**NETWORKING CONCEPTS AND CYBER SECURITY 2**

**MODULE CODE: COMP40002**

**DATA BREACH INCIDENT:**

**SECURITY OPERATIONS AT UNIVERSITIES**

**Group Assignment:**

HAN23080577

HAN23080227

HAN23080330

HAN23070023

HAN23080181

HAN23080514

*#Word Count: 3296*

***Abstract***

*Due-to-the-evolving-Cyber-threat-landscape,-Cybercriminals-have-found-new-and-ingenious ways-of-breaching-defenses-in-networks.-Due-to-the-sheer-destruction-these-threat-actors-can-cause-to-an-organization,-most-modern-day-organizations-have-focused-their-attention-towards-protecting-their-critical-infrastructure-and-sensitive-information-through-multiple-methods.*

Contents

[**I.** **Introduction** 4](#_Toc170358159)

[**II.** **Stanford University** 4](#_Toc170358160)

[2.1. Case Study 4](#_Toc170358161)

[**III.** **Security Domains** 5](#_Toc170358162)

[3.1. Security and Risk Management 5](#_Toc170358163)

[3.2. Asset Security 5](#_Toc170358164)

[3.3. Security Architecture and Engineering 5](#_Toc170358165)

[3.4. Communication and Network Security 6](#_Toc170358166)

[3.5. Identity and Access Management 6](#_Toc170358167)

[3.6. Security Assessment and Training 7](#_Toc170358168)

[3.7. Security Operations 7](#_Toc170358169)

[3.8. Software Development 8](#_Toc170358170)

[**IV.** **Our Scenario** 8](#_Toc170358171)

[4.1. Main Domain 8](#_Toc170358172)

[**4.1.1.** **Benefits** 9](#_Toc170358173)

[**4.1.2.** **Challenges** 12](#_Toc170358174)

[**4.1.3.** **Summary** 13](#_Toc170358175)

[4.2. Organization Hierarchy 14](#_Toc170358176)

[4.3. Technical Details 14](#_Toc170358177)

[4.4. Security Details 14](#_Toc170358178)

[4.5. The Breach 15](#_Toc170358179)

[4.6. The Investigation 15](#_Toc170358180)

[4.7. Policy 16](#_Toc170358181)

[**4.7.1.** **Statement of Purpose:** 16](#_Toc170358182)

[**4.7.2.** **Authorized Uses** 17](#_Toc170358183)

[**4.7.3.** **Prohibited Uses** 18](#_Toc170358184)

[**4.7.4.** **Systems Management** 19](#_Toc170358185)

[**4.7.5.** **Violations of Policy** 21](#_Toc170358186)

[**4.7.6.** **Policy Review and Modification** 21](#_Toc170358187)

[**V.** **Forensics** 22](#_Toc170358188)

[**VI.** **Conclusion** 24](#_Toc170358189)

[**VI.** **Reference** 25](#_Toc170358190)

# **Introduction**

In the modernized technological world, data security lies among the essential priorities of organizations and institutions. In a cyber-security context, the target of criminals is the immense amount of identity information and financial credentials stored within the system. This report addresses data breaches in educational institutions, which occur for various reasons, and one of the most common factors that contribute significantly to such cases is ransomware attacks.

Based on the data breach of Stanford University, given the significant losses associated with the Akira ransomware and the university’s vulnerability to respond, it is essential to acknowledge how to effectively manage and recover from a cyber-attack. The report covers eight domains of CISSP to provide information regarding a university data breach, focusing on the ‘Security and Operations’ domain to emphasize the importance of detecting, preventing, responding, and recovering from a ransomware attack. In addition, a basic version of the Issue-Specific Security Policy (ISSP) is generated to highlight guidelines and standards for the university, followed by network forensics.

# **Stanford University**

## **Case Study**

On September 27th, 2023, Stanford University discovered that it had been hit with a severe ransomware attack. The attack, which stole the personal information of over 27,000 individuals, including date of birth, Social Security numbers, government IDs, passport numbers, driver’s license numbers, biometric data, email addresses with passwords, usernames with passwords, security questions and answers, credit card information and much more. The attacker was identified as the Akira ransomware group, first gaining access to the system on May 12th, 2023. The university had managed to cut them off the system shortly after detection on Sep 27th, notified federal and local law enforcement, and worked with external cybersecurity firms to remove any traces of the malicious actors.

# **Security Domains**

## **Security and Risk Management**

This domain focuses on clarifying goals, mitigating risks, ensuring compliance with laws and regulations, and maintaining business continuity. This domain is specialized in securing the data and managing risks.

The security and risk management focus in the university environment is to protect students, staff, and resources while keeping a conducive environment in good condition for education and research. In Summary, this domain ensures that universities work smoothly. Securing their assets and giving students a safe learning environment (Coursera, n.d.) (NIST, NIST Risk Management Framework RMF, 2024).

## **Asset Security**

The focus of this domain is to protect digital (virtual) and physical assets, considering the threats they pose when breached. Naturally, this involves handling data - whether it means storing, maintaining, retaining, or destroying them. People working in this domain may need to focus on properly disposing of and destroying old devices, including anything with confidential information.

In the university context, there are various policies and methods implemented to protect their physical and digital assets. They also ensure the confidentiality, integrity, and availability of information assets as well as securing physical assets from threats or unauthorized access (Imam, 2021).

## **Security Architecture and Engineering**

This domain focuses on enhancing data security by making sure tools, systems, and processes are effective and risk-free. The responsibility of a security analyst is to set up a firewall - a set of protocols used to monitor and filter incoming and outgoing computer network traffic - to prevent attacks from third parties.

In context, creating a vigorous and quick-to-bounce-back environment can protect their operations and data from attacks by third parties. This involves operating, implementing, and maintaining the security of facilities as well as ensuring policies are up-to-date (CISSP).

