INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024

# Grayson Insurance Cybersecurity Strategic Plan Part 1

**Onyinyechukwu Ujah, Miriam Duru, Samuel Akinola**

**University of Dallas, United States**

**DOI: https://doi.org/10.51583/IJLTEMAS.2024.130719**

**Received: 28 July 2024; Accepted: 08 August 2024; Published: 20 August 2024**

**Introductory Letter**

Dear Team,

Grayson Insurance, as the name suggests, is an insurance company, which operates in the U.S and all across Europe. In recent weeks, we conducted an assessment on some of the cybersecurity policies that affect our company, including the Federal Information Security Management Act (FISMA) and the General Data Protection Regulation (GDPR). This was followed by conducting a risk assessment on some of the most important information assets that Grayson Insurance uses, including customer data, employee information, patient medical records, and company information. Some of the vulnerabilities that were uncovered from the assessment include phishing attacks, insider threats, data breaches through cyberattacks, and intellectual property theft. The next step is to come up with a Strategic Cybersecurity Plan that is aligned with Grayson Insurance's business and IT priorities.

In the current digital world, the significance of a strong cybersecurity strategy cannot be overlooked. With cyberattacks growing more sophisticated day-by-day, organizations need to implement proactive measures to protect their digital assets. As the risk analysis disclosed, from intellectual property to customer information, the implications of a data breach through cyberattacks can be catastrophic. Therefore, Grayson Insurance's strategy to ensure that we are free from cyberattacks involves implementing a proactive approach to cybersecurity. The goal is to ensure that all employees at Grayson Insurance, from the Board of Directors, to me your President, Upper Management, Middle Management, Supervisors, and our dedicated Frontline Staff understand the importance of cybersecurity and practice the necessary measures of ensuring all our digital assets are protected against cyberthreats.

Cybercriminals continue to develop sites that collect users' data, which are then used in online frauds and identity thefts. Many malicious attacks and data leaks have also been caused by employee negligence (otherwise known as insider threats). Furthermore, America alone continues to face a series of data breaches through cyberattacks, and, as indicated by HIPPA, in the last two years, approximately 42 million healthcare records have been exposed through data breaches (Palatty, 2023). Our company also has dozens of intellectual properties, which, if exposed to malicious actors or our business competitors, then it might affect our business. Therefore, I call upon all the stakeholders mentioned above to embrace and drive the best cybersecurity practices, like the ones stipulated in the NIST Framework. From top-level executives to frontline workers, everyone at Grayson Insurance should remember that play a crucial role in protecting the company's digital assets, and we should thus invest in the right technologies to stay a step ahead of cybercriminals to protect our company. Sincerely, President of Grayson Insurance

**I. Business Mission & Vision & Values**

This strategic plan will present two types of missions, visions and values regarding Grayson Insurance, i.e., from a business and security perspective. This section will focus on the business perspective of these factors. Business mission, vision, and values outline the fundamental purpose and goals of a company, i.e., it often communicates the company's core identity and the reason for its existence (Cardona & Rey, 2022).

**Mission**

Our business mission is to offer a constantly high level of quality service to our clients at competitive, fair rates. We are not only committed to keeping the utmost integrity and professionalism standards in our association with our clients, but also endeavour to understand their financial situations and offer them the highest quality services, information, and products to help them attain their goals. We also want to create a friendly and competitive workplace for our staff and provide fair opportunity for growth in the company to anybody with the desire and talent to grow, regardless of color, race, age, religion, sex, ancestry or national origin, veteran's status or disability, and marital status.

**Vision**

We hope that when people hear or think about Grayson Insurance, they will envision a company that aims to help them live better and safer lives, with more security. This includes going beyond what about general insurance companies in the U.S. and Europe offer their clients. We hope to be considered as the most empathetic and attentive insurance company to both U.S. and Europe citizens by doing the following:

- Improving our skills through ongoing education and training

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024

- Offering quality insurance products, which meet our clients' ever-growing needs
- Expanding customer access to our services through both innovative and conventional communication networks

**Values**

Our business values are manifold:

**Trust**: We also try to gain new customers and keep our long-standing customers by being reliable, honest, and consistent in offering our services.

**Knowledge**: We pursue training and education so as to be in a better position to give our clients the best advice regarding insurance coverages and other related products.

**Connection**: We avail ourselves to our clients across all online platforms, by telephone, and in person offering services to our long-standing clients and reaching out for new customers who might benefit from our services.

