WSCC Incident Response Plan

Introduction

The Incident Response Plan for Washington State Community College has been created to provide a structured and comprehensive approach to effectively respond to and mitigate incidents that may occur within our institution. This plan outlines the necessary steps, roles, and responsibilities to ensure a swift and coordinated response, aimed at minimizing the impact of incidents on the college community, its resources, and its reputation.

At Washington State Community College, we recognize the importance of maintaining a safe and secure environment for our students, faculty, staff, and visitors. This plan serves as a proactive measure to identify and address potential incidents that could disrupt our operations, compromise sensitive information, or endanger the well-being of individuals within our community.

Roles and Responsibilities

The successful execution of the incident response plan at Washington State Community College relies on the involvement and coordination of the whole IT Department. The department operates with a shared governance model, and as such incident response is the responsibility of all departmental staff members. However, these efforts are coordinated by the senior Information Systems Analyst and the Network and Systems Admin. These positions will serve as the primary contact points for incident response and will provide updates and findings to the VP of Organizational Effectiveness.

The VP of Organizational Effectiveness has the responsibility to report the incident and any accompanying information to the rest of management and leadership. The VPOE will coordinate with the college's president and vice presidents to allocate funds and resources for incident response as required, as well as work with the marketing department and other positions to coordinate the college's messaging regarding the incident.

Faculty, staff and students also play a vital role in incident response by promptly reporting incidents, following incident response procedures, and participating in security awareness training programs. It is important that all individuals understand their roles and responsibilities, and actively contribute to incident response efforts. Regular training and awareness programs help ensure that everyone is prepared to fulfill their responsibilities effectively.

Preparation and Prevention

At Washington State Community College, we are committed to safeguarding our institution through regular risk assessments. These assessments have identified several key risks, including ransomware attacks, compromised systems, data leaks, and DDoS attacks.

To proactively prevent incidents and ensure the security of our college, the IT department has taken several measures. An on-going partnership with a trusted third-party cybersecurity provider has been developed to enhance our defense against cyber threats. Their expertise and advanced security solutions help us mitigate risks and respond effectively to incidents.

The IT department regularly conducts security awareness training programs in collaboration with a reputable third-party organization. These programs educate our staff, faculty, and students about best practices, potential risks, and incident reporting procedures, fostering a culture of vigilance and proactive involvement in maintaining a secure environment. A next-generation firewall with Intrusion Detection System (IDS) capabilities has been deployed to strengthen network security. This firewall provides effective control over network traffic and protects external services from unauthorized access and potential threats.

WSCC's data backup system follows the robust industry-standard 3-2-1 method, ensuring the redundancy and availability of critical data and systems. It can instantly create and deploy virtual copies of servers, whether on-premises or in the cloud, enabling quick recovery and minimal downtime in case of incidents.

The IT department has deployed a high availability server cluster, which ensures continuous availability of critical services and applications. This cluster can withstand the failure of up to two servers without causing service outages or disruptions. Through fault-tolerant technologies like load balancing and automatic failover, system reliability and uninterrupted access to essential services is maintained.

The college utilizes enterprise-grade antivirus software on systems and endpoints. This comprehensive solution detects and prevents malware, viruses, and other malicious activities. The central administration of this software ensures the security of our servers and endpoints, and alerts IT staff members to detections immediately.

Through these proactive measures, Washington State Community College aims to prevent incidents, safeguard sensitive data, and maintain a secure environment for our students and employees.

Incident Identification and Reporting

IT security incidents cover a wide range of possible circumstances and severity levels. These include instances such as sharing sensitive data, confidential documents or login credentials with unauthorized parties; clicking on suspicious links in phishing emails; detecting unusual network traffic patterns that suggest potential security breaches; malware or ransomware infection; zero-day exploitation; and observing suspicious activity like unauthorized access to the Network Operations Center (NOC).

Incidents should be reported to PCService@wscc.edu or the contacts listed in the roles and responsibilities section of the plan. These designated contacts are the main channels for reporting incidents. In urgent situations, like ransomware and fully compromised systems, the IT Department will contact third party cybersecurity firms already under contract for additional support.

