

Research in Data Security & Compliance

Physical Security

Physical security is put into place to protect physical assets of the company from physical threats [1]. These physical assets could be; equipment, employees, facilities, information systems, and more. Physical threats would include; theft, vandalism, natural disasters or fires [1].

Physical security is an incredibly important aspect to consider, as despite the drastic increase of cyber security technology, physical attacks are still utilised and put information systems at risk. These forms of attacks can lead to data theft, which in turn can cause damage to the company's reputation [2].

Components in Physical Security:

- Surveillance Systems: Security cameras, motion detectors, alarm systems, and other forms of surveillance will allow for 24/7 observation of sensitive areas and machinery [1][2].
- Access Controls: Having employees be restricted from specific areas depending on their permission levels is a good way to make it harder for anyone to steal sensitive data. If data is still destroyed or stolen with this in place it will also narrow down the list of suspects[1][2]. This can involve keycards that unlock doors for a short period of time so that those with access can enter, or biometric locks so only specific individuals can enter specific areas [1][2].
- Environmental Controls: Systems put in place to optimise the conditions surrounding the IT equipment. This would involve temperature, humidity, airflow and other regulators within data/server rooms in order to prevent damage or failure to the equipment [1][2].

Why is Physical Security Important?

As mentioned above, physical security is still what makes most companies vulnerable [3]. Whether it be easily socially engineered staff, or poor access control in which anyone can have access to sensitive environments [3].

A good example of this would be back in 2017, a group of cybercriminals found a vulnerability in Equifax's web application. This exploit allowed the hackers to gain access to sensitive information of over 147 million users [4].

This breach was only possible due to the weak physical security measures Equifax had put into place [4]. The exploit in question utilised a known vulnerability that was still in place within the

software as Equifax had failed to update the software in order to patch it, as well as weak access control within their facility [4].

Cryptography

Cryptography is used to secure communication and data by encrypting any and all information, making it impossible for those who are not intended to see it, unable to read said information [5]. Cryptography plays an important role in data security for companies and users alike, it ensures that sensitive information being sent to and from applications and users is only viewed and interacted with the authorised individuals [5].

Cryptographic Algorithms:

- Symmetric Cryptography: This form of cryptography uses a single key for the encryption and decryption of information [6]. This would involve standards such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES) [6]. This form of algorithm is typically used in stored passwords, files, and databases [6].
- Asymmetric Cryptography: This form of cryptography uses two keys, one being a public key that is used to encrypt the data, and a private key that is used to decrypt the data [7]. Standards such as Rives-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC). This form of cryptography is used to secure communication over unsafe networks [7].

Key Management Practices

- Key Generation: Secure key generation is necessary for strong cryptographic encryption [8]. Stronger key generation can prevent brute-force attacks from cracking them and therefore no one will be capable of intercepting and reading information being sent through the network [8].
- Key Distribution: Secure key distribution is also a very important aspect of cryptography as the only two individuals who are meant to have these keys are the users and recipients of the data being sent [8]. Secure key distribution usually involves key management protocols such as Transport Layer Security (TLS) and Key Management Interoperability Protocol (KMIP) for secure transport of the keys [9].
- Key Storage: Storing keys as securely as possible is important to protect against unauthorised users from getting their hands on tangible data [8]. Key storage practices would include hardware security modules (HSMs), and secure key vaults.

Where is Cryptography used?

Cryptography encrypts data being transmitted from one point to another in order to prevent that data being intercepted and viewed by unwanted individuals [10]. One example of this type of

cryptography is Secure Socket Layer (SSL) and Transport Layer Security (TLS), which are protocols used to securely send data to and from the internet and a user [11].

Intrusion Detection and Prevention Systems

Intrusion Detection and Prevention Systems (IDPS) are security measures placed to find and respond to unauthorised activity within a network [12]. IDPS plays an important role in securing data as it is used to continuously monitor the network traffic for any malicious activity or unauthorised access to information stored [12].

A couple examples different types of IDPS are;

- Network-based IDPS (NIDPS): NIDPS are used to monitor network traffic in real time, this is handy against Denial-of-Service (DoS) attacks, Bruteforce attacks and other suspicious activity [12].
- Host-based IDPS (HIDPS): HIDPS involve themselves with file integrity, system logs, and application behaviour in order to detect any signs of the integrity of the system being compromised [12].

