# Welcome to The Knowledge House Incident and Disaster Recovery & Business Continuity Plans

This presentation is a critical part of our commitment to securing The Knowledge House's operations, data, and trust of our stakeholders. Our discussion today will revolve around the importance of incident response, disaster recovery, and business continuity for The Knowledge House. We aim to illustrate our strategies to safeguard our systems and data, emphasizing how each team member plays a crucial role in these processes.

# The Cost of Cyber Incidents

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

# Incident Response and Recovery

# What is an Incident Response Plan?

An Incident Response Plan is a set of strategic guidelines designed to help us detect, respond to, and recover from security incidents. These incidents vary in severity, ranging from unintentional disclosure of confidential information by an employee to more severe scenarios like cyberattacks or data breaches.

# Components of an Incident Response Plan

Our Incident Response Plan is structured into five stages - Initial Response, Containment, Eradication, Recovery, and Post-Incident Analysis. Each stage has specific procedures designed to minimize the impact of the incident and ensure efficient recovery.

# Initial Response: Identification

The first step in any response strategy is identification. We actively monitor our systems, network traffic, and any arising security alerts, striving to detect and evaluate any unusual activity that could indicate a potential security incident.

# Initial Response: Incident Confirmation

Once we've identified potential unusual activity, the Incident Response Team (IRT) must validate if it's a legitimate security incident. This involves gathering evidence, scrutinizing logs, and communicating with relevant stakeholders to ascertain the situation.

# Containment: Isolation

Upon confirming a security incident, the immediate priority is to prevent further damage. This may involve disabling compromised accounts, isolating affected systems, or blocking malicious network traffic to halt the spread of the threat.

# Containment: Preserve Evidence

While containing the incident, it is essential to document and preserve any evidence meticulously. This information is valuable for future forensic analysis, aiding in understanding the attack and potentially necessary for legal proceedings.

# Eradication: Investigation

After containment, we move to understand what triggered the incident. This stage involves conducting a thorough investigation to identify the root causes and any vulnerabilities or weaknesses that might have contributed to the incident.

# Eradication: Remediation

Identifying the weaknesses that led to the incident allows us to develop and implement a plan to address them. Remediation actions can range from patching systems and updating security configurations to removing malware.

# Recovery: Systems Restoration

The recovery phase involves restoring the affected systems and services to their normal operational state. We diligently ensure the systems are secure and that our data integrity is uncompromised in the process.

# Recovery: Data Recovery

In scenarios where data was lost or compromised during the incident, we utilize backups or other reliable sources to recover it. Our primary goal is to minimize data loss and restore operations swiftly and securely.

# Recovery: Communication

Transparent and timely communication plays a key role in the recovery phase. We ensure all stakeholders are informed about the incident, its impact, and the steps we're taking to recover and prevent similar incidents in the future.

# Post-Incident Analysis: Incident Review

Once the incident is resolved, we conduct a comprehensive review of the incident response process. This evaluation is crucial in assessing how the incident occurred, how effective the response was, and identifying areas for improvement.

# Post-Incident Analysis: Implement Improvements

Based on the incident review, we identify and implement necessary improvements to prevent similar incidents in the future. This could involve updating security policies, implementing new technology, or providing additional staff training.

# Post-Incident Analysis: Report and Document

The final step in our incident response process is to generate and distribute an incident report to relevant stakeholders. This report includes a timeline of the incident, an analysis of its cause and impact, a detailed description of the response actions, and recommendations for future improvement.

# The Importance of Incident Response

Rapid incident response can significantly reduce the cost of a data breach. Companies that contained a breach in less than 30 days saved over $1 million compared to those that took more than 30 days. Effective incident response plans can also reduce the time to contain a breach, further minimizing impact.

# Incident Response: Conclusion

The incident response process is dynamic and should be regularly reviewed and updated to reflect changes in technology, threats, and organizational requirements. The goal is not just to react to incidents, but to continuously improve our defenses and resilience against future threats.

# Disaster Recovery & Business Continuity

# Business Continuity and Disaster Recovery in Numbers

93% of companies without disaster recovery who suffer a major data disaster are out of business within one year. Only 50% of organizations feel prepared to respond to a disaster recovery event. Effective business continuity and disaster recovery plans are a critical investment to ensure the survival and success of our operations.

# What is Disaster Recovery and Business Continuity?

**Disaster Recovery** involves restoring our critical IT systems following a disaster, while **Business Continuity** ensures that we can continue to operate during a disruption. Both are essential for maintaining the trust of our students, donors, and other stakeholders.

# Identifying Critical Assets and Operations

Identifying critical assets and operations is a key step in disaster recovery and business continuity planning. At The Knowledge House, these include our online course delivery system and our credit card payment processing system.

# The Importance of Online Course Delivery System

Our online course delivery system is the backbone of our educational services. It enables us to provide high-quality, accessible learning opportunities to our students. A disruption to this system could significantly impact our ability to educate our students.

# The Importance of Credit Card Payment Processing Systems

Our credit card payment processing system is another critical asset. It allows us to process payments from students and donors efficiently. Any disruption could impact our revenue and donor confidence

# Disaster Recovery: Key Steps

Disaster recovery involves the following steps:

1. Assessment: Understanding the nature and extent of the disaster.
2. Restoration: Bringing our systems back to their operational state.
3. Testing: Ensuring the restored systems work as intended.
4. Documentation: Keeping a detailed record of all disaster recovery actions.

# Business Continuity: Key Steps

Business continuity focuses on maintaining operations during a disruption. It involves:

1. Business Impact Analysis: Identifying crucial business functions and resources.
2. Risk Assessment: Identifying threats to these functions and resources.
3. Implementation: Creating and implementing the continuity plan.
4. Training: Educating staff on the plan and their roles.
5. Testing: Conducting regular tests to ensure the plan is effective.

# Disaster Recovery and Business Continuity: Conclusion

Planning for disaster recovery and business continuity is a continuous process. As our organization grows and changes, so should our plans. Regular reviews and updates, along with staff training, are essential for keeping our plans effective.

# Building a Stronger Cybersecurity Culture at TKH Together

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