Vol. XVI & Issue No. 08 August - 2023
INDUSTRIAL ENGINEERING JOURNAL

DEFINING AND DESIGNING THE ORGANISATION STRUCTURE OF INFORMATION SECURITY & DATA PROTECTION FOR AN INDIAN STEEL MANUFACTURING COMPANY

Sachin M S
B N Bhagat
Ramesh Kumar R
Sharath Kumar
Rama Shanker Singh

Abstract:

Industry 4.0 and Industrial Internet of Things (IIOT) is revolutionising the way companies manufacture, improve, and distribute products. While incorporation of digital technologies and advanced automation has led to optimized processes and new levels of efficiencies, they have also thrown open the Challenges of cyber security and data protection. Continuously evaluating the effectiveness of implemented cyber security Processes and technology to protect, detect and respond to potential cyber security incidents and alerts are a must. Considering the changing cyber security landscape, making the organization more resilient against the potential cyber incidents is critical. This study is aiming to provide insights into the designing an information security and data protection organisation for a major steel manufacturing company. Firstly, we define the evolving threat and regulatory landscape and the changing role of information security and data protection with the advent of IIOT. Secondly, we focus on the parameters to consider while designing the organisation for information security and data protection (ISDP). Thirdly we discuss the structured way in which the final organization structure for ISDP is arrived at and the expected deliverables of the team.

Keywords: Organisation Design, Industrial Internet of Things, Cyber Security, Industry 4.0

1. INTRODUCTION

1.1 Technology Advancement in Manufacturing Industry

As part of Industry 4.0, companies are adopting new technologies like Internet of Things (IoT), cloud computing and Artificial Intelligence. Such technologies enabled higher level of automation, predictive maintenance, and optimization. It also has helped the business in incorporating the production data into the ERP system for fast and data-based decision making.

To survive in competitive global marketplace, the companies are required to be more agile and flexible. The enhancement in technology led to controlling of manufacturing operations from anywhere around the world. Platforms like Microsoft Teams, Zoom, Google Hangouts have opened the possibility of conducting business meetings in through video conferencing. The demand created by these platforms has created a major impact to the technology builders to focus on similar products. Many tech giants like Facebook, Amazon etc are now focusing on the concept of metaverse which will bring a paradigm shift in the digital world.

Along with the wonders that technology and data are contributing to the manufacturing industries, there are many potential vulnerabilities associated with these advanced technologies as well. One of the primary threats associated is Information security and data protection area. According to the enterprise risk management survey conducted by AQPC in 2021, one out of every 10 top risks assessed by respondents fall into the cyber-risk category.

1.2. Evolving Threats related to Data Security

Threats to an organization related to information security is also evolving along with the technology advancement. Some important threats associated today's business scenario are listed in Table-1.

Table 1. Factors associated with different cyber threats

Domain	Factors
Remote working is a Norm	Access enterprise Apps at anytime from anywhere
	Users logging from atypical locations and devices at irregular times pose difficulty in identifying anomalous behaviour
	Reliance on home router / Wi Fi without advanced security capabilities
	Changing risk values due to increased variability of access
Digital Transformation & Adoption of Cutting Edge Technologies	Adoption of Cloud computing Vs On premise
	Use of cutting-edge technologies to Transform Business (Bots, AI, ML, IoTs, Drones etc.)
	Industry 4.0, Industrial Automation Convergence of IT & OT
	Business Intelligence & Analytics Data Vs Information

Nature & Motives of Cyber Incidents are changing	Increasing trend of Targeted attacks on business-critical systems
	Organized business & groups (RaaS-Ransomware as Service)
	Cyber risk is no longer limited to financial crime
	Need for rapid visibility, understanding, & prioritization of vulnerabilities
Managed Service Model	Adoption of Managed Service Model (Ex. Software as a Service, Wi Fi as a Service, Security as a service etc.)
	Focus on supply chain risk with increasing demand for third party risk assessments

1.3. Data Security Infrastructure

Data Security Infrastructure consists of application solutions and governance processes [1] Information security and IT support of business are developed in close relationship. One need to follow an architectural approach for managing processes [2]. There should be a linkage between architecture, strategy of information security and business strategy [3].

Majority of the organization follows three lines of defence mechanism– maker, checker, and auditor for governing the IT security (Assets & Data). All the installation and configuration of the system in organisation level is done by Information Technology department. It is monitored and assessed by Information Security & Data privacy team. The audit team will evaluate the system in a timely manner. This paper focuses on data monitoring and assessment area (checker roll) - its changing role in today's context, the need of strengthening the team to meet the requirements in this technology revolution.

2. CHANGE IN SCENARIO OF ISDP FUNCTION

With the transition to digital processes especially after the pandemic, the criticality and workload of Information security department has increased significantly. This increased workload can be classified into two groups, one is volume increase due to the upscaling of digital resources. Variation of some of the Key Performance Indicators (KPI) over last few years are shown in Figure-1a. Second is due to the additional roles which this function has to take to reduce the risk of data vulnerability. Figure-1b shows change in roles of ISDP in today's context.

Fig-1a. KPI Trend of ISDP

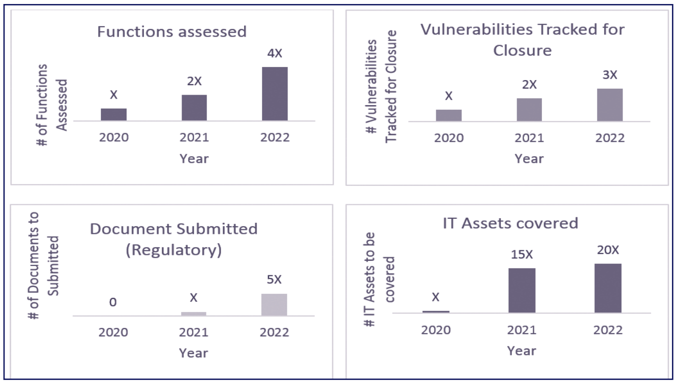
