

2. Identify Critical Assets and Operations: Identify the assets and operations that are crucial for the organization's functioning, such as your online course delivery system and the credit card payment processing system.

   To effectively function, non-profit organizations rely on several crucial assets and operations. Here are key elements essential for their functioning:

1. Mission and Vision: A clear mission and vision statement provide the guiding principles and purpose for the non-profit organization. It defines the overall goals and objectives that drive its activities.

2. Leadership and Governance: Effective leadership and governance structures are vital for decision-making, strategic planning, and ensuring compliance with legal and ethical standards. This includes a board of directors or trustees responsible for providing oversight and setting policies.

3. Human Resources: Skilled and dedicated individuals, including staff members, volunteers, and advisors, are essential assets for a non-profit organization. Having the right people with the necessary expertise, passion, and commitment contributes to the organization's success.

4. Funding and Financial Management: Non-profits need financial resources to sustain their operations, support programs, and cover administrative costs. Funding can come from various sources, including donations, grants, sponsorships, fundraising events, and government support. Effective financial management ensures proper allocation of resources and transparent reporting.

5. Partnerships and Collaboration: Collaborating with other organizations, businesses, governments, and community stakeholders enhances the non-profit's capacity to achieve its mission. Partnerships provide access to resources, expertise, networks, and amplifies the organization's impact.

6. Programs and Services: The core activities of a non-profit revolve around designing and delivering programs and services aligned with their mission. These initiatives address the needs of their target beneficiaries or communities, and their successful implementation contributes to the organization's impact.

7. Volunteer Management: Volunteers play a significant role in non-profit organizations, contributing their time and skills to support various activities. Effective volunteer management involves recruiting, training, and engaging volunteers to ensure their efforts align with organizational goals.

8. Technology and Infrastructure: Non-profits require appropriate technology infrastructure, including hardware, software, and online platforms, to support their operations, communication, data management, and program delivery. This infrastructure facilitates efficiency and effectiveness in various areas of the organization.

9. Public Relations and Communication: Non-profits need to effectively communicate their mission, activities, and impact to stakeholders, including donors, supporters,

beneficiaries, and the public. Strategic communication helps raise awareness, build relationships, and generate support for the organization's work.

10. Evaluation and Learning: Establishing systems for monitoring, evaluation, and learning allows non-profits to assess the effectiveness of their programs, track progress toward goals, and make informed decisions. This continuous improvement process strengthens the organization's impact and accountability.

It's important to note that the specific assets and operations required may vary based on the non-profit's size, focus area, geographic location, and available resources. Organizations should assess their individual needs, prioritize their requirements, and develop strategies to ensure the smooth functioning of their operations.

Credit Card Payment Processing system: Jane's notes

Payment Card Industry Data Security Standard (PCI DSS):

This is an information security standard that applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers (PCI Security Standards Council, 2021).

It was developed to enhance cardholder data security and to ensure the safe handling and storage of sensitive customer credit card information and data (PCI Security Standards Council, 2021).

Main Components of PCI DSS:

1. Build and Maintain a Secure Network and Systems
    - Install and maintain a firewall configuration to protect cardholder data.
    - Do not use vendor-supplied defaults for system passwords and other security parameters.
2. Protect Cardholder Data
    - Protect stored cardholder data.
    - Encrypt transmission of cardholder data across open, public networks.
3. Maintain a Vulnerability Management Program
    - Protect all systems against malware and regularly update anti-virus software or programs.
    - Develop and maintain secure systems and applications.
4. Implement Strong Access Control Measures
    - Restrict access to cardholder data by business need-to-know.
    - Identify and authenticate access to system components.
    - Restrict physical access to cardholder data.
5. Regularly Monitor and Test Networks
    - Track and monitor all access to network resources and cardholder data.
    - Regularly test security systems and processes.
6. Maintain an Information Security Policy

- Maintain a policy that addresses information security for all personnel (PCI Security Standards Council, 2021).

