**Assignment**

**Individual**

**KDS – Name SME**

**Session 14**

**To** **be Submitted Week 15**

**Tugas Personal ke-4**

1. Jelaskan bagaimana cara menghitung resiko.

**Answer:**

Risk score reflects the severity of a risk **by multiplying probability and impact** though other factors, such as weighting may also be part of calculation.

**In order to calculate risk score, we need assign a value to each of the probability** (e.g. 1-100)  **and impact levels** (e.g. 1, 2, 3, 4, 5) or could be categorized into 5 levels: Very Low, Low, Medium, High, or Very High.

**REFERENCES :**

Whitman, M.E., Mattoro, H.J. (2013). Principles of Incident Response and Disaster Recovery.

1. Apa yang harus ditulis dalam dokumen disaster recovery plan dan bagaimana cara menulisnya.

**Answer:**

1. **Create a Disaster Response Team and Document Responsibilities**

Assign each team member specific tasks during the response and document them so everyone knows who is in charge of what and also need backup staff for key team members in case a designated lead isn’t available during a crisis.

1. **Set Clear Recovery Time Objective and Recovery Point Objective**

Recovery Time Objective (RTO) is the length of time an application can be down before the business is negatively impacted.

Recovery Point Objective (RPO) is the most data that can be lost before the business is significantly harmed (i.e., how much buffer you need between an outage and the most recent working backup).

1. **Make a Blueprint of the Network Infrastructure**

Different components of the system have different levels of importance to business continuity, so be sure to indicate the priority of each service as mission-critical, essential, or nonessential so they can be restored in the appropriate order and don’t forget to include system dependencies in the blueprint, because they may impact how to prioritize recovery.

1. **Select a Disaster Recovery Solution**

Look for a disaster recovery solution like Storage capacity, recovery timeline, and configuration complexity that will affect the cost of a disaster recovery solution. In many cases, must choose between a solution that offers quick recovery times but may lose days of data and a solution that maintains system availability but kills with high complexity and costs.

1. **Create a Checklist of Criteria for Initiating the Disaster Response Plan**

Creating a checklist of criteria to identify what constitutes a disaster helps the recovery team know when it’s time to jump into action without wasting resources or money by overreacting to a minor threat.

1. **Document the Disaster Recovery Process**

To ensure data and operations are restored quickly after a disaster, create step-by-step instructions in plain language so the team can start the disaster recovery effort as soon as it’s safe to do so also store a copy of the disaster recovery plan away from the network—preferably in the cloud—to protect it from corruption during a ransomware attack or physical loss from a natural disaster.

1. **Test the Disaster Recovery Plan**

Conduct regular tests of the disaster recovery plan to ensure it will work when it's need it to by run a partial recovery test twice a year and a full recovery simulation annually. Additionally, it doesn’t hurt to periodically spring surprise drills on the company so Disaster Recovery Team can get an accurate assessment of how well the processes will work in the event of a real emergency.

1. **Review and Update Disaster Recovery Plan Regularly**

Changes may include employees leaving or joining the company, policies being modified to meet new regulations or standards, or business units being consolidated so the disaster recovery plan needs to be reviewed and updated regularly to reflect these changes and how they impact the recovery process.

**REFERENCES :**

Whitman, M.E., Mattoro, H.J. (2013). Principles of Incident Response and Disaster Recovery.

1. Apa yang harus ditulis dalam dokumen business continuity plan dan bagaimana cara menulisnya.

**Answer:**

1. **Identify objectives and goals of the plan**

In addition to identifying the activities that must continue, the harder task can be achieving agreement with the stakeholders and clients on what activities have to be maintained at peak performance and service levels, what activities and services will need to stop (even if only temporarily), and what activities and services will be provided at a lower level.

Once knew what is most important, prioritize the activities for continuous delivery versus recovery, estimate the time required to recover and the issues that are unique to the organization also determine how long can business operate without key revenue generating products or services while incurring costs to recover.

1. **Establish an emergency preparedness team**

Select a few cross-functional managers or leaders, and anyone else who may bring something valuable to the table and make sure someone is designated as the leader to keep things moving forward and make decisions when necessary.

1. **Perform a Risk Assessment and Business Impact Analysis (BIA)**

Identify the biggest potential threats to the business, then research and analyze them thoroughly and discuss with the team what would happen if team had to reduce, modify, or eliminate essential services or functions also don’t forget to document all the identified issues and related business impact.

1. **Identify essential business functions**

Determine how the organization will maintain essential services/functions in the event of an emergency like:

1. **Inventory management and supply continuity**

Think about what happens when company encounter a product shortage such as will company have enough inventory? Do company have an inventory management tool or system to help manage inventory? Do company have a plan for times with low or no inventory?.