## **Communication and Network Security**

Communication and Network Security focuses on managing and securing physical networks and wireless communications. The protection of data resources is the main challenge for organizations with remote, hybrid, and on-site systems. Therefore, managing external connections is a necessity. Security protocols - such as limiting access to the network - help protect users and secure an organization’s network whenever employees travel or work outside of the main office. In context, universities emphasize strategies aimed at safeguarding data in transit, preventing unauthorized access, and maintaining the integrity and availability of network services (NICCS, 2024).

## **Identity and Access Management**

Identity and Access Management is most responsible for validating the identity of the user to secure the system and data. It covers authentication, authorization, and access control mechanisms to ensure that only authorized users can access specific resources (Educause, n.d.) (Council, 2023).

In the university, the IAM will manage the credentials of the students, faculty, and staff, ensuring that the right person can access their resources and protect them from cyber-criminals (SailPoint, 2024).

Benefits: Secures data and identities, boosting productivity and reducing IT workload.

Drawbacks: Requires significant investment and human power, skilled staff, and balancing security and usability.

## **Security Assessment and Training**

Security Assessment and Training are responsible for designing, validating tests, and conducting security assessments for systems and networks. This involves regular checks and procedures to verify the effectiveness of security and privacy controls, ensuring they meet security requirements. Training focuses on educating users to prevent incidents, recognize phishing and social engineering tactics, and report suspicious activities (O'Reilly).

Security assessments include regular tests of university security measures, such as firewalls and access controls, ensuring they function correctly. Training targets students, staff, and professors, teaching cybersecurity best practices like identifying phishing attempts, maintaining password hygiene, and reporting suspicious activities (Scarfone, Souppaya, Cody, & Orebaugh, 2008).

Advantages: Find security holes before attackers, and help understand the university's security posture.

Disadvantage: Requires skilled people, expensive costs, and training takes time and effort.

## **Security Operations**

The Security operations (SecOps) is responsible for maintaining and restoring the organization’s systems and networks on an ongoing basis. This approach aligns with the principles of the National Institute of Standards and Technology (NIST) which emphasizes detection, response, and recovery as key security functions. It involves identifying, containing, and recovering from incidents. It also focuses on monitoring for suspicious activity, such as identifying, prioritizing, and patching the vulnerabilities of the software or system (Cortex, n.d.) (Belding, 2022).

## **Software Development**

The Software Development System focuses on the integration of security practices in the entire software development life cycle. Because of several vulnerabilities in software products, software developers are forced to produce more secure systems from the very beginning of the development process (Keramati, Hssan, & Hosseinabadi, 2008).

The Software development domain can be applied to the university when creating a web application, for example, and in the early design phase. When developing the application, the developer will have to consider security and coding practices to identify potential vulnerabilities (Microsoft, 2024).

Benefits: Significant cost advantage after deploying the software (Cost of post-deployment patching will be minimized).

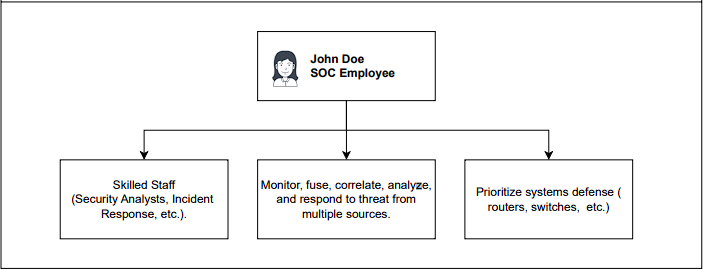
Drawbacks: Increase of development time, Higher initial costs, Complexity in implementation.

# **Our Scenario**

## **Main Domain**

The paper focuses on the Security Operations domain, in which it will discuss the responsibility of a security operations center and its challenges regarding cyber security development. In a university context, the security operations are responsible for responding to incidents (such as phishing attacks, handling malware, and mitigating data breaches). Also, it will focus on the security monitoring of the university network traffic for unauthorized access attempts. Regular process to analyze university systems and applications (Scan, prioritize, and patch the vulnerabilities). The SecOps can work with the IT team and spread the information and education to the university staff, students, and employees (Ross, McEvilley, & Oren, 2022).

In an organization, a security operations center (SOC) is the core of the system’s defense. The SOC is responsible for defending and monitoring all network activities and systems logs, to detect, analyze, and respond to cyber-attacks (NIST, Security and Privacy Controls for Information Systems and Organizations, 2020).



*Figure 1. SOC’s Responsibility.*

*Conducted from* (NIST, Security and Privacy Controls for Information Systems and Organizations, 2020)

In general, the security operations domain includes the following terms, which are controlled by the SOC:

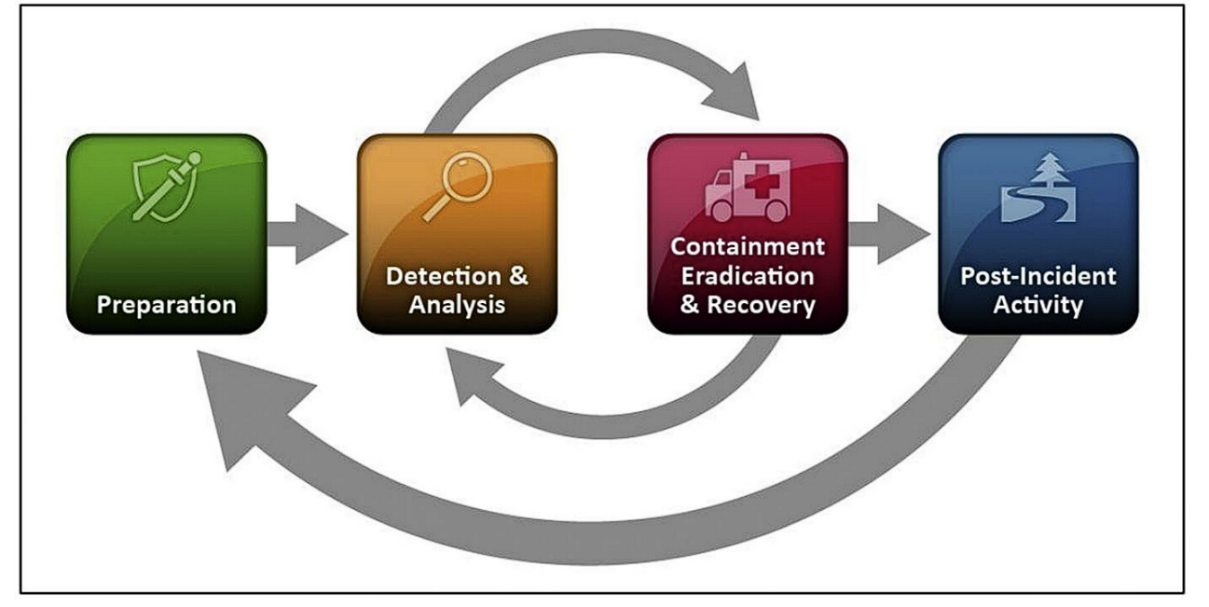
* Business Continuity Plan (BCP)
* Continuity of Operations Plan (COOP)
* Disaster Recovery Plan (DRP)
* Mean Time to Repair (MTTR)
* Mean Time Between Failures (MTBF)
* Redundant Array of Inexpensive Disks (RAID)