Policy Behind the Creation of PCI DSS

- The PCI DSS was developed in 2004 by the founding payment brands of the PCI Security Standards Council, namely, American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc.
- The key policy reason behind its creation was to consolidate the various industry data security standards into one unified framework to manage the ongoing evolution of the Payment Card Industry (PCI) security standards (Vijayan, 2007).

References:

PCI Security Standards Council. (2021). PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1. Retrieved from https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv321.pdf

Vijayan, J. (2007). Q&A: New security standards council aims to 'take PCI to the next level.' Computerworld. Retrieved from https://www.computerworld.com/article/2544689/q-a--new-security-standards-council-aims-to--take-pci-to-the-next-level-.html

TKH & PCI DSS

If a medium-sized non-profit organization accepts credit or debit card donations through its website, then it is indeed involved in payment card processing, and so it must comply with the Payment Card Industry Data Security Standard (PCI DSS).

How the requirements of PCI DSS could apply to The Knowledge House:

- Build and Maintain a Secure Network and Systems: The non-profit organization needs to ensure that its donation processing system is secured by firewalls, and that all default passwords provided by vendors (for instance, for servers or software systems) are changed.
- Protect Cardholder Data: The organization should never store sensitive cardholder data unless absolutely necessary, and if it is stored, it should be encrypted or otherwise protected. Data that is transmitted (such as to payment processors) should always be encrypted as well.
- Online Donations: If the non-profit organization is accepting donations online through their website and these donations are processed using a credit or debit card, they are required to be compliant with PCI DSS (Williams, 2016).
- Cardholder Data Security: The non-profit must ensure that it is securely handling and storing any cardholder data that it collects during the donation process. This includes encryption of data both in transit and at rest, as well as secure disposal of data when no longer required (PCI Security Standards Council, 2021).
- Third-Party Processors: If the non-profit uses a third-party payment processor, the organization is still responsible for ensuring the processor is PCI compliant. While the

processor will handle much of the technical and operational aspects of card data security, the non-profit has an obligation to ensure their service providers also adhere to PCI DSS (Jones, 2020).

- Regular Audits: Non-profits accepting card payments are required to conduct regular PCI DSS audits, which could be an annual or quarterly process depending on the organization's transaction volume. These audits should be performed by a Qualified Security Assessor (QSA) or an Internal Security Assessor (ISA) (PCI Security Standards Council, 2021).
- Data Breach Liability: In the event of a data breach, a non-profit organization can be held liable for the financial losses resulting from the breach if it is found to be non-compliant with the PCI DSS at the time of the breach (Fenton, 2018).

References:

Williams, K. (2016). The ABCs of PCI Compliance for Nonprofits. Network for Good. Retrieved from https://www.networkforgood.com/nonprofitblog/pci-compliance-nonprofits/

Jones, C. (2020). What is PCI Compliance and Why It's Important for Your Business. Business News Daily. Retrieved from https://www.businessnewsdaily.com/10930-pci-compliance.html

Fenton, H. (2018). Data Breaches: Nonprofits Are Also at Risk. Venable LLP. Retrieved from https://www.venable.com/insights/publications/2018/10/data-breaches-nonprofits-are-also-at-risk

PCI Security Standards Council. (2021). PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1. Retrieved from https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv321.pdf

Non Compliance of PCI DSS

- Fines and Penalties: Non-compliance with PCI DSS can lead to monetary penalties. These are usually levied by the credit card companies themselves and can range from $5,000 to $100,000 per month. The actual amount depends on the size of the organization, the duration of non-compliance, and the number of transactions processed (Gibson, 2018).
- Card Replacement Costs and Forensic Audits: If a breach occurs and the organization is found to be non-compliant, they could be responsible for the costs associated with replacing compromised cards and conducting forensic audits to determine the cause and extent of the breach (Gibson, 2018).
- Increased Transaction Fees: Merchants who are not PCI compliant may face increased transaction fees from their banks or payment processors (Gibson, 2018).
- Reputation Damage: Data breaches can significantly damage an organization's reputation. For a non-profit, this could mean a decrease in donations as donors lose trust in the organization's ability to safeguard their data (Fenton, 2018).
- Loss of Credit Card Privileges: In severe cases, the non-profit could lose the ability to accept credit card payments altogether, which could significantly impact its ability to raise funds (Williams, 2016).

