Course: IT RISK MANAGEMENT AND CONTROL

Week 9

Topic: Incident Management and Response

Lecturer: Ninyikiriza Deborah Lynn

TODAYS outline

1. Review of week 8 Material
2. Incident Response Planning
3. Incident Detection and Reporting
4. Managing and Recovering from Incidents

Week 8 Review

Before we start looking at week 9 material, let’s first do a q uick review of our previous lecture material (week 8)

In week 8, we discussed the following;

1. Access control and Identity Management (AIM)

- A critical component of IT risk management and control which focuses on managing and securing user identities , access rights, and permissions within an organization.

Week 8 Review

2. Access

- The ability of a subject (user) and an object (computers) to int eract.

3. Access Control

- Access control is the process of following rules to allow or de ny access to the computer user.

4. The access control process steps;

- 1. Identification: The process by which a subject identifies its elf to the access control system.
- 2. Authentication: Verification of the subject's identity.
- 3. Authorization: The decision to allow or deny the subject to access an object.

Week 8 Review

5. Authentication methods;

1. Password: A secret word or combination of characters that is known o nly to the subject.

2. Token: Something the subject has that no one else does, such as a s mart card, driving license, passport etc.

3. Fingerprint scan: Involves optical analysis of a person's fingerprint the n compare the results with the recorded sample to verify his /her identity.

6. Principal components of any access control

Policies—The rules that govern who gets access to which resources.

Subjects—The user, network, process, or application requesting access t o a resource.

Objects—The resource which the subject desires to access (e.g, files, da tabases, printers, and physical facilities).

Week 8 Review

- ***7. Elements of access control***
- Policies—Clear statements of the business requirements r egarding access to resources.
- Procedures—Nontechnical methods, such as business pr ocesses and background checks, used to enforce policies.
- Tools—Technical methods, such as file system access co ntrols and network firewalls, used to enforce policies.

Week 8 Review

8. subjects of access control

Authorized: Have presented authenticated credentials and have been approved for access to the resource.

Unauthorized: Have presented authenticated credentials but ar e not approved for access to the resource.

Unknown: Have not presented authenticated credentials.

9. Objects of Access control

- Information—Any type of data
- Technology—Applications, systems, and networks
- Physical location—Physical locations such as buildings and r ooms.

Week 8 Review

10. Principles of Access Control

1. Identification Principle

- Identification is the process of recognizing and distinguishing an individual or entity in the system

2. Authentication Principle

- Authentication verifies the identity claimed during the identification phase.

3. Authorization Principle

- Authorization determines what a user is allowed to access or perform within the system.

Week 8 Review

4. Accountability Principle

- Accountability ensures that actions can be traced back to spe cific individuals or systems, providing an audit trail of access and activity.

5. Least Privilege Principle

- Least privilege grants users only the minimum level of access necessary to perform their duties

6. Separation of Duties principle

- Separation of duties ensures that no single individual has con trol over all aspects of any critical or high-risk process.

Week 8 Review

7. Need-to-Know principle

- Need-to-know restricts access to data based on specific requirements for users to complete their job tasks.

11. Is Identity Management

- Identity management is the process of creating, maintaining, and closing u ser accounts and providing the mechanisms used to authenticate users

12. Identity and Access Management (IAMs)

- Identity and Access Management systems are tools and processes that hel p organizations manage who can access their digital resources and what t hey can do within those resources

.

Week 8 Review

13. Elements of IAMs

1. Identity Management

- IAM systems aim to create and manage the digital iden tities of users within the organization

2. Access Management

- IAM systems control which resources each user can ac cess and what actions they can perform.

3. Authentication management

- IAM systems verify that a user’s identity is legitimate be fore allowing access.

Week 8 Review

4. Authorization

- AIMs enforce access rules that determine what each authenticated us er is allowed to do within the system.

5. Monitoring and Auditing

- IAMs track user activities and ensure that access policies are followed.

14. Advantages IAMs

- Improved Security: IAM systems reduce unauthorized access, ensurin g that only the right people can access sensitive information.
- Better Compliance**:** They help organizations to comply with regulations by keeping records of who accessed what information and when.
- Enhanced Efficiency**:** IAMs automates access management, making it easier for IT teams to onboard, offboard, and manage user access.