IDPSs have varying uses, but for the most part they serve as detection mechanisms which identify security issues on the network [12]. However, there are multiple methods which are used by IDPSs to detect said threats [12]. Signature based detection is used to compare typical network traffic against the current events of the system to find anomalies occurring in real time [13].

Furthermore, an additional use for IDPSs is prevention, which is to prevent malicious activity from occurring on the network whenever it is detected [12]. They do this by blocking/filtering the network traffic and removing any untrusted, or malicious data [12]. This malicious data is then quarantined for the network administrators to view and deal with or is removed entirely [12].

IDPS are used with application security in many ways, their real-time monitoring for threats prevents cyber attacks as well as protects possible vulnerabilities [14]. They prevent data breaches and service disruptions [14].

IDPSs also have downsides to being used, despite their critical role in securing the network, they do tend to flag false positives [15]. This means that some traffic across the network will flag as malicious and will be blocked from being used. This can be due to the misconfiguration of the network or activities being used after a long time of being dormant, and therefore not being part of the signature used to compare the traffic on the network [15].

Another issue that IDPSs bring would be the scaling issue. Having an IDPS set up for a large network, typically an organisation's network, can bring issues for the IDPS in terms of

monitoring the network for threats [15]. This means organisations will need to select an IDPS carefully depending on their network systems infrastructure [15].

Security Technologies

Security technologies a large range of tools used to secure networks and data from being accessed by unwanted individuals [16]. These technologies are utilised in modern day applications to ensure the security of all data being stored and transmitted is tight and impenetrable [16].

Types of Security Technologies:

Firewalls

A firewall's purpose is intended to control the incoming and outgoing traffic from a network based on rules established by the network administration [17]. They work as a form of defence against threats incoming from external networks [17]. They work by inspecting the packets of incoming traffic and checking for anything that may harm the network [17].

Access Controls

Access controls are responsible for allocating authorisation to users to view, edit, delete or add information [18]. This is useful as it makes it more difficult for data leaks to occur, and prevents potential cyber attacks from occurring by restricting the number of accounts that can view the sensitive information [18]. As mentioned prior to this section, some technologies used with access control would be biometric technologies that allow personnel into sensitive areas of a facility, or role-based access control (RBAC) which is used to grant permissions to users on a network [18].

Endpoint Security Solutions

Endpoint security solutions are used to protect endpoint devices, such as; desktops, phones, laptops, tablets, and more from cyber attacks [19]. Some security solutions would include anti-viruses, device encryption, and mobile device management (MDM) [19].

Virtual Private Network (VPN)

A virtual private network (VPN) is used to create a secure connection between a device and an endpoint across an untrusted network [20]. VPNs use various cryptographic protocols such as SSL/TLS, and Internet Protocol Security (IPsec) to encrypt data being sent through the traffic [20].

StresSolutions Security Unit

Introduction

I have been tasked by StresSolutions to develop an information security unit in order to secure their operations, clients and reputation. In doing some research I found that the following content provided, if followed accurately, will provide a strong defence against cyber threats.

Organisation Structure

Having an organisational structure within the company would be ideal. This is useful for effectively taking care of data and its security. This can be split up into individual teams:

- Information Security Officer (ISO):

This is a role designed to be the foreman of the security of all information within the network [21]. This individual will have a responsibility for designing, implementing, and maintaining all the information coming into the company [21]. The ISO will report directly to the highest management positions and will serve the company as the advocate of security procedures and policies [21].

- Security Operations Team:

Below the ISO, there will be a security operations team. This team will be responsible for handling every day tasks for security management [22]. This team will monitor network traffic, and will report any anomalies and or malicious traffic [22]. They will work to identify any future threats as well as find vulnerabilities within the company and then patch those vulnerabilities before they can be exploited [22].

- Compliance & Governance Team:

This team will be in charge of ensuring that the security policies and requirements are being met within the company [23]. The team should conduct regular audits, implement control systems, provide guidance on legal/ethical handling of data, as well as assessing the security posture of the company [23].

- Risk Management Team:

The risk management team will be responsible for identifying, documenting, and reporting security risks across the network [24]. They should write up documentation of potential threats, risk assessments, and develop mitigation strategies for possible security concerns [24].

