DrillBit

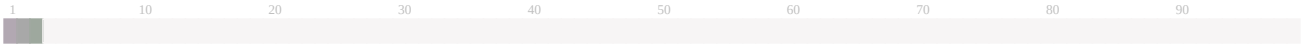
The Report is Generated by DrillBit Plagiarism Detection Software

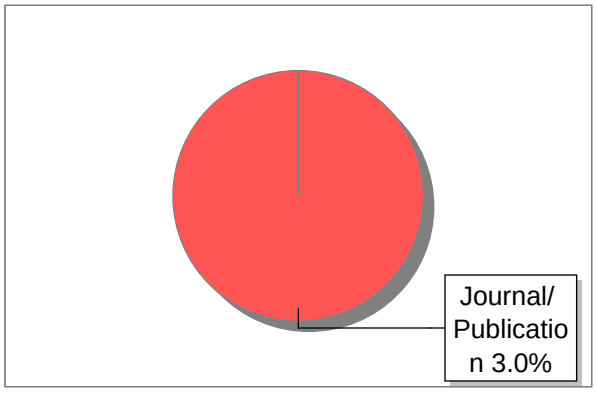
Submission Information

Author Name	Navya Peram
Title	CASE STUDY
Paper/Submission ID	1076360
Submitted by	jyothih6@gmail.com
Submission Date	2023-11-03 10:25:39
Total Pages	4
Document type	Project Work

Result Information

Similarity **3 %**





Report Content

Exclude Information

Quotes	Excluded
References/Bibliography	Excluded
Sources: Less than 14 Words Similarity	Excluded
Excluded Source	**0 %**
Excluded Phrases	Not Excluded

A Unique QR Code use to View/Download/Share Pdf File

DrillBit

DrillBit Similarity Report

3	1	A
SIMILARITY %	MATCHED SOURCES	GRADE

A-Satisfactory (0-10%)
B-Upgrade (11-40%)
C-Poor (41-60%)
D-Unacceptable (61-100%)

LOCATION	MATCHED DOMAIN	%	SOURCE TYPE
1	espace.library.uq.edu.au	3	Publication

iPremier Case Study

NAVYA PERAM
PES1UG21CS924

Question #	Answer
1	The response of the iPremier Company was very abysmal, due to a multitude of reasons: • The company lacked a proper communication channel, rather than a clear-cut order of communication. The response to the attack involved the CIO receiving a multitude of calls from various managers with varying and conflicting opinions. Rather than calling for a meeting and discussing the solution together, each chose to give their own opinions. Moreover, each person wanted the CIO to act in a manner that would prioritize their respective areas over the technical and security areas. • The CIO was over his head and unable to control the proceedings. Considering that the attack had originated under his domain, he had to have a clear hold over the passage of information. This was not the case, as he wasn't aware that an employee under him Leon had passed the information to another higher-up in the company or on the further passage of information. • Absence of appropriate emergency measures such as the business continuity plan(BCP). The company had failed to establish and prepare fail-safe procedures to follow in the case of an emergency. The emergency plans such as the BCP, disaster recovery plan(DRP) and incident response plan(IRP) were outdated and irrelevant. Furthermore, the employees were untrained and had no idea of the actions to be taken in the case of an emergency. • Bob Turley wasn't an efficient and resourceful CIO. He was unaware of the majority of plans and procedures in his domain. Moreover, he had neglected to check and observe the emergency plans and security measures since his arrival, which is of extreme importance considering the company's high-value transactions. If I was Bob Turley, then: • First, I would contact the service company Qdata and ask for the contacts of higher administrators. Asking them to look into the problem immediately and temporarily suspend the website to prevent the stealing of any information, in case data was breached. • Considering the absence of emergency measures, I would have initiated a meeting with all the heads and available employees to discuss and figure out the most effective methods to efficiently negotiate the given situation. • Check for the occurrence of different kinds of attacks, considering that on multiple occasions, DDoS attacks act as smokescreens behind which multiple data breaches or ransomware occur. • Maintain consistent monitoring of the website to notice any changes occurring in the system, to be able to immediately investigate the situation if it escalates. • Further strengthen the security measures against the system, to prevent multiple attacks from occurring based on the response from Qdata and the information personnel. In case the source of weakness in the system is identified by the security personnel, then secure and strengthen the particular area immediately.

