Incident Response, Disaster & Business Continuity Plans

THE KNOWLEDGE HOUSE

Introduction

The Knowledge House (TKH), holds a significant responsibility to ensure the trust of our stakeholders, community, and employees. As we move towards a progressively digital world, this responsibility extends beyond providing quality educational resources and experiences. The need to maintain robust cybersecurity measures and a foolproof plan for tackling cyber incidents becomes crucial.

TKH's operations are driven by an extensive online infrastructure, which facilitates not just our educational services, but also sensitive transactions like credit card donations. Therefore, safeguarding the integrity and confidentiality of our operations and data becomes a paramount concern. Moreover, our geographical and operational footprint subject us to various regulations and laws at both federal and state levels, including NIST standards, and regulations specific to New York, Georgia, and California. Non-compliance can result in penalties and can severely impact our reputation and trustworthiness in the community we serve.

The objective of creating an Incident Response and Disaster Recovery Plan is twofold. Firstly, the plan serves as a roadmap to manage and mitigate any potential cybersecurity incidents, ensuring that our services remain uninterrupted, and our stakeholders' data is safe. Secondly, it provides a clear path to recovery in case a disaster strikes, ensuring continuity of operations with minimal disruption.

At this point, you may be wondering why an organization like ours, centered around education, needs to prioritize cybersecurity and disaster recovery planning. Let's delve a bit into that.

Why do we need an Incident Response and Disaster Recovery Plan?

1. Protecting Sensitive Data: The very nature of our work involves handling sensitive information - student data, staff records, and credit card information from donors. An unforeseen cyber incident can jeopardize this information, affecting individuals' privacy and potentially leading to financial losses.

2. Legal Compliance: As mentioned earlier, TKH is subject to various cybersecurity laws and regulations. Having an established plan helps ensure that we meet these regulatory requirements, mitigating legal risks.

3. Maintaining Operational Continuity: Cyber incidents or disasters can disrupt our online operations, impeding our ability to deliver educational services. A well-prepared plan can help minimize downtime and accelerate recovery, ensuring we can continue our mission with minimal disruption.

4. Preserving Reputation: Trust is a crucial factor in the non-profit sector. A data breach or extended downtime can erode that trust. Through proactive planning, we can better manage these incidents, preserving the reputation that TKH has worked so hard to build.

This guide will detail our comprehensive strategy for incident management and disaster recovery, laying out clear roles and procedures. The plan is designed to be accessible and understandable, even for our team members without a technical background. After all, cybersecurity and disaster preparedness is a team effort, and every member of the TKH family has a role to play in it.

Our approach to developing this plan is grounded in foresight, proactivity, and collective responsibility. We believe that with the right team, clear roles and responsibilities, established protocols, and continuous learning and adaptation, we can rise to the challenge of managing any incident that may come our way.

The plan is divided into two main sections, each with its unique structure and components:

Incident Response and Management Plan: This part outlines our strategy for responding to cybersecurity incidents in a timely, effective manner. It includes the formation of an Incident Response Team (IRT), defining their roles and responsibilities, creating incident classification criteria, outlining incident response procedures, creating an incident reporting mechanism, providing appropriate training, and conducting regular incident response drills.

Disaster Recovery and Business Continuity Plan: Here, we discuss how to recover our operations should we face a significant disaster. It involves identifying critical assets and operations, conducting a thorough risk assessment, developing disaster recovery strategies, setting up a Disaster Recovery Team (DRT), creating a communication plan, documenting the disaster recovery plan, and testing and refining our strategies.

Our goal in creating and implementing this plan is to ensure that our organization can effectively respond to and recover from any disruptions, thereby minimizing their impact on our operations, our employees, and the communities we serve.

As we move forward, we hope every member of TKH, from our instructional staff to our operations team, will join us in this commitment to ensure the ongoing security and continuity of our services. Let this plan serve not only as a guide but also as a reminder of the importance of our collective responsibility to ensure the safety, security, and resilience of our organization in the face of any adversity.

Together, we can make TKH a model for cybersecurity and disaster preparedness in the educational tech non-profit sector.

Immediate Mitigating Actions

Upon identifying a cybersecurity incident, immediate actions must be taken to prevent the situation from escalating.

1. Disable Existing Domain Administrator Accounts: The first step should be to disable all existing Domain Administrator accounts. This is crucial to prevent unauthorized access and further exploitation of these accounts.
2. Transition to New Accounts: Following the disabling of old accounts, new administrator accounts should be created. This ensures continued control over the domain while reducing the risk of unauthorized access using compromised credentials.
3. Rotate All Local and Domain Credentials: Changing all local and domain credentials is an important step in preventing unauthorized access. This includes passwords for all users, as well as keys and certificates, if applicable.
4. Lock Down the OS Environment: Securing the operating system environment is necessary to prevent further exploitation. This includes ensuring all user accounts are secure, removing any unneeded services, and ensuring that the OS is properly patched and updated.
5. Update with Relevant Security Patches: Any outstanding security patches that are relevant to the breach should be applied immediately. Patches often fix known vulnerabilities that may have been exploited during the breach.
6. Discover and Audit Newly Created Accounts: Review all user accounts created on or after the incident date. This may reveal unauthorized accounts set up by the attacker. Any suspicious activity associated with these accounts should be investigated and dealt with immediately.
7. Monitor Privileged Accounts: Keep a close eye on privileged accounts for any suspicious activity. This includes administrators and service accounts, as these are often targeted by attackers due to their elevated permissions.
8. Reset Kerberos Tickets: Kerberos tickets, which are used for authenticating network services, should be reset. This step would help prevent the continued use of any stolen tickets, effectively cutting off an attacker's access to authenticated resources.

