NETWORKING CONCEPT & CYBER SECURITY

Assessment & Analysis of the University of California San Francisco ransomware attack 2020

HAN22080031

HAN22080413

HAN22080120

HAN22080256

CONTENTS

Introduction 3

Prevalence of data breaches in educational systems.....4

UCSF ransomware attack 2020 5

8 domains of cybersecurity.....6

Security & Risk Management.....7

.....8

Security Operation.....9

Communications & Network Security.....10

Security Architecture & Engineering 12

Identity & Access Management 13

Security Assessment & Testing.....16

Software Development Security.....16

Asset Security.....17

Forensics & Security Audit.....18

Security Audit & Policy 19

Forensics.....27

References.....32

INTRODUCTION

Prevalence of data breaches in educational systems

Since 2005, over 2,691 data breach cases have been reported by US colleges/universities and have affected over 32 million individual records (Sam, 2023). During the COVID-19 pandemic, most colleges/universities were forced to carry out lectures in a virtual environment, making the educational system more vulnerable to cyber-attacks (Mololuwa, 2022).

This drastically increased the number of cyber-attacks with 2,97 million records leaked in 2020 and 2,6 million records leaked in 2021 and the highest recorded amount of data breach cases per year at 771 in 2021, classifying COVID-19 as the largest-ever cybersecurity threat (Sam, 2023).

During the COVID-19 pandemic, the most common cyber-attack was a ransomware attack. The attacker would inject a system with encryption malware that encrypted data such as Microsoft Word documents, images, databases, etc. The private key to decrypt the data would only be available after the victim had paid a specific amount of ransom hence the name ransomware attack (Trellix 2023).

UCSF ransomware attack 2020

On June 3, 2020, the University of California San Francisco IT staff detected a security breach incident in a part of the UCSF School of Medicine's IT environment that started 2 days prior on June 1, 2020. Several IT systems within the School of Medicine had to be "isolated from the core UCSF network" (CBS San Francisco, 2020) and shut down to stop the attack as it was occurring.

The attack consisted of malware that encrypted any data within range without any specific target which "left the servers inaccessible" (CBS San Francisco, 2020) with UCSF luckily stating, "this incident did not affect our care delivery operations, overall campus network, or COVID-19 work" (UCSF, 2020).

UCSF started working with cybersecurity experts and eventually got in contact with the Netwalker ransomware group (which was responsible for the ransomware attack). After a series of negotiations, the UCSF "made the difficult decision to pay some portion of the ransom" (UCSF, 2020) which was equivalent to $1.14 million as "the data that was encrypted is important to some of the academic work" (UCSF, 2020) that UCSF was pursuing.

8 DOMAINS OF CYBERSECURITY

Security & Risk Management

The focus of security & risk management is the identification and mitigation of cyber threats. To fulfill this task many concepts of risk and risk management such as probability, likelihood, and consequence must be discussed (Clinton L., David J. 2013). Therefore, a risk management framework is needed to accommodate all the areas of risk management.

ISO31000 is a risk management framework used for the identification, analysis, evaluation, treatment, monitoring, and communication of risks. Each department of an organization will be assigned accountabilities and responsibilities based on the assessed risk which is calculated based on the previously mentioned concepts such as probability, likelihood, and consequence. Necessary resources will also be allocated to each department for risk prevention (ISO 2009).

For this framework to be implemented at the University of California San Francisco (UCSF), the UCSF must follow the three stages of establishing context, risk assessment, and risk treatment.

In the first stage, UCSF should analyze its strengths and weaknesses and determine all existing risks. The UCSF should also take into account areas in their organization that they can afford to risk and what areas shouldn’t be at risk at all costs. Afterward, all possible consequences of UCSF's weaknesses should be listed.

UCSF will end up with a long list of risks and consequences that will be used for the risk assessment process. Each risk should be grouped based on the type of consequences such as financial risks, environmental risks, or security risks. Finally, each risk should be reviewed for the last time and ranked on the consequence scale, a scale from A to E based on the consequence, and the likelihood scale, a scale from 1 to 6 based on the likelihood of occurrence. A final list should be formed and should have all risks, their affected department, and a ranking of the severity of the consequence and likelihood of occurrence (Clinton L., David J. 2013).