**Teamwork**: We love teamwork. We consider people within the company (staff) and outside the company (clients) as one team, which helps us to effectively offer our services.

**Respect**: We treat all our clients and each other with courtesy, dignity, and appreciation.

**Integrity and Professionalism**: We conduct ourselves with transparency and honesty in all we do. We also strive to be responsible and courteous in our interaction with clients as well as other businesses.

**Fun & Humor**: They say life is never that serious. We try not to take anything too serious by ensuring that our work environment is friendly and welcoming to our employees and customers. Being happy is part of our culture.

**Commitment**: We give our clients full attention, anticipate their needs, and are always upfront with our terms and conditions, including coverage details.

**II. IT Philosophy**

While philosophy is broadly referred to as the study of fundamental nature of knowledge, existence, and reality, especially in the academic realm, it can simply be considered as the ideas, values, and principles behind a phenomenon (Reijers, 2021). Therefore, with regard to the current strategic cybersecurity plan, information technology (IT) philosophy can be considered as the guideline principles, values, and/or ideas that influence the approach and perspective of Grayson Insurance towards IT. At Grayson Insurance, the IT philosophy will be dictated by the fact that the company requires strong and proactive cybersecurity practices, which align with the company's global presence in the insurance industry. As indicated in the policy analysis phase, two cybersecurity policies that affect our company include FISMA and GDPR. Therefore, our IT philosophy will not only take into consideration these regulations, but also the vulnerabilities that were identified in the risk assessment phase regarding the critical information assets, and hardware and software used at Grayson Insurance, the functions that are outsourced, the use of cloud technology, technical solutions important to the company, the company's bring your own devices status, and the working arrangements at the company that might affect its cybersecurity posture.

Grayson Insurance's IT philosophy will focus on the following matters: digital transformation, cybersecurity classification, risk management, security controls, proactive cybersecurity, and business and IT alignment. By embracing digitalization, Grayson Insurance intends to streamline data collection processes and prioritize frictionless methods so as to improve customer services, while upholding security standards. Some of the services that Grayson Insurance will outsource with an aim of improving customer services, while upholding security standards, include customer support services (helpdesk support, live chat support), cloud service management (cloud hosting, data backup and recovery), application development and maintenance (software development, patch management), cybersecurity services (managed security services, penetration testing), data analytics and business intelligence, and web and mobile application development.

For instance, outsourcing helpdesk services and live chat support will ensure Grayson Insurance provides 24/7 handling of queries and issues. Outsourcing cloud services can help in optimizing the storage of data, scalability, and ensuring that a company complies with security protocols. Another advantage is that they provide routine data backup, helping companies with fast recovery to avoid prolonged downtimes (Mtsweni et al., 2021).

Furthermore, as indicated in the risk analysis phase, Grayson Insurance will make use of a data classification scheme that classifies data as personally identifiable information (PII), financial data, protected health information (PHI), intellectual property (IP), and more. This classification will ensure that the company will comply with such relevant, industry regulations as GDPR, Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), and Payment Card Industry Data Security Standard (PCI DSS), among others.

Since Grayson Insurance is vulnerable to phishing attacks, insider threats, cyberattacks on patient records, and intellectual property theft, some of the technical solutions that the company will adapt to ensure it is not affected by these vulnerabilities include implementing email filtering systems, multi-factor authentication (MFA), encryption, intrusion detection systems, and

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024

regular security training. Grayson Insurance will also allow employees to use their personal mobile devices for work-related activities. The Bring Your Own Device (BYOD) policy at Grayson Insurance will follow the recommendations stipulated at the NIST Special Publication (NIST SP) - 1800-22 (Howell et al., 2023). According to the NIST SP - 1800-22, companies should allow employees to user their own devices for work-related activities only if those devices meet the minimum security requires (e.g., up-to-date antivirus software), registered with the IT department, password and biometric protected, limited network use, data encrypted, owners undergo mandatory security awareness training, and undergo compliance audits (Howell et al., 2023).

Lastly, Grayson Insurance will attempt to link its business mission, vision, and values with the security mission, vision, and values in order to prioritize not only the protection of data, but also the integration of technology to support the company's overall mission of being a globally compliant provider of customized insurance services. In essence, the IT philosophy at Grayson Insurance is based on a proactive, adaptive, and integrated approach to cybersecurity to ensure all operations are resilient in the digital era.

