



RESEARCH IN DATA SECURITY AND COMPLIANCE

Gurpartap S Khatkar

Table of Contents

Task One.....	2
Evolution of Threat Landscape	2
Protection, Detection, Reaction and Safeguarding of Data	2
Protection	2
Detection	2
Reaction	3
Safeguarding	3
Cryptography	3
Security Technologies	4
Physical Technologies	4
Security Framework.....	5
Task Two	7
Why Information Security Can Break your Business?	7
How Information Security Can Make your Business?	7

Task One

Protecting, detecting, reacting, and safeguarding applications within an organisations IT systems and infrastructure is imperative in the current digital landscape. The evolving nature of cyber threats necessitates a proactive and robust approach towards securing organisational assets. This first report encompasses the significance of creating a fortified environment for application security within modern organisations.

Evolution of Threat Landscape

The modern landscape of cyber threats has evolved significantly, posing severe risks to organisations. Cyberattacks have grown in sophistication, diversity, and frequency, targeting sensitive data, financial resources, and property. A threat actor is someone who with cause harm intentionally to exploit weaknesses in digital systems. This dynamic landscape underscores the critical need for organisations to establish a multi-layered defence mechanism to counter diverse threats effectively. [1]

Protection, Detection, Reaction and Safeguarding of Data

Protection

- ◇ **Preventing Unauthorised Access:** As cyber threats continue to evolve and become more sophisticated, data protection is critical component of a comprehensive cybersecurity strategy. It involves implementing encryption, firewalls, access controls, and regular security audits to a safeguard against potential threats.
- ◇ **Preserving Confidentiality:** It ensures that sensitive information remains confidential preventing its exposure to unwanted people. Organisations like a bank hold onto crucially valuable data which, if gets into the wrong hands can really ruin lives.
- ◇ **Maintaining Integrity:** Protecting data helps maintain its accuracy ensuring that it hasn't been altered or tampered with.

Detection

- ◇ **Timely Identification of Breaches:** Detection anomalies, unusual activities, or breaches in real-time allows for prompt response and mitigation efforts. Anomaly detection systems use machine learning algorithms to identify unusual patterns in network traffic, user behaviour, or system activities. [2]
- ◇ **Understanding Threats:** Detection helps understanding the nature and scope of potential threats, enabling organisations to toughen defences and close vulnerabilities attackers might exploit.
- ◇ **Honeypots:** These are decoy systems or networks specifically designed to lure attackers. Monitoring these can provide insights into attack methodologies and help in early detection. [3]

Reaction

- ◇ **Responding to Breaches:** Reacting promptly to a data breach is essential to minimise its impact, prevent any further access and stop any potential damage. If all if not some data can be recovered then do so. [4]
- ◇ **Containing the Breach:** Taking immediate action upon detection helps in containing the breach, limiting the exposure of sensitive data, and reducing potential harm to individuals or the organisation itself.
- ◇ **Communication and Compliance:** Reacting appropriately involves notifying affected parties, stakeholders, and regulatory authorities as required by laws and regulations, ensuring compliance and transparency.

Safeguarding

- ◇ **Continuous Monitoring and Improvement:** Safeguarding data involves continuously monitoring systems, networks, and processes to stay ahead of evolving threats and vulnerabilities.
- ◇ **Adopting Best Practices:** Implementing best practices and security protocols helps in safeguarding data against emerging threats and staying resilient in the face of sophisticated attacks. Keeping up to date with laws and regulations such as The Data Protection Act which was introduced in 2018. This controls how personal information is used. [5]
- ◇ **Employee Training and Awareness:** Educating employees about security protocols, potential risks, and their roles in maintaining data security is crucial for safeguarding against internal threats like human error or malicious intent.

These elements work together as a comprehensive strategy to protect against data breaches, unauthorised access, and other security risks. They ensure that organisations are equipped to both prevent security incidents and respond effectively if and when they occur.

It is integral to maintaining trust, complying with regulations, mitigating risks, and fostering an environment conducive to growth, innovation, and ethical practices. There are many security measures we can take to take control of data and they include, cryptography, security technologies, physical technologies, and a security framework.