The risk treatment stage of the ISO31000 process focuses on reducing, avoiding, and transferring risks. This process is harder to implement for UCSF due to the budget requirement of this process. UCSF can simply give this list to all affected departments and spread awareness of such risks and if possible, allocate resources to departments of higher risk. One of the best options for risk mitigation is changing the policy to enforce higher standards and having a specific security audit for data breach cases.

Consequence Scale

Scale	Rank	Descriptor
Catastrophic	A	Organization will cease to function if harm is realized
Very high	B	Major impact on organization's ability to function and may lead to a prolonged period of nonfunction; a major change in operations will be required
High	C	Significant effect on organization's operations and activities
Medium	D	Impact on organization's ability to function, but recoverable with little effort
Low	E	Covered by usual allowances
Unknown	U	Consequence of harm being realized is unknown

Likelihood Scale

Scale	Rank	Descriptor
Certain	1	The event will be realized
Very high	2	Highly probable
High	3	Moderately probable
Medium	4	Probable
Low	5	Improbable

Security Operation

SecOps (security operations) consists of an organization's internal information security and IT operations team and focuses on protecting the organization from cyber threats. Inside the SecOps, there is the Security Operations Center (SOC) department which is responsible for the detection and prevention of cyber threats.

An intrusion detection system (IDS) is a device or software application designed to monitor and detect unauthorized or malicious activities within a computer network or system. Its primary purpose is to identify potential security threat incidents, such as intrusion attempts, policy violations, or suspicious behavior, and report them to the administrator. Implementing such a device or software in the UCSF network system would let the SOC department have more control over the network traffic in the UCSF network.

There are two types of IDS the UCSF should implement into its network system, a network intrusion detection system (NIDS) and a host intrusion detection system (HIDS).

Network intrusion detection systems (NIDS) are set up within network devices such as routers, switches, and firewall-located devices and examine the traffic within the network. The passing traffic on the subnet is being monitored and matched with a collection of known cyber-attacks such as port scanning, denial-of-service (DoS) attacks, and malware communication.

During the UCSF ransomware attack case, the intrusion of the encryption malware could have been detected with the implementation of NIDS.

Host intrusion detection systems (HIDS) run on independent hosts or devices. Similar to NIDS, HIDS monitors incoming and outcoming traffic within hosts and devices by taking snapshots of existing system files and comparing them to previous snapshots. Binary patterns are also compared to records of malware in a database to identify dangerous packets in a method called signature-based detection.

When a threat is detected by an IDS, an intrusion prevention system (IPS) will alert the administrator or take action to stop it. The two most compatible IPS with the UCSF network system are network-based IPS (NIPS) and host-based IPS (HIPS). Both IPS can block traffic from blacklisted IP addresses, reset connections, log malicious activity for future investigation, and alert administrators.

Communications & Network Security

Communications and network security deal with network operations that defend and protect the network system from threats and ensure the “availability, integrity, authentication, confidentiality, and non-repudiation” (Yi Qian 2014) of information on both users and management. Many network protocols will be used to restrict or stop access to network areas.

When mentioning network security, UCSF should implement the ACL protocol due to its effectiveness and quick implementation. An access control list (ACL) is a list of specified users who are either granted or denied access to a network system.

There are 2 types of ACL, standard and extended ACL. To make UCSF's security system more advanced, an extended ACL should be implemented due to its ability to block both source and destination IP addresses, which the standard ACL doesn't have. Therefore, reducing connections of potentially dangerous IP addresses or ports.

Due to the tremendous amount of network traffic in the UCSF network system, the connection should stay controlled to protect students and staff whether on-site or on the cloud. The UCSF can ensure reliable wireless communication based on 3 crucial factors which are authentication, encryption, and integrity. The PEAP (protected extensible authentication protocol) should be used for its advanced security and wide usage.