**Security Organization Chart**

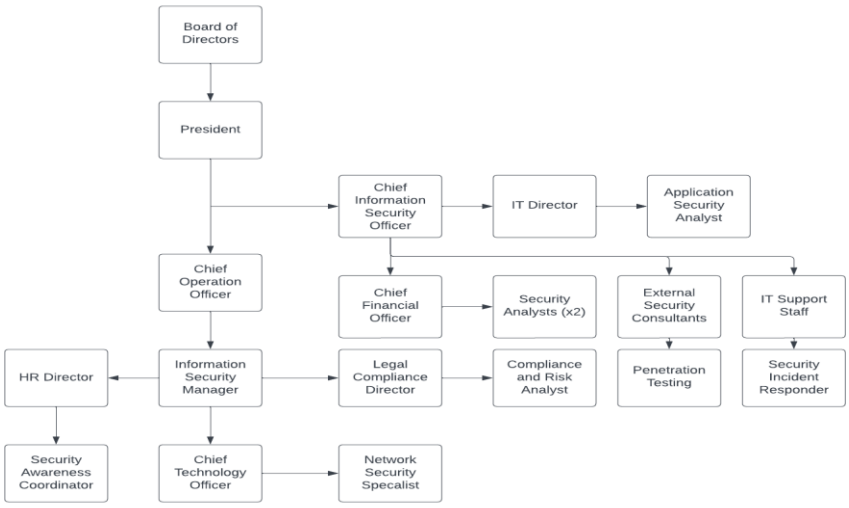


Figure 1: Grayson Insurance Proposed Organizational Chart

From the organization chart above:

- The CISO will hold a strategic position; they will report directly to the CEO to showcase importance of cybersecurity at the executive level.
- The Information Security Manager will oversee the daily security operations and manage various security roles within the team.
- Security Analysts, Network Security Specialist, Application Security Specialist, and Compliance and Risk Analyst will report to the Information Security Manager.
- The Security Awareness Coordinator will collaborate with HR to improve Grayson Insurances' security awareness among employees.
- External Security Consultants, including a Penetration Testing Specialist, will be required for specialized assessments.
- Lastly, Security Incident Responders will work closely with IT support staff to address and resolve security incidents as they occur.

**Security Organization Description**

Table 1: Roles and Responsibilities

| Security Role | Responsibilities |
|---|---|
| **Chief Information Security Officer (CISO)** | Develop and implement the overall security strategy and policies for Grayson Insurance.<br>Provide leadership and oversight to the entire security team.<br>Report directly to the CEO on security matters and incidents.<br>Ensure compliance with industry regulations and standards. |
| **Information Security Manager** | Manage day-to-day security operations.<br>Supervise security analysts, network security specialists, and application security specialists.<br>Collaborate with other department heads to align security initiatives with |

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024

| | |
|---|---|
| | business goals.<br>Report to the CISO. |
| **Security Analysts (x2)** | Conduct threat assessments and vulnerability analyses.<br>Implement and monitor security measures.<br>Investigate and respond to security incidents.<br>Report to the Information Security Manager. |
| **Network Security Specialist** | Manage network security infrastructure and protocols.<br>Collaborate with IT teams to ensure secure network configurations.<br>Conduct regular security audits on network systems.<br>Report to the Information Security Manager. |
| **Application Security Specialist** | Ensure the secure development and deployment of applications.<br>Conduct code reviews and application vulnerability assessments.<br>Collaborate with development teams to address security findings.<br>Report to the Information Security Manager. |
| **Security Awareness Coordinator** | Develop and implement security awareness training programs.<br>Collaborate with HR to integrate security awareness into organizational culture.<br>Monitor and assess the effectiveness of security training initiatives.<br>Report to the CISO. |
| **Compliance and Risk Analyst** | Ensure compliance with industry regulations and standards.<br>Assess and manage security risks across the organization.<br>Conduct regular compliance audits.<br>Report to the CISO. |
| **Penetration Testing Specialist (Contractor)** | Conduct periodic penetration tests to identify vulnerabilities.<br>Provide expertise in assessing external and internal security posture.<br>Deliver comprehensive reports on security testing findings.<br>Report to the CISO. |
| **Security Incident Responder (x2)** | Respond to and mitigate security incidents promptly.<br>Conduct post-incident analyses and provide recommendations for improvements.<br>Collaborate with IT support staff to address security issues.<br>Report to the Information Security Manager. |

It is impossible for the security team to handle all security activities within a company or else they can be overwhelmed with tasks especially in such large organizations as Grayson Insurance (Perwej et al., 2021). As indicated earlier, in many companies, the Help Desk Support Group is normally granted the responsibility for helping users reset their forgotten passwords. For Grayson Insurance, the task of resetting forgotten passwords will also be granted to the Help Desk Support Group. The HR Department will be given the task of implementing strong onboarding and offboarding process to manage access control and ensuring the employees adhere to BYOD regulations. The IT team will work with the security team to create secure network configurations and develop applications with built-in security measures.

