**A Study on Small Company Security Management**

Table of Contents

[Introduction: 3](#_Toc155640323)

[Company Overview and Structure: 3](#_Toc155640324)

[Risk Assessment Overview: 4](#_Toc155640325)

[Main Risk Analysis: 5](#_Toc155640326)

[1. Govern (GV): 5](#_Toc155640327)

[2. Identify (ID): 6](#_Toc155640328)

[3. Protect (PR): 7](#_Toc155640329)

[4. Detect (DE): 8](#_Toc155640330)

[5. Respond (RS): 9](#_Toc155640331)

[6. Recover (RC): 9](#_Toc155640332)

[Recommendations: 10](#_Toc155640333)

[1. Design a Risk Management Plan: 10](#_Toc155640334)

[2. Social Media restriction at the workplace: 11](#_Toc155640335)

[3. Cyber Security focused training campaigns: 11](#_Toc155640336)

[4. Creating a Business Continuity (BCP) and Disaster Recovery Plan: 12](#_Toc155640337)

[Conclusion: 13](#_Toc155640338)

[References: 14](#_Toc155640339)

# **Introduction:**

Small enterprises have grown to be popular targets for attackers, but they are finding it difficult to implement cyber-security procedures that large businesses frequently employ. Because small firms employ a sizable fraction of the workforce, there is a pressing need for effective and appropriate cyber-security solutions (Tam et al., 2021). Infotech Private Limited, a small-sized digital marketing company established in September 2022, hired “ABC Consultancy Services” to conduct a Risk Assessment of their organization.

Companies nowadays prefer conducting Risk Assessments to help them identify the improvement points in their internal network to improve their business outcomes.

This report focuses on the gaps in their current cyber structure and the improvements that can be made in the future. The Assessment was conducted using NIST CSF 2.0. The management of the company had conducted an internal meeting before proceeding with the audit and finalized the framework on which the audit would be based. NIST CSF 2.0 was concluded to be the most suitable framework as it can help to create a foundation for a secure cyber environment. Figure 1 shows the Info-Tech network topology.

A computer network diagram with many computers

Description automatically generated with medium confidence

Figure : Info-Tech Pvt. Ltd. Network Topology

An Info-Tech Pvt. Ltd's network topology is an organized arrangement that is intended to improve the company's communications and data handling performance, management and security. The architecture is designed to meet the unique operating demands of each department while providing strong data protection and seamless connection.

The Core Layer, the topology's core point, is located in the heart of the network. The Multi-Layer Switch (MLS) functioning at this layer is critical for maintaining high-speed connectivity and managing data routing throughout the network. It is the aggregation point for all the VLANs and is accountable.

The Distribution Switches branch out from the Core, which acts as a control centre for network traffic to and from the Access Layer. These switches serve as gatekeepers, effectively imposing access regulations and making routing decisions to guide traffic. They connect to the access layer switches. They also serve as focal areas for VLAN traffic management and redundancy, ensuring that the network can withstand and respond to possible outages.

The Access Layer connects end-user devices to the network. Each department's devices are linked to their corresponding Access Switch, which enforces port-level security standards using features such as port security and ensures that each device is assigned the relevant VLAN. The Access Switches are immediately linked to the Distribution Switches, which connect to the Core MLS.

To enhance resilience, the network has redundant trunk lines connecting the Core and Distribution Switches. These trunks support several VLANs, allowing for diverse traffic flow across the network. The Spanning Tree Protocol (STP) is used to intelligently manage these trunks, ensuring that no loops exist inside the network and that backup pathways are quickly available if a major connection fails.

The network's structure is intended to provide interconnectivity across all devices in the company. The MLS uses Layer 3 routing to enable communication across VLANs while connecting to the external router that leads to the Internet. The router is protected by a powerful firewall that monitors and regulates entrance and egress traffic, protecting the internal network from external threats.

The topology features several security mechanisms. The firewall at the network's perimeter filters traffic using Access Control Lists (ACLs), VPN services allow secure remote access, and the internal VLAN structure separates critical departmental data. Intrusion Prevention Systems (IPS) are strategically situated to detect and stop harmful activities.