1. **Order fulfillment and shipping deadlines**

If a crisis hits, can company still fill orders and meet shipping deadlines? It may be helpful to diversify shipping providers.

1. **Ecommerce platform functionality**

If a crisis were to happen, can company adjust the platform to show out-of-stock items? Can company handle an influx of customers in a situation where supply is greatly increased? Do company have strong cybersecurity and all of the data backed up.

1. **Maintaining customer service**

During a crisis, customers need transparency and empathy and company need to provide a communications plan for the marketing/communications teams and the customer support team.

1. **Prepare a plan for each essential function/service**

The "company engine" runs as a combination of parts, including Customers, Team Members, Suppliers, Inventory, and Shipping. Each of these parts has to have its own plan such as How will company address the situation with the customers? Does that communication plan change when it’s the kind of disruption that may have also put their lives in danger?, Will company be prepared to switch to another supplier to make sure company don’t run out of inventory? Do company know what the options are if company shipping partner experiences a disruption?.

1. **Review and make sure every business function has been addressed**

Business Continuity Team should present a draft of the Business Continuity Plan to company emergency preparedness team for review and/or comment because they understand the overall corporate impact of an emergency, they should review to ensure that the plan Is consistent for all business units/departments and Addresses all critical elements.

1. **Train staff, test, revise, and update the plan**

Present the plan to all company stakeholders and suggest being proactive by performing trial runs for a gut check that each part of the plan works as it should and will help Business Continuity Team identify any missing aspects or weaknesses. Then, once team have made any updates based on the feedback, begin to train all staff accordingly.

**REFERENCES :**

Whitman, M.E., Mattoro, H.J. (2013). Principles of Incident Response and Disaster Recovery.

1. Apa beda antara forensic dan anti-forensic? Dalam melakukan forensic bagian hardware dan software apa yang perlu di review?

**Answer:**

**Forensic is** a technique used in the connection with the detection of crime or relating the application of scientific method and techniques to the investigations of crime.

**Anti-Forensic refers to** those techniques which are designed so that it becomes difficult or impossible to retrieve information during an investigation.

**Hardware Forensic Review:**

1. Forensic Toolkit like mobile toolkit which contains everything needed to perform a complete Forensic Acquisition such as Write Blockers like USB, FireWire, SATA, IDE to avoid any altering in the main evidence, wipers, Hard Drive Duplicators, Power Adapters, imaging hardware, and etc.
2. Password Recovery tools and Distributed Network Attack to use the power of machines across the network.
3. Hardware for data recovery which can fix the bad sectors that were partially corrupted and cannot be imaged through normal software.

**Software Forensic Review ( I Used Steganography as an Example):**

A picture containing text, electronics, display

Description automatically generated

This technique used to hide a text message or audio message and the result is an image very similar to the original image and seems to be minimally changed through naked eyes which give the resultant file is again made to go through decryption algorithm so as to extract the text message or audio msg embedded in it.

**REFERENCES :**

Whitman, M.E., Mattoro, H.J. (2013). Principles of Incident Response and Disaster Recovery.

1. Pada saat melakukan assessment, bagaimana cara memberikan bobot pada setiap item yang sudah kita identifikasikan? Berdasarkan kepada kriteria apa sebaiknya pemberian nilai bobot ini diberikan?

**Answer:**

**How to Give Value for Each Item Identified and What Criteria this Value is Given:**

1. **Brainstorming**

Think insightful questions can reveal weaknesses in organization that may not have considered such as is organization manufacturing process fully safe? Are all the employees properly trained?.

1. **Thinking Pessimistically**

At this stage, it’s important to avoid overconfidence and thinking something “can’t” or “won’t” happen by challenge all of the assumptions about potential risks and be prepared for any or all of them to occur.

1. **Seek Expert Feedback**

If you experience the same type of losses multiple times, it suggests there’s a risk that is improperly managed and that’s the brokers can also play a role in helping organization to assess organization business risks and recommending insurance coverage to help protect against the risk in case they occur.

1. **Conduct External Research**

Pay attention to similar organization competitors or companies. Any losses, risk management successes, news releases, or even legal precedents can help to identify the same types of risks in organization.

1. **Analyze customer complaints**

Customers may help in risk identification as well like What do customers most often complain about or what types of issues do they report? Such as provide valuable feedback that can help identify and mitigate against reputational risks..

**REFERENCES :**

Whitman, M.E., Mattoro, H.J. (2013). Principles of Incident Response and Disaster Recovery.