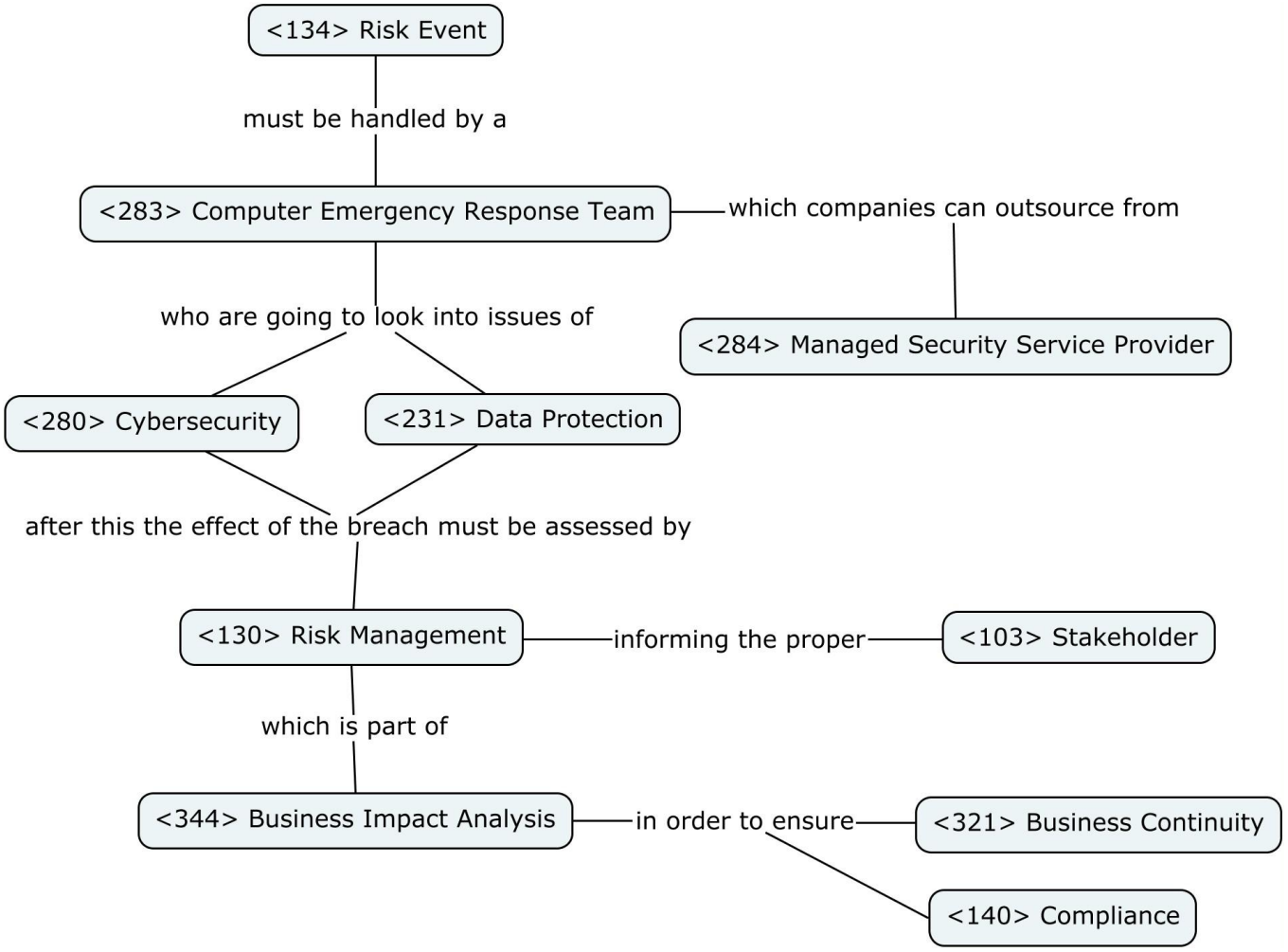
Maria Campos 95629

Data Breach Management

CMAP and Description



A data breach is a **risk event** that must be handled by a **Computer Emergency Response Team,** which companies can outsource from **Managed Security Service Providers,** that have an incident response plan elaborated to look into issues of **Cybersecurity** and **Data Protection** to assess the integrity, availability and confidentiality of the information. After this the consequences of the breach must be assessed by **Risk Management,** from which informing the proper **stakeholders** is one of the tasks. This constitutes part of the **Business Impact Analysis** process, in order to ensure **Business Continuity,** to recover from the disruption as soon as possible, and **Compliance**, to ensure adherence to the proper regulations and laws in place.