**Security Organization Justification**

Normally, the first task of a CISO is to come up with an efficient team. An efficient team is one that aligns with the needs of an organization, which will assist the CISO to enhance the company's cybersecurity posture and reduce the risk to its business operations (Alshaikh, 2020). According to Alshaikh (2020), there is no standard approach to coming up with such a team, because every organization has unique cybersecurity requirements. As recommended by Yoo et al. (2020), some of the critical roles that need to be filled when planning such a team include risk assessment manager, security office, and cybersecurity analyst. In modern organizations, risk assessment and management are some of the most critical aspects. Risk management forms the baseline of all cyber organizations (Alshaikh, 2020). Security operations, on the other hand, include many operations depending on the size of a company. Security operations at Grayson Insurance will include data security, incidence management, infrastructure and network security, and threat monitoring, among others. A cyber security analyst will also be brought in to help in conducting the cybersecurity awareness training, which as indicated in the risk analysis phase, is one of the control measures in ensuring Grayson Insurance' employees always practice strong cybersecurity practices.

As noted in the organizational chart presented in Fig. 1 earlier, Grayson Insurance will include CISO. Risk assessment will be done by nearly all parties, including Information Security Manager, Security Analysts, Network Security Specialist, Application Security Specialist, Security Awareness Coordinator, Compliance and Risk Analyst, Penetration Testing Specialist (Contractor), and Security Incident Responders. The role of the cyber security analyst will be fulfilled by the Security Awareness Coordinator whose responsibilities will include: (1) developing and implementing security awareness training programs, (2) collaborating with HR to integrate security awareness into organizational culture, and (3) monitoring and assessing the effectiveness of security training initiatives. This is one of the reasons the organizational chart presented in Fig. 1 was selected.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024

Alshaikh (2020) writes that, with an aim of saving on resources, organizations are pushing the notion of doing more with less. Partnerships that leverage the experience and skills of other organizational members are overly important. As indicated in Fig. 1, Grayson Insurance's ecosystem comprises of internal partners (e.g., CISO, Information Security Manager, Security Analyst) and external partners (e.g., Penetration Testing Specialist). The organizational chart will focus on a number of partnerships with the CISO working together with the President to ensure that cybersecurity is at the executive level, the Security Analysts, Network Security Specialist, and Application Security Specialist will work together with the Information Security Manager. The HR will work together with Security Consultants and Security Incident Responders to create awareness among the employees on the significance of cybersecurity. As such, Grayson Insurance will only need to hire the External Security Consultants on a part-time basis.

The organizational chart earlier presented on Grayson Insurance best describes a top-down approach to organizational planning. The chart starts with the CEO at the top, and is followed by other executive positions and department heads. Grayson Insurance follows a centralized form of leadership with the Board and CEO at the top of the organization.

**III. Security Mission & Vision Statements**

As earlier indicated, there is a difference between business and security mission, vision and value statements. A security mission statement specifically addresses a company's commitment to safeguarding its assets, information, and people. It establishes the principles and objectives for the organization's security practices.

**Mission**

The mission of Grayson Insurance is to work continuously to evolve our cybersecurity capability to detect, prevent, and respond to not only existing, but also emerging cyberthreats. As a key institution for financial protection and risk management, the mission of our Grayson Insurance is the push the limits of the conventional use of technology, but with do this with a focus on safeguarding our systems, information, customers, and employees. We believe that a cyber-safe insurance company is one that has reduced vulnerabilities to cyberthreats, while ensuring that our clients continue receiving exceptional services using our digital platforms. The risk-based approach to cybersecurity that we apply enables us to fulfil these needs, while at the same time, ensuring minimal exposure to cyberthreats.

**Vision**

At Grayson Insurance, everything done at the company is inspired by our vision. Our vision is be regarded as an outstanding, world-class cyber-evangelist, leader, and defender, who craft and deliver superlative and strong cybersecurity practices consistently, leading to superior services the astound and delight our clients.