- Consultancy and Training Team:

This team's role is to advocate security awareness and practices to all other employees working at the company. They should be in charge of setting up and delivering computer security training, set up security awareness campaigns, as well as provide guidance on security procedures when asked by staff.

Organisational Structure Chart:



Policies and Procedures

Having policies and procedures in place will help keep the integrity of the company secure. These policies and procedures can include monthly password changes, along with a policy that involves having lengthy, strong passwords for all users.

Policy Development Process:

The company should create a process for the development of policies. This process should involve a review and approval of policies [25]. This process should also involve a collaboration with the Information Security Officer (ISO), and HR personnel [25].

Data Classification Policy:

This policy should be put into place in order to define how different forms of data should be categorised based on how sensitive that data is [26]. There should, at the least, be four separate categories; public, internal, confidential, and restricted, each category will allow easier handling of access controls [26]. Specific roles in the company can have access to specific categories of information, therefore making this data easier to manage and keep safe [26].

Access Control Policy:

Along with the Data Classification Policy, having an Access Control policy would involve preparing outlines of who is and is not allowed to view specific data [27]. These policies would typically include user authentication rules, role-based access controls (RBAC), user privileges and more [27].

Incident Report Policy:

An incident report policy involves establishing procedures for assessing and containing security incidents that occur within the company [28]. There should be roles and responsibilities established within the incident response team and will handle these sorts of situations [28].

Acceptable Use Policy (AUP):

This policy is used to define what is and is not acceptable actions in regards to the company's technology [29]. The policy would forbid things such as video games from being played on the systems, or movies and such being downloaded on the network [29]. This would mitigate the chances of malware being able to compromise the integrity of the company's network [29].

Data Privacy Policy:

This policy is used to protect the sensitive data of personnel and users across all of the company's projects and facilities [30]. This policy would outline what is and is not acceptable when it comes to data collection, data retention, data sharing, and consent requirements [30]. This is also so that the company can stay within the requirements of the GDPR and CCPA [30].

Security Awareness Training Policy:

The security awareness training policy is to be put in place to ensure that all the employees at SS are computer literate enough to not put the company's data at risk [31]. This would involve training employees and teaching them how to spot potential threats and scams, and how to handle the potential threat [31].

Compliance

The company should aim to be compliant with restrictions set by the current laws and regulations. This is so that the company can stay ethical and out of any legal turmoil that may cost them money and their reputation.

The best methods to follow these laws and ethics is to implement the following concepts:

Regular Compliance Program:

The company should establish a regular check done by the Compliance and Governance team mentioned prior [32]. This program would involve applying current laws and regulations to how the company handles data, this is so that the company can avoid lawsuits for not following the GDPR requirements [32].

Compliance Assessments and Audits:

Having regular compliance assessments and audits in order to evaluate the company's data handling is vital to avoid potential data leaks and lawsuits. These assessments should involve protection practices, security controls, privacy policies and other mentioned procedures above.

Privacy Policies:

The company should develop transparent privacy policies that clearly state how the company handles data collection, data sharing, and data protection [32]. These policies should be put into place with the users rights in regards to data access, restriction, and deletion, kept in mind in compliance with GDPR guidelines [32].

Ethical Guidelines and Code of Conduct:

SS should create ethical guidelines and code of conduct that represent the company's devotion to keeping their integrity secure [32]. This would include implementing principles such as honesty, transparency, confidentiality, and respect when it comes to handling clients and their data [32].

Vendor Management:

The company should implement a vendor management process to ensure that third party vendors also meet security and compliance standards [33]. This is so that the data being sent to and from third parties is still kept secure and is not going to bring the reputation of the company down in the eyes of the public or other potential partners [33].

Record Keeping and Documentation:

Having records that document the efforts put in to be compliant with legally required policies and procedures is good practice to prove that the company is in fact doing what it can to protect its employees and clients [34]. This would involve keeping documents such as risk assessments, audit reports, incident response documents, and training records [34].

Governance and Strategic Planning for Security

Governance is a framework of policies, procedures and security mechanisms which are used to oversee activities within a company's network. Strategic planning for security involves having a long-term goal and defining priorities to achieve said goal [35]. Setting procedures and policies so that a project can live for as long as it can without being compromised is an important task.