Week 8 Review

14. Best Practices for Access Control

1. Apply the Principle of Least Privilege

2. Enforce Role-Based Access Control

Enforce Role-Based Access Control

3. Implement Multi-Factor Authentication (MFA)

4. Regularly Review and Audit Access Permissions

5. Utilize Separation of Duties

6. Adopt the Need-to-Know Principle

7. Implement Strong Password Policies

8. Log and Monitor Access Activities

9. Educate Employees on Access Control Policies

Week 9: Incident Management and Response

- Incident Management and Response in IT risk managemen t and control refers to the structured approach of detecting, responding to, managing, and recovering from IT-related in cidents, particularly cybersecurity threats.
- IMR is critical within IT risk management as it helps organiz ations to address incidents effectively, minimize their impac t, protect sensitive data, and ensure business continuity.

Incident Management and Response

- Strategies are built around the assets of concern, thinking thr ough risks and attacking scenarios likely to occur.
- The incident response plan is built on a strategy of detection, containment, and eradication of intrusions and infections befo re they impact sensitive data and business operations.
- In analysis, fundamental protection and prevention capabilitie s are included alongside detection and response measures.
- These measures are built around use cases and derived fro m the attack scenarios identified to deploy resources and buil d the strategic objectives of the incident response plan.

The Incident Response Strategy

- The incident response plan forms the strategy for respondi ng to events and incidents.
- The plan contains the purpose, scope, definitions and ele ments of incident response.
- Roles and responsibilities, definitions and escalation step s are common elements addressed in the incident respons e plan.
- The purpose of the plan presents the team with the “why” behind the plan. Why does the cybersecurity team care ab out planning for events and incidents? And why will time a nd money be invested in improving the company’s ability t o successfully respond to incidents?

The Incident Response Strategy

- The scope of the plan highlights the authorization given th e incident response team to take necessary steps when de aling with events.
- Roles and responsibilities dictate who is on the response t eam and how he or she is expected to act when events ar e investigated.
- In the response strategy, definitions such as for questions l ike What is an event, an incident or a breach are important as well.