# **Company Overview and Structure:**

Infotech Private Limited is a digital marketing company consisting of 50 employees based in Chhattisgarh, India. The company had 1 single office from which the operation takes place daily. As opposed to the modern working method, the company was following the traditional method of all the employees working from the office, there was no hybrid mode of working available so far. According to the Chief Executive Officer (CEO), the management felt working from the office provides a better means of communication and increases productivity, as the staff strength is limited, working together from the office helps in achieving better results.

The CEO and Chief Technology Officer (CTO) were the individuals with the maximum authority in the workplace hierarchy who were responsible for overseeing the management group of the company. Other departments such as Human Resources (HR), Information Technology (IT), Sales and Marketing, Finance and Legal team all had their separate department Heads/Managers who were responsible for making sure the team operation was working smoothly.

The company was focused on providing digital marketing services such as managing social media platforms for their clients, brand management, publishing and managing blogs, launching advertising campaigns, etc. During the last 2-3 months the company acquired many reputed clients and hence before expanding to a medium-sized organization, the management wanted to conduct a Risk Assessment to improve the cyber security levels overall which will assist in improving their reputation as well.

The company uses the Zoom platform to conduct internal staff meetings and external meetings with clients. The company has their official email communication channel on Gmail which they use to send out important messages to its clients.

The reason behind selecting the NIST CSF 2.0 framework was even though the final version is yet to be released in 2024, the draft is still used by many organizations globally to review their cyber posture. The major issue for organizations in managing Information Security is how to handle it while attempting to get the optimal resource configuration to satisfy business objectives (Ashenden, 2008). As a small-scale company, they are constantly facing many challenges from their rival companies, however, by providing quality services, they have maintained good professional relationships with their clients.

# **Risk Assessment Overview:**

Apart from the remarkable effect on society and industry, the pandemic created an unusual variety of cyber-crime-related situations that also had an impact on society and business. The pandemic's increased fear raised the likelihood of cyber-attacks succeeding, increasing both the number and type of cyber-attacks (Lallie et al., 2021). The NIST CSF 2.0 is based upon 6 major controls: Govern (GV), Identify, Detect, Protect, Respond, and Recover (Refer to Figure 1). This audit report would also be helpful for the management to prove to their client that they were serious about the current cyber threats and their impact on the business.

The online environment has grown more susceptible to systematic and long-lasting cyberattacks. Cybersecurity strategies improve security mechanisms for detecting and responding to threats (Shaukat et al., 2020). The 6 controls in NIST CSF 2.0 have many sub-sections and not all of them apply to small organizations such as Infotech Private Limited, however, the general framework is still enough to manage the information security in the company.

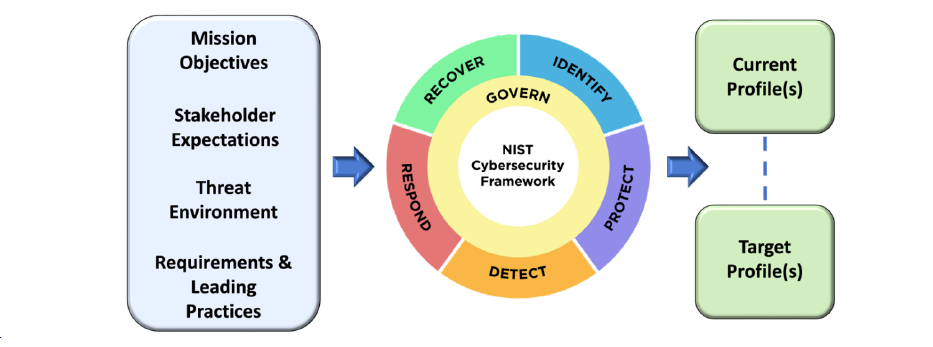


Figure . NIST CSF 2.0 controls

# **Main Risk Analysis:**

Before proceeding with the risk analysis, the consultants had many meetings with the management of the organization and some of the staff members who were responsible for various tasks such as coordination with the clients, etc. Their feedback was noted, and appropriate Risk Analysis was done by verifying the evidence provided by the respective stakeholders.