This list represents a preliminary reaction to a cybersecurity incident, and additional actions will be necessary as part of a comprehensive incident response and recovery process.

Incident Response Team (IRT): Roles, Responsibilities and Contact Information

The creation of an Incident Response Team (IRT) is an essential part of our cybersecurity strategy. The IRT is a group of professionals tasked with preparing for and responding to any security incidents or breaches that might occur within the organization. This includes not only managing the immediate response to an incident but also carrying out post-incident analysis to prevent future incidents.

In the context of The Knowledge House (TKH), we suggest the following structure for our IRT:

IT Technician: As a technical expert, the IT Technician will play a crucial role in identifying and containing security incidents. This includes monitoring our systems for any unusual activity, isolating affected systems to prevent further spread, and aiding in the recovery process.
Name: *Contact Information:*

Chief Technology Officer (*CTO*): The CTO will provide the strategic oversight needed during a security incident. Their role includes making high-level decisions, allocating resources, and liaising with the rest of the executive team to ensure they are aware of the situation and its implications.
Name: *Contact Information:*

Senior Manager of Data, Operations, and Technology: With their comprehensive knowledge of TKH's operational and technological landscape, this individual will contribute significantly to incident detection, analysis, and recovery. Their understanding of our data management practices will also help ensure that we meet any regulatory obligations during and after an incident.
Name: *Contact Information:*

Fiscal and Operations Manager: The Fiscal and Operations Manager can provide valuable insights on the potential financial and operational impacts of an incident. They can also aid in resource allocation decisions and contribute to post-incident recovery strategies.
Name: *Contact Information:*

Digital Media Specialist: This individual can handle external communications during and after an incident, ensuring that all messaging aligns with TKH's branding and values. This can include creating press releases, managing social media updates, and coordinating communication with other stakeholders.
Name: *Contact Information:*

Manager of Curricula and Instruction: Their insights into the daily operations and the needs of our instructional staff can help ensure that our response strategies are practical and effective. They can also help communicate with our instructional staff during and after an incident, ensuring they understand what happened and what they need to do.
Name: *Contact Information:*

MSP/ Technical Support Specialist: This third-party specialist can provide additional technical expertise, particularly in terms of incident detection and containment. They can also help ensure that any solutions we implement align with our existing infrastructure and the services provided by the MSP.
Name: *Contact Information:*

Each member of the IRT should have a clear understanding of their responsibilities during a security incident. This clarity helps ensure a coordinated and effective

response. Additionally, we suggest that the IRT conduct regular training exercises to keep their incident response skills sharp. We recommend making use of an incident response template to provide a good starting point for developing the IRT's procedures.

By establishing a well-defined and well-trained IRT, TKH will be better prepared to handle any cybersecurity incidents that may arise. With a team of dedicated individuals from different departments working together, we can ensure a swift and effective response, thereby minimizing any potential damage and disruption.

Incident and Threat Classification

In cybersecurity, an incident is broadly defined as any event that compromises the integrity, confidentiality, security, or availability of an organization's information systems, networks, or data. These incidents, which can be intentional or unintentional, pose potential harm to the organization's operations and assets. However, not all incidents are equal, and their potential impact can vary greatly. Thus, it's crucial to establish clear criteria for classifying and prioritizing incidents.

One widely accepted approach is the Vocabulary for Event Recording and Incident Sharing (VERIS) framework, a standard developed by the Verizon Threat Research Advisory Center (Verizon, 2020). The framework provides a universal language for describing, sharing, and analyzing incidents, improving response capabilities.

Incident classification in VERIS revolves around four key criteria:

1. Incident Category: An event involving malware deployment, which may result in the execution of malicious software, can be classified under this category. Unauthorized access, such as someone illicitly accessing confidential data or systems, also falls under this category. Denial of Service (DoS) incidents, which prevent or inhibit the normal function of systems or networks, are classified here. Other examples include physical theft/loss of assets, errors resulting from unintentional actions, and social engineering, which involves manipulation or deception of individuals to gain unauthorized access.
2. Incident Pattern: If an incident's method is a flood of requests causing a denial or degradation of service, it fits the DoS/DDoS pattern. Exploitation incidents result from exploiting vulnerabilities in a system or network. If the method of attack involves phishing—deceptive attempts to obtain sensitive information—it falls under the Phishing pattern. Unauthorized Access, Theft/Loss, and Fraud patterns are also common.
3. Asset: The asset criterion is focused on what was affected by the incident. An incident involving the compromise of important data falls under the Information asset category. If the incident disrupts or damages network systems or hardware, it's classified under the Infrastructure category. Physical refers to incidents involving tangible assets, like hardware or other physical property. The People category involves incidents related to user accounts or personal information, and

the Reputation category pertains to incidents affecting the organization's brand or reputation.