The Incident Response Strategy

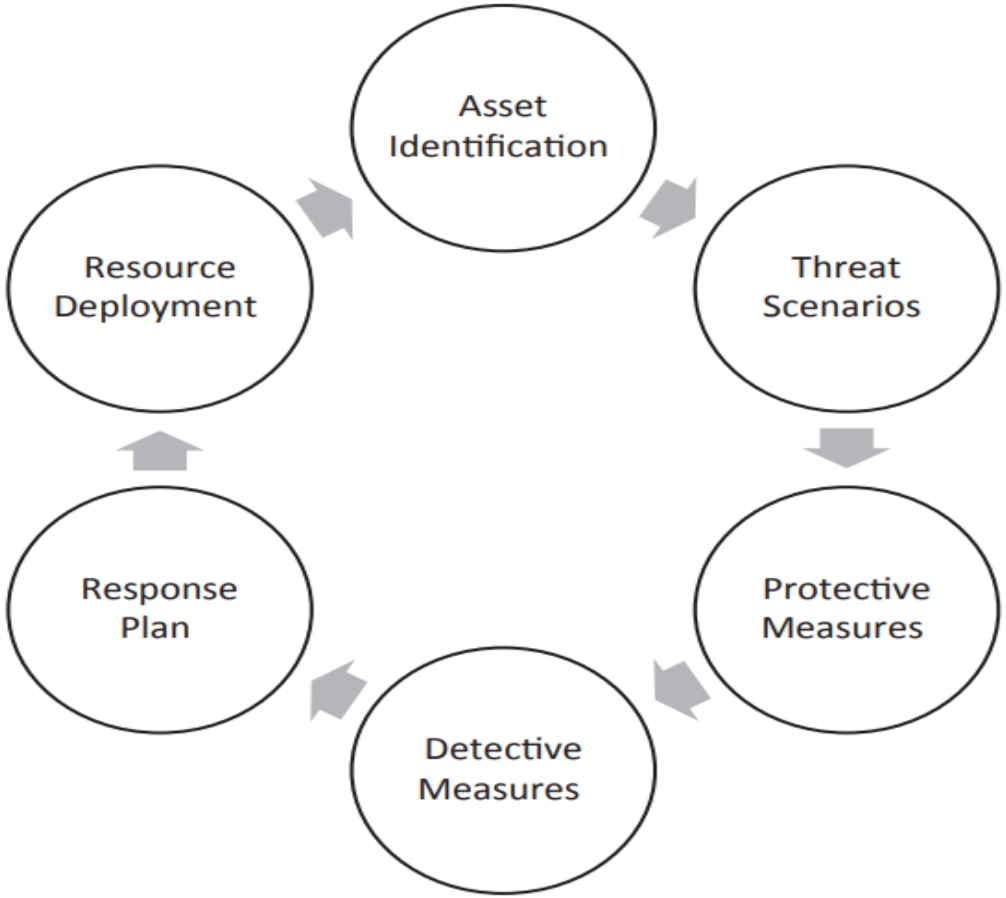

Figure 1: Cyclical approach to building a strategic response plan

Incident Response Planning

- Incident response plans are designed to protect the organization, maintain the confidentiality, integrity, and availability of data and other data assets, to avoid disruptions to business and reputational damage.
- Data assets include intellectual property, trade secrets, strategy, company financials and customer information.
- If these elements are affected by an incident, the organization could have varying degrees of impact.
- This is why the incident response team exists.

Incident Response Planning

Qn: What are the Incident Response Goals for any organization?

- The goals of incident response vary from organization to organization however common ones include the following;
  - ✓ To protect the organization’s infrastructure, assets, and business operations.
  - ✓ To comply with federal, state, and local regulations.
  - ✓ To minimize the potential for negative publicity.
  - ✓ To prevent or minimize financial liabilities.
  - ✓ To minimize customer disruptions

Incident Response Planning

Roles and Responsibilities in incident response planning;

- Roles and responsibilities state the expectations of each perso n on the team.
- The team includes, a group of legal and compliance members, IT leadership members, external consultants, a group of senior management and external legal counsel.
- Within their groups, each of the individuals has a role in incide nt response.

Incident Response Planning

Roles and Responsibilities con't…

- No matter how the groups are organized and named, missing defined roles and responsibilities opens the door to chaos an d actions not aligned with the incident response plan.
- It is therefore important to discuss and understand the roles o f each member within their groups, and the need to stick to ac tions outlined in each group .
- Post response reviews going over roles and responsibilities e mphasizes the need to adhere to what’s outlined in the plan.

Incident Response Planning

How to Respond to Incidents

- Within the incident response plan, the strategy for the inci dent response program is outlined.
- This includes goals, roles, and responsibilities ie; how to analyze and triage events; and the requirements for escal ation.
- The phases of the incident response plan and the strategi es for each are also documented.
- The most common incident response phases are identific ation, containment, eradication and recovery.
- The strategic importance and objectives of each are also outlined.

Important terms in incident response

1. Triage

- When incidents are brought to the attention of help desk analysts, security analysts, analyze and prioritize each.
- ***Triage*** therefore is the process of quickly assessing and prioritizing incidents to determine the appropriate level of response.
- Triage helps security teams to evaluate the severity, urgency, and potential impact of each incident, ensuring resources are allocated efficiently and the most critical threats are addressed first.
- In some situations of complex incidents, there is need for ***escalation*** of the event.

Important terms in incident response

2. Escalation

- Escalation is the process of raising an incident to a higher lev el of authority or expertise when it requires additional attention , resources, or specialized knowledge.
- Escalation usually happens when an incident is too complex, severe, or impactful for the current response team to handle al one, or when it needs faster resolution due to its potential to di srupt critical systems.

Incident Response Planning phases

The most common incident response phases are identification, containment, eradication and recovery.