Cryptography

- ◇ **Confidentiality:** One of the primary benefits of cryptography is ensuring confidentiality. It allows for secure communication by encoding information in a way that only authorised parties can access. This prevents unauthorised access to sensitive data, ensuring that only intended recipients can decipher and read the encrypted information.
- ◇ **Data Integrity:** Mathematical algorithms that create a message summary or digest to confirm message identity and integrity. These are known as Hash functions. It can authenticate the integrity of data, confirming that it hasn't been modified by unauthorised parties.
- ◇ **Authentication:** Cryptography enables the verification of the identities of communicating parties. Through digital certificates, public and private key pairs, and

digital signatures, it ensures that the sender and receiver can authenticate each other's identity, reducing the risk of impersonation or unauthorised access.

- ◇ **Securing Transactions:** Cryptography plays a pivotal role in securing online transactions, particularly in financial and e-commerce sectors. Secure encryption methods protect payment information, personal details, and other sensitive data during online transactions, instilling confidence in users and reducing the risk of fraud or data theft.

Security Technologies

Security technologies refers to tools, practices and systems designed to protect data, systems, and networks from unauthorised attacks. The benefits of implementing security technologies are that it provides protection against cyber threats, complies with regulations, data confidentiality and integrity.

Some common security technologies include:

1. **Firewalls** - A combination of hardware and software is built to prevent specific information from moving between the outside (untrusted) and the inside (trusted) network. This could be a separate computer system or a software service running on existing router or a separate network containing supporting devices.
2. **Access Control Systems** - Mechanisms that manage and regulate who can access certain resources or systems, often involving passwords, biometrics, multi-factor authentication, etc.
3. **Virtual Private Networks (VPNs)** - Also known as VPNs are used to create an end-to-end private network connection. It carries information within a private network, but the information is transported over a public network. The traffic is encrypted to keep data confidential.
4. **Authentication:** I can prove I am a user of the system. This can be done by validating and verifying the unauthenticated entity's purported identity, Multi-Factor Authentication, and smart cards and security key fobs.
5. **Authorisation:** Here is what I can do with the system. This requires the matching of an authenticated entity to a list of information assets and corresponding access levels. Authorisation credentials/ tickets are issued by an authenticator and accepted by all systems within the authentication domain.

Physical Technologies

Physical technologies play a crucial role in safeguarding data by providing layers of security measures to protect against unauthorized access, theft, or damage. [6] Here's a brief overview of how these technologies contribute to data protection:

1. **Biometric Access Control Systems:** We can install and use products like fingerprint scanner and iris scanner. This will allow access to sensitive area or devices only to the authorised person. This ensures that physical access to data is restricted.
2. **Environmental Controls:** Adding the support of fire suppression systems, temperature, and humidity monitoring, helps protect data storage equipment from physical damage caused from environment issues such as fires and water damages. We can also check if

the systems are overheating due to poor cooling installation. This makes the integrity and availability of data by preventing hardware failures due to adverse conditions.

3. **Secure Storage Enclosures:** Using secure enclosures, cabinets, and safes for storing physical data storage devices adds an extra layer of protection against theft or unauthorised access. In case of a physical security breach or damage to one site, data remains accessible from alternate locations, ensuring the business data is kept safe.
4. **Backup Locations:** Maintaining redundant data storage facilities in secure, geographically diverse locations ensures data availability and resilience against physical threats like natural disasters, theft, or equipment failures. There is a way of backing up data that is known as the 3-2-1 strategy. This is when you have three copies of data, shared over two different storage medias while also having one offsite backup. By following this strategy, you mitigate the risk of losing your data. [7]
5. **Surveillance and Monitoring Systems:** Surveillance systems provide real-time monitoring and recording of activities in and around areas where data is stored. They act as a deterrent to potential intruders and help in investigating security incidents. Additionally, they offer evidence in case of security breaches or unauthorised access, aiding in identifying culprits and preventing future incidents. [8]

Security Framework

Security frameworks give a manageable structure to providing rules needed to an organisation. This helps protect a business from cybersecurity threats. Finding the right security measures is key and it should be based on a few considerations such as what is your organisation for, do you collect, process, or keep data and if you're contracted to work for a federal agency. [9]