4. Attribute: This criterion is all about the specific features of the incident. For instance, if an incident involves the unauthorized disclosure of sensitive information, it affects the Confidentiality attribute. If an incident disrupts the accuracy or reliability of data or systems, it impacts the Integrity attribute. Incidents affecting Availability hinder access to systems or services. The Accountability attribute is affected when an incident impedes the organization's ability to attribute actions to individuals. Non-Repudiation incidents impact the organization's ability to prove the validity or integrity of communications.

When prioritizing incidents, various factors come into play:

- Impact Severity: High-priority incidents often have severe impacts on the organization, resulting in substantial financial loss, operational disruption, or reputational damage.
- Scope and Scale: An incident affecting a larger number of systems or users may be prioritized over one with a smaller reach.
- Threat Source: The source of the threat could indicate if it is a targeted attack or a widespread vulnerability, thus affecting its priority.
- Exploitability: If the incident reveals a systemic vulnerability that is easily exploitable, it may be given high priority for rectification.
- Relevance to Critical Assets: High-value assets or sensitive information being involved can push an incident up the priority list.
- Regulatory and Compliance Requirements: Incidents involving breaches of legal, industry, or regulatory obligations often receive high priority due to potential fines or penalties.
- Incident Response Complexity: Incidents requiring complex and resource-intensive responses may need to be prioritized to ensure adequate resource allocation.
- Historical Context and Patterns: Understanding past trends and patterns can help identify potential risks and prioritize incidents.

Building upon the foundations of our classification and prioritization criteria, we can delve deeper into a widely accepted cybersecurity model, the CIA Triad (Confidentiality, Integrity, and Availability), which serves as a robust framework for classifying incidents and determining response requirements.

The CIA Triad (Confidentiality, Integrity, and Availability) is a framework for incident classification that helps to prioritize the level of incident response required for a cyber attack. CIA is as follows:

1. **Confidentiality** – Incidents involving unauthorized access to systems, including privileged account compromise. The more confidential the data or the more important the systems are to the business, the higher the potential impact.

2. **Integrity** – Incidents involving data poisoning, including leveraging a privileged account to corrupt or modify data. The more sensitive the data, the higher the potential impact.

3. **Availability** – Incidents that impact the availability or proper functioning of services, such as Distributed Denial of Service (DDoS) or ransomware, including use of privileged accounts to make unauthorized changes. The more critical the services to the business, the higher the potential impact.

Conclusion

We hope that this Incident and Disaster Response and Recovery & Business Continuity Plans guide serves as a comprehensive roadmap for The Knowledge House (TKH) to tackle and mitigate any potential cybersecurity incidents while maintaining the continuity of our operations with minimal disruptions. As we have laid out in this guide, our intention is not just to protect the sensitive data of our stakeholders, but also to ensure that we remain legally compliant, preserve our reputation, and importantly, uphold the trust of the community we serve.

This guide is not just a set of procedures and plans; it is a manifestation of our dedication towards building a secure and resilient organization. By implementing and regularly updating these strategies, we aim to meet the ever-evolving challenges in cybersecurity and disaster management.

From protecting sensitive data, complying with laws and regulations, maintaining operational continuity, to preserving our reputation, each element is carefully thought out and developed to suit our specific operational and regulatory needs. Furthermore, we have structured the guide to be as understandable as possible, ensuring that every member of TKH, regardless of their technical background, can actively participate in our collective responsibility.

This plan extends to two main areas: Incident Management and Disaster Recovery and Business Continuity. Each section is tailored to address specific scenarios and provides clear procedures to follow, ensuring that our organization is equipped to respond effectively and promptly to any incident or disaster.

As we embrace this journey of enhancing our cybersecurity measures and disaster preparedness, we invite every member of TKH, from our instructional staff to our operations team, to join us in our commitment. Every individual's participation strengthens our collective capacity to respond and recover from any potential disruptions.

The preparation of this plan embodies the essence of TKH – a dedication to not just providing quality education but also ensuring the safety and security of our community. Let us remember that while the challenges we face may be complex, our response should be rooted in simplicity, transparency, and collective effort. As we navigate this

increasingly digital world, let this plan serve as a beacon, guiding us towards building a safer and more resilient organization. Together, let's make The Knowledge House a model for cybersecurity and disaster preparedness in the educational tech non-profit sector.

Incident Response, Disaster & Business Continuity Plans

Secure Program Capstone 2023
Project Manager & Author: Jane Pierre

COPYRIGHT NOTICE AND DISCLAIMER