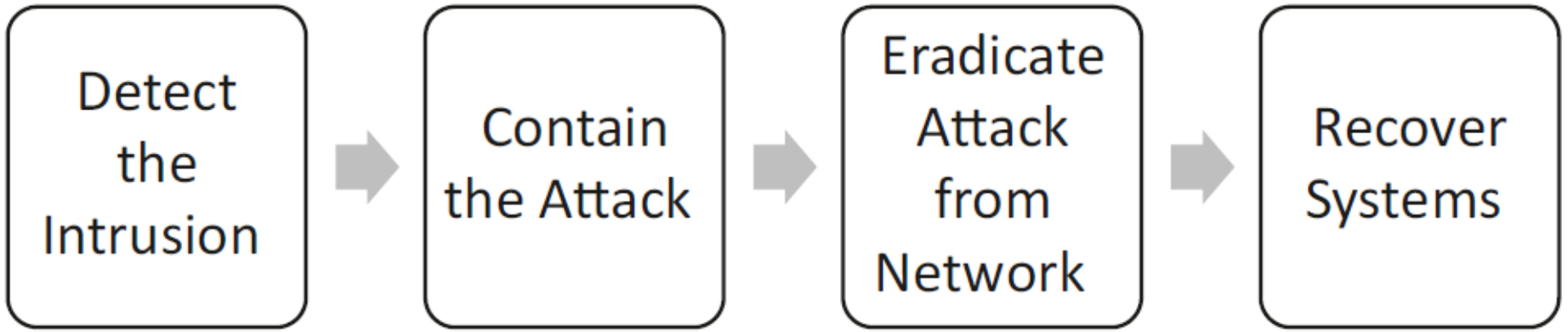

Figure 2. *Four response phases of the incident response plan*

Incident Response Planning phases

1. Intrusion detection/ identification

- The first step is Intrusion detection which enables early det ection and accurate identification of incidents.
- Using monitoring tools such as Security Information and Ev ent Management (SIEM) systems, intrusion detection/preve ntion systems (IDPS), and behavioral help to detect potenti al security threats.
- Incidents are assessed and classified based on severity to determine an appropriate response. Identifying root causes is also essential to target the specific threat rather than just the symptoms.

Incident Response Planning phases

2. Containment

- The next step is containment which is the process of limiting the impact of the detected incident and preventing further spread.

We have two types of Containment;

- . **Short-term Containment:** Involves immediate actions like disconnecting infected systems from the network or temporarily blocking specific services to prevent damage from escalating

Long-term Containment: Planning for a sustainable solution, such as removing affected systems from production and addressing vulnerabilities. This can include patching software, strengthening security configurations, and isolating systems that could become compromised.

Incident Response Planning phases

3. Eradication

- Eradication involves the removal of the root cause of the i ncident to prevent recurrence.
- This step includes activities such as removing malware, d eleting malicious accounts, patching vulnerabilities, and u pdating software.
- Documenting each action taken in the eradication phase i s crucial for maintaining records and meeting compliance requirements.

Incident Response Planning phases

4. Recovery

- Recovery aims at safely restoring and validating the affected systems to resume normal operations.
- Once all the malicious files and programs are removed from a ffected end points and devices, systems are brought back ont o the network, and production resumes.
- The cybersecurity team should keep a close eye on those sys tems, and the rest of the network to trap any signs incase the malicious software is still present in the network.

Incident Detection and Reporting

- Incident detection and reporting are crucial steps in IT In cident Management and Response which aim at ensurin g that issues impacting IT services are identified and ad dressed promptly.

1. Incident Detection

- Incident Detection is the process of suing monitoring too ls to identify and recognize events that may pose a risk t o IT systems, data, or operations.
- This includes checking system logs, network traffic, appli cation performance, and user behavior analytics.

Incident Detection and Reporting

Effective Incident detection involves activities like;

- Continuous Monitoring; Using tools to monitor networks, system s, and applications for anomalies or unusual behavior.
- Automating Alerts; Alerts are generated through automated mon itoring systems such as high CPU usage or low storage space, i ndicating a potential incident.
- Vulnerability Scanning and Penetration Testing; Regular tests to uncover potential weak points that could lead to incidents.
- User Reporting Mechanisms; Encouraging employees to report suspicious activities or potential security issues to complement automated detection.
- Automated Tools and Analytics; Leveraging AI, machine learnin g, and log analysis to detect patterns that could signal a cyber a ttack or a system malfunction.

Incident Detection and Reporting

1. Incident Reporting

- Incident Reporting involves documenting and communic ating incidents after detection to ensure a coordinated re sponse and future prevention.