## **Govern (GV):**

|  |  |  |
| --- | --- | --- |
| **Function** | **Sub-Category** | **Summary** |
| Govern | 1. Organizational Context | The governance function helps the organization create a governance model and helps the management team implement the policies and procedures.  Infotech Private Limited had an Information Security Policy (ISP) in place. An Information Security Policy maintains the protection of an organization's information assets and information technology by following a particular approach. Assistance from management is critical throughout the implementation of information security rules (Angraini et al., 2019). The policy was reviewed recently, and the version history was updated from 1.0 to 1.1. This policy covered all the assets in place at the company. There was no separate Cyber Security policy in place as the cybersecurity section was covered in this same policy. To ensure Information Security Policy compliance, reviews must be performed on a regular and random basis (Angraini et al., 2019).  During the assessment, it was found that the company did not have a documented Risk Management and Treatment Plan available in place. The management of the company did not feel it necessary to document a separate Risk plan as according to their understanding, Infosec policy was enough for cyber compliance. However, the severity of not having a documented Risk Management Policy/Plan was brought forward to them. Processes for handling and mitigating risks ought to be linked to organizational and sub-organizational goals. Organizations should aim to identify all material risks to their goals and sub-objectives, develop controls and mitigations that yield residual risk in line with a target risk appetite, and monitor the entire procedure, making periodic modifications as needed (Power, 2009).  Another major non-compliance to be noted by the consultants during the assessment was that the company created advertisement campaigns and blogs for their clients. As per the research done by Gupta et al. (2023), Because of its ability to analyze huge volumes of data and make predictions, AI has allowed businesses to accurately tailor their social media campaigns and materials to specific audiences. Businesses can reach the most consumers by learning about their customers' opinions, sentiments, and reactions to their products and brands via social media. For this purpose, the employees were using social media websites for acquiring content, however social media section was not covered in the Infosec policy. NIST CSF does not contain any requirement as to a social media policy, however, for appropriate cybersecurity governance, safe usage of social media should be covered in the policy and employee training also needs to include safe use of social media. Websites like Facebook, Twitter, etc. should not be accessible on company desktops/laptops as this can lead to data breaches. |
| 1. Risk Management Strategy |
| 1. Cybersecurity Supply Chain Risk Management |
| 1. Roles, Responsibilities, and Authorities |
| 1. Policies, Processes, and Procedures. |

## **Identify (ID):**

|  |  |  |
| --- | --- | --- |
| **Function** | **Sub-Category** | **Summary** |
| Identify | Asset Management | The governance function helps the businesses to assist them in determining the organization's existing risk associated with cybersecurity (NIST CSF 2.0).  The Asset management part was covered sufficiently in the Information Security Policy. All the assets like desktops, laptops, printers, company telephones, etc. were part of this section. However, as there was no Risk Management plan in place at the company, it was recommended by the consultants that major risks associated with these assets should also be documented in the Risk Plan.  Since its inception in September 2022, the company has not gone through any Cyber Audit and Risk Assessment, hence, there have been no continual improvements in the cyber defense strategy of the organization.  There are essentially two types of businesses: those that have undergone a digital assault and those that are yet to recognize it. Developing a cybersecurity vision is a difficult task, as is implementing fundamental safety precautions (Sabillon et al., 2017). The consultants recommend that as the organization evolves in strength and resources, they should conduct annual evaluations to help them find out the weaknesses in their overall cyber posture. |
| Risk Assessment |
| Improvement |