iPremier Case Study

NAVYA PERAM
PES1UG21CS924

2	The operating procedures of the company were inadequate: • The team was unprepared and incompetent in the face of an emergency. Continuous training and evaluations at regular intervals along with frequent exposure to various scenarios will help them be better equipped to deal with emergencies in the future. • Absence of emergency procedures, with the one plan they had, BCP was also difficult to find during the emergency. Constant upgrading and implementation of multiple plans with the roles and responsibilities of the team would be necessary. • Establish a clear hierarchy of personnel to be called during such times along with an established emergency team to be contacted consisting of members encompassing various departments across the organization, for a more overall effective view of the problem. In this case, there were hurried calls with multiple departments with no promise of effective action in the end. • Developing an Incident Response Process for fast and effective strategies to be quickly implemented in the face of an attack. Considering that time is of the utmost importance in such cases, the process must contain methods to identify and contain the attack along with the procedures to be followed to contain and effectively minimize damage. In the time taken for Leon to contact Joan, along with their calls to the CIO and multiple members for a source of action, heavy damages could have occurred if it had been a more high-risk attack. • Establishment of alternate communications to be used in the case of the shutdown of the main source of communication. • A detailed Disaster Recovery Plan (DRP) and backup restoration plan to be created. To ensure fail-safe protection of data in the occurrence of any breaches. This would have been helpful if they had decided to shut down the computers. • Create a specialized emergency response team or have contacts with such external teams having a large amount of experience to call upon during such situations. If they had a proper team along with Joanne and Leon to immediately call upon, it would have been easier and faster for them to identify the attack and respond to it. • Establish continuous and constant 24/7 monitoring of the network to be able to immediately access any discrepancies that occur and to take effective action immediately. • To hire a company with advanced and state-of-the-art technology along with experienced employees and constant 24/7 monitoring. A company dealing with high transactions and high net-worth individuals should have invested in a more dependable and strategic company with proper procedures and quick responses. Considering the inability of Qdata to either retain staff or afford the required technology, they should have immediately changed to a more competent company. • The company should have prioritized the security and protection of its systems over personal commitments to other companies and the inculcation of new features. With the majority of the trades occurring over the internet, they should have made the decision to strengthen their security their utmost priority.
3	The company could enforce various steps to prepare for a similar attack in the future:

NAVYA PERAM
PES1UG21CS924

	• Primarily, document and record all the actions that were taken during this emergency. This can be used to identify the weaker areas of both their implemented strategies and plans, to further their knowledge and competency in such conditions. • Examine and process all the files present in the system to make sure that no external files or malware were installed during the attack. • Establishment of stringent security protocols and mechanisms to be considered during an attack or breach of the systems. Create multiple plans as backups for the various courses of action to be taken in case any single plan falls through. • Transfer the management of the server to a more capable and prominent company with advanced technology and resources. • Make constant and continuous evaluations of the security systems by hiring independent security teams at regular intervals. • Continuous and constant management of the firewalls and the system by an in-house security team. With instant blocking of applications with requests higher than the usual limit. • Implement frequent training sessions with a variety of attacks, for the teams to familiarize themselves with the various procedures to implement during an attack.
4	After the attack, the various concerns I would have are: • A big concern would be the reputation of the company, any negative impact would cause a massive downfall of stocks, reducing the market value of the company. • A similar concern would be the view of the company in the public eye, damage to the company's reputation would greatly impact the customer's trust in the company. In turn, pushing the customers to the rival companies, effectively destabilizing the company's position in the industry. • Another concern would be the occurrence of any data breaches. Considering that DDoS attacks often mask more sinister activities such as ransomware or illegal attainment of data, investigating the method of attack and the breaches that occurred would be a primary concern. • Secure customer data and make sure that no access has been gained to the company's database during the attack. Check that the company's employee and financial information is secure. • Various actions can be taken such as installing secure firewalls and efficient security systems along with constant 24/7 monitoring and effective team strategies. • There would also be a need for better strategy and marketing to increase the value of the company, by implementing various ideas towards increasing customer membership. • Use of DDoS mitigation services to reduce and filter out any harmful traffic by only allowing permitted traffic through the systems. • Implement multiple layered security approaches with firewalls, intrusion detection, and access control to efficiently manage the systems and the network of the company. • Ensure that the customers were notified about a slight delay in online services and offer any alternative source in the meantime, to prevent any impact to customer satisfaction and trust.