The Incident Reporting process;

1. Incident Classification and Documentation:

- This step involves categorizing the incident by type and severity, then thoroughly documenting details about wha t happened, when, and how it was detected.

The Incident Reporting process cont..

2. Notification Protocols;

- The next step is to notify the appropriate internal teams e.g the IT, risk management, the legal teams well as the external parti es like clients or regulatory bodies and, if found necessary.

3. Root Cause Analysis;

- This step involves investigating the root cause of the incident t o understand what allowed it to occur and prevent recurrence.

4. Incident Log and Tracking;

- The last step involves maintaining a log of all incidents for aud it purposes, ongoing risk assessments, and to identify patterns or areas needing strengthened controls.

3 Key Components of Effective Detection and Reporting

1. Incident Management System (IMS);

- A centralized system (e.g., ServiceNow, JIRA) facilitates logging, categorizing, tracking, and reporting incidents.

2. Collaboration Tools;

- Integrations with communication platforms like Microsoft Teams helps to notify teams and ensure real-time coordination during incident response.

3. Documentation and Knowledge Base;

- Documenting incident details for future reference and adding to the knowledge base helps in faster response and training for future incidents.

Best Practices in Incident Detection and Reporting

- *Conduct regular employees training;* Train IT staff on identi fying signs of incidents and reporting them quickly.
- *Define Clear Metrics;* Establish metrics for timely detection, timely reporting, and timely resolution to measure effective ness.
- *Post-Incident Review:* Conduct root cause analysis and po st-incident reviews to improve detection and response proc esses continually.
- *Ensure efficient incident detection and reporting*; so that IT teams can minimize downtime, reduce the impact on users

Managing and Recovering from Incidents

- Managing and recovering from incidents in IT risk manag ement is a crucial process for ensuring business continui ty and minimizing the impact of unexpected disruptions.
- It involves the following step-by-steps;

1. Preparation

- *Risk Assessment:* Identify potential risks and vulnerabi lities that could lead to incidents, such as cyber-attack s, hardware failures, or human errors.
- *Incident Response Plan:* Develop a documented plan outlining roles, responsibilities, procedures, and tools f or handling incidents.
- *Team Training*: Train incident response teams a nd employees on their roles and familiarize the m with incident response processes.
- *Tools & Technology:* Implement tools for monito ring, detection, analysis, and containment, like I ntrusion Detection Systems (IDS) and (SIEMs)

Managing and Recovering from Incidents

2. Detection and Analysis

- Identify Incidents: Use monitoring tools to detect unusual beha vior or alerts. Incident identification can come from automated tools, user reports, or external threat intelligence.
- *Classify & Prioritize:* Determine the type and severity of the inc ident to prioritize response efforts. This includes understandin g the impact, affected assets, and potential threat sources.
- *Analyze Root Cause*: Perform an initial analysis to understand the root cause, looking at attack vectors, vulnerabilities, and h ow the incident began to prevent similar occurrences in future.

Managing and Recovering from Incidents

3. Containment

- *Short-Term Containment:* Take immediate action to prevent the incident from spreading. This may involve disconnecting affected systems from the network or isolating malicious software.
- *Long-Term Containment:* Implement longer-term fixes to secure affected systems, which might involve applying patches, reconfiguring firewalls, or changing access credentials.

Managing and Recovering from Incidents

4. Eradication

- *Remove Threat:* Fully remove any malicious elements e.g malware and unauthorized access from affected s ystems and networks.
- *Perform vulnerability Patching:* Apply necessary patch es or security updates to address vulnerabilities that co ntributed to the incident.
- *Verify Clean System:* Ensure all affected systems are c lean and free of any remaining threats before moving t o recovery.

Managing and Recovering from Incidents

5. Recovery

- *Restore Systems;* Begin restoring affected systems to t heir normal operational state e.g by reinstallation of ope rating systems, restoring data from backups etc.
- *Test & Monitor:* Carefully monitor systems to detect any signs of lingering issues or recurrence of the incident.
- *Gradual Reintegration:* Depending on the incident's sca le, restore systems gradually to production, starting wit h the least critical systems to minimize disruption risk.