PEAP is an authentication protocol used in wireless networks and Point-to-Point connections. Each user will be provided with different keys, the server will create a TLS (transport layer security) tunnel and only allow users with authenticated keys to communicate. By applying this method to the university network system, USCF can prevent attacks like man-in-the-middle or Wi-Fi attacks.

For the integrity and encryption part, UCSF can use the Galois/Counter Mode Protocol (GCMP) which uses AES (advanced encryption standard) as encryption and the GMAC (graduate management admission council) to protect integrity. By implementing these protocols, UCSF can ensure the integrity of information sent and received by hosts which cannot be modified or seen by attackers or a third party.

Security Architecture & Engineering

Security architecture and engineering talks about designing and documenting a security program in a way that creates consistency and control over information. The model that UCSF should implement is the Biba Model which allows access to modification of information based on the four classifications:

- Highly trusted
- Trusted
- Slightly trusted
- Untrusted

The first rule of the Biba model is “No Write Up”, meaning a person can only write or modify information with an equal or lower level of integrity. This ensures that highly trusted documents are not being tampered with untrusted information.

The second rule is “No Read Down”, meaning a person can only read information with an equal or higher level of integrity. This is to prevent people with trusted status from getting untrusted information that could be written in trusted documents.

These two rules are often considered too restrictive. That is why there are often two additional principles added to make the model more flexible:

- Low Water Mark Policy for Objects: each time someone accesses an object, the integrity level of the object changes down to the lowest level of the two. This can indicate that certain objects have been contaminated.
- Low Water Mark Policy for Subjects: each time someone accesses an object, the integrity level of that person changes down to the lowest level of the two. This principle protects against Trojans.

Information that is trusted and is weighted more than other information, is not subject to modification without the right permission. The staff is also unable to read information with a lower trust level to ensure that false information that could damage or make the system vulnerable does not get through.

Identity & Access Management

IAM, also known as Identity and Access Management, focuses on managing users' identities and permissions on a network. Although different companies can have different IAM policies, the common goal of any IAM initiative is to ensure that the right users and devices can access the right resources at the right time, with appropriate reasons.

In simple terms, IAM aims to prevent threat actors from getting into the network system while making sure that authorized users can perform their work without being provided

more permissions than needed. With each company network being unique, leading to different policies, processes, and tools, IAM initiatives all cover these four key elements:

Identity lifecycle management (ILM)

Identity lifecycle management is the process of creating and maintaining a digitalized identity for every entity on a network. A digital identity tells the network who or what the entity is, and its permissions in the network. The information of the identity often includes standard account information such as name, ID number, login information, the role of the entity in the organization, their responsibilities, and access permissions. ILM is made of cycles of accepting new entities, modifying their accounts and permissions as time passes, and removing those entities that no longer need those permissions. UCSF can utilize this process to manage identity roles according to the university environment.

access control

Access control is a security technique that dictates who or what can view, use, or modify resources in a network environment. Many IAM systems use role-based access control (RBAC) to set and enforce access policies. In the RBAC system, a user's permissions are based on their job function or job role.

Nowadays, many companies apply the least privileged principle when setting user access permissions. Users are only allowed the lowest level of permissions necessary to complete the task, and they are revoked as soon as the work is done. This prevents users from being over-provided with permissions, which can pose a security risk to the organization. By utilizing access control, UCSF can avoid giving certain staff more permissions than they need, preventing permission overprovisioning.

authentication and authorization

IAM systems don’t just create identities and assign permissions, they also enforce those permissions through authentication and authorization. Authentication is the process of authenticating users and their roles. When a user requests access to a certain resource, the IAM system matches their credentials with the ones stored in their database and access is granted if they match. Once a user is authenticated, the IAM system checks the database for their access privileges, then authorizes the user to only access the resources and perform the tasks their permissions allow. Authentication and authorization are necessary for UCSF because weak authentication can lead to breaches from unknown threat actors, therefore compromising a section of the whole system.

identity governance

Identity governance is the process of tracking what users do with their resource access. IAM systems monitor users to ensure they don't abuse their privileges. Identity governance is

important for UCSF as it can prevent staff from accidentally or intentionally sabotaging the university's network system. Identity governance is also important for regulatory compliance. The UCSF can use activity data to make sure its access policies comply with data security regulations such as the General Data Protection Regulation (GDPR) or the Payment Card Industry Data Security Standard (PCI-DSS).

