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:*

Mosyle 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 Mosyle.
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.

When ranking the level of risk to the organization and the type of incident response required, you must take into account the extent to which privileged accounts are compromised, including those associated with business users, network administrators, and service or application accounts. When privileged accounts are involved in the breach, the level of risk increases exponentially as does the response required.

Sample Cyber Incident	CIA category	Privileged Account Breach	Business Impact	Risk Level
An employee shares information with an unauthorized third party, but the information is not personal or protected by regulatory requirements.	C	No	Low	Low
Malware hidden within a program leverages local credentials to execute but access privileges of the network administrator. Adware appears on the computer.	C, I	Yes	Low	Medium
A cyber criminal uses a pass-the-hash technique to steal passwords and access multiple databases and root accounts.	C	Yes	High	High
The cyber criminal uses privileged access to overwhelm the system with requests, slowing performance and damaging the user experience.	C, I, A	Yes	High	High

By using these classifications and prioritization criteria, organizations can better manage their incident response processes and mitigate cybersecurity risks.

Incident Response Procedures

Incident Response, Disaster & Business Continuity Plans

In our digitally connected world, having an Incident Management Plan in place is a crucial step in ensuring effective and timely response to any cybersecurity incident. As part of The Knowledge House team, your actions and awareness can make a significant difference in our organization's ability to prevent, identify, and recover from security incidents. Specifically, our focus will be on data breaches involving sensitive information like online credit card data, given the nature of our online operations.

The Incident Response Team (IRT) at The Knowledge House should follow these general steps in the event of an incident:

1. Initial Response:

Identification: Our first line of defense will be to establish a consistent process for detecting potential security incidents. This involves actively monitoring our systems, network traffic, and any security alerts.

Incident Confirmation: Once we have detected a potential incident, it falls to the IRT to investigate and confirm the incident's nature, severity, and potential impact. Gathering evidence, reviewing logs, and communicating with relevant stakeholders are key actions at this stage.

Contact Third-Party Cybersecurity Provider: Before proceeding with the initial response, contact Mosyle, our third-party cybersecurity provider. Share the preliminary details of the potential incident. This step ensures that they are informed about the situation at the earliest possible time, and can provide additional resources, expertise, and support as needed.

Involvement of IT Technician: As part of this communication, a Tech Support Specialist should be assigned to the case. The Tech Support Specialist will be actively involved in the following stages of the Incident Response Procedures, working closely with the IRT and providing technical support and guidance.

2. Containment:

Isolation: To prevent further damage, the team will take immediate steps to isolate and contain the incident. This may involve actions such as disabling compromised accounts, isolating affected systems, or blocking malicious network traffic.

Preserve Evidence: It's important to document and preserve any evidence related to the incident for future forensic analysis and potential legal proceedings.

3. Eradication:

Investigation: In this phase, a detailed analysis of the incident is conducted to understand the root causes and identify any vulnerabilities or weaknesses that led to the breach. This may involve analyzing logs, conducting vulnerability assessments, and engaging external experts if necessary.

Remediation: Once we've identified the vulnerabilities and weaknesses, we'll develop and implement a plan to address these. This can include actions such as patching systems, updating security configurations, and removing malware or unauthorized access points.

4. Recovery:

Systems Restoration: After the eradication phase, we aim to restore affected systems and services to their normal operational state, ensuring their security and integrity in the process.
Data Recovery: Any lost or compromised data will be recovered from backups or other reliable sources.
Communication: The IRT will develop a strategy to inform all stakeholders (employees, customers/donors, and relevant authorities) about the incident, its impact, and the recovery steps we've taken.

5. Post-Incident Analysis:
Incident Review: After the incident has been fully resolved, the IRT will conduct a comprehensive review to evaluate the incident response process. This includes examining how the incident occurred, assessing the effectiveness of the response, and identifying any areas for improvement.
Implement Improvements: Based on the incident review, necessary improvements should be implemented to prevent similar incidents in the future. This may involve updating security policies, implementing new technology, or providing additional staff training.
Report and Document: The final incident report will be created and distributed to relevant stakeholders. This report should include a timeline of the incident, an analysis of the incident's cause and impact, a detailed description of the response actions, and recommendations for future improvement.