Firstly governance is used to establish specific roles and responsibilities for individuals/teams. This is something I have already discussed previously in this report, this means to appoint someone as the ISO and then having the aforementioned teams report back to them. Governance is used to set policies upon the users of the network so that the integrity of all projects, and user/staff data is kept secure [35].

Strategic planning for security would involve prioritising risk assessments, allocating resources to the appropriate individuals. By ensuring that the security efforts done by the company are appropriately set up to follow SS's business objectives, the previously mentioned information security unit can support any growth the company goes through while actively minimising risks [35].

Overall, implementing a strong governance structure and strategic plans for securing information, the company will be left with a strong/secure foundation to manage their security. The approach I have discussed, if it were to be implemented, will ensure that security is the company's top most priority [35].

Risk Management

Risk management is a vital aspect of any company, especially when it comes to data security. That is why I've made it a point to bring this up a few times previously in this report. This is to ensure that all bases are covered when it comes to the security of data and the integrity of the company's reputation [36].

Risk management is used to prevent problems before they become reality [36]. Essentially, a team is tasked to find potential threats and vulnerabilities and patch any chance of those issues coming back and hurting the company later down the line [36]. I believe that SS can appropriately, and effectively, manage their risks by incorporating the following into their security unit:

Risk Identification:

Identifying risks is the main point to the risk management team, they'll need to find potential threats across all of the company's projects and facilities [37]. This would mean the team would have to assess the technology systems within the company, personnel hired within the company, and third party connections associated and interacting with the company to find potential vulnerabilities [37].

Risk Assessments:

The risk management team should consistently be assessing threats, vulnerabilities, and anything else that could be potentially harmful to the company and its interests [38]. Which means when assessing a risk, the team should also document the potential impact that risk could have if left to its own devices [38]. This will help the company prioritise which vulnerability they should patch first [38].

Risk Prevention Strategies:

Developing risk prevention strategies is good practice, as when risks are found it gives employees the tools they need in order to mitigate its effects and or patch it entirely [39]. This would involve implementing firewalls, intrusion detections systems (IDS), data encryptions, and technical controls [39]. Additionally, having security policies, training programs, and access controls, would also reduce the chances that human error will compromise the company [39].

Risk Reports:

Once risks or vulnerabilities are identified, the risk management team should document what they found and the impact the exploit could potentially have on the company and its reputation [40]. These reports will give clear communications to the higher management as to what is happening and what current plans are in place to mitigate the possible issues [40].

Contingency Planning

Contingency planning, in essence, is a backup plan for the company. It involves predicting and preparing for potential disruptions to their services and business operations [41]. Some issues such as natural disasters, security breaches, or a fire emergency, can be detrimental to the company if not handled properly [41]. I believe that if SS can implement the following to have effective contingency plans:

Risk Assessments and Impact Analysis:

As mentioned prior to this section of the report, risk assessments and impact analysis can be conducted to prevent vulnerabilities and threats from harming the company and its services [42]. However if the company were to be affected regardless, having these documents would prove the company had made efforts in order to prevent data breaches and such from occurring [42].

Business Continuity Planning (BCP):

If SS were to develop a business continuity plan (BCP) then it would ensure that the company could continue providing their services to the public even during a disruption event, such as a security breach [43]. This plan should encompass methods to maintain key services and access critical resources [43].

Disaster Recovery Planning (DRP):

Having a recovery plan is a standard for most companies in the world, and SS will not be an exception. After a potentially devastating event, in which the services of the company had to go down, a plan to recover from such losses is vital to keep the company afloat [44]. This would involve setting recovery objectives, setting recovery time objectives (RTOs) and setting recovery point objectives (RPOs) [44]. These will allow the company to recover any information/data they may have lost due to the unfortunate event [44].

Data Backup and Recovery:

SS should incorporate the standard practice of backing up their data on a regular basis [46]. This is so that in the face of a catastrophic event which leads to the company having to shut down due to a hack, then they can at the least revert back to a point in time where the malicious software wasn't in the network, or if just backing up the data, then at the least the company will not have lost all the data they had [46].