Security Assessment & Testing

Security assessment and testing is a CISSP domain that focuses on security assurance, identifying how security is contributing and being utilized for the goals and objectives of the organization, and ensuring the right level of security. In other words, security assessment and testing ensure that security systems are tested and operate effectively.

UCSF benefits from this domain as frequent security assessment ensures that the university network is safe and can discover vulnerabilities early on.

Software Development Security

Software development security is the result of securing software, ridding it of bugs and vulnerabilities, as that can be a

big threat to an organization’s security. Security needs to be included as an integral part of the software development life cycle (SDLC) as well as the system life cycle (SLC).

Asset Security

Asset security is the 2nd CISSP domain that aims to protect the organization’s assets that are deemed important or valuable through security structures and controls. Asset security is important because a single minor vulnerability can cause a system to be exposed to a potential attack, which can potentially compromise an organization.

FORENSICS & SECURITY AUDIT

Security Audit & Policy

There are 3 most important control assessments that the UCSF should implement which would play an essential role for the university's security.

Administrative/Managerial controls consist of policies and procedures that focus on how an organization manages data and employee responsibilities.

Administrative Controls			
Control Name	**Control type and explanation**	**Needs to be implemented (X)**	**Priority**
password policies	preventative: create a strong password which can prevent brute force attacks or dictionary attacks	X	High
disaster recovery plans	corrective: assure that systems always run even during downtime		
least privilege	preventative: ensure access is not being over distributed and only being distributed when necessary	X	High

access control policy	preventative; improve confidentiality and integrity of data by monitoring access and privileges	X	High

Technical controls consist of solutions such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), etc.

Technical Controls			
Control Name	**Control type and explanation**	**Needs to be implemented (X)**	**Priority**
IDS/IPS	detective: detects and prevents intrusion	X	High
encryption	deterrent: uses RSA and AES to improve the confidentiality of sensitive data	X	Medium
backup	corrective: create backups to support ongoing altered data events	X	High

SIEM tools	detective: analyze and alert administrator if attack occurs	X	High

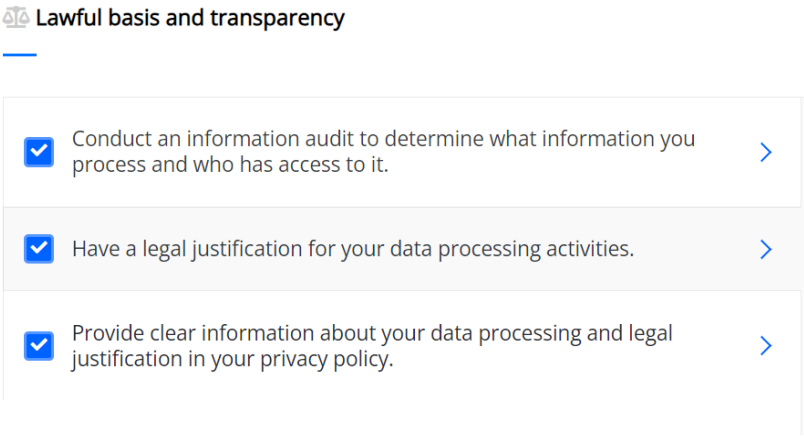
Physical controls focus on the prevention of physical access to physical assets which includes door locks, surveillance cameras and badge readers.