1. **General Data Protection Regulation (GDPR):** This is a regulation set by the European Union that focuses on data protection and privacy for all individuals within the EU. It outlines regulations concerning the collection, processing storage, and transfer of personal data. Not being compliant with GDPR regulations can result in fines and penalties for organisation.
2. **Health Insurance Portability and Accountability (HIPAA):** HIPAA is a United States legislation that is aimed at protecting patients' healthcare data and ensures the security and confidentiality of protected health information. HIPAA sets the standards for healthcare providers, health plans, and healthcare clearinghouses, requiring safeguards for the protection of sensitive patient information. [9]
3. **ISO 27001:** ISO 27001 is an internationally recognized standard for information security management systems (ISMS). It provides guidance to companies/ organisations to help manage and control their information security. It offers a systematic approach to managing company information such as, intellectual property, financial data, and employee/ employers' details through risk management processes, controls, and further improvement. [10]
4. **ISO 27701:** This is an extension of the ISO 27001 standard and is mainly focused on privacy information management. It sets out guides for an organisation to establish, implement, maintain, and continually improve a privacy information management system based on the principles of ISO 27001.

5. **Payment Card Industry Data Security (PCI DSS):** This is a set of security standards designed to ensure companies process, store, and transmit credit card information properly. Major credit card companies like Visa, Mastercard and American Express require tight security for the data. The secure handling of cardholder information is crucial. Using firewalls, data encryption and regular monitoring. Failure to comply can lead to a loss in customers due to data breach of customer information. [9]

Task Two

Why Information Security Can Break your Business?

Data security breaches pose an imminent threat capable of shattering a business on multiple fronts. The ramifications of such breaches are far-reaching, causing irreparable damage that extends beyond immediate financial disaster. An example of a data breach was the cyberattack against Yahoo! In 2013, over one billion users had their accounts infiltrated and attackers managed to get access to accounts without the need for passwords. [11]

Firstly, a breach can decimate customer trust, the key to any successful business. When sensitive data falls into malicious hands, it can destroy the confidence of entrusted customers. The huge loss of trust then leads to the even bigger loss of customers and clients and the result of a tarnished reputation that can take years to rebuild. The financial toll is equally as devastating. The cost of remediation, forensic investigations, legal fees, and compliance penalties drain resources. [12] A breach often disrupts business operations, leading to downtime, decreased productivity, and the diversion of crucial resources to rectify the situation. Beyond these immediate setbacks, the theft of intellectual property or trade secrets threatens a company's competitive edge, providing rivals with an unfair advantage. Additionally, the psychological impact on employees can't be overlooked, a breach can cause distress, impairs morale, and can really drop the morale of the workforce and the productivity. Lastly, the ripple effect extends to partners and stakeholders, damaging relationships, and collaborative efforts. The cumulative impact of a data breach transcends the immediate financial loss, profoundly undermining the fundamental pillars of a business- trust, credibility, financial stability, and the operational work of the business.

How Information Security Can Make your Business?

Implementing robust data security measures not only protect valuable information but fosters trust among clients and stakeholders, consequently bolstering the reputation of the business. By employing the correct barriers like encryption, access controls, firewalls, and regular security audits, a company can decrease the chances of attacks or stop an attack getting worse. Enhanced data security instils confidence among customers, affirming that their personal and financial information is safeguarded from potential threats. This assurance makes a stronger bond with customers improving loyalty and trust. Compliance with data protection regulations such as GDPR (General Data Protection Regulation) becomes more achievable, avoiding legal action and fines. Data security serves as a foundational pillar upon which a successful and sustainable business can thrive. It not only safeguards sensitive information but also fosters trust among stakeholders, promotes efficiency within the organisation, ensures regulatory compliance, and safeguards the financial health of the company. Making data security a top priority is essential in today's interconnected digital landscape to fortify and future-proof any business endeavour. [13]

As discussed above why the protection of data is so important, it is curial that a company like StressSolutions(SS) establish a proper security to unit to keep themselves and customers safe. There are ways of establishing a robust security unit.

