Group 2: Business Continuity Plan Checklist

Business Continuity Plan

**Introduction**

Ransomware attacks on the nation's summit systems lead to a loss of system and data confidentiality, integrity, and availability. The Reveton ransomware denied summit attendees access to conference data, and the computer screens displayed a message indicating a system hack that outputs a message mimicking federal law enforcement authority. Notably, ransomware attacks evolve quickly, and there is no particular framework for combatting new attacks. If a system is hacked, one primarily has two options, pay the ransom or attempt system recovery by rolling back to a previous back-up point. Hackers cannot be trusted to release system resources once the ransom is paid. With this in mind, the system's protection will rely heavily on historical data copies and a wide array of protection mechanisms, as detailed below.

**Identifying critical systems**

**Security Categorization of Summit Data and systems**

In line with the “FIPS 199: Standards for Security Categorization of Federal Information and Information Systems", (2004), summit attendees could not access data required for the conference, and the impact can be categorized as high. Comprehensively, a "high" potential impact implies that losing availability, integrity, and confidentiality leads to catastrophic repercussions on the summit participants, organizational assets, and operations ("FIPS 199: Standards for Security Categorization of Federal Information and Information Systems Assessment", 2004). The Reveton ransomware will probably lead to financial losses and crippled mission capability till the critical systems and services are restored.

The following process will be used to identify critical systems.



Figure 1 – Identification of critical systems.

Step 1: Identification of various information types

The incident response and recovery team will report about the summit’s mission statement and business process and note the specific types of data fed in the system, processed, stored, and output from the system. Vital activities will include identifying mission-dependent categories of data, support and management information, and other significant information categories (Stine et al., 2008). The core aspects of focus entail functions of the summit and the conference, techniques used by the nation's summit to achieve its objectives, support functionalities needed by the summit, and information related to the management of resources.

Step 2: Determination of provisional impact levels

There are three possible categories of potential impacts: low, moderate, and high, associated with the system and its information confidentiality, integrity, and availability. The summit’s system will be categorized into critical elements and assigned potential impacts (Stine et al., 2008). This step is documented in liaison with the system’s information security personnel.

Step 3: Assessment of provisional impact levels

Each part of the critical system's provisional effect level will be reviewed depending on the critical system's elements' functions. The incidence response and management team will readjust the levels of an impact considering availability, integrity and confidentiality parameters, software development lifecycle levels, or organizational policies (Stine et al., 2008). The mission owners and other critical IT personnel will collaborate in generating a report on assessed impact levels.

Step 4: Assignment of system categories

After that, the incidence response team will identify security categorizations for information and the information system. This is attained by evaluating the possible impact levels concerning confidentiality, integrity, and availability (Stine et al., 2008). Depending on the security objectives, the team will adjust impact levels and conform to federal guidelines about assessment, approval, and reporting of all decisions.

Output: Security Categorization

The summit management entity will use the categorization as requirements and specifications for security measures in the risk management process.

**Threats**

Ransomware refers to a particular malware that encrypts files and services on systems and may erase data or hinder access to critical content like in the nation's summit. The ransomware is designed to prevent accessing a system till a particular condition, pay a ransom, is met (Gallegos-Segovia et al., 2017). Typically, most ransomware use bitcoin technology since it is hard to trace who owns the network. Blockchains manage the transactions. Various ransomware has been known to exploit smartphone devices, operating systems, application and web servers, domain name systems, and other essential computing infrastructure.

**Infection Vectors**

The major propagation channels of ransomware include actions initiated by legitimate system users such as visiting compromised websites or clicking on malicious hyperlinks, phishing, and emails. In some cases, ransomware is spread through drive-by downloads and malware adverts that seem authentic, often do not need user involvement to launch an attack (Gallegos-Segovia et al., 2017). Most of such attacks are typically indiscriminate. In the case of the nation’s summit conference, this was a specific target-attack. Ransomware may extract and transfer system information, execute anti-detect functionalities, and distributed denial of service. With the instances detailed above, malware's variants may delete system files whether the ransom was paid or not.

**Analysis: Occurrence, information stored, and impact on the system and its users.**

The occurrence of ransomware attacks depends wholly on network and system security measures and policies in place. Management needs an incidence response plan, data back-ups, anti-virus software, monitoring third party services, restriction of internet access, updated systems and software, and frequent user training on compliance with the latest federal guidelines on cybersecurity policies ("Ransomware ", 2020). Failure to adhere to the parameters as mentioned above implies a potential ransomware attack for the summit conference.

The critical systems at risk include but are not limited to data centers. These refer to the summit's computing resources – servers that facilitate network connections, local storage, memory and processing, storage infrastructure – valuable data stored in the system such as user credentials, back-ups, system files, security policies, and measures' documentation and incidence response plans, and network infrastructure – a collection of utilities that link users internally and externally, storage systems and other data center infrastructure either virtually or physically ("Cisco” 2020). Comprehensively, data centers enable collaboration, communication, and access to virtual desktops, machine learning, artificial intelligence, big data functionalities, databases, enterprise resource planning, productivity applications, files, and email sharing. Deductively, a successful ransomware attack means a complete failure of the business and delivers a "HIGH" potential impact.