Protection Mechanisms

Protection mechanisms have already been discussed previously within this report, they are simply used to secure the data and facilities within the company. This is vital for any company as it will make the difference between a secure company and a company that ends up on the news for storing their passwords in plain text. Some mechanisms SS can put in place would be the following:

Access Control Measures:

Access control has been discussed in length prior to this portion of the report, but it should not be understated how important they are in terms of data security. Implementing access control mitigates a lot of the human error that is likely to cause issues for a company, it does this by limiting the amount of users who can access specific data to only those who absolutely require it [47].

Encryption Technologies:

Having encryption technologies in place to ensure that data being stored, and transmitted across networks is secure is very common practice among companies. This is to ensure that even if there was a data breach, any and all sensitive information stored within the company will be completely unreadable [48]. Utilising SSL/TLS to encrypt data that's sent across networks will prevent anyone from intercepting that data as well, which makes this a vital aspect of security [48].

Endpoint Security Solutions:

Endpoint security solutions have also been discussed previously within this report, they encompass technologies such as firewalls, anti-viruses, intrusion detection systems (IDSs), intrusion prevention systems (IDPS) [49]. These security practices are used to lower the chances that malware can get into a system connected to the network [49]. Furthermore, implementing a guest network for users to connect to for WI-FI is also common practice [50]. This is because the company can't control what employees or clients do on their phones while at home, and it could mean that there is some form of malicious code that could breach the network hiding within their device [50].

Conclusion

In conclusion, I have thoroughly planned a detailed information security unit for StresSolutions. This plan, if utilised as intended, will prevent a large variety of cyber threats, as well as prepare the company for the potentially worst case scenarios. This plan encompasses all that the company needs to know about data security, and how to mitigate the fallout from potentially devastating events.

Furthermore, I have also discussed my research on data security earlier on in this report. With that founded understanding of Cryptography, Intrusion detection and prevention systems (IDPS), as well as how physical security operates and its impacts, I believe I have covered all that I was tasked to do for this document.

References

- [1] M. Cobb, "What is physical security?," *SearchSecurity*, Apr. 2021.
<https://www.techtarget.com/searchsecurity/definition/physical-security>
- [2] "Physical security," *ProtectUK*.
<https://www.protectuk.police.uk/advice-and-guidance/risk/physical-security>
- [3] "What is Physical Security & Why is it Needed?," *internationalsecurityjournal.com*, Dec. 01, 2023.
<https://internationalsecurityjournal.com/what-is-physical-security/#:~:text=Robust%20physical%20security%20acts%20as>
- [4] J. Fruhlinger, "Equifax data breach FAQ: What happened, who was affected, what was the impact?," *CSO Online*, Feb. 12, 2020.
<https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html>
- [5] K. Richards, "What is Cryptography?," *SearchSecurity*, Sep. 2021.
<https://www.techtarget.com/searchsecurity/definition/cryptography>
- [6] simplilearn, "The Most Effective Data Encryption Techniques," *Simplilearn.com*, Mar. 26, 2020. <https://www.simplilearn.com/data-encryption-methods-article>
- [7] K. Brush, L. Rosencrance, and M. Cobb, "What is Asymmetric Cryptography? Definition from SearchSecurity," *SearchSecurity*, Sep. 2021.
<https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography>
- [8] P. Saha, "10 Enterprise Encryption Key Management Best Practices," *Encryption Consulting*, Dec. 17, 2022.
<https://www.encryptionconsulting.com/10-enterprise-encryption-key-management-best-practices>
- [9] "What is Key Management Interoperability Protocol (KMIP)? | Thales," *cpl.thalesgroup.com*.
<https://cpl.thalesgroup.com/faq/key-secrets-management/what-key-management-interoperability-protocol-kmip>
- [10] "What is Cryptography? Definition, Importance, Types," *Fortinet*.
<https://www.fortinet.com/uk/resources/cyberglossary/what-is-cryptography#:~:text=The%20art%20of%20cryptography%20has>
- [11] Amazon Web Services, "SSL vs TLS - Comparing Communication Protocols - AWS," *Amazon Web Services, Inc.*, 2024.
<https://aws.amazon.com/compare/the-difference-between-ssl-and-tls/>