References:
Gibson, S. (2018). The Real Cost of PCI DSS Non-Compliance. SecurityMetrics. Retrieved from https://www.securitymetrics.com/blog/real-cost-pci-dss-non-compliance

Fenton, H. (2018). Data Breaches: Nonprofits Are Also at Risk. Venable LLP. Retrieved from https://www.venable.com/insights/publications/2018/10/data-breaches-nonprofits-are-also-at-risk

Williams, K. (2016). The ABCs of PCI Compliance for Nonprofits. Network for Good. Retrieved from https://www.networkforgood.com/nonprofitblog/pci-compliance-nonprofits/

How a Secure Program Keep TKH in PCIDSS Compliance

1. Secure Cardholder Data: The program should ensure that all cardholder data is securely stored and transmitted. This includes encryption of data both in transit and at rest, secure disposal of data when no longer required, and minimization of stored data (PCI Security Standards Council, 2021).
2. Use of Firewalls: Implement and maintain firewalls to protect internal networks from unauthorized access. These firewalls should be properly configured and updated regularly (SANS Institute, 2015).
3. Maintain a Secure Network: This involves changing vendor-supplied defaults, maintaining a vulnerability management program, and developing and maintaining secure systems and applications (PCI Security Standards Council, 2021).
4. Access Controls: Implement strong access control measures. This includes limiting access to cardholder data to those with a business need-to-know, implementing strong user authentication methods, and controlling physical access to systems (PCI Security Standards Council, 2021).
5. Regular Monitoring and Testing: Regularly monitor and test networks to identify and rectify any vulnerabilities or breaches. This includes tracking and monitoring all access to network resources and cardholder data, as well as regularly testing security systems and processes (PCI Security Standards Council, 2021).
6. Information Security Policy: Maintain a robust information security policy that is communicated to all personnel. This should outline all security measures, responsibilities, and expectations in relation to cardholder data security (SANS Institute, 2015).

References:

PCI Security Standards Council. (2021). PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1. Retrieved from https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv321.pdf

SANS Institute. (2015). A Practical Guide to the Payment Card Industry Data Security Standard (PCI DSS). Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/practical-guide-payment-card-industry-data-security-standard-pci-dss-35962

Access Management Procedures

- A procedure detailing how access rights are assigned, reviewed, changed, and revoked. This should cover who is authorized to grant access, how access requests are validated, and how often access rights should be reviewed.

Software and Systems Update Standards

- Regular updates to systems and software applications are crucial in maintaining security. A standard can be set for timely updates and patches to mitigate vulnerabilities.

By Lucas Higgs

Access Management Procedures: (*Access management policy* 2022)

Background

Access to the Enterprise's electronic information resources must be managed in a manner that maintains the confidentiality, integrity, and availability of Enterprise resources, and in a manner that complies with any applicable legal and regulatory requirements.

Definitions

- Authentication: The process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
- Authorization:Access privileges granted to a user, program, or process or the act of granting those privileges
- Multi-Factor Authentication (MFA):Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/personal identification number (PIN)); (ii) something you have (e.g., token generation device); or (iii) something you are (e.g., biometric).
- Least Privilege: The principle that a security architecture is designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

- Privileged Access Management (PAM):The process of managing and protecting credentials to accounts that have some level of administrative access to devices or systems, including local administrator accounts and superusers.
- User: Individual or (system) process, acting on behalf of an individual, authorized to access a system
    - Organization User: An organizational employee or an individual whom the organization deems to have equivalent status of an employee, including a contractor, guest researcher, or individual detailed from another organization.
    - Non-Organization User: A user who is not an organizational user
    - Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Policy Statement

Access Management is the process of identifying, tracking, controlling, and managing user access rights to information systems. Any user who requests access to systems, applications, or data, must have their identity authenticated. Additionally, user access should be further restricted following the principle of Least Privilege, and in alignment with any Enterprise defined segregation of duties guidelines.