## **Protect (PR):**

|  |  |  |
| --- | --- | --- |
| **Function** | **Sub-Category** | **Summary** |
| Protect | Identity Management, Authentication, and Access Control | The Protect function helps businesses with appropriate implementation and improvement to reduce the likelihood of cybersecurity crashes (Sulistyowati et al., 2020).  Each employee in the organization had their unique ID created by the Information Technology (IT) department once they joined the company. As the number of employees was less, access management was relatively easy to handle as compared to the large organizations. The main aim of the access verification system was that only authorized and legal users should be using the resources (Wu et al., 2021).  The office consisted of 3 main rooms and all the rooms had CCTV monitoring available in it. The office was located in a corporate building consisting of various offices and this building had security guards which used to monitor the individuals entering and leaving the building premises. For a small organization, the consultants deemed these measures as sufficient for physical security.  However, the major threat observed in this control was the fact that for almost a year, the company did not conduct any cyber training and awareness campaigns.    According to Mohannadi et al., (2018), even small enterprises need a mailing service to connect with their employees, clients, and stakeholders. Malicious emails can harm an organization's reputation. A phishing assault occurs when an attacker sends junk mail to employees of a company while appearing to be a legitimate one. It is quite difficult for an employee to decide whether or not to click the link. These decisions might be aided by effective information security awareness training. Information security awareness increases the user's understanding of the significance of best practices (Chua et al., 2021). Human-related factors are included in the annual cost of a data breach report. Human errors cause financial and reputational damage (Chang et al., 2021). |
| Awareness and Training |
| Data Security |
| Platform Security |
| Technology Infrastructure Resilience |

## **Detect (DE):**

|  |  |  |
| --- | --- | --- |
| **Function** | **Sub-Category** | **Summary** |
| Detect | Continuous Monitoring | The Detect function designs and conducts relevant activities to detect cybersecurity events as soon as possible (Sulistyowati et al., 2020).  During the assessment, we reviewed that the network devices such as switches, routers, etc. were all kept in a different room and only the 2 admins from the IT department had the key to access this locked room.  As of January 2024, there were no cyber incidents recorded by the organization. However, looking at current cyber trends, it is always good to be on the lookout for more methods to improve cyber security in terms of monitoring the network services, hardware and software. |
| Adverse Event Analysis |

## **Respond (RS):**

|  |  |  |
| --- | --- | --- |
| **Function** | **Sub-Category** | **Summary** |
| Respond | Incident Management | The response function is concerned with helping the organization to respond to the anomalous activities occurring in their workplace (Sulistyowati et al., 2020).  Incident Management was effectively covered in the Information Security Policy. The Incident Management section included the stakeholders to whom the staff must report the incident and who will be responsible for handling the mitigation methods. A company expends significant efforts to keep its computer systems incident-free; consequently, fast resolution of incoming incidents is necessary to achieve that goal (Gupta et al., 2008). The communication method was effectively mentioned in the Incident Management section. It stated that the department heads were the 1st level of escalation and 2nd level would be the CTO, if 1st and 2nd level both do not respond in the given timeframe then the incident can be escalated to the 3rd level i.e. the CEO. |
| Incident Analysis |
| Incident Response Reporting and Communication |
| Incident Mitigation |

## **Recover (RC):**

|  |  |  |
| --- | --- | --- |
| **Function** | **Sub-Category** | **Summary** |
| Recover | Incident Recovery Plan Execution | The Recover function is reserved for activities to maintain resilience strategies and restore abilities that may have been affected by a cybersecurity event (Sulistyowati et al., 2020). A cyber incident, like an emergency, is typically unplanned, sudden, urgent, and serious; thus, being prepared is the key to reducing, containing, and controlling cyber events. regardless of whether the incident is foreseen (or predicted), such as catastrophic weather predictions or forecasts, security threat and risk announcements, or alert systems, the institution's or mission's preparedness will determine the rate at which the incident can be managed, restricted, or/and its impact minimized (Onwubiko and Ouazzane, 2022). As the company had not faced any cyber breach in the last year or so since it was started, the management did not create a Business Continuity and Disaster Recovery plan. During the audit discussion it was confirmed that the management initially planned to document a BCP-DR plan, however, due to limited resources, limited staff, and financial burden, they couldn’t effectively create a specific plan for the same. This was a breach of cyber security as cyber attackers do not look at the size of the company before stealing data, any chunk of data stolen is money earned for them. |
| Incident Recovery Communication |

# **Recommendations:**

After successfully analyzing the 6 major controls, the consultants recommend the following changes which would help the company to manage information security in a better way.

## **Design a Risk Management Plan:**

* A Risk Management Plan for a small-sized organization should start by focusing on the daily operations of the company and what are the weak points where an attacker can penetrate the network.
* Restriction of social media in the workplace could be one of the first steps in it.
* After listing out the possible risks, try to develop the roles and responsibilities of staff and management in a scenario where a risk has been identified.
* As per Roth et al. (2020), Process models can be utilized to determine the linkages among the cause, occurrence, and consequence of production hazards. A process model might also include compensation mechanisms and risk monitoring indicators. Risk acceptance, reduction and avoidance can be considered as part of general risk treatment methods.