Physical Controls			
Control Name	**Control type and explanation**	**Needs to be implemented (X)**	**Priority**
closed-circuit television	preventative: monitor people accessing to sensitive data or trying to access to certain locations	X	High
locking cabinets (for network gear)	preventative; protecting network gear from unauthorized access and	X	High

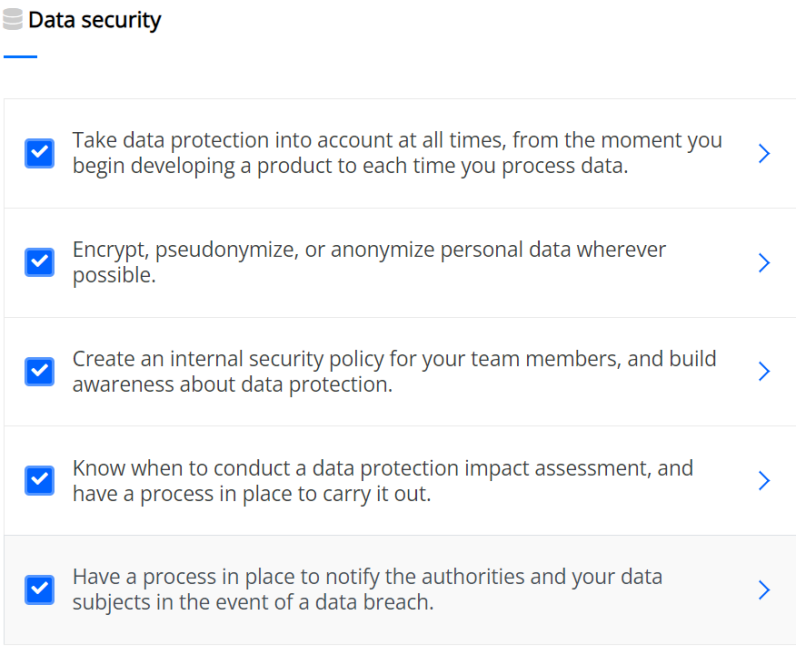
	altering network gear		
fire detection and prevention	preventative: fire detection system	X	High
locks	preventative: physical and digital assets are more secure	X	Hight

Compliance checklist

The best Compliance checklist that the UCSF should follow is the GDPR due to its compliance laws dictating how businesses in the European Union process and protect data privacy. The four phases in this process involve planning, gap analysis, closing the gaps, and evaluation of new procedures. A GDPR compliance audit strengthens data security and builds customer trust, this is the best option for universities like UCSF to comply in order to strengthen data security to avoid cyber threats.

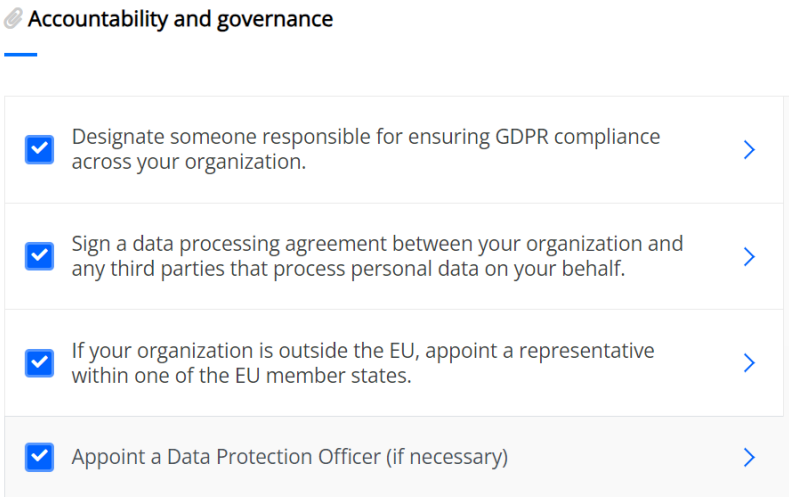


The UCSF should show that they have the authorization to store data and conduct a list that consists of the purpose of processing data, what kind of data is being processed, who has access to it in the organization, and any third parties.