Our proactive and reactive measures in response to cybersecurity incidents aim to minimize potential damage and ensure that we can resume our operations safely and swiftly. The objective is not just to react to incidents, but to continuously improve our defenses and resilience against future threats. Through active participation and ongoing training, each team member plays a crucial role in maintaining the cybersecurity of our organization.

To demonstrate and improve the effectiveness of The Knowledge House incident response team and security tools, The Knowledge House requires a record of all actions taken during each phase of an incident. Supporting documentation is required, including all forensic evidence collected such as activity logs, memory dumps, audits, network traffic, and disk images.

Incident Reporting Checklist

Everyone in The Knowledge House should feel confident that we are prepared to address cybersecurity incidents effectively. Remember, your role is not just about responding to incidents; it is about being vigilant, informed, and proactive in helping to safeguard our systems and data. Your vigilance and quick action can significantly bolster our collective cybersecurity efforts.

Incident Response, Disaster & Business Continuity Plans

Below is the reporting checklist to use when documenting actions taken to combat a high-level privileged account attack. At The Knowledge House, it is our goal to meet compliance requirements and prioritize business continuity to minimize impact and cost.

Phase of Cyber Incident	Action	Team Member/System	Day/Time Action Taken
Incident Discovery and Confirmation	Describe how the team first learned of the attack (security researcher, partner, customer, auditor, internal security alert, etc.)		
	Analyze audit logs to identify unusual or suspicious account behavior that indicates a likely attack and confirm attack has occurred.		
	Describe potential attacker, including known or expected capabilities, behaviors, and motivations.		
	Identify access point and source of attack (endpoint, application, malware downloaded, etc.) and responsible party.		
	Prepare an incident timeline to keep in ongoing record of when the attack occurred and subsequent milestones in analysis and response.		
	Check applications for signatures, IP address ranges, files hashes, processes, executables names, URLs, and domain names of known malicious websites.		
	Evaluate extent of damage upon discovery and risk to systems and privileged accounts in particular. Audit which privileged		

	accounts have been used recently, whether any passwords have been changed, and what applications have been executed.		
	Review your information assets list to identify which assets have been potentially compromised. Note integrity of assets and evidence gathered.		
	Diagram the path of the incident/attack to provide an “at-a-glance” view from the initial breach to escalation and movement tracked across the network		
	Collect meeting notes in a central repository to use in preparing communications with stakeholders		
	Inform employees regarding discovery.		
	Analyze incident Indicators of Compromise with threat intelligence tools		
	Share information externally about breach discovery. You may choose to hold communications during this phase until you have contained the breach in order to increase your chances of catching the attacker. If so, make sure that aligns with your compliance requirements.		
Containment and Continuity	Enable temporary privileged accounts to be used by the technical and security team to quickly access and monitor systems.		
	Protect evidence. Back up any compromised systems		

	as soon as possible, prior to performing any actions that could affect data integrity on the original media.		
	Force multi-factor authentication or peer review to ensure privileges are being used appropriately.		
	Change passwords for all users, service, application, and network accounts.		
	Increase the sensitivity of application security controls (allowing, denying, and restricting) to prevent malicious malware from being distributed by the attacker.		
	Remove systems from production or take systems offline if needed.		
	Inform employees regarding breach containment.		
	Analyze, record and confirm any instances of potential data exfiltration occurrences across the network		
	Share information externally regarding breach containment (website updates, emails, social media posts, tech support bulletins, etc.)		
Eradication	Close firewall ports and network connections.		
	Test devices and applications to be sure any malicious code is removed.		
	Compare data before and after the incident to ensure systems are reset properly.		