## **Social Media restriction at the workplace:**

* Allowing employees to access Facebook, Twitter, etc. on their work desktops could lead to potential data breaches.
* As businesses rely more on digital operations and the internet, data breaches have become more widespread. Data breaches now come at higher costs. Managers prioritize preventing, detecting, and controlling data breaches to avoid public relations catastrophes and management terminations (Schlackl et al., 2022).

## **Cyber Security focused training campaigns:**

* As per Chowdhury and Gkioulos (2021), Lack of expertise and readiness among individuals tasked with identifying and combating cyber-attacks is a leading cause of modern incidents.
* The training should be held by individuals who have expertise in handling cyber events and can demonstrate effective and simple steps of cyber hygiene to the staff.
* Training and Awareness campaigns should be held at regular intervals and the material should be focused on raising the awareness levels of staff (Refer to Figure 2).
* As most of the staff was between the age of 25-30, Raising awareness among the young employees about simple tasks such as identifying phishing emails and suspicious links by conducting mock phishing campaigns can go a long way in creating a healthy Information Security Management.
* The senior management of the company such as the CEO, CTO, and the department heads should also lead from the front and help the employees in terms of improving their cyber knowledge.



Figure . Steps to develop effective training material

## **Creating a Business Continuity (BCP) and Disaster Recovery Plan:**

* To initialize developing a BCP-DR plan, identifying the potential root cause of the disaster is important.
* Business Continuity can be defined as Identifying and preserving vital company operations and assets required to sustain an acceptable level of work, protecting those resources, and creating procedures to ensure that the company survives in times of business interruption (Mónica et al., 2020).
* As the organization creates advertising content, blogs, etc. for their clients, there is a significant amount of confidential data available with the company. Keeping a secure backup of this data is a very important step in the BCP process.
* The incremental backup method can be very efficient in allowing appropriate time for the smooth operation of the backup process.
* Disaster recovery can be a challenging process depending on the size of the cyber-attack and the affected resources of the organization.
* It is recommended that management do adequate research and look into getting in touch with industry leaders and professionals who have successfully helped other organizations develop BCP-DR plans.
* In case of a disaster, it is important to avoid the blame game and discourage employees from believing everything was their fault. Learning the lessons post the incident and adapting to effectively mitigate it can be beneficial to the organization.

# **Conclusion:**

The Risk Assessment based on NIST CSF 2.0 was conducted in a very efficient manner and the organization staff and management were helpful by giving honest answers and feedback during the discussion.

The above-mentioned Recommendations can help the organization improve their current Infosec hygiene and develop strategies to contain the cyber damage from any malicious attack in the future.

A lot of vulnerabilities can be discovered when looking at human-related and technical information security threats. Organizations need to address vulnerabilities through targeted methods. Organizational approaches to human information security were compared to technical security to strengthen the argument for a more balanced perspective. The companies that successfully integrate human-centered policies show how a balanced approach yields positive outcomes. Continuous training contributes to a good posture.

Understanding the cognitive processes and risk perception of individuals is paramount in developing effective strategies to mitigate threats. The complexity of human factors is highlighted by academic insights and advocates for an approach that integrates both technical and psychological dimensions such as effective training campaigns, mock phishing campaigns, etc. The human element is a real weakness that needs immediate attention. Recognizing this fact opens the door to a thorough study of how businesses can handle the complicated world of cybersecurity.

The audit report and the outcome of this Risk Analysis should be discussed internally by the Senior Management of the organization and develop a strategy to implement these recommendations in their company infrastructure. Taking a calculated and rational approach will help the company to have better control to manage security. To improve quality and maintain business functionality, organizations should sensibly adopt controls to eliminate faults. To effectively manage information security risks, organizations must recognize and put in appropriate controls in the face of vulnerabilities, risks, regulations, and financial limits (Baker and Wallace, 2007).

