GRC Mastery Case Study: Cyber Security Incident Response

GRC Mastery Case Study: Cyber Security Incident Response

Scenario

Attached is the publicly available Cyber Security Incident Response Plan for Virginia Tech.

Instructions

As a Cyber Security Consultant you're tasked with understanding and assessing the cyber security incident response plan.

The following questions can be answered using the information provided in the attached plan.

What is the main purpose of the Virginia Tech Cybersecurity Incident Response Plan?

To provide a disaster recovery guide for natural disasters

To outline the process for information technology upgrades

To assist personnel in handling cyber incidents effectively- Correct

To establish financial audit procedures

Who has full authority to act in response to cyber incidents at Virginia Tech?

President of the University

IT Security Officer (ITSO)- Correct

Data Trustees and Stewards

Faculty Council

When should the CIRT (Cyber Incident Response Team) be activated?

Only for enterprise or multi-departmental level incidents- Correct

When a local departmental incident occurs

For any incident involving faculty systems

Whenever an external audit is scheduled

What are the six elements of cyber incident response mentioned in the plan?

Documentation, Coordination, Communication, Recovery, Restart, Reassess

Planning, Testing, Budgeting, Reporting, Analysis, Cleanup

Training, Planning, Logging, Monitoring, Reporting, Closure

Preparation, Identification, Containment, Eradication, Recovery, Post-incident activities- Correct

Which document provides guidance for handling incidents involving personally identifiable information (PII)?

Appendix D – Sensitive Data Notification- Correct

Appendix F – Compromise Questionnaire

Appendix H – Notification of Outside Organizations

Appendix A – CIRT Organizational Chart

What is a primary goal of the containment phase?

Immediately notify the media

Prevent attackers from further damaging systems and stealing data- Correct

Restore normal operations as quickly as possible

Train staff to use new systems

How should a cyber incident be reported?

Through email, phone, or initiating a Service Now trouble ticket- Correct

By notifying the public immediately

Through social media announcements

By sending a written report to the university president

What is the final phase of incident response?

Analysis

Recovery

Containment

Incident Closure- Correct

What metric determines when to escalate a cyber incident to enterprise level?

Level of funding involved

Severity and impact affecting multiple departments- Correct

Number of staff members affected

Time elapsed since incident detection

What is a key takeaway from the post-incident phase?

To implement new software immediately

To issue fines to the responsible parties

To stop using affected systems permanently

To create a follow-up report and hold a lessons learned meeting- Correct

Recommendations:

GRC Mastery by Abed Hamdan