User account provisioning must include creation of unique credentials for new users and disablement and revocation of a terminated user's access privileges upon termination.

Privileged access must only be provided to users as needed. Users with privileged user accounts must also have an organizational user account, which follows the principle of least privilege, and must use this organizational user account for their day-to-day job functions. Privileged user accounts must only be used when elevated privileges are required by the system or application.

Where there is any requirement for shared usage of an account this must be signed off by the IT Security division and all usage must be audited and traceable to an individual authorized user account.

All remote access to the Enterprise's network must utilize a secure solution, which employs multi-factor authentication, and a secure network encryption protocol.

Multi-Factor Authentication

The Office of Information Technology has taken several steps to protect and monitor our Information Systems. As part of its efforts, the OIT has enabled Multi-Factor Authentication which provides a common method of protection for companies like ours, that utilize and store sensitive, personal, and financial information.

Access Management Procedures ChatGPT:
Access management procedures for a nonprofit organization are designed to ensure the security and integrity of the organization's systems, data, and resources while enabling authorized individuals to fulfill their roles effectively. Here are some key considerations for access management procedures in a nonprofit organization:

1. User Roles and Permissions: Clearly define user roles within the organization based on job responsibilities and functions. Assign appropriate access permissions to each role to ensure the principle of least privilege. Limit access to sensitive data or critical systems only to individuals who require it for their work.

2. User Authentication: Implement strong authentication mechanisms to verify the identity of users accessing the organization's systems. This can include the use of secure passwords, two-factor authentication, or biometric authentication methods, depending on the organization's resources and requirements.

3. User Account Management: Establish procedures for creating, modifying, and terminating user accounts. Ensure that new accounts are created for authorized individuals only, and promptly remove access for employees or volunteers who leave the organization. Regularly review and update access privileges to reflect any changes in roles or responsibilities.

4. Data Access Controls: Apply access controls to protect sensitive data. Utilize encryption techniques to secure data at rest and in transit. Implement data classification to identify and categorize data based on its sensitivity, allowing for more granular access controls.

5. Regular Access Reviews: Conduct periodic access reviews to ensure that access privileges align with current job roles and responsibilities. Remove unnecessary or outdated access permissions promptly to minimize the risk of unauthorized access.

6. Training and Awareness: Educate employees, volunteers, and stakeholders about the importance of access management and cybersecurity best practices. Provide training on password security, recognizing phishing attempts, and handling sensitive information appropriately.

7. Monitoring and Logging: Implement monitoring and logging mechanisms to track user activities, detect unauthorized access attempts, and identify potential security incidents. Regularly review logs for anomalies or suspicious behavior.

8. Incident Response: Establish an incident response plan to address security incidents promptly. Define procedures for reporting and handling security breaches, including unauthorized access attempts, data breaches, or compromised user accounts.

9. Third-Party Access: If the nonprofit organization works with external partners or vendors, establish guidelines for granting and managing their access. Implement contracts or agreements that outline access requirements, data protection measures, and accountability.

10. Compliance with Regulations: Ensure that access management procedures align with applicable data protection and privacy regulations, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA), depending on the organization's jurisdiction and activities.

Remember, access management procedures should be regularly reviewed, updated, and communicated to all relevant stakeholders to maintain their effectiveness and address any emerging security risks or changes in organizational structure.