(Conrad, Misenar, & Feldman, 2016)

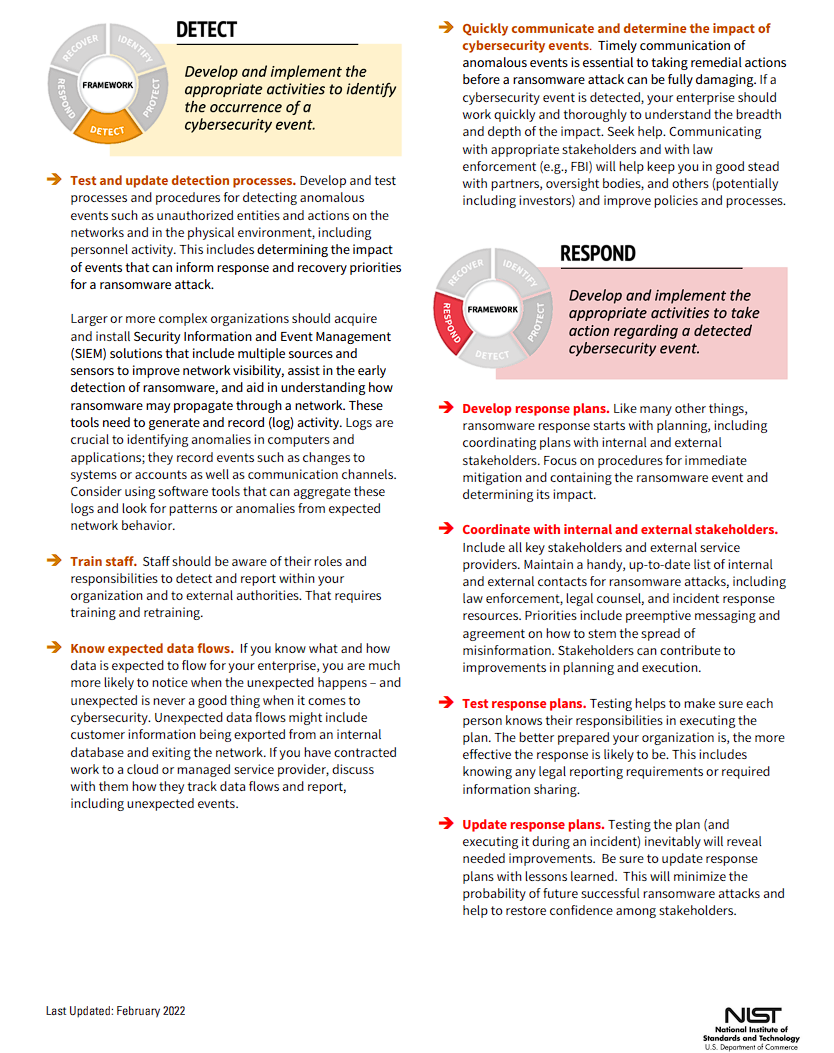
### **Benefits**

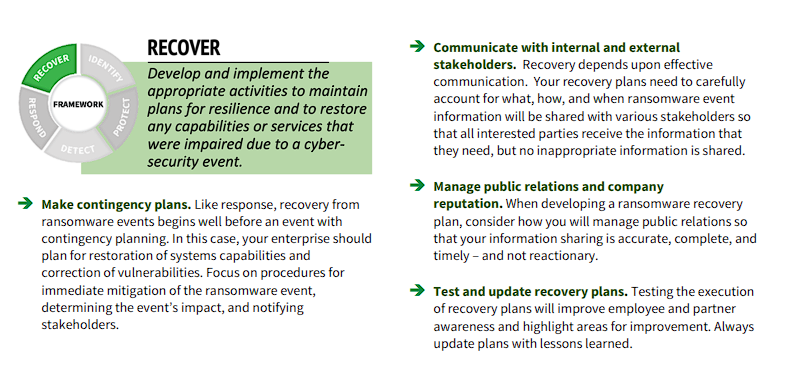
The use of SOC is essential for organizations to avoid potential cybersecurity threats. In the modernized technology world, cyber-attacks have evolved continuously and become sophisticated on an ongoing basis; hence, the SOC contributes a significant part in protecting against cyber criminals (Mughal, 2022).

* The Beneficial Factors of Technologies:
* Security Orchestration, Automation, and Response (SOAR): The implementation of SOAR generates and records incident response progress, improving its effectiveness (Watson, 2021).
* Endpoint Detection and Response (EDR): EDR implementation is for monitoring and protecting endpoints, or network devices (Illinois, n.d.).
* Network Detection and Response (NDR): NDR implementation is for monitoring and securing network traffic to analyze malicious security activities and respond on time (Vectra, n.d.).
* Artificial Intelligence (AI): The implementation of AI increases automation and allows faster response to threats. Moreover, AI enhances accuracy in detecting potential attacks.