1. Establish Clear Objectives and Policies:
 - ◇ Define what the information security unit aims to achieve, such as protecting sensitive data, ensuring compliance, minimising risks, and maintaining business continuity.
 - ◇ Develop detailed policies covering various aspects like access control, data handling, incident response, acceptable use. These policies should align with industry standards and legal requirements.
2. Designate Qualified Personnel:
 - ◇ Hire or designate experienced professionals with expertise in information security and compliance. Someone like an IT security specialist.
3. Conduct Risk Assessment:
 - ◇ Identify potential risks, vulnerabilities, and threats to the organisation's assets, including data, infrastructure, and processes.
 - ◇ Evaluate the likelihood and impact of these risks to prioritise mitigation efforts effectively.
4. Compliance with Regulations:
 - ◇ Stay informed about legal and industry-specific regulations applicable to the business like the General Data Protection Regulations which regulates how companies collect, process, and store personal data of EU citizens.
5. Business Continuity Planning (BCP):
 - ◇ A BCP is a comprehensive strategy that outlines procedures and protocols a company or organisation follows to ensure that essential functions can continue during and after a disruptive event or disaster. [14]
 - ◇ Regular tests of the BCP through drills or simulations to identify weaknesses and improve response times.
6. Data Recovery and Backup Systems:
 - ◇ Develop robust backup systems with redundancy and encryption to protect critical data.
 - ◇ Periodically test data recovery processes to ensure data integrity and accessibility during emergencies.
7. Security Awareness Training:
 - ◇ Conduct regular training sessions to educate employees about security best practises, phishing awareness, and data handling.
 - ◇ Foster a culture of security where employees understand their role in maintaining security standards.

Another way to keep structure is by having an Information Security Chart. An Information Security Organisational Chart is a visual representation outlining the hierarchy, roles, and responsibilities within an organisation's cybersecurity team. It illustrates the reporting structure from top-level positions, like the Chief Information Security Officer (CISO), down to security analysts and specialists. This chart aids in clarifying roles, streamlining communication,

allocating resources effectively, managing risks, ensuring compliance, and making informed decisions within the realm of information security. [15]

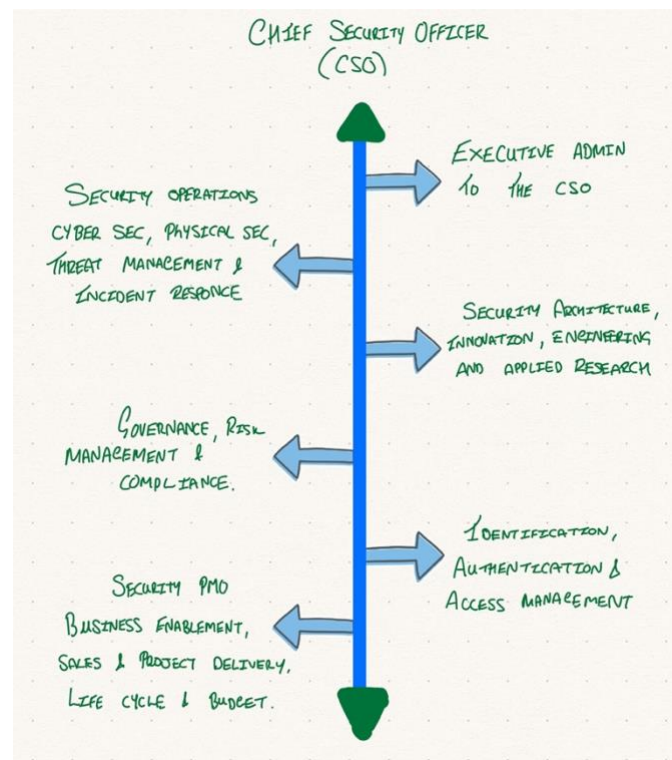


Figure 1 Organisational Chart

Conclusion

Information security stands as a cornerstone for the vitality and sustainability of any IT organisation in today's interconnected digital landscape. This paper has elucidated the paramount importance of robust information security measures and their multifaceted significance within an IT organisation. safeguarding sensitive data and systems is imperative to maintain operational integrity. In conclusion, the significance of information security for an IT organisation cannot be overstated. It serves as an essential for operational continuity, regulatory compliance, stakeholder trust, proactive risk management, and fostering a conducive environment for technological advancements. Organisations must prioritize and continually invest in robust information security frameworks to navigate the complexities of the digital landscape and ensure sustained success in the ever-evolving technological ecosystem.