- [12] K. Scarfone and P. Mell, "Intrusion Detection and Prevention Systems," *Handbook of Information and Communication Security*, pp. 177–192, 2010, doi: https://doi.org/10.1007/978-3-642-04117-4_9.
- [13] "What Is Signature-Based Detection? | Corelight," *corelight.com*.
<https://corelight.com/resources/glossary/signature-based-detection#:~:text=Signature-based%20detections%20for%20networks>.
- [14] "Intrusion Detection and Prevention System (IDPS)," *Rapid7*.
<https://www.rapid7.com/fundamentals/intrusion-detection-and-prevention-systems-idps/>
- [15] Rapid7, "The Pros & Cons of Intrusion Detection Systems," *Rapid7*, Jan. 11, 2017.
<https://www.rapid7.com/blog/post/2017/01/11/the-pros-cons-of-intrusion-detection-systems/>
- [16] K. Johnson, "Top 7 types of data security technology," *SearchSecurity*, 2022.
<https://www.techtarget.com/searchsecurity/feature/Top-7-types-of-data-security-technology>
- [17] Cisco, "What Is a Firewall?," *Cisco*, 2019.
https://www.cisco.com/c/en_uk/products/security/firewalls/what-is-a-firewall.html
- [18] B. Lutkevich, "What is Access Control?," *TechTarget*, Jul. 2022.
<https://www.techtarget.com/searchsecurity/definition/access-control>
- [19] "What is Endpoint Security? How Does It Work?," *Fortinet*.
<https://www.fortinet.com/uk/resources/cyberglossary/what-is-endpoint-security>
- [20] "What Is a VPN? - Virtual Private Network," *Cisco*.
https://www.cisco.com/c/en_uk/products/security/vpn-endpoint-security-clients/what-is-vpn.html
- [21] "Information Security Officers (ISOs) | Texas Department of Information Resources," *dir.texas.gov*.
[https://dir.texas.gov/information-security/information-security-officers-isos#:~:text=An%20Information%20Security%20Officer%20\(ISO](https://dir.texas.gov/information-security/information-security-officers-isos#:~:text=An%20Information%20Security%20Officer%20(ISO)
- [22] "Security Operations Center (SOC) Roles and Responsibilities," *Palo Alto Networks*.
<https://www.paloaltonetworks.co.uk/cyberpedia/soc-roles-and-responsibilities>
- [23] PricewaterhouseCoopers, "Governance, Risk and Compliance," *PwC*.
<https://www.pwc.co.uk/services/risk/governance-risk-and-compliance.html>
- [24] "Risk Management Team Roles: Who takes care of Project Risk?," *MI-GSO|PCUBED*, Sep. 27, 2021.
<https://www.migso-pcubed.com/blog/risk-management/risk-management-team-roles/#:~:text=The%20Enterprise%20Risk%20Management%20Team>

- [25] “How to Develop Policies and Procedures,” *SafetyCulture*.
<https://safetyculture.com/topics/policies-and-procedures/>
- [26] M. Knowles, “Data Classification Policy: Definition, Examples, & Free Template,” *Hyperproof*, Feb. 22, 2024.
<https://hyperproof.io/resource/data-classification-policy/#:~:text=What%20is%20a%20data%20classification>
- [27] “User Access Control Policy Contents.” Available:
<https://assets.publishing.service.gov.uk/media/65ba34774ec51d000dc9f212/dwp-user-access-control-policy.pdf>
- [28] Health Education England, “Incident Reporting Policy 2021,” *Health Education England*, Sep. 21, 2021. <https://www.hee.nhs.uk/incident-reporting-policy-2021>
- [29] P. Kirvan, “What is acceptable use policy (AUP)? - Definition from WhatIs.com,” *WhatIs.com*, Jun. 2022.
<https://www.techtarget.com/whatis/definition/acceptable-use-policy-AUP#:~:text=An%20AUP%20sets%20rules%20related>
- [30] GOV.UK, “Data Protection Act,” *Gov.UK*, 2018. <https://www.gov.uk/data-protection>
- [31] N. Gursky, “6 Sections Every Security Awareness Training Policy Needs,” *CybeReady*, Sep. 20, 2023.
<https://cybeready.com/awareness-training/sections-security-awareness-training-policy-needs#:~:text=A%20security%20awareness%20training%20policy%20is%20a%20comprehensive%20document%20that>
- [32] Sharon, “What are the 8 elements of a compliance program?,” *Neopay*, Mar. 07, 2022.
<https://www.neopay.co.uk/what-are-the-8-elements-of-a-compliance-program/#:~:text=A%20compliance%20program%20should%20include>
- [33] “Managing Privacy and Data Security Risks in Vendor Relationships.” Available:
<https://legal.thomsonreuters.com/content/dam/ewp-m/documents/legal/en/pdf/pl-samples/managing-privacy-and-data-security-tr1794189.pdf>
- [34] “Record Keeping And Documentation Requirements,” *financialcrimeacademy.org*, Jan. 19, 2024.
<https://financialcrimeacademy.org/record-keeping-and-documentation/#:~:text=Firms%20must%20keep%20records%20of>
- [35] S. Mishra, K. Herman, H. Wimmer, C. Redman, E. Copello, and D. Richard, “JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH.” [Online]. Available:
<https://www.jisar.org/2020-13/n2/JISARv13n2.pdf#page=13>