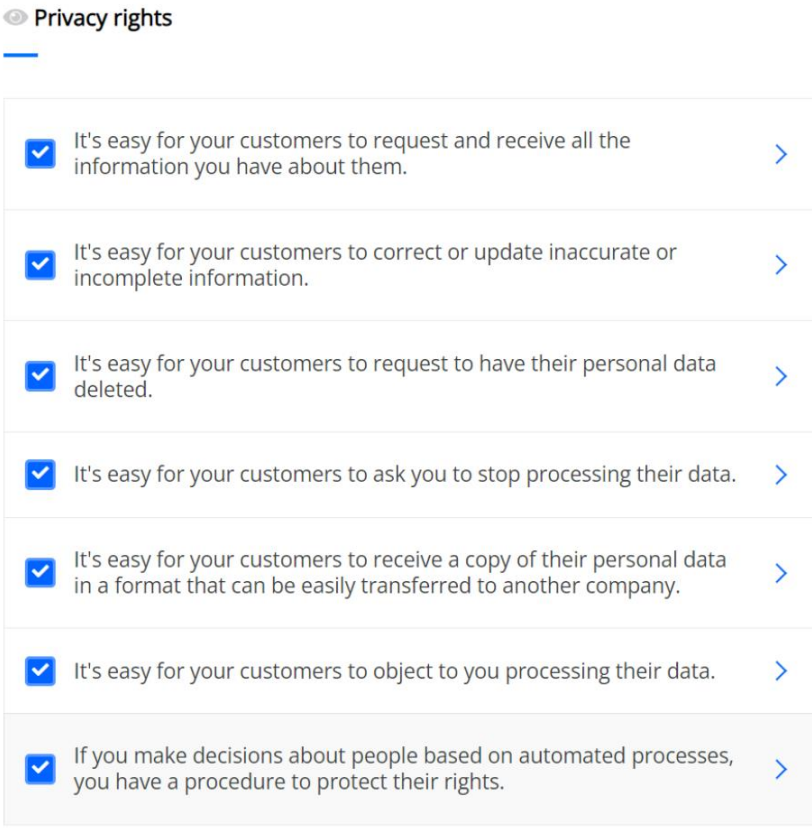


In this category, UCSF should provide the data stored and customer and staff-kept data. Moreover, UCSF should also train its employees to be aware of internal data protection policies. Lastly and most importantly, if there is a breach case like ransomware, UCSF must announce it to the supervisory authority within 72 hours. Failure to notify the issue can be penalized up to 10 million euro or 2% of the company revenue.

Accountability and governance



UCSF should choose a Data Protection Officer as the one who is responsible for it. If the UCSF cooperates with third parties, the data protection officer should make an agreement and sign a contract on data processing responsibilities.



It is advised for UCSF to provide each student with a school account and request personal data. UCSF should give their students permission to update their false information.

Forensics

Intro

So far, we've discussed many preventative measures that UCSF can implement to enhance their security system, but now we are going for the investigation part in the case study and provide some forensic guidance.

Digital forensic

"Digital forensic science is a branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to cybercrime." (EC-council) There are many different forensic fields, but in this essay, we are just going for field that related to the case study and they are the most 2 important one which are computer forensic and network forensic.

Computer forensics

"Computer forensics is the investigation of computer crimes with the objective of identifying and prosecuting the perpetrator. It involves the collection, examination and safeguarding of information from and related to computer systems that can be used to pinpoint and prosecute the perpetrator." (Cybrary) If UCSF is attacked again by malware or ransomware like in the

case study, we can investigate the culprit by going through some processes.

Firstly, preserving the UCSF network by cutting the whole network or at least the network was attacked from mainstream connection, leaving the system offline, effectively isolating it from affecting, or being affected by other network sections. After isolating the affected sections, identification methods come in to find out the abnormalities in the system by using tools. UCSF can use tools like Prodiscover because of the high-quality evidence collection feature. Having collected some crucial information, UCSF forensic investigators will go to the third phase which is extraction. In the extraction phase, investigators will identify abnormalities in the system by using tools like Sleuth Kit (+Autopsy) because it can help forensic investigators extract essential data like evidence related to ransomware from logs. After that, documentation will be compiled with necessary information about what exactly happened in the system. Finally, the Interpretation stage will take place and the investigators will need to interpret their results to the parties that are responsible for fixing the system.