**Information system security categorization**

|  |  |  |
| --- | --- | --- |
| Critical Element | Function | Potential Impact (If Failure occurs) |
|  | Confidentiality | Integrity | Availability |
| Monitoring systems- Nagios | Facilitate monitoring uptime and health system of a data center. | HIGH | HIGH | MODERATE |
| Security – Routers, firewalls, switches, servers, applications, anti-viruses, cybersecurity policy compliance, checkpoints, and proxies. | Consistently uphold the systems confidentiality, integrity, and availability. | HIGH | HIGH | HIGH |
| Environmental Controls – cooling systems, power distribution, and fire suppression | Maintain a standard and practical working environment for a data center. | HIGH | MODERATE | HIGH |
| Redundancy – Cloud and local back-ups | Maintain system availability in case of a breach. | HIGH | MODERATE | HIGH |
| Scalability – Virtualized databases and email and file servers. | To adapt to the growth of business data over long periods. | HIGH | MODERATE | HIGH |

**Security engineering**

The summit's security engineering component will serve as the backbone to uphold the three principles of cybersecurity, confidentiality, integrity, and availability. This can be further broken down into encryption, software development controls, physical security, and security architecture and design.

 During the organization's software development, processing control, and data file control procedures will be incorporated. The information system will have functions that log audit trails of exceptions in the system or activities outside a specified scope. Additionally, if a user attempts to key in a value or variable excess for a transaction, the system should drop and log the activity for investigation. High-level programming languages allow the specification of appropriate file inputs. Therefore, if a user deliberately keys in a wrong format or uploads an incompatible file type, the system should reject that transaction. Concerning data processing controls, the software must record a file image's state before and after a transaction. Tracking changes in the file can be easier provided; there is a historical back-up. With recent advancements in the control versioning of systems using Git and composer installers, developers must enforce policies that ensure only the latest individual module software is used. For instance, databases and servers used must be the latest stable versions.

Encryption in systems refers to converting standard data into an encoded format, cipher, which can only be understood once converted back to the standard file through decryption. This functionality is facilitated by mathematical functions and a unique decryption or encryption passphrase, key (Norberg, 2020). Typically, encryption enables verification of authentic transactions, detection of intentional or accidental changes to the information, enforcement of confidentiality by protecting data stored on computer devices, and information transmitted through computer networks. Major encryption elements include a key length – a programmed length of the passphrase (Norberg, 2020). The longer the key, the more secure the encryption. Encryption keys facilitate the encoding and decoding of information, making it hard for attackers to find the information useful, whereas encryption algorithms are mathematical functions incorporated in systems to decrypt and encrypt data. Notably, the organization's software engineering team will consider using symmetric or asymmetric encryption types. Symmetric encryption utilizes secret keys to encrypt system information; then, the same key is used to decrypt the coded data. A prominent cryptography system that will use such a case is the data encryption standard (Norberg, 2020). On the other hand, asymmetric cryptography facilitates using a pair of keys, one that decrypts and the other encrypts system information. Note that either of them can decrypt or encrypt, although once a key is used to encrypt, it cannot be used to decrypt. Its counterpart does the decryption (Norberg, 2020). In this case, the organization will also incorporate RSA encryption during the software development lifecycle to enhance the security of system data and functions.

Physical security will go a long way to protect trespassers from accessing the organization's computing infrastructure. The organization's main entrance must use CCTVs to monitor user traffic in and out of the building, data centers, and critical systems' locations (Havens, 2016). Intrusion detection systems and fire suppression systems will be installed to maintain data integrity and availability while preventing systems' destruction (Havens, 2016). It would be appropriate to use the department of defense’s recommendations for building secure walls that are natural-disaster proof ("UFC 4-020-01 DoD Security", 2008). Data centers must be raised and located at least two floors above the ground floor for story buildings. The entrance to storage units with secure databases, servers, switches, and routers will use biometric fingerprints and optical scanners (Yang et al., 2019). All staff must wear identity tags displayed for easy identification. Such ID tags (RFID magnetic cards) will be used to open magnetic door locks (Hanks, 2016). Should a user attempt forced entry, a silent alarm will be triggered to the main security center for immediate investigation. Such measures will minimize the chances of a breach by physical means.

Security architecture and design entail implementing rigorous techniques for future and current organizational security procedures, data security systems, organizational and personnel to enable the organization's security processes and practices to synchronize with the organization's strategic direction and primary goals (Dosal, 2019). The most effective way to get an appropriate security architecture and design for the organization to systematically improve computer network security and mitigate risks involves four steps.