**

*Figure 2. NIST Incident Response Life Cycle*. *Conducted from* (Conrad, Misenar, & Feldman, 2016)

**

**

*Figure 2 & 3. Detect, Respond, and Recover Procedures in a ransomware attack. Conducted from* (NIST, Getting Started with Cybersecurity Risk Management | Ransomware, 2022)

* The Beneficial Factors of Standards, Guidelines, and Policies:

Operations security involves all individuals, resources, media, network devices, and the threats related to each of these factors (Conrad, Misenar, & Feldman, 2016). Policies will benefit the process by implementing regulations and guidelines for users, along with the standards for requirements.

### **Challenges**

The most common threats that are recorded by SOCs are phishing attacks, however, education on defense training shows inefficient results since the issues continue to exist (Soneji, et al., 2019).

* Emerging cyber threats:

The constant modernization of IT infrastructures requires a continuous identification and analysis of incidents. In particular, well-known attacks such as malware, ransomware, etc. will be recognized by their common patterns, hence, new threats become harder to detect since there are no procedures to respond. Moreover, individuals who have access to the university network are exposed to cyber threats without the required knowledge to avoid potential incidents (Veilberth, Bohm, Fichtinger, & Pernul, 2019).

* Information Overload:

Without advanced automation and machine learning capabilities, the SOC or Computer Incident Response Team (CIRT) faces an extensive amount of information reported by users. Furthermore, the costs for sophisticated adversaries and artificial intelligence are required to scan and extract data, ensuring the mitigation of malicious activities. Thus, the detection and response department cannot analyze and resolve all threats in a proper time (NIST, Security and Privacy Controls for Information Systems and Organizations, 2020).

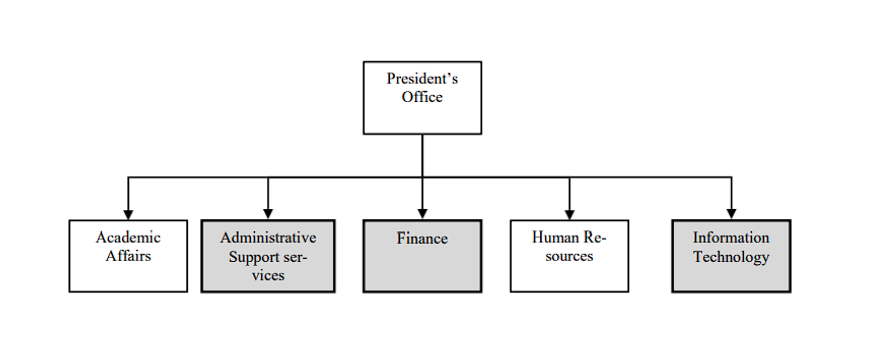
* Lack of Best Practices and Standards:

In the current context, there is no universal standard for a SOC framework to implement and audit, indicating a lack of best practices for security operations. Despite the contribution from the industry guidelines, cyber-attack still occurs through the same patterns as utilizing an inattentive moment of a user. Therefore, the needs for further education and practices are crucial to protect sensitive data resources. In addition, best practices require the collaboration of regulators, standardization methods, and industry professionals (Veilberth, Bohm, Fichtinger, & Pernul, 2019).

### **Summary**

In general, the security operations domain provides distinctive options for recovery and response process, while enhancing the management of detecting and avoiding cyber threats, such as ransomware attacks. The challenges that affect SOCs indicate further development and innovation for security guidelines. Regarding all individuals in an organization, awareness training is important in detecting and preventing such attacks. Moreover, the unique processes of a SOC are inapplicable to integrate across the organization, increasing a major concern in cost management. In the context of the challenges, security practices need comprehensive guidelines and definitions for each distinctive area of the SOC or it would be impossible to define and mitigate those incidents. Hence, technological developments, best practices, and guidelines need alignment and integration with the current organization infrastructure to maximize the advancement of security operations (Veilberth, Bohm, Fichtinger, & Pernul, 2019). According to (Soneji, et al., 2019) the majority of cyber-attacks such as ransomware and malware occur by losing user credentials and phishing emails, thus, all individuals must take responsibility for acknowledging cyber threats and reporting on time.

## **Organization Hierarchy**



*Figure 4. Organization Hierarchy*

## **Technical Details**

Since 2010, the university has used Windows Active Directory to manage all their PCs and Laptops, making it easy for Administrators to manage the network and for users to access their resources on the network. Active Directory uses a directory hierarchical structure that stores data about objects. These objects include accounts, servers, volumes, physical computers, printers, etc. (Microsoft) 

## **Security Details**

The AD domain uses standard usernames and passwords for login. The password must consist of over 12 characters, including upper and lowercase letters and at least one special character.  Students are required to change their passwords every year.

## **The Breach**

Data breaches, putting it simply, occur when the security in context has been bypassed or negatively affected, leading to either third parties being able to access classified information of organizations/groups, or that information being released out in public. What is not simple, however, is the process by which the problem occurs to corporations, even the most prestigious ones out there. Despite technological advancements, data breaches are still one of the most prominent threats out there, because all it takes is one opening. These openings manifest in different ways, however, the two main causes are quite straightforward: the insiders giving away information, whether innocently or maliciously – normally coming from a disgruntled employee, or in rare occasions, specialized agents, and opportunistic hackers looking for quick pay. The following section of the paper will highlight the importance of the eight domains of CISSP in an organization’s data security.

One day, the IT department was notified that multiple PCs and laptops were hit with ransomware demanding that the University pay the hackers money or else they would release all of their data to the public and leave the data completely unrecoverable as they had encrypted most of their volumes in their internal servers and computers.