Network forensics

Network forensics is the investigation of a digital assault that describes how the incident occurred, and the parties involved in the situation. The investigation is conducted as a post-incident response to a digital attack, but it is not an incident that complies with the organization's terms and policies. Were UCSF to be breached by a network-related incident, network forensics would be the preferred investigative method, and the process would go in this order:

With the daily flow of network information - also known as packets, UCSF's network security tools such as intrusion detection system and firewall might contain large amounts of sensitive data that need to be carefully extracted. Therefore, UCSF's network staff should be trained to use tools for extracting sensitive data, which requires legal warrants and authorization to ensure the privacy of the UCSF network is unharmed.

Second, because of UCSF's extensive network throughout the campus, there would be large incoming and outcoming network traffic daily, captured by logging tools such as Wireshark. For that reason, it is essential to capture and analyze the problem at that moment, in which SIEM (Security Information and Event Management) tools would be most preferred.

Third, after capturing the affected network sections using network tools, that data is then identified

by the network forensics specialists for further investigation. This data is also required to be preserved, and consequently, it is going to be analyzed to identify crucial evidence.

Fourth, from the crucial evidence that is gathered, UCSF's cyber analyst can then investigate and analyze said evidence to determine whether an attack happened, or it was a false alarm.

Fifth, after investigation and analysis of the evidence to determine it was an actual attack, techniques such as data mining and soft computing are used to examine the data and correlate the attack patterns. Further investigation of this phase should result in conclusive data on the attack and the prosecution of the threat actor.

Sixth, a presentation is needed to present observations from the breach, including an explanation of the steps taken, as well as the gathered data to reach the investigation's conclusion. Documentation of the incident is also created to satisfy legal requirements, as well as being served as a rulebook for future network-related breaches.

Lastly, assuming that the assault is ongoing while the investigation has already begun, the real-time network traffic would be shown for investigators. In that

case, UCSF should immediately activate the SOAR (Security, Orchestration, Automation & Response) model to mitigate the damage of the assault, though it might not be able to deal with unknown malwares and viruses.

REFERENCES

- Anchit Bijalwan, *Network Forensics(2022) Privacy and Security*

- Alexander S. Gillis, *intrusion prevention system (IPS), techtarget*, viewed 24 June 2023

<https://www.techtarget.com/searchsecurity/definition/intrusion-prevention>

- Ben Lutkevich, *access control, techtarget*, viewed 24 June 2023

<https://www.techtarget.com/searchsecurity/definition/access-control>

- CBS San Francisco 2020, *UCSF Medical School Officials Pay Hackers $1.14Million Ransom to Recover Stolen Data*, CBS Broadcasting Inc., viewed 14 June 2023,

<https://www.cbsnews.com/sanfrancisco/news/cyber-attack-ucsf-medical-school-ransom/>

- Cyberark, *Security Operations, Cyberark*, viewed 24 June 2023

<https://www.cyberark.com/what-is/security-operations/#:~:text=Security%20operations%2C%20also%20known%20as,improve%20collaboration%20and%20reduce%20risks>

- CYBRARY 2022, *CISSP Study Guide: Computer Forensics, CYBRARY, viewed 14 June 2023*
<https://www.cybrary.it/blog/computer-forensics#:~:text=Computer%20forensics%20is%20the%20investigation,pinpoint%20and%20prosecute%20the%20perpetrator>

- Clinton L. Smith, David J. Brooks (2013) *Security Science: The Theory and Practice of Security*, Elsevier

- Eccouncil *, What is Digital forensic, Eccouncil , viewed 14 June 2023*

<https://www.eccouncil.org/cybersecurity/what-is-digital-forensics/>

- *Google Cyber Security Course, Play It Safe: Manage Security Risks*

<https://docs.google.com/document/d/1my5OKuwJ-6eV9mxLHyYFuUokZtzoiJrbapfpHuCa7G8/edit?resourcekey=0-jchcadvBSSwRds8zK84ydw>