Reporting incidents is a shared responsibility among our staff, faculty, and students. It is important for everyone to promptly report any suspected or confirmed incidents using the designated reporting channels or contacts mentioned above. When reporting, individuals should provide accurate and detailed information

about the incident, including its nature, observable symptoms or effects, and any relevant contextual details. Additionally, it is crucial for all stakeholders to cooperate with the incident response team by providing any requested additional information or assistance with investigations.

By actively engaging in incident reporting, our staff, faculty, and students play a crucial role in upholding the security and well-being of our college community. Together, we can effectively address incidents, protect sensitive information, and maintain a secure environment for teaching, learning, and collaboration.

Initial Response

The initial response phase is crucial in promptly addressing incidents and minimizing their impact. Washington State Community College follows a structured approach to ensure an effective initial response. The following steps are taken:

1. **Notification of Incident**: Once any indication of an incident is discovered, it is the responsibility of the individual who identified it to report it to the IT department. This can be done through email by sending an explanation of what happed to PCService@wscc.edu. If the nature of the Incident is a fully compromised system, then it is recommended that you also try to make contact via phone to make sure immediate action is taken.
2. **Engagement of IT**: Once IT is made aware of an incident it is up to that individual to alert the rest of the team and to relay any important information.
3. **Immediate Action**: In the event of an incident, immediate action is necessary to contain and control the impact of the incident. This includes quarantining the affected endpoints from the network, disabling user account access and sanitization of the rest of the environment to make sure the incident stays as localized as possible.
4. **Information Gathering**: after the incident is contained then the IT department can gather more data from on the initial cause of the issue. How far it may have spread and who all may be at risk.
5. **Communication**: Once the initial assessment of the incident has been made IT will need to communicate any information to staff of service outages along with an initial report of this incident to the VP of Organizational Effectiveness.
6. **Engagement of Third-Party Support**: Third party support will be contacted in case of a significant incident or threat such as ransomware. Third parties may need to be contacted to help remediate of give direction on best practices in these situations.

By following this structured initial response approach, Washington State Community College aims to swiftly address incidents, contain their impact, and set the foundation for a comprehensive and coordinated incident response.

Assessment and Investigation

To ensure an effective response to incidents at Washington State Community College, a thorough assessment and investigation process is followed. This section outlines the key steps taken to assess the impact and severity of incidents and to conduct comprehensive investigations.

1. **Initial Assessment**: Upon the discovery and report of an incident, an initial assessment is conducted to determine its potential impact. This assessment considers various factors; whether sensitive data was compromised, the scale of the incident, and any service outages caused.
2. **Evidence Preservation**: Preserving evidence is key in incidents like data leaks, compromised systems, or suspicious activity. It helps with further analysis and possible legal actions. We take steps to keep important data, logs, network traffic records, and other evidence secure for investigations.
3. **Root Cause Analysis**: A comprehensive investigation is conducted to determine the root cause of the incident. This analysis involves examining logs, system configurations, network traffic, and other relevant data to identify the underlying vulnerabilities or weaknesses that led to the incident.
4. **Coordination with Third Parties**: In some situations, we may seek the help of third-party cybersecurity firms with their expertise and assistance during investigations. Collaborating with these firms can offer valuable insights, specialized tools, and extra resources to aid in the investigation process.
5. **Data Breach Analysis**: In situations where data breaches or leaks occur, we conduct a comprehensive analysis to assess the full impact of the unauthorized access or exposure of sensitive information.
6. **Documentation and Reporting**: During the assessment and investigation phase, we keep detailed records of our findings. This documentation is important for future reference, future analysis, and to provide to law enforcement.
7. **Remediation and Preventive Measures**: After completing the investigation, we take necessary steps to address the incident and minimize its impact while also preventing similar incidents in the future. This could involve fixing vulnerabilities, strengthening security measures, updating policies and procedures, and providing extra training or awareness programs for our staff, faculty, and students.

By following this comprehensive assessment and investigation process, Washington State Community College can effectively analyze incidents, determine root causes, implement remediation measures, and enhance its overall security posture.