	Inform employees regarding eradication.		
	Share information externally regarding eradication (website updates, emails, social media posts, tech support bulletins, etc.)		
Recovery	Download and apply security patches.		
	Close network access and reset passwords.		
	Conduct vulnerability analysis.		
	Return any systems that were taken offline to production.		
	Inform employees regarding recovery.		
	Share information externally regarding recovery (website updates, emails, social media posts, tech support bulletins, etc.)		
Lessons Learned	Review forensic evidence collected.		
	Assess incident cost.		
	Write an Executive Summary of the incident		
	Report to executive team and auditors if necessary.		
	Implement additional training for everyone involved in incident response and all employees.		
	Update incident response plan.		
	Inform employees regarding lessons learned, additional training, etc.		

	Share information externally (website updates, emails, social media posts, tech support bulletins, etc.)		

Disaster Recovery and Business Continuity

While effective incident response is vital to managing the immediate fallout from cyber attacks or other forms of data breach, disaster recovery and business continuity plans take a longer-term view, addressing the strategies and procedures for restoring operations and ensuring the ongoing resilience of the organization after a significant disruption.

Identifying Critical Aspects and Operations

A key aspect of this planning is understanding what our critical assets and operations are. In the context of The Knowledge House, our critical assets are not just our physical hardware and software, but also our data, and particularly the digital platforms that enable our online course delivery and credit card payment processing system. These systems are essential to our ability to serve our students, process transactions, and function as an organization. If these systems were to be significantly disrupted, it could impact our ability to deliver our services and impact our reputation.

1. *Fellow Sensitive Personal and Financial Information*:

This information includes but is not limited to student identification data, contact information, course enrolment details, academic progress, and financial data related to stipend disbursement. This information is not only vital for our daily operations but also protected by legal and regulatory requirements concerning privacy and data protection.

2. *Online Course Delivery System:*

Our online course delivery system is the backbone of our educational services, facilitating the delivery of course content, communication between students and faculty, and evaluation and grading of student work. Any interruption of this system would directly affect our ability to deliver our services and meet our educational mission.

3. *Credit Card Payment Processing System*:

Our ability to process payments securely and efficiently is crucial to our operations. This system not only allows us to transact with our students but also ensures the privacy and security of their financial information. Disruption to this system would not only affect our financial operations but could also potentially expose us to legal and reputational risks.

In the event of a significant disruption, our disaster recovery and business continuity plans outline the steps we will take to restore these critical systems and ensure the ongoing viability of our operations.

Disaster Recovery Team (DRT)

The Knowledge House has a designated DRT which includes vital personnel from our IT department, the CEO, CTO, and representatives from our third-party cybersecurity partner, Moslye. This team is equipped and prepared to assess, respond, and direct recovery operations in case of a disruptive incident.

Assessment Phase: At the onset of a disaster, the primary responsibility of the DRT is to evaluate the scope of the disruption, the systems affected, and the severity of the impact on operations. This involves classifying the type of incident (natural disaster, cyber attack, human error, etc.), the assets compromised, and the extent of the operational impairment caused by the disaster.

*Restoration Pha*se: The Restoration Phase comes into play once a comprehensive assessment is completed. Depending on the nature and extent of the disruption, this could involve various operations, such as fixing or replacing physical infrastructure, recovering data from backups, or even complete system rebuilds. Our strategic partnership with Moslye is critical during this phase, providing expert guidance and resources to expedite recovery efforts.

DRP Testing: An untested DRP can lead to an inefficient response during a real crisis. Regular simulation exercises will be conducted to challenge our disaster response procedures, giving the DRT practical experience and revealing any weaknesses or gaps in the plan. These simulations will be followed by a thorough review process to continuously improve and update the DRP.

Business Continuity Plan

While our DRP focuses on the technical aspects of disaster recovery, the Business Continuity Plan (BCP) ensures that the broader operational functionality of The Knowledge House remains intact during and following a significant disruption. Business Continuity Team (BCT):

The BCT is composed of the same members as the DRT, reflecting the close interconnection and complementary nature of our disaster recovery and business continuity strategies.