The consultants recommend that the company continue to conduct Risk Assessment audits in the future as they look forward to becoming a medium-sized organization. Future audits can be conducted on FMEA, ISO 27001, etc. to improve the cyber structure of the company.

# **References:**

1. Tam, T., Rao, A. and Hall, J., 2021. The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. Computers & Security, 109, p.102385.
2. Ashenden, D., 2008. Information Security management: A human challenge? Information security technical report, 13(4), pp.195-201.
3. Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C. and Bellekens, X., 2021. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & security, 105, p.102248.
4. Shaukat, K., Luo, S., Varadharajan, V., Hameed, I.A. and Xu, M., 2020. A survey on machine learning techniques for cyber security in the last decade. IEEE access, 8, pp.222310-222354.
5. National Institute of Standards and Technology (2023) The NIST Cybersecurity Framework 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29 ipd. https://doi.org/10.6028/NIST.CSWP.29.ipd
6. Alias, R.A., 2019. Information security policy compliance: Systematic literature review. Procedia Computer Science, 161, pp.1216-1224.
7. Power, M., 2009. The risk management of nothing. Accounting, organizations and society, 34(6-7), pp.849-855.
8. Sabillon, R., Serra-Ruiz, J., Cavaller, V. and Cano, J., 2017, November. A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). In 2017 International Conference on Information Systems and Computer Science (INCISCOS) (pp. 253-259). IEEE.
9. Sulistyowati, D., Handayani, F. and Suryanto, Y., 2020. Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss. JOIV: International Journal on Informatics Visualization, 4(4), pp.225-230.
10. Y. G. Wu, W. H. Yan and J. Z. Wang., 2021. Real identity based access control technology under zero trust architecture. International Conference on Wireless Communications and Smart Grid (ICWCSG), Hangzhou, China, 2021, pp. 18-22, doi: 10.1109/ICWCSG53609.2021.00011.
11. Al-Mohannadi, H., Awan, I., Al Hamar, J., Al Hamar, Y., Shah, M. and Musa, A., 2018, August. Understanding awareness of cyber security threat among IT employees. In 2018 6th international conference on future internet of things and cloud workshops (ficloudw) (pp. 188-192). IEEE.
12. Chang, C.H., Kontovas, C., Yu, Q. and Yang, Z., 2021. Risk assessment of the operations of maritime autonomous surface ships. Reliability Engineering & System Safety, 207, p.107324.
13. Chua, H.N., Teh, J.S. and Herbland, A., 2021. Identifying the effect of data breach publicity on information security awareness using hierarchical regression. IEEE Access, 9, pp.121759-121770.
14. Gupta, R., Prasad, K.H. and Mohania, M., 2008, June. Automating ITSM incident management process. In 2008 International Conference on Autonomic Computing (pp. 141-150). IEEE.
15. Onwubiko, C. and Ouazzane, K., 2020. SOTER: A playbook for cybersecurity incident management. IEEE Transactions on Engineering Management, 69(6), pp.3771-3791.
16. Gupta, M., Kumar, R., Sharma, A. and Pai, A.S., 2023, July. Impact of AI on social marketing and its usage in social media: A review analysis. In 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-4). IEEE.
17. Roth, S., Weber, M., Hohmann, A. and Reinhart, G., 2020, December. Risk assessment and treatment planning for energy-flexible production systems using an additional cost model. In 2020 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM) (pp. 85-90). IEEE.
18. Schlackl, F., Link, N. and Hoehle, H., 2022. Antecedents and consequences of data breaches: A systematic review. Information & Management, 59(4), p.103638.
19. Chowdhury, N. and Gkioulos, V., 2021. Cyber security training for critical infrastructure protection: A literature review. Computer Science Review, 40, p.100361.
20. Mónica, R., Henry, Q., Estela, M. and Washington, F., 2020, June. Why implement continuity plans in Organizations? Approach of a prospective study based on ITIL. In 2020 International Conference on Intelligent Systems and Computer Vision (ISCV) (pp. 1-5). IEEE.
21. Baker, W.H. and Wallace, L., 2007. Is information security under control?: Investigating quality in information security management. IEEE Security & Privacy, 5(1), pp.36-44.