## **The Investigation**

After a thorough investigation of the entire domain, many tracks were found that the hackers had left behind during the attack. The hacker used a compromised student account to gain an initial foothold on the system with a post of university password change. Then, they abused the Kerberoasting vulnerability within the domain to obtain the hash of the svc\_sql service account. (Mitre, Steal or Forge Kerberos Tickets: Kerberoasting, 2020).

The attacker then cracked the password. The investigation revealed that the admin set a weak password for the SQL service account on the domain controller, resulting in the attacker managing to find out that svc\_sql has SeImpersonatePrivilege right*,* which allows the attacker to escalate to NT AUTHORITY\SYSTEM. This is known as the highest privileged Windows account in a machine, in this case, the domain controller itself (Mitre, Access Token Manipulation, 2017).

After the hacker successfully hacked the system, they extracted a large amount of sensitive data such as names, emails, and ID/social security numbers of all university students and left behind ransomware that quickly spread throughout the network as they had in their possession the credentials of most computers within the domain by dumping the NTDS, which contains the credentials of all users within the domain (Mitre, OS Credential Dumping: NTDS, 2020).

## **Policy**

In a university context, the following Issued-Specific Policy is conducted to align with the organization’s current policies regarding information security (Whitman & Mattord, 2019).

### **Statement of Purpose:**

The ISSP provides clear guidelines to prevent, detect, and respond to such attacks as Akira’s ransomware. This policy is based on the NIST Special Publication framework, which outlines principles and practices for securing information technology systems.

#### **Scope and Applicability**

Applicability refers to defining the subjects that the policy applies to (NISTpubs, SECTION II: MANAGEMENT CONTROLS, 2014). This policy provides guidelines for all persons who have access to administrative databases, university resources, and data collection. It covers the possible parts where ransomware’s attack begins.

The policy covers all internet-based devices in the university infrastructure, such as computer devices, smartphones, apps, and third-party services.

#### **Roles and Responsibilities**

* The Users of Systems:

Students and staff must be notified and instructed about common threats such as malware, ransomware, account security, etc. to avoid and minimize the risk of accidentally installing ransomware.

* Users of Systems Responsibility:

Detecting threats and reporting to the SOC (NISTpubs, Chapter 3: Roles & Responsibilities, 2012).

### **Authorized Uses**

#### **User Access**

It is essential to monitor the authority’s actions, all approval permissions must be recorded for further investigation. Besides, individual activities also required detailed clarification regarding unauthorized connections/ applications.

#### **Fair and Responsible Use**

Protecting data privacy serves as a key legal issue in the context of this scenario (Whitman & Mattord, 2019). Users are required to utilize database resources and network resources only for work purposes and follow basic guidelines and standards to avoid threats such as phishing emails, untrusted links, etc.

#### **Protection of Privacy**

Users must follow principles according to data protection laws and the university’s data privacy and are responsible for protecting personal data along with the organization’s resources. According to NIST Special Publication 800-12, password security should be implemented to secure personal accounts by applying rules on password requirements, log-in attempts, technical protection of the password file, etc. to protect authentication and identification of the users.

### **Prohibited Uses**

#### **Disruptive Use or Misuse**

Users must avoid using the system’s network for personal purposes since an individual’s action can affect the university’s security operations. According to (Swanson, Hash, & Bowen, 2016), the university should conduct regulations on preventing unauthorized data and connections.

The law of Privacy and Information Security states that organizations and their employees are responsible for protecting sensitive data. Consequences for disruptive use of resources include fines, imprisonment, and the withdrawal of professional licenses (Stanford, n.d.).

#### **Criminal Use**

To keep the PII confidentiality impact level as being “low”, the university should implement Intranet Activity Tracking, which generates a web-use audit log recording the connections accessed by users (NIST, NIST Special Publication 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), 2010). The log contains:

* IP address
* URL of the website before and after accessing
* Date and time
* Topics that are accessed within the organization’s website

In this way, criminal actions such as exposing the database to ransomware attacks for self-gained purposes would be recognized and investigated.

#### **Copyrighted, Licensed, or Other Intellectual Property**

* Software Usage Restrictions:

The university should use a specialized tracking application to be able to control:

* The use of software and associated applications following copyright laws and contract agreements
* The distribution of information regarding quantity licenses to avoid unauthorized reproduction of copyrighted products.

In addition, the establishment of restrictions on access to open-source software is required to mitigate the derivative use of that software (NIST, NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, 2013).

#### **Other Restrictions:**

The university must prohibit activities that affect the confidentiality and integrity of internal systems, including un-trusted connections and unauthorized software.

### **Systems Management**

#### **Management of Stored Materials**

The recovery backup is required to ensure the loss of information in the system is recoverable, this records the data onto other systems such as cloud storage, local hard drive storage, etc. (NIST, NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, 2013). According to CP-9, Contingency Planning-Information System Backup, regular data backup checks, and upgrades are essential to secure the protection of data sources. The backup prioritizes information based on sensitivity and risk level (NIST, PROTECTING DATA FROM RANSOMWARE AND OTHER DATA LOSS EVENTS, n.d.).

In a ransomware attack, academic resources and individual personal information are the priorities of the backup. The Cloud-based backup service providers and encryption should be implemented to store the data backup and secure its access (NIST, Securing Data Integrity Against Ransomware Attacks:, 2020) (ISO-27002, ISO 27002:2022, Control 5.23 – Information Security for Use of Cloud Services, 2022).

#### **Employee Monitoring**

Information security monitoring is to maintain the awareness of risks and threats conducted by employees (NIST, Information Security, 2011). According to (ISO-27002, ISO 27002:2022, Control 8.16 – Monitoring Activities, 2022), the university should identify network behavior as a baseline to analyze across the network to detect unauthorized access to internal data resources.