Maria Campos 95629

Description of the Subject

I have decided to propose the topic of **Data Breach Management**, since it is relevant to have principles and guidelines on how to deal with data breaches, so that organizations can effectively deal with threats in moments that can cause panic and disruption of **business continuity**. This topics' relevancy is also helped by the fact that data compromises have been increasing within the past few years in the United States, and the rest of the world experiences a similar trend. [2]

Data Breach Management is a vast area of study which includes various subtopics that are related to the course material. For example, Data Breach Management deals with **compliance** and regulatory requirements and is heavily dependent on **Risk Management** and **Computer Emergency Response Team (CERT)** activities.

One of the key aspects of Data Breach Management is elaborating an Incident Response Plan, which consists of a set of procedures and guidelines that specifies how an organization should act in the case of any security incident.

The development of this plan starts by gathering input from various **stakeholders**, like the legal and compliance departments in order to assess the organization's **risks**, needs and regulatory requirements (e.g: **GDPR**). Then, proceed to outline the responsibilities of each member from the **CERT** to maximize coordination and cooperation. After this, one must specify the tools to be used to detect and monitor incidents, these may be available from a **Managed Security Service Provider (MSSP).** It can provide tools such as firewall, intrusion detection, vulnerability scanning and anti-virus services. Then, it is vital to educate the staff about incident response and make them understand the importance of having an Incident Response Plan, in order to have everyone in the organization on the same page and able to follow the procedure in the case of a data breach, possibly reducing the length of the disruption. An important step is also making sure the communication between the organization and law enforcement and legal teams is effective in order to quickly report incidents and ask for needed expertise when necessary. And finally, when the data breach does happen and after it has been dealt with, assess what went wrong and what went right and learn from previous mistakes and make sure the organization's security measures and response plans are in continuous improvement, basically performing a **Business Impact Analysis**. [3]

Data Breach Management is also related to **Compliance.** Organizations need to follow certain steps in order to respect data protection regulations. For example, under GDPR law in the European Union, organizations must report a data breach incident to the authorities within 72 hours. There is also a need for proper and detailed reporting of the incidents, with extensive and detailed descriptions of what

transpired, as well as a need to notify the affected individuals to inform them about the effects the data breach has had on their data, rights and freedom. Organizations must prioritize compliance if they want to protect their data, maintain regulatory compliance and foster trust in their clients about their data handling practices.

Data Breach Management also entails proper **Monitoring** because organizations must be constantly using monitoring tools to identify unusual activity that could cause a potential data breach, for example monitoring network traffic. To ensure effective monitoring, companies can use various strategies such as using the previously mentioned **MSSPs** but they can also train their existing IT staff to improve their knowledge in **cybersecurity** and threat detection and making sure to use user friendly monitoring tools.

The aftermath of the data breach also needs to be addressed. After the breach occurs and the incident has been contained, organizations must have a Recovery Plan in order to mitigate further damage and restore normalcy to the system. Organizations must restore data from backups, make sure that the recovered data is free from malware and validate it for **integrity**. The, review the effectiveness of their response to the incident and correct any gaps in the security control and implement the required improvements to prevent similar incidents in the future.

To sum up, Data Breach Management is essential for organizations to effectively handle security incidents, comply with regulations, and restore normal operations after a breach. It involves creating an Incident Response Plan, monitoring for potential breaches, prioritizing **compliance**, and implementing a Recovery Plan. By following these practices, organizations can better protect their data and maintain customer trust and ensure **business continuity**.

References

[1] The Key Steps To Effective Data Breach Management [Online] https://www.metacompliance.com/blog/data-breaches/the-key-steps-to-effective-data-breach-management

[2] Annual number of data compromises and individuals impacted in the United States from 2005 to 2022 [Online] https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed

[3] What Is an Incident Response Plan for IT? https://www.cisco.com/c/en/us/products/security/incident-response-plan.html#~how-to-create-a-plan