- GDPR.EU, *GDPR checklist for data controllers*, GDPR.EU, viewed 24 June 2023

<https://gdpr.eu/checklist/>

- Heather L. 2020, *UCSF pays hackers $1.1M to regain access to medical school servers, Fierce Healthcare*, viewed 14 June 2023

<https://www.fiercehealthcare.com/tech/ucsf-pays-hackers-1-14m-to-regain-access-to-medical-school-servers>

- IBM, *What is identity and access management (IAM)?*, IBM, viewed 24 June 2023

<https://www.ibm.com/topics/identity-access-management>

- International Standards Organization (2009) *International Standard ISO31000: Risk management – Principles and guidelines*, International Standards Organization

- Jeremy McDowell 2021, *Free CCNA | Standard ACLs | Day 34 | CCNA 200-301 Complete Course*, Jeremy's IT Lab, viewed 14 June 2023

<https://www.youtube.com/watch?v=z023_eRUtSo&list=PLxbwE86jKRgMpuZuLBivzlM8s2Dk5lXBQ&index=66&t=2478s>

- Jeremy McDowell 2022,*Free CCNA | Wireless Security | Day 57 | CCNA 200-301 Complete Course, Jeremy's IT Lab, viewed 14 June 2023*

<https://www.youtube.com/watch?v=wHXKo9So5y8&list=PLxbwE86jKRgMpuZuLBivzlM8s2Dk5lXBQ&index=111>

- Kristelle Feghali 2021, *Biba and Bell-LaPadula: Cybersecurity Models*, securelyours, viewed 24 June 2023

<https://securelyours.com/biba-and-bell-lapadula-cybersecurity-models-630eed6a83f5>

- Mololuwa A. (2022) *Impact of Covid-19 Pandemic on Online Security Behavior within the UK Educational Industry*, Dorset United Kingdom: Bournemouth University

- Mind Tools Content Team, *SWOT Analysis, MindTools*, viewed 24 June 2023 <https://www.mindtools.com/amtbj63/swot-analysis>

- Panda Security 2020, *43 COVID-19 Cybersecurity Statistics*, Panda Security mediacenter, viewed 17 June 2023, <https://www.pandasecurity.com/en/mediacenter/news/covid-cybersecurity-statistics/>

- pp_pankaj 2023, *Intrusion Detection System (IDS)*, geeksforgeeks, viewed 24 June 2023

<https://www.geeksforgeeks.org/intrusion-detection-system-ids/>

- Rob Witcher 2023, *CISSP Domain 6: Security Assessment and Testing – A Guide To Pass the Exam*, destcert, viewed 14 June 2023

<https://destcert.com/cissp-domain-6-security-assessment-and-testing/>

- Rob Witcher 2023, *CISSP Domain 2: Asset Security – What You Need To Know To Pass Your Exam [2022]*, destcert, viewed 14 June 2023

<https://destcert.com/domain-2-asset-security/#:~:text=Asset%20security%20and%20protection%20are,that%20it%27s%20important%20or%20valuable>

- Rob Witcher 2023, *CISSP Domain 8: Software Development Security – Know This for the Exam [2023], destcert*, viewed 14 June 2023

<https://destcert.com/cissp-domain-8-software-development-security/>

- Sam C. 2023, *US schools leaked 32 million records in 2,691 data breaches since 2005, Comparitech*, viewed 17 June 2023, <https://www.comparitech.com/blog/vpn-privacy/us-schools-data-breaches/>

- Trellix 2023, *What Is Ransomware?*, Trellix, viewed 24 June 2023, <https://www.trellix.com/en-us/security-awareness/ransomware/what-is-ransomware.html>

- UCSF 2020, *Update on IT Security Incident at UCSF, UCSF Campus News, viewed 14 June 2023*,

<https://www.ucsf.edu/news/2020/06/417911/update-it-security-incident-ucsf>