#### **Virus Protection**

The university should ensure that the policies have covered the prevention of malware and ransomware incidents. The responsibility lies in both internal and external factors that access to the university network, including:

* Scan the applications, files, and email attachments before accessing.
* Prohibit sending and receiving various types of files (zip files, exe files, etc.) via e-mailing and e-messaging
* Restrict the use of removable storage
* Specify and provide regular updates on anti-virus software.
* Restrict the use of personal internet devices in the internal network

(NIST, NIST Special Publication 800-83 Guide to Malware Incident Prevention and Handling for Desktops and Laptops, 2013)

#### **Encryption**

Encryption is defined as transforming visible data into an encrypted form. The university should use cryptography, which is a mathematical formula to encrypt the data to protect the sensitive information in the network, such as personal identity, credit cards, academic research, etc. (NIST, Chapter 19: Cryptography, 2014). The university should use encryption for sensitive files.

### **Violations of Policy**

#### **Procedures for Reporting Violations**

In a ransomware attack, logs of modification of files and Active Directory changes to logging adjustments are required to record and detect suspicious attachments and the data that have been modified by it.

* The log and report of the system should be available to support the IT team in addressing the threat
* The detection should be available to analyze the modifications made before and after the installation of the attachment
* The mitigation and containment should be available to alert users when the attachment appears.
* The forensics/analytics should be available to analyze the network traffic made by the suspicious file.

(ISO-27002, ISO 27002:2022, Control 6.4 – Disciplinary Process, 2022)

### **Policy Review and Modification**

#### **Procedures for Modification**

* Review of information security management system (ISMS), which addresses internal and external issues that are relevant to the university breach
* Review awareness training of employees on ransomware attacks, such as information security in general, and its best practices.
* Review user access rights determination and definition
* Review back-up test

(Petrov, 2022)

# **Forensics**

“Forensic science” is defined as the application of scientific principles to detect criminal vestiges, including analyzing, interpreting, or collecting pieces of evidence from crime scenes during the investigation to assist in decision-making legally regarding civil law or regulatory issues (Office, 2016).Along with the outburst of the digital era with the rapid growth of the Internet, in 2012, Marcus J. Ranum first mentioned the term “Network Forensics,” which became a crucial topic nowadays and placed an emergency alert in network security. “Network Forensics” can be considered a sub-sub-branch of forensic science in general that involves detecting attackers’ behavior after a crime happens on the network to prevent the same scenario from occurring (Bijalwan, 2021).

Network forensics investigates the attacks that come from both ingress and egress traffic, analyzes traffic data logged through firewalls or IDS or at network devices like routers and switches, and indicates whether there was an anomaly log. If there indicated an attack, network forensic techniques empower investigators to trace back the attackers to provide evidence to prosecute the perpetrators (R.C. & Pilli, 2016).

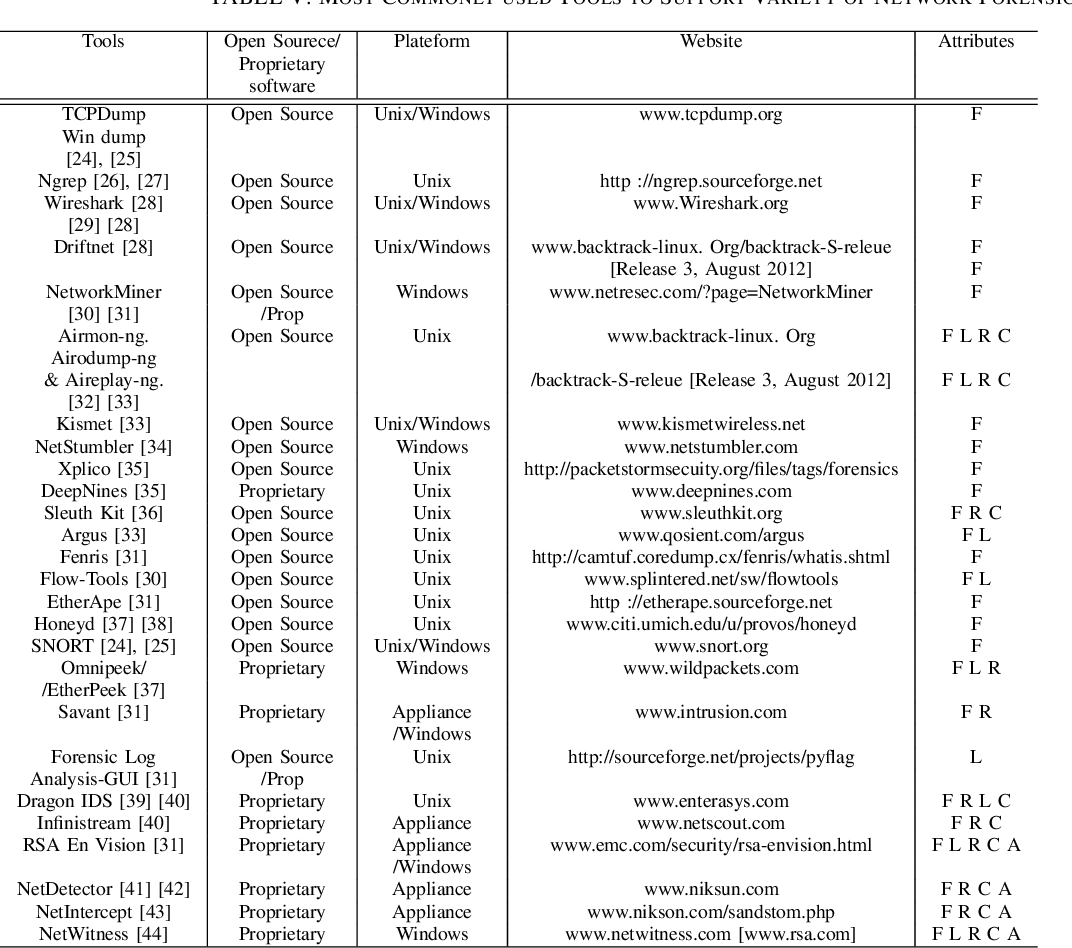
Authentication and reliability are pivotal in forensic evidence due to their contribution to acceptance in a court of law. That consequently required the tools and techniques used during the investigation to meet all legal and technological conditions in a court. In this context, network forensics helps identify corporate network vulnerabilities that make implementing the necessary security enhancements convenient (Qureshi, Akhtar, Tunio, Nazir, & Ullah, 2021).