Managing and Recovering from Incidents

6. Perform Post-Incident Review (Lessons Learned)

- *Conduct a review meeting;* Involve all relevant teams in a post-incident meeting to discuss the incident response process, the effectiveness of containment and recovery measures, and areas for improvement.
- *Document findings;* Record what happened, what worked, what didn't, and why, in a detailed incident report.
- *Update response plans;* Refine the incident response plan based on lessons learned, including updating processes, tools, and training as needed.
- *Implement preventive controls:* Implement additional controls or mitigations to prevent similar incidents from occurring in the future, such as improved access control measures.

Week 9 Summary

1. Incident Management and Response

- Refers to the structured approach of detecting, responding to, managing, and recovering f rom IT-related incidents, particularly cybersecurity threats.

2. Incident Response Strategy

- Strategies are built around the assets of concern, thinking through risks and attacking sce narios likely to occur.

3. Incident response planning Goals for organizations;

- ✓ To protect the organization’s infrastructure, assets, & operations.
- ✓ To comply with federal, state, and local regulations.
- ✓ To minimize the potential for negative publicity.
- ✓ To prevent or minimize financial liabilities.
- ✓ To minimize customer disruptions

Week 9 Summary

4. Roles and Responsibilities in incident response planning

- Involves various teams.
- The teams include, a group of legal and compliance members, IT lead ership members, external consultants, a group of senior management and external legal counsel.
- Each of the individuals on each team has a role in incident response.

5. Important terms

1. Triage: *The* process of quickly assessing and prioritizing incidents to d etermine the appropriate level of response

2. Escalation: The process of raising an incident to a higher level of aut hority or expertise when it requires additional attention, resources, or spe cialized knowledge.

Week 9 Summary

6. Incident Response Planning phases

1. Intrusion detection

Enables early detection and accurate identification of incidents.

2. Containment

- The process of limiting the impact of the detected incident and pr eventing further spread.

- Short-term Containment: Involves immediate actions like discon necting infected systems from the network or temporarily blockin g specific services to prevent damage from escalation.

- Long-term Containment: Planning for a sustainable solution, suc h as removing affected systems from production and addressing vulnerabilities.

Week 9 Summary

Incident Response Planning phases CONT…

3. Eradication

- Eradication involves the removal of the root cause of the incident to prevent recurrence.

4. Recovery

- Recovery aims at safely restoring and validating the affected syst ems to resume normal operations.

7. Incident detection and reporting

Incident Detection

- Incident Detection is the process of suing monitoring tools to iden tify and recognize events that may pose a risk to IT systems, dat a, or operations

Week 9 Summary

8. Effective Incident detection involves activities like;

- Continuous Monitoring
- Automating Alerts
- Vulnerability Scanning and Penetration Testing
- User Reporting Mechanisms
- Automated Tools and Analytics

Week 9 Summary

9. Incident Reporting

- Incident Reporting involves documenting and communicating incidents after detection to ensure a coo rdinated response and future prevention

The Incident Reporting process;

1. Incident Classification and Documentation
2. Notification Protocols
3. Root Cause Analysis
4. Incident Log and Tracking

10. Components of Effective Detection and Reporting

1. Incident Management System (IMS)
2. Collaboration Tools
3. Documentation and Knowledge Base

Week 9 Summary

11. Best Practices in Incident Detection and Reporting

- *Conduct regular employees training;*
- *Define Clear Metrics;*
- *Post-Incident Review:*
- *Ensure efficient incident detection and reporting*

12. Managing and Recovering from Incidents

1. Preparation
2. Detection and Analysis
3. Containment
4. Eradication
5. Recovery
6. Perform Post-Incident Review (Lessons Learned)

References

- *Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents" by Eric C. Thompson, Apress,2018*
- *Cybersecurity Incident Response and Management, Regner Sabillon, IGI Global, 2021.*
- *Incident Response & Computer Forensics" by Jason T. Luttgens, Matthew Pepe, and Kevin Mandia, McGraw-Hill Education, 2014*
- *The Cybersecurity Incident Response Guide: Managing Cyber Threats in Real Time" by Michael Baker, Wiley, 2020.*

End of Week 9

NEXT LECTURE we will look at-;

***Week 10**:* Business Continuity and Disaster Recovery

See u There!