Business Impact Analysis (BIA)

In the wake of a disruptive incident, the BCT will carry out a detailed BIA. This analysis will include an assessment of the disruption's impact on our primary operations, such as course delivery and payment processing, and the broader implications for our organization, including reputational and financial effects.

Continuity Planning: The Continuity Planning phase is initiated based on the findings of the BIA. The BCT will create and implement a plan to ensure the continuation of our services. This might involve the use of alternative course delivery methods, increased communication with students and staff, or temporary adaptations to our usual procedures.

BCP Testing: Like the DRP, regular testing and updating of the BCP are vital to ensure it can effectively guide us through a real crisis. Regular drills will be conducted, allowing the BCT to refine the plan and ensure its effectiveness.

Incident Response, Disaster & Business Continuity Plans

THE KNOWLEDGE HOUSE

The importance of disaster recovery and business continuity planning cannot be overstated for The Knowledge House. By being prepared for any disruptions, we ensure that our commitment to our students and our mission continues unhindered.

Compliance and Legal Obligations

As an educational non-profit organization operating in the states of New York, Georgia, and California, The Knowledge House is subject to various legal and compliance requirements, particularly in the areas of data privacy and security. This includes obligations under state laws for non-profit organizations, federal laws concerning data protection, and specific standards like the Payment Card Industry Data Security Standard (PCI DSS) and the National Institute of Standards and Technology's Special Publication 800-171 (NIST 800-171).

PCI DSS Compliance: Our credit card payment processing system involves the handling of sensitive cardholder data, making us subject to the PCI DSS. This requires us to implement strong access control measures, regularly monitor and test networks, maintain a vulnerability management program, protect stored cardholder data, encrypt transmission of cardholder data across public networks, and maintain an information security policy.

NIST 800-171 Compliance: Our Incident and Disaster Response and Recovery and Business Continuity Plan are part of a larger security program that complies with the NIST 800-171. This involves safeguarding and distributing material deemed sensitive but unclassified (CUI). As such, we are obligated to ensure that we maintain systems capable of limiting access to such information and respond effectively to potential security incidents.

Non-Profit State and Federal Laws: Being a non-profit organization, we're subject to a variety of laws at the state and federal level. This includes requirements for financial transparency, restrictions on political activities, and obligations to use funds for their intended purpose. We must also comply with various employment laws, such as equal employment opportunity regulations and workplace health and safety standards.
Data Protection Laws: We must adhere to the data protection regulations of New York, Georgia, and California, as well as federal laws. This includes laws related to the collection, use, and protection of personal data, particularly in the context of our students' personal information and our online educational platforms.

Incident Reporting: In the event of a significant incident, such as a data breach, we have legal and compliance obligations to report these incidents to various stakeholders. This can include notification to affected individuals, reporting to state regulators, and potentially informing federal authorities. These reporting obligations can be subject to specific timeframes, and failure to report can result in significant penalties.

By clearly documenting these legal and compliance requirements as part of our incident response plan, we are prepared to respond immediately to any incident, ensuring we

meet our obligations without the need for time-consuming legal discovery during a crisis.

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.

THE KNOWLEDGE HOUSE

Additional Resources and References

Accenture. (2019). Ninth Annual Cost of Cybercrime Study.

Accenture. (2019). The True Cost of Cybercrime.

Bertino, E., & Ghinita, G. (2021). Cybersecurity and Privacy in Databases. Springer.

CERT Division, Software Engineering Institute, Carnegie Mellon University. (2018). Defining Incident Management Processes for CSIRTs: A Work in Progress. Retrieved June 11, 2023, from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=538927

Cisco. (2021). 2021 Cybersecurity Report: Empowering Your Business to Close the Cybersecurity Gap.