**IV. Security Core Values**

Some of the core values that will guide our Strategic Cybersecurity Plan include confidentiality, integrity, availability, and accountability. Confidentiality implies that data will only be available to authorized parties. Confidential data is one that has hardly been compromised by unauthorized people (i.e., people who should not have access to such data or those who do not need it) (Det Norske Veritas, n.d.). For Grayson Insurance, ensuring confidentiality will imply that all the information is organized with regard to people who will have access to it.

Integrity, on the other hand, is the certainty that data has not been degraded or tampered with during or after submission (i.e., data has not been modified without authorization, either unintentionally or intentionally) (Det Norske Veritas, n.d.). At Grayson Insurance, we transmitted a lot of patient medical records between our payment providers and health care institutions. If such data is tampered with, then it might affect the care our clients are given.

Availability is the act of ensuring that the systems a company holds are available to authorized users the moment they need it. Such systems have to function properly, have the appropriate security controls, and the right communication channels (Det Norske Veritas, n.d.). Grayson Insurance operations systems that are considered as critical (e.g., power generation, cloud computing because we offer 24/7 services). These systems normally have extreme requirements associated with availability. They need to be resilient against cyber threats, hence the reason why this core value was selected.

Lastly, accountability is the act of being responsible by both individuals and the organization as a whole for their cybersecurity practices (Det Norske Veritas, n.d.). according to Det Norske Veritas (n.d.), establishing clear roles, responsibilities, and consequences for non-compliance promotes a culture of security awareness. The role and responsibilities of each security team member have been listed in Table 1; these roles are vital in mitigating insider threats, ensuring compliance with regulations, and fostering a proactive approach to cybersecurity across Grayson Insurance, thus the reason why this core value was also selected.

**V. Security Issues and Challenges**

Grayson Insurance faces unique cybersecurity challenges, which require strategic attention. These challenges include data privacy and compliance, cyber insurance risks, phishing and social engineering, and supply chain security. As the significance of safeguarding user data by companies continues to grow, so do the difficulties related to data privacy and compliance to both location and international regulations (Ironhack, 2024). Ensuring data remains private is a crucial activity for all organization,

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024

even though it is never a simple process. It is a multifaceted procedure involve data backing up, archiving, creating cybersecurity teams, etc., which adds additional costs to a company's operations. Grayson Insurance deals with a vast amount of sensitive client information. The company has to ensure compliance with data protection regulations, such as GDPR or HIPAA, to protect customer privacy. According to Ironhack (2024), non-compliance could result in severe legal and financial consequences.

As an insurance company, Grayson Insurance must address the evolving risks associated with underwriting cyber insurance policies. Unlike traditional insurance, cyber insurance does not have a strong history of claims data, which makes it difficult for companies like Grayson Insurance to correctly assess cyber risks. In other words, there are no standardized methods of evaluating cyber risks, which makes the work of underwriters more challenging (Kaushik, 2024).

As discussed in the risk analysis phase, Grayson Insurance is also susceptible to phishing attacks that exploit human vulnerabilities. Employees may unintentionally disclose sensitive information, which pose a significant threat to the company's assets. Therefore, educating staff on recognizing and avoiding phishing attempts and implementing reliable email security measures can help in mitigating this challenge (Alkhalil et al., 2021).

The last challenge is Grayson Insurance's supply chain security. As indicated in the Organizational Chart (Fig. 1), our company depends on different vendors to meet our technological needs and services. The dependency of different departments both within and outside the organization can pose cybersecurity risks for the Grayson Insurance. Therefore, Grayson Insurance will have to ensure that all third-parties have implemented high-security measures, conduct regular assessments on their cybersecurity posture, and implement appropriate risk management strategies to prevent any cyberattacks that might also affect Grayson Insurance.

## VI. Conclusion

In conclusion, this paper has come up with a Strategic Cybersecurity Plan for Grayson Insurance. The aim was to ensure that the plan aligns with the company's business needs, while reducing its cybersecurity needs. This plan focuses on a proactive cybersecurity strategy and an adaptive IT philosophy. The proactive nature of the strategy goes hand in hand with Grayson Insurance's vision of being a globally compliance insurance services provider. The IT philosophy, on the other hand, addresses all vulnerabilities through digital transformation, and business-IT alignment. The top-down approach to management ensures that cybersecurity starts at the top and the outsources of services (e.g., cloud computing) also ensures that Grayson Insurance adequately protects itself from such risks extended downtimes among others. The company should, nonetheless, take into consideration such challenges as data privacy, cyber insurance risks, phishing, and supply chain security to ensure that they remain ahead of the curve.