Bibliography

- [1 B. Lenaerts-Bergmans, "Threat Actors," 28 Feb 2023. [Online]. Available:
| <https://www.crowdstrike.com/cybersecurity-101/threat-actor/>. [Accessed 28 Nov 2023].
- [2 Cisco, "5 Ways To Detect A Cyber Attack," HuffPost, 30 January 2017. [Online].
| Available: https://www.huffpost.com/archive/ca/entry/5-ways-to-detect-a-cyber-attack_n_13880814. [Accessed 1 Dec 2023].
- [3 Kaspersky, "What is a honeypot?," [Online]. Available:
| <https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot#>. [Accessed 1 Dec 2023].
- [4 Information Commissioner Office, "72 hours - how to respond to a personal data breach,"
| [Online]. Available: <https://ico.org.uk/for-organisations/advice-for-small-organisations/72-hours-how-to-respond-to-a-personal-data-breach/#:~:text=If%20you%20can%20recover%20the,who%20will%20be%20most%20impacted.&text=If%20it%27s%20been%20sent%20to,it%20is%2C%20retrace%20you>. [Accessed Dec 1 2023].
- [5 gov.uk, "Data Protection," [Online]. Available: <https://www.gov.uk/data-protection>.
| [Accessed 28 Nov 2023].
- [6 M. Cobb, "Physical Security," April 2021. [Online]. Available:
| <https://www.techtarget.com/searchsecurity/definition/physical-security>. [Accessed 1 December 2023].
- [7 "Data Backup in Depth: Concepts, Techniques, and Storage Technologies," [Online].
| Available: <https://cloudian.com/guides/data-backup/data-backup-in-depth/#:~:text=Common%20choices%20include%20internal%20and,for%20failover%20during%20local%20outages..> [Accessed 30 Nov 2023].
- [8 F. Liu, "Significance of data protection in physical security systems," [Online]. Available:
| <https://www.sourcesecurity.com/insights/co-4108-ga.14991.html>. [Accessed 30 Nov 2023].
- [9 R. Reddy, "Top IT Security & Privacy Framework," 1 November 2022. [Online].
| Available: <https://www.zluri.com/blog/security-privacy-frameworks/>. [Accessed 30 Nov 2023].
- [1 "What is ISO 27001 information security management?," [Online]. Available:
0] <https://www.itgovernance.co.uk/iso27001>. [Accessed Nov 2023].
- [1 D. E. Holmes, Big Data, Oxford: Oxford University Press, 2017.
1]
- [1 J. Nimar, "How Information Security Can Make or Break Your Buinesss," LinkedIn, 30
2] September 2014. [Online]. Available: <https://www.linkedin.com/pulse/20140930144814-10206101-how-information-security-can-make-or-break-your-business/>. [Accessed 10 Dec 2023].
- [1 C. D.Costa, "The Importance of Information Security For Your Business," Medium, 9 Sep
3] 2019. [Online]. Available: <https://medium.com/@clairedigitalogy/the-importance-of-information-security-for-your-business-9a0fe0bb1e34>. [Accessed 10 Dec 2023].
- [1 V.-L. Brunskill, "Buiness Continuity Plan (BCP)," TechTarget, May 2022. [Online].
4] Available: <https://www.techtarget.com/searchdisasterrecovery/definition/business-continuity-action-plan>. [Accessed 10 Dec 2023].
- [1 L&CO Staff Auditors, "What are the Roles and Responsibilities of Information Security?,"
5] Linford&Co llp, 19 June 2019. [Online]. Available: <https://linfordco.com/blog/information-security-roles->

responsibilities/#:~:text=What%20is%20an%20Information%20Security,into%20those%20C%2Dlevel%20roles.. [Accessed 10 Dec 2023].

[1] IBM, “What is cybersecurity?,” [Online]. Available:

6] <https://www.ibm.com/topics/cybersecurity>. [Accessed 30 Nov 2023].