In network forensic investigation, the main processes are strategically operated based on OSCAR principles.



*Figure 5. Process in OSCAR principles, conducted from* (Jaswal, 2019)*.*

Additionally, using relevant tools in investigating also helps the university to gather essential information about the intrusion more accurately and reliably. Network forensic tools are designed to compete with network hardware devices and make them available to retrieve while preserving network traffic. Host-based and network-wide-based are the common uses of network forensic tools, including general-purpose tools, specific task tools, or libraries/framework tools (Qureshi, Akhtar, Tunio, Nazir, & Ullah, 2021).



*Figure 6. Forensic tools, conducted from* (Qureshi, Akhtar, Tunio, Nazir, & Ullah, 2021)*.*

# **Conclusion**

To-conclude,-the-report-addresses-a-scenario-of-Stanford’s-data-breach-to-emphasize-the-vital-role-of-the-Security-Operations-domain-in-detecting-and-responding-to-cyberattacks.-In the-current-world-of-technology,-the-constant-development-of-information-security-is-required-due-to-the-continuous-cases-of-cyber-criminals.-The-data-breach-at-Stanford-caused-a-significant-loss-to-the-university's-financial-state,-the-stolen-identity-and-banking-credentials-of-individuals-could-be-utilized-to-perform-illegal-activities.-Therefore,-securing-private-and-sensitive-information-is-crucial-for-an-organization-to-protect-not-only-the-business-but-also-the-legal-rights-of-each-individual-inside.-Additionally,-the-eight-domains-of-CISSP-serve-as-essential-guidelines-and-standards-for-a-qualified-and-secured-cyber-environment.

# **Reference**

Belding, G. (2022, March 21). CISSP domain 7: Security operations — What you need to know for the exam [Updated 2022]. *InfoSec*. Retrieved June 24, 2024, from https://www.infosecinstitute.com/resources/cissp/security-operations/

Bijalwan, A. (2021). *Network Forensics: Privacy and Security.* Chapman and Hall/CRC. Retrieved 06 26, 2024

CISSP. (n.d.). Domain 3: Security Architecture and Engineering. In P. C. Security, *CISSP Certification Exam Outline.*

Conrad, E., Misenar, S., & Feldman, J. (2016). *Chapter 8 - Domain 7: Security Operations.* doi:https://doi.org/10.1016/B978-0-12-802437-9.00008-4

Cortex. (n.d.). Security Operations (SecOps). *Cortex*. Retrieved June 24, 2024, from https://www.paloaltonetworks.com/cyberpedia/what-is-security-operations

Council, F. T. (2023, November 8). Identity And Access Management: 18 Important Trends And Considerations. *Forbes*. Retrieved June 24, 2024, from https://www.forbes.com/sites/forbestechcouncil/2023/11/08/identity-and-access-management-18-important-trends-and-considerations/

Coursera. (n.d.). Professional Certificates - Cybersecurity. *Coursera*. Retrieved June 2024, 24, from https://www.coursera.org/programs/british-university-v-google-learning-program-24fx4/professional-certificates/google-cybersecurity?collectionId=qUSVb

Educause. (n.d.). Identity and Access Management. *Educause*. Retrieved June 24, 2024, from https://library.educause.edu/topics/cybersecurity/identity-and-access-management

Illinois. (n.d.). End Point Detection & Response (EDR). *Doit Illinois*. Retrieved June 24, 2024, from https://doit.illinois.gov/initiatives/cybersecurity/slcgp/end-point-detection-and-response--edr-.html

Imam, F. (2021, June 16). CISSP domain 2: Asset security - What you need to know for the Exam [updated 2021]. *InfoSec*. Retrieved June 24, 2024, from https://www.infosecinstitute.com/resources/cissp/cissp-domain-2-asset-security-need-know-exam/

ISO-27002. (2022). ISO 27002:2022, Control 5.23 – Information Security for Use of Cloud Services. *ISO*. Retrieved June 24, 2024, from https://www.isms.online/iso-27002/control-5-23-information-security-for-use-of-cloud-services/

ISO-27002. (2022). ISO 27002:2022, Control 6.4 – Disciplinary Process. *ISO*. Retrieved June 24, 2024, from https://www.isms.online/iso-27002/control-6-4-disciplinary-process/

ISO-27002. (2022). ISO 27002:2022, Control 8.16 – Monitoring Activities. *ISO*. Retrieved June 24, 2024, from https://www.isms.online/iso-27002/control-8-16-monitoring-activities/

Jaswal, N. (2019). *Hands-On Network Forensic.* Retrieved June 24, 2024, from https://paper.bobylive.com/Security/Hands-On-Network-Forensics.pdf

Keramati, H., Hssan, S., & Hosseinabadi, M. (2008). *Integrating software development security activities with agile methodologies.* doi:https://doi.org/10.1109/AICCSA.2008.4493611

Microsoft. (2024, May 24). Microsoft Security Development Lifecycle (SDL). *Microsoft*. Retrieved June 24, 2024, from https://learn.microsoft.com/en-us/compliance/assurance/assurance-microsoft-security-development-lifecycle

Mitre. (2017, December 14). Access Token Manipulation. *Mitre Attack*. Retrieved from https://attack.mitre.org/techniques/T1134/

Mitre. (2020, February 11). OS Credential Dumping: NTDS. *Mitre Attack*. Retrieved June 24, 2024, from https://attack.mitre.org/techniques/T1003/003/

Mitre. (2020, February 11). Steal or Forge Kerberos Tickets: Kerberoasting. *Mitre Attack*. Retrieved June 24, 2024, from https://attack.mitre.org/techniques/T1558/003/