Software and Systems Update Standards: (Bingham, 2022)

- Knowing your network, systems, devices, software, and users is first on this list because you can't adequately plan out software update deployments without this information.
    - Here's some of the essential information you should know about your IT environment:
        - The makes and models of the hardware devices on your network
        - Utilized operating systems
        - Utilized applications
        - Network structure and resources
        - Hours of operation
        - Critical systems
        - Users
        - VIP users
        - Security concerns
- While this may seem like a lot of information to gather, many available systems can manage the task for you.
    - For example, PDQ Inventory is a device management platform that automatically scans your network for Windows devices, gathering, organizing, and centrally storing detailed system configuration information for you. It can take care of getting to know your devices and systems while you get to know your users and their needs.
- Stay informed
    - While some systems release updates on a pretty regular basis, for example, Microsoft and Adobe release updates on Patch Tuesday (the second Tuesday of

every month), other systems don't have a steady release schedule. Even Microsoft and Adobe frequently release out-of-band security patches to address vulnerabilities.
    - To help stay informed about the latest software updates, consider subscribing to RSS feeds, following developer social media accounts, and signing up for mailing lists for systems you utilize.
- Compliance standard requirements
    - Many organizations must adhere to specific standards to meet regulatory requirements, such as PCI DSS and SOC 2. Some regulatory standards require deploying software updates within a particular time frame of release. Identifying which compliance standards your organization is required to meet will help you plan your patch deployment schedule.
- Develop a schedule that works for your organization
- Once you've gotten to know your IT environment and your regulatory requirements, it's time to develop a software patch deployment strategy that works for your organization. This step is often the most difficult because of the substantial number of factors to consider.
- Since each organization is unique, there is no one-size-fits-all approach to developing a deployment schedule, but here are a few tips to help out:
    - Don't deploy updates that require restarts during the middle of the day. This practice is considered *full contact IT,* and it is generally frowned upon — by users at least.
    - Establish a maintenance window that doesn't conflict with peak operation hours and heavy network traffic periods.
    - Some updates, like Microsoft Windows feature updates, can lock down a system for a considerable amount of time. Consider deploying these types of updates after regular business hours.
    - Divide your systems into preview, broad, and critical software update groups. The preview software update group is your tester group, which should receive updates shortly after release. The broad group should consist of the majority of your systems. These systems should receive patches after testing is complete. Essential systems belong in the critical software update group and should receive patches once they've been thoroughly tested and potentially delayed indefinitely if there are compatibility issues.
- Be Transparent

    - Once you've nailed down the perfect patch deployment schedule, inform your users of when to expect updates and their potential impact on their system. The workforce is a pretty tech-savvy bunch these days. Most users have a basic understanding of software updates and what it means for their systems. Keeping them informed builds trust.
    - If you ever get users complaining about updates, remind them of the risks associated with vulnerabilities and the consequences of a security breach. This info usually helps them understand why we do what we do.
- Be Ready to Adapt
    - Certain patches, such as Microsoft's updates, you can count on. Every Patch Tuesday, they'll become available to the masses. Other updates, however, aren't as routine.
    - IT teams need to be able to adapt and respond to patching needs, especially when a zero-day vulnerability is disclosed. Vendors take critical vulnerabilities very seriously and release patches ASAP. Ensuring your IT team can properly respond to out-of-band and last-minute critical software updates is an essential part of securing your organization's digital assets.
- Servers require special care
    - Servers are often a crucial part of an organization's IT infrastructure. As such, always take extra caution when updating servers. Windows Server receives cumulative updates every Patch Tuesday, just like its desktop OS counterpart. Consider delaying server patches for several days. This gives the tech community time to report any unintended behaviors or compatibility issues introduced by the updates. However, if a server is exposed because of a critical vulnerability, immediate patching is always recommended, though I'd still suggest doing it after hours — just in case.
- Proper testing saves you time and energy
- One of the most important aspects of deploying software updates is properly testing them before distributing them to the masses. Properly testing patches will save you a ton of time and aggravation if a problematic update needs to be uninstalled. Here are a few things to consider when establishing your testing process:
    - Send out patch deployments to your test machines and users as quickly as possible. This gives your testers adequate time to thoroughly test updates before they need to be deployed to your broad group.