Centre for the Protection of National Infrastructure (CPNI). (2018). Cyber Security Incidents: A Good Practice Guide for Incident Management. Retrieved June 11, 2023, from https://www.cpni.gov.uk/cyber-security-incidents

Cybersecurity & Infrastructure Security Agency (CISA). (2019). Cyber Incident Response. Retrieved June 11, 2023, from https://www.cisa.gov/cyber-incident-response

Cybersecurity & Infrastructure Security Agency (CISA). (2021). Cybersecurity Resources Road Map: A Guide for Critical Infrastructure SMBs.

Cybersecurity Ventures. (2021). Official Annual Cybercrime Report.

Cybersecurity Ventures. (2021). Cybercrime To Cost The World $10.5 Trillion Annually By 2025.

Deloitte. (2020). Deloitte's 2020 Future of Cyber Survey.

Delinea. (n.d.). Free Incident Response Plan - Fully Customizable Template. Retrieved June 11, 2023, from https://delinea.com/resources/free-incident-response-plan-template

F5 Labs. (2020). 2020 Application Protection Report.

Gartner. (2020). Business Continuity Management Program Primer for 2021.

Gartner. (2022). Top Security and Risk Management Trends.

IBM. (2019). Cost of a Data Breach Report.

IBM. (2021). Cost of a Data Breach Report.

IBM. (2021). Cyber Resilient Organization Report.

IDG. (2021). Security Priorities Study. International Data Group.

IT Governance. (2022). Cyber Resilience Green Paper. IT Governance Publishing.

Javelin Strategy & Research. (2019). 2019 Identity Fraud Study: Fraudsters Seek New Targets and Victims Bear the Brunt. Retrieved June 11, 2023, from https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-study-fraudsters-seek-new-targets-and-victims-bear-brunt

McAfee. (2021). Economic Impact of Cybercrime.

Microsoft. (2021). Microsoft Digital Defense Report.

MITRE Corporation. (2020). ATT&CK for Enterprise. Retrieved June 11, 2023, from https://attack.mitre.org/matrices/enterprise/

National Archives & Records Administration. (2020). Vital Records and Records Disaster Mitigation and Recovery.

National Cyber Security Alliance. (2021). Small Business Online Security Infographic.

National Institute of Standards and Technology. (2012). Guide for Conducting Risk Assessments. doi:10.6028/NIST.SP.800-30r1

National Institute of Standards and Technology. (2013). Security and Privacy Controls for Federal Information Systems and Organizations. doi:10.6028/NIST.SP.800-53r4

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity.

Payment Card Industry Data Security Standard (PCI DSS). (2020). Maintaining Payment Security.

Ponemon Institute. (2021). 2021 Cost of a Data Breach Report.

Privacy Rights Clearinghouse. (2022). Chronology of Data Breaches. Privacy Rights Clearinghouse.

PwC. (2021). Digital Trust Insights.

SANS Institute. (2018). Incident Handler's Handbook. Retrieved June 11, 2023, from https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

SANS Institute. (2021). The Essential Guide to Cybersecurity for SMBs.

Symantec. (2021). Internet Security Threat Report.

U.S. Securities and Exchange Commission. (2020). The Importance of Cybersecurity Policies and Procedures.

Varonis. (2021). 2021 Data Risk & Security Report.

Verizon. (2018). Vocabulary for Event Recording and Incident Sharing (VERIS). Retrieved June 11, 2023, from http://veriscommunity.net/

Verizon. (2020). Verizon's 2020 Data Breach Investigations Report.

Verizon. (2021). 2021 Data Breach Investigations Report.

World Economic Forum. (2020). The Global Risks Report 2020.

ZDNet. (2021). A Winning Strategy for Cybersecurity.

Incident Response, Disaster & Business Continuity Plans

Secure Program Capstone 2023
Project Manager & Author: Jane Pierre
Research Contributors: Elizabeth Bond, Mishelly Sandoval, Lucas Higgs, Shamar Brown, Tianna Green, Frederick Asante, Jonathan Henao and Aaron Kaah

COPYRIGHT NOTICE AND DISCLAIMER