Mughal, A. A. (2022). *Building and Securing the Modern Security Operations Center (SOC).* doi:https://orcid.org/0009-0006-8460-8006

NICCS. (2024, May 19). CISSP 2021: Communication & Network Security. *NICCS*. Retrieved June 24, 2024, from https://niccs.cisa.gov/education-training/catalog/skillsoft/cissp-2021-communication-network-security

NIST. (2010). *NIST Special Publication 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).* Retrieved June 24, 2024, from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf

NIST. (2011). *Information Security.* Retrieved June 24, 2024, from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf

NIST. (2013). *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations.* Retrieved June 24, 2024, from https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf

NIST. (2013). *NIST Special Publication 800-83 Guide to Malware Incident Prevention and Handling for Desktops and Laptops.* doi:http://dx.doi.org/10.6028/NIST.SP.800-83r1

NIST. (2014, August 4). Chapter 19: Cryptography. *NIST*. Retrieved June 24, 2024, from https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter19.html

NIST. (2020). *Securing Data Integrity Against Ransomware Attacks:.* Retrieved June 24, 2024, from https://nvlpubs.nist.gov/nistpubs/cswp/NIST.CSWP.10012020-draft.pdf

NIST. (2020). *Security and Privacy Controls for Information Systems and Organizations.* National Institute of Standards and Technology, U.S. Department of Commerce. Retrieved June 24, 2024, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

NIST. (2022). *Getting Started with Cybersecurity Risk Management | Ransomware.* Retrieved June 24, 2024, from https://csrc.nist.gov/files/pubs/other/2022/02/24/getting-started-with-cybersecurity-risk-management/final/docs/quick-start-guide--ransomware.pdf

NIST. (2024, June 14). NIST Risk Management Framework RMF. *NIST*. Retrieved from https://csrc.nist.gov/projects/risk-management/about-rmf

NIST. (n.d.). *PROTECTING DATA FROM RANSOMWARE AND OTHER DATA LOSS EVENTS.* Retrieved June 24, 2024, from https://www.nccoe.nist.gov/sites/default/files/legacy-files/msp-protecting-data-extended.pdf

NISTpubs. (2012, January 31). Chapter 3: Roles & Responsibilities. *NIST*. Retrieved June 24, 2024, from https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter3.html

NISTpubs. (2014, July 25). SECTION II: MANAGEMENT CONTROLS. *NIST*. Retrieved June 24, 2024, from https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter5.html

Office, E. (2016). *REPORT TO THE PRESIDENT Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods.* Retrieved June 24, 2024, from https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast\_forensic\_science\_report\_final.pdf

O'Reilly. (n.d.). *Network Security Assessment: Know Your Network.* Retrieved June 24, 2024, from https://books.google.com.vn/books?hl=pt-BR&lr=&id=Gm\_0CwAAQBAJ&oi=fnd&pg=PR5&dq=Security+Assessment+and+Testing+microsoft&ots=uCjw-3cKF3&sig=iP5Jcv5Bgc8jPb8koetWZOif8G4&redir\_esc=y#v=onepage&q=security&f=false

Petrov, M. (2022, June 14). Mandatory Manual Reviews and Audits – ISO 27001 Requirements. *Digital Edge*. Retrieved June 24, 2024, from https://knowledge.digitaledge.net/compliance/mandatory-manual-reviews-and-audits-iso-27001-requirements

Qureshi, S., Akhtar, F., Tunio, S., Nazir, A., & Ullah, F. (2021). *Network Forensics: A Comprehensive Review of Tools and Techniques.* Retrieved June 24, 2024, from https://thesai.org/Downloads/Volume12No5/Paper\_103-Network\_Forensics\_A\_Comprehensive\_Review.pdf

R.C., J., & Pilli, E. S. (2016). *Fundamentals of Network Forensics.* Retrieved June 24, 2024, from https://content.e-bookshelf.de/media/reading/L-7875078-fd50acbb40.pdf

Ross, R., McEvilley, M., & Oren, J. (2022). *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.* doi:https://doi.org/10.6028/NIST.SP.800-160v1

SailPoint. (2024, May 28). What is identity and access management (IAM)? *SailPoint*. Retrieved June 24, 2024, from https://www.sailpoint.com/identity-library/identity-and-access-management/

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008, September). *NIST SP 800-115 Technical Guide to Information Security Testing and Assessment.* doi:https://doi.org/10.6028/NIST.SP.800-115

Soneji, A., Kokulu, F. B., Shoshitaishvili, Y., Zhao, Z., Ahn, G.-J., Bao, T., & Doupe, A. (2019). *Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues.* London. Retrieved June 24, 2024, from https://dl.acm.org/doi/pdf/10.1145/3319535.3354239

Stanford. (n.d.). Protecting Sensitive Data at Stanford. *Stanford Unversity*. Retrieved June 24, 2024, from https://uit.stanford.edu/security/sensitivedata

Swanson, M., Hash, J., & Bowen, P. (2016). *NIST SP 800-18 Rev. 1 Guide for Developing Security Plans for Federal Information Systems.* doi:https://doi.org/10.6028/NIST.SP.800-18r1

Vectra. (n.d.). Network Detection and Response (NDR). *Vectra*. Retrieved June 24, 2024, from https://www.vectra.ai/topics/network-detection-and-response

Veilberth, M., Bohm, F., Fichtinger, I., & Pernul, G. (2019). *Security Operations Center: A Systematic Study and Open Challenges.* doi:https://doi.org/10.1109/ACCESS.2020.3045514

Watson, K. K. (2021). *Orchestration of Information Technology (IT) Automation Frameworks .* Retrieved June 24, 2024, from https://www.cisa.gov/sites/default/files/publications/Orchestration%2520of%2520Information%2520Technology%2520Automation%2520Frameworks\_508c.pdf

Whitman, M. E., & Mattord, J. H. (2019). *Management of Information Security* (6th ed.). Retrieved June 24, 2024, from https://read.kortext.com/reader/pdf/281741/ii