iPremier Case Study

NAVYA PERAM
PES1UG21CS924

	• A final concern I would have would be any impending lawsuits against the company by the rival company MarketTop, especially considering the DDoS situation it had faced with iPremier at its source. This could greatly impact the company's standing in the current market. Therefore, legal meetings and counsel sessions need to be considered.

iPremier Case Study

NAVYA PERAM
PES1UG21CS924

Question #	Answer
1	The response of the iPremier Company was very abysmal, due to a multitude of reasons: • The company lacked a proper communication channel, rather than a clear-cut order of communication. The response to the attack involved the CIO receiving a multitude of calls from various managers with varying and conflicting opinions. Rather than calling for a meeting and discussing the solution together, each chose to give their own opinions. Moreover, each person wanted the CIO to act in a manner that would prioritize their respective areas over the technical and security areas. • The CIO was over his head and unable to control the proceedings. Considering that the attack had originated under his domain, he had to have a clear hold over the passage of information. This was not the case, as he wasn't aware that an employee under him Leon had passed the information to another higher-up in the company or on the further passage of information. • Absence of appropriate emergency measures such as the business continuity plan(BCP). The company had failed to establish and prepare fail-safe procedures to follow in the case of an emergency. The emergency plans such as the BCP, disaster recovery plan(DRP) and incident response plan(IRP) were outdated and irrelevant. Furthermore, the employees were untrained and had no idea of the actions to be taken in the case of an emergency. • Bob Turley wasn't an efficient and resourceful CIO. He was unaware of the majority of plans and procedures in his domain. Moreover, he had neglected to check and observe the emergency plans and security measures since his arrival, which is of extreme importance considering the company's high-value transactions. If I was Bob Turley, then: • First, I would contact the service company Qdata and ask for the contacts of higher administrators. Asking them to look into the problem immediately and temporarily suspend the website to prevent the stealing of any information, in case data was breached. • Considering the absence of emergency measures, I would have initiated a meeting with all the heads and available employees to discuss and figure out the most effective methods to efficiently negotiate the given situation. • Check for the occurrence of different kinds of attacks, considering that on multiple occasions, DDoS attacks act as smokescreens behind which multiple data breaches or ransomware occur. • Maintain consistent monitoring of the website to notice any changes occurring in the system, to be able to immediately investigate the situation if it escalates. • Further strengthen the security measures against the system, to prevent multiple attacks from occurring based on the response from Qdata and the information personnel. In case the source of weakness in the system is identified by the security personnel, then secure and strengthen the particular area immediately.