## VII. Closing Cybersecurity Gaps

It is acknowledged that although many organizations have a cybersecurity strategy in place, there is still a considerably high prevalence of cybersecurity breach incidents. According to Wiley et al. (2020), this is because organizations do not approach the matter of cybersecurity proactively. For instance, while most of the organizations formulate appreciable security strategies, it is noted that the focus is primarily on the technology infrastructure and processes. However, the human factor is often overlooked, yet users have been identified as the weakest link in cybersecurity strategies and initiatives (Marion & Fixson, 2021). While many organizations adopt a multi-pronged approach towards cybersecurity that entails encryption, firewalls, and antivirus software, they do not prioritize awareness and training programs for their staff members. There is a notable leadership gap at the senior management level in terms of making responsible decisions about how to improve cybersecurity.

Tidd and Bessant (2020) recommended a proactive approach in which organizations not only invest in state-of-the-art technological tools but also consider creating and nurturing a security-first culture among its employees. This involves having clearly defined plans for continuous training programs as well as assessment and review of the cybersecurity policy. Similarly, Wiley et al. (2020) also found that a significant majority of cybersecurity breach incidents result from human error. Therefore, it is critical that organizations develop strong leadership teams that will give high priority to cybersecurity by nurturing a culture of acceptance towards awareness and use of enhanced security practices by employees. A trend that has been found to be counterproductive is the priority security professionals place on investing in complex technology. Such complex technology overwhelms security personnel and IT users who are often undertrained and inadequately informed about the basics of cybersecurity (Da Veiga et al., 2020). Therefore, it is critical that organizations consider the human factor in cybersecurity and prioritize on fostering a culture of awareness and responsible use of technology among employees, besides the heavy investments in technological measures.

## References

1. Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060.
2. Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98, 102003.
3. Cardona, P., & Rey, C. (2022). Management by missions: Connecting people to strategy through purpose (p. 156). Springer Nature.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024


4. Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. Computers & Security, 92, 101713.
5. Det Norske Veritas. (n.d.). The three-pillar approach to cyber security: Data and information protection. Retrieved from https://www.dnv.com/article/the-three-pillar-approach-to-cyber-security-data-and-information-protection-165683#:~:text=Confidentiality%20in%20this%20context%20means,not%20have%20access%20to%20them.
6. Howell, G., Boeckl, K., Grayson, N., Lefkovitz, N., Ajmo, J., Craft, R., McGinnis, M., Sandlin, K., Slivina, O., Snyder, J., & Ward, P. (2023). Mobile device security: Bring Your Own Device (BYOD), Special Publication (NIST SP). Gaithersburg, MD: National Institute of Standards and Technology.
7. Ironhack. (2024). Data privacy regulations: Compliance challenges and best practices. Retrieved from https://www.ironhack.com/gb/blog/data-privacy-regulations-compliance-challenges-and-best-practices
8. Kaushik, N. (2024). Risks, trends, challenges for cyber insurance. Retrieved from https://www.insurancethoughtleadership.com/cyber/risks-trends-challenges-cyber-insurance#:~:text=Unlike%20traditional%20insurance%2C%20cyber%20insurance,uncertainty%20remains%20a%20significant%20challenge.
9. Marion, T. J., & Fixson, S. K. (2021). The transformation of the innovation process: How digital tools are changing work, collaboration, and organizations in new product development. Journal of Product Innovation Management, 38(1), 192-215.
10. Mtsweni, P., Mokwena, S. N., & Moeti, M. N. (2021). The impact of outsourcing information technology services on business operations. South African Journal of Information Management, 23(1), 1-7.
11. Palatty, N. J. (2023). 80+ healthcare data breach statistics 2024. Retrieved from https://www.getastra.com/blog/security-audit/healthcare-data-breach-statistics/#:~:text=95%25%20of%20all%20identity%20theft,incidents%20affecting%202.5%20million%20people.
12. Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. International Journal of scientific research and management, 9(12), 669-710.
13. Reijers, H. A. (2021). Business process management: The evolution of a discipline. Computers in Industry, 126, 103404.
14. Tidd, J., & Bessant, J. R. (2020). Managing innovation: integrating technological, market and organizational change. John Wiley & Sons.
15. Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. Computers & security, 88, 101640.
16. Yoo, C. W., Goo, J., & Rao, H. R. (2020). Is cybersecurity a team sport? A multilevel examination of workgroup information security effectiveness. Mis Quarterly, 44(2).