Response, Recovery and Remediation

The response and recovery phase is critical in minimizing the impact of incidents and restoring normal operations at Washington State Community College. The following steps are taken during this phase:

1. **Mitigation Strategies**: Immediate actions are taken to lessen the impact of the incident and prevent further harm. This may be isolating affected systems, removing harmful software, recovering data from backups, or applying updates to fix vulnerabilities.
2. **Restoring Resources**: At this stage Washington State Community College would be working to restore systems back to their functional state. This may include fixing or replacing compromised hardware, adjusting software and network settings, or recovering data from backups.
3. **Communication and Coordination**: Clear and consistent communication is maintained with relevant people throughout the response and recovery phase. Regular updates are provided on the progress of recovery efforts, expected timelines, and any necessary precautions or instructions.
4. **Business Continuity**: If the incident has caused disruptions to critical operations, a business continuity plan is put into action. This plan outlines procedures to restore systems that are the most

crucial to operation. Once those systems are operational then the IT department would then transition to other subjacent sytems.

5. **Analysis after the Incident**: Once the incident is resolved and operations return to normal, a thorough analysis is conducted to learn from the incident. This analysis involves reviewing the actions taken during the incident response, identifying strengths and areas for improvement, and capturing lessons learned. The findings from this analysis would be used to improve future responses.
6. **Updating Policies and Procedures**: Based on the lessons learned, relevant policies and procedures are reviewed and updated to address any identified weaknesses or gaps. This includes making changes to security measures, incident response protocols, training programs, and preventive controls.
7. **Training and Awareness**: Ongoing training programs and awareness initiatives are conducted to keep staff, faculty, and students informed about incident response procedures, best security practices, and the evolving threat landscape. These programs help foster a culture of security and preparedness.

By following this structured response and recovery approach, Washington State Community College aims to minimize the impact of incidents, restore normal operations, and improve overall incident response capabilities.

Training and Awareness

Washington State Community College understands that cyber threats are always changing and it's crucial to equip our staff, faculty, and students with the latest knowledge and skills to tackle these risks. To make this happen, we have teamed up with a trusted cybersecurity education provider to introduce modern training programs.
Our training programs use engaging videos, interactive quizzes, and tests that mimic phishing attacks to create an immersive and effective learning experience. Through these methods, we aim to raise awareness, educate participants about current cyber threats, and give them the tools to recognize and handle potential risks.

Engaging Videos: Our training modules include interesting videos that show real-life situations and the impact of cyber threats. These videos teach participants about different types of attacks, like phishing, social engineering, malware, and ransomware. By using visual storytelling, we help people understand and remember important cybersecurity concepts.
Interactive Quizzes: We also include quizzes to reinforce the knowledge gained from the videos. These quizzes let participants test their understanding and application of cybersecurity best practices. Getting instant feedback helps them solidify their understanding and grasp the training material more deeply.
Phishing Simulation Tests: Since phishing attacks are common, we regularly run tests to replicate real-world scenarios and assess participants' ability to recognize and respond to phishing emails effectively. These simulations increase awareness, improve response skills, and encourage caution when dealing with suspicious emails or links.

Our collaboration with a third-party provider ensures that our training programs benefit from the expertise and industry insights of cybersecurity professionals. By staying up-to-date with the latest threats, industry trends, and best practices, we deliver comprehensive and relevant training content to keep our community well-prepared.

Conclusion

The Incident Response Plan for Washington State Community College provides a comprehensive framework to effectively address and mitigate incidents that may occur within our institution. By establishing clear procedures, roles, and responsibilities, we aim to safeguard the college community, its resources, and its reputation.

The plan encompasses various crucial elements, including risk assessment, prevention measures, incident identification and reporting, assessment and investigation, response and recovery, post-incident analysis, and ongoing training and awareness. These components work together to create a proactive and robust incident response capability.

At Washington State Community College, we recognize the ever-evolving nature of cyber threats and the importance of preparedness. By contracting third-party cybersecurity firms, utilizing modern training programs, and engaging in continuous improvement through post-incident analysis, we strive to stay ahead of emerging risks and protect sensitive data and systems.

We emphasize the shared responsibility of all staff, faculty, and students in promptly reporting incidents, adhering to incident response procedures, and actively participating in security awareness initiatives. Together, we can create a culture of vigilance and preparedness, enhancing the overall security posture of our college.

Washington State Community College remains committed to providing a safe and secure environment for its community members. Through effective incident response planning and proactive measures, we are well-prepared to mitigate the impact of incidents and swiftly recover from disruptions. Together, we can navigate the ever-changing landscape of cybersecurity and uphold the integrity and resilience of our institution.