First, it is reasonable to use an existing business network security architecture. This lays out a framework that the organization will adapt to strengthening its measures by using learning points, highlighting weaknesses, strengths, and proper recommendations from past failures (Dosal, 2019). A significant example is *the Sherwood Applied Business Security Architecture - SABSA.* Secondly, the organization's cybersecurity team will conduct a network security evaluation to determine technological needs. This will facilitate focus on particular security gaps and save the company's resources than if a security architecture was to be built from scratch. Thirdly, bring on board the management, from the CEO to the support team, on the adopted framework's behavioral benefits (Dosal, 2019). Practically, the IT team will lead by example in adopting the new security measures to eliminate the possibility of users' double standards. Fourthly, the cybersecurity team will plan and effectively communicate changes and expectations from users moving forward. Users must be aware of what to do, the how, why, and appropriate company resources allocated to securing the organization's systems.

Perhaps in due course of adopting excellent security technologies, the software engineers will consider creating a blockchain-based security model. With blockchain's immutability, decentralized nature, peer-to-peer network management, and distributed ledgers, the organization will attain a significantly secure information system (Monrat et al., 2019). Consequently, ransomware and other malware attacks will be minimized.

**Operating system security**

Operating systems provide a platform where applications run. However, in the context of the information security chain, users have, over time, proven to be the weak link. Common threats to operating systems and enterprise applications range from denial of service, worms, trap doors, trojan horses, and viruses (Jaeger, 2008). Users must consistently be trained on the benefits of conforming to computer security policies created by cybersecurity experts. Knowledge of common threats and how to avoid them will improve overall system security (Jaeger, 2008). Network administrators will configure servers to have a password expiration period where the user must reset a new unique password, for instance, after five days. The password should contain a mixture of uppercase and lowercase letters, numbers, and at least a special character, and should be at least ten characters long. The longer and stronger the credentials, the safer the OS (Jaeger, 2008). Additionally, users must use authentic purchased anti-virus software to improve a computer's security. OS vendors typically create updates and patches to security gaps. It will be necessary for users to set their computers to update the OS once connected to the internet.

Users whose devices are configured to use network operating systems would be safer to incorporate firewalls in the network. Firewalls entail a combination of hardware and software between the public and the intranet (Chen et al., 2018). Firewalls enhance network OS security by creating virtual private networks between the internet and the organization, monitoring network traffic in and out of the organization, logging internal subversions and network penetrations, controlling services accessed using access lists and blocking OS users from accessing malicious phishing sites and emails (Chen et al., 2018). Overall, they play an essential role in maintaining confidentiality, integrity, and availability of operating systems, applications, and system information.

References

Chen, H., Cho, J. H., & Xu, S. (2018, April). Quantifying the security effectiveness of firewalls and DMZs. In *Proceedings of the 5th Annual Symposium and Bootcamp on Hot Topics in the Science of Security* (pp. 1-11).

Cisco | What Is a Data Center?. (2020). Retrieved 17 November 2020, from https://www.cisco.com/c/en/us/solutions/data-center-virtualization/what-is-a-data-center.html#~types-of-data-centers

Dosal, E. (2019). How to Build a Strong Enterprise Security Architecture Framework. Retrieved 17 November 2020, from https://www.compuquip.com/blog/building-a-strong-enterprise-security-architecture-framework

FIPS 199: Standards for Security Categorization of Federal Information and Information Systems Assessment. (2004). Retrieved 17 November 2020, from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

Gallegos-Segovia, P. L., Bravo-Torres, J. F., Larios-Rosillo, V. M., Vintimilla-Tapia, P. E., Yuquilima-Albarado, I. F., & Jara-Saltos, J. D. (2017, October). Social engineering as an attack vector for ransomware. In *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)* (pp. 1-6). IEEE.

Hanks Jr, D. R. (2016). *Juniper QFX10000 Series: A Comprehensive Guide to Building Next-Generation Data Centers*. " O'Reilly Media, Inc.".

Havens, s. (2016). Unified facilities criteria (UFC).

Jaeger, T. (2008). Operating System Security. Retrieved 17 November 2020, from https://books.google.co.ke/books/about/Operating\_System\_Security.html?id=P4PYPSv8nBMC&redir\_esc=y

Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access*, *7*, 117134-117151.

Norberg, S. (2020). Cryptography. In *Advanced ASP. NET Core 3 Security* (pp. 57-101). Apress, Berkeley, CA.

Ransomware: Facts, Threats, and Countermeasures. (2020). Retrieved 17 November 2020, from https://www.cisecurity.org/blog/ransomware-facts-threats-and-countermeasures/

Stine, K., Kissel, R., Barker, W., Fahlsing, J., & Gulick, J. (2008). Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories. Retrieved 17 November 2020, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

UFC 4-020-01 DoD Security Engineering Facilities Planning Manual | WBDG - Whole Building Design Guide. (2008). Retrieved 17 November 2020, from https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-020-01

Yang, W., Wang, S., Hu, J., Zheng, G., & Valli, C. (2019). Security and accuracy of fingerprint-based biometrics: A review. *Symmetry*, *11*(2), 141.