iPremier Case Study

NAVYA PERAM
PES1UG21CS924

2	The operating procedures of the company were inadequate: • The team was unprepared and incompetent in the face of an emergency. Continuous training and evaluations at regular intervals along with frequent exposure to various scenarios will help them be better equipped to deal with emergencies in the future. • Absence of emergency procedures, with the one plan they had, BCP was also difficult to find during the emergency. Constant upgrading and implementation of multiple plans with the roles and responsibilities of the team would be necessary. • Establish a clear hierarchy of personnel to be called during such times along with an established emergency team to be contacted consisting of members encompassing various departments across the organization, for a more overall effective view of the problem. In this case, there were hurried calls with multiple departments with no promise of effective action in the end. • Developing an Incident Response Process for fast and effective strategies to be quickly implemented in the face of an attack. Considering that time is of the utmost importance in such cases, the process must contain methods to identify and contain the attack along with the procedures to be followed to contain and effectively minimize damage. In the time taken for Leon to contact Joan, along with their calls to the CIO and multiple members for a source of action, heavy damages could have occurred if it had been a more high-risk attack. • Establishment of alternate communications to be used in the case of the shutdown of the main source of communication. • A detailed Disaster Recovery Plan (DRP) and backup restoration plan to be created. To ensure fail-safe protection of data in the occurrence of any breaches. This would have been helpful if they had decided to shut down the computers. • Create a specialized emergency response team or have contacts with such external teams having a large amount of experience to call upon during such situations. If they had a proper team along with Joanne and Leon to immediately call upon, it would have been easier and faster for them to identify the attack and respond to it. • Establish continuous and constant 24/7 monitoring of the network to be able to immediately access any discrepancies that occur and to take effective action immediately. • To hire a company with advanced and state-of-the-art technology along with experienced employees and constant 24/7 monitoring. A company dealing with high transactions and high net-worth individuals should have invested in a more dependable and strategic company with proper procedures and quick responses. Considering the inability of Qdata to either retain staff or afford the required technology, they should have immediately changed to a more competent company. • The company should have prioritized the security and protection of its systems over personal commitments to other companies and the inculcation of new features. With the majority of the trades occurring over the internet, they should have made the decision to strengthen their security their utmost priority.
3	The company could enforce various steps to prepare for a similar attack in the future:

NAVYA PERAM
PES1UG21CS924

	• Primarily, document and record all the actions that were taken during this emergency. This can be used to identify the weaker areas of both their implemented strategies and plans, to further their knowledge and competency in such conditions. • Examine and process all the files present in the system to make sure that no external files or malware were installed during the attack. • Establishment of stringent security protocols and mechanisms to be considered during an attack or breach of the systems. Create multiple plans as backups for the various courses of action to be taken in case any single plan falls through. • Transfer the management of the server to a more capable and prominent company with advanced technology and resources. • Make constant and continuous evaluations of the security systems by hiring independent security teams at regular intervals. • Continuous and constant management of the firewalls and the system by an in-house security team. With instant blocking of applications with requests higher than the usual limit. • Implement frequent training sessions with a variety of attacks, for the teams to familiarize themselves with the various procedures to implement during an attack.
4	After the attack, the various concerns I would have are: • A big concern would be the reputation of the company, any negative impact would cause a massive downfall of stocks, reducing the market value of the company. • A similar concern would be the view of the company in the public eye, damage to the company's reputation would greatly impact the customer's trust in the company. In turn, pushing the customers to the rival companies, effectively destabilizing the company's position in the industry. • Another concern would be the occurrence of any data breaches. Considering that DDoS attacks often mask more sinister activities such as ransomware or illegal attainment of data, investigating the method of attack and the breaches that occurred would be a primary concern. • Secure customer data and make sure that no access has been gained to the company's database during the attack. Check that the company's employee and financial information is secure. • Various actions can be taken such as installing secure firewalls and efficient security systems along with constant 24/7 monitoring and effective team strategies. • There would also be a need for better strategy and marketing to increase the value of the company, by implementing various ideas towards increasing customer membership. • Use of DDoS mitigation services to reduce and filter out any harmful traffic by only allowing permitted traffic through the systems. • Implement multiple layered security approaches with firewalls, intrusion detection, and access control to efficiently manage the systems and the network of the company. • Ensure that the customers were notified about a slight delay in online services and offer any alternative source in the meantime, to prevent any impact to customer satisfaction and trust.

NAVYA PERAM
PES1UG21CS924

	• A final concern I would have would be any impending lawsuits against the company by the rival company MarketTop, especially considering the DDoS situation it had faced with iPremier at its source. This could greatly impact the company's standing in the current market. Therefore, legal meetings and counsel sessions need to be considered.