- [36] IBM, "What is risk management? | IBM," *www.ibm.com*, 2023.
<https://www.ibm.com/topics/risk-management#:~:text=Risk%20management%20is%20the%20process>
- [37] "What Is Risk Identification? Definition and Tools," *Indeed Career Guide*.
<https://www.indeed.com/career-advice/career-development/risk-identification#:~:text=Risk%20identification%20is%20the%20process>
- [38] "What Is Data Risk Assessment?," *Palo Alto Networks*.
<https://www.paloaltonetworks.com/cyberpedia/data-risk-assessment#:~:text=A%20data%20risk%20assessment%20is>
- [39] S. Noss, "Data Risk Mitigation: How To Keep Your Organization's Data Safe," *DataGrail*, Jul. 28, 2023. <https://www.datagrail.io/blog/data-privacy/data-risk-mitigation/>
- [40] B. Posey, "What is Risk Reporting? How to Build an Effective Report," *SearchSecurity*, Oct. 2021. <https://www.techtarget.com/searchsecurity/definition/risk-reporting>
- [41] J. Martins, "6 Steps to Create a Contingency Plan to Prevent Business Risks • Asana," *Asana*, Apr. 23, 2021. <https://asana.com/resources/contingency-plan>
- [42] O. Hillel, "Business Impact Assessment vs. Risk Assessment: What's the Difference?," *Centraleyes*, Apr. 11, 2022.
<https://www.centraleyes.com/business-impact-assessment-vs-risk-assessment/#:~:text=The%20main%20difference%20between%20the>
- [43] W. Kenton, "What You Should Know About Business Continuity Planning (BCP)," *Investopedia*, Oct. 29, 2023.
<https://www.investopedia.com/terms/b/business-continuity-planning.asp>
- [44] "What Is a Disaster Recovery Plan? | IBM," *www.ibm.com*, Apr. 16, 2024.
<https://www.ibm.com/topics/disaster-recovery-plan#:~:text=A%20disaster%20recovery%20plan%20>
- [45] "The Difference Between RTO & RPO," *Rubrik*.
<https://www.rubrik.com/insights/rto-rpo-whats-the-difference>
- [46] "Data Backup and Recovery Explained | NinjaOne," *www.ninjaone.com*.
<https://www.ninjaone.com/blog/data-backup-and-recovery-explained/#:~:text=Data%20backup%20is%20the%20practice>
- [47] "Access Control Models and Methods | Types of Access Control," *Delinea*.
<https://delinea.com/blog/access-control-models-methods#:~:text=There%20are%20four%20types%20of>

[48] C. Kidd, "Data Encryption Methods & Types: Beginner's Guide To Encryption," *Splunk-Blogs*, Nov. 29, 2022.

https://www.splunk.com/en_us/blog/learn/data-encryption-methods-types.html

[49] "Endpoint Security," *www.sharp.co.uk*.

<https://www.sharp.co.uk/it-services/cyber-security-services/endpoint-security#:~:text=Endpoint%20Security%20focuses%20on%20protecting>

[50] SupportMyMac, "Why Your Organization Should Have a Guest Wi-Fi Network," *SupportMyMac*, Jun. 01, 2019.

<https://supportmymac.ca/why-your-organization-should-have-a-guest-wi-fi-network/#:~:text=It%20gives%20organizations%20the%20ability>