    - Your test group should include a subset of machines that reflects the diversity of your organization's assets as a whole.
    - Enlist test users that are more likely to provide relevant and informational feedback.
    - Keep your test group small enough that if a problem patch is distributed, it’s easy to remove.
- Automate to stay up to date
    - Sysadmins have a lot of responsibilities on their plates. Often, the only way for them to reliably distribute patches across thousands of devices and systems is to use patch management software to automate the process. A patch manager solution can utilize automatic deployment rules to distribute updates across an organization. While various solutions provide this functionality, few products make it as easy as PDQ Deploy. Sysadmins struggling to keep up with their patch management needs can download a free 14-day trial to see for themselves how easy deploying patches can be.
- Audit your deployments
    - Auditing ensures updates are being deployed successfully and you don't have systems on your network that are missing patches. One system left with an unpatched vulnerability is all it takes for a bad actor to access your organization's network and assets.
    - To help your audits run smoothly, look for tools that provide intelligent reporting features, such as PDQ Deploy and Inventory. PDQ allows you to configure auto reports, ensuring you have all the information you need whenever you need it.

Software and systems update standards:
Nonprofit organizations, like any other entities, can benefit from following software and systems update standards to ensure the security, stability, and efficiency of their operations. Here are some common standards and best practices for software and systems updates in nonprofit organizations:

1. Regular Patch Management: Implement a patch management process to keep software and systems up to date with the latest security patches, bug fixes, and updates. This includes operating systems, applications, and firmware.

2. Software Version Control: Maintain a centralized repository or version control system to manage software versions and track changes. This helps ensure that the organization is using the latest stable versions of software and enables easy rollback if necessary.

3. Change Management Process: Establish a formal change management process to evaluate, approve, and implement updates. This process should include testing updates in a controlled environment before deploying them to production systems.

4. Scheduled Maintenance Windows: Define regular maintenance windows or downtime periods during which system updates and maintenance activities are performed. Communicate these windows to staff and stakeholders to minimize disruption.

5. Vendor Notifications: Stay informed about software and system updates by subscribing to vendor notifications and security mailing lists. This helps to receive timely information about vulnerabilities, patches, and updates relevant to the organization's technology stack.

6. Security Updates and Vulnerability Management: Stay proactive in addressing security vulnerabilities by regularly scanning systems for vulnerabilities, using tools like vulnerability scanners. Promptly apply security updates and patches to mitigate potential risks.

7. Backup and Disaster Recovery: Implement a robust backup strategy to protect data and ensure business continuity. Regularly test backups and ensure the ability to restore systems in case of failures or security incidents.

8. Documentation and Knowledge Sharing: Maintain up-to-date documentation of software and systems configurations, update processes, and related procedures. This documentation aids in knowledge sharing, troubleshooting, and facilitating smooth transitions during staff turnover.

9. User Awareness and Training: Educate staff and users about the importance of software and systems updates, including the potential risks of neglecting updates and how to report issues. Promote a culture of security and compliance within the organization.

10. Monitoring and Performance Optimization: Implement monitoring tools and practices to track system performance, identify bottlenecks, and proactively address issues. Regularly review system logs and performance metrics to detect anomalies or indicators of potential problems.

It's important to note that the specific standards and practices may vary depending on the size, complexity, and budget of the nonprofit organization. It's recommended to consult with IT professionals or consider industry-specific frameworks, such as the NIST Cybersecurity Framework, for additional guidance.

Resources:

- *Access management policy*. St. George's University. (2022, April 12). https://www.sgu.edu/office-of-information-technology/computing-policies/access-management/#:~:text=Policy%20Statement,must%20have%20their%20identity%20authenticated.
- Bingham, B. (2022, March 22). *10 best practices for deploying software updates*. PDQ. https://www.pdq.com/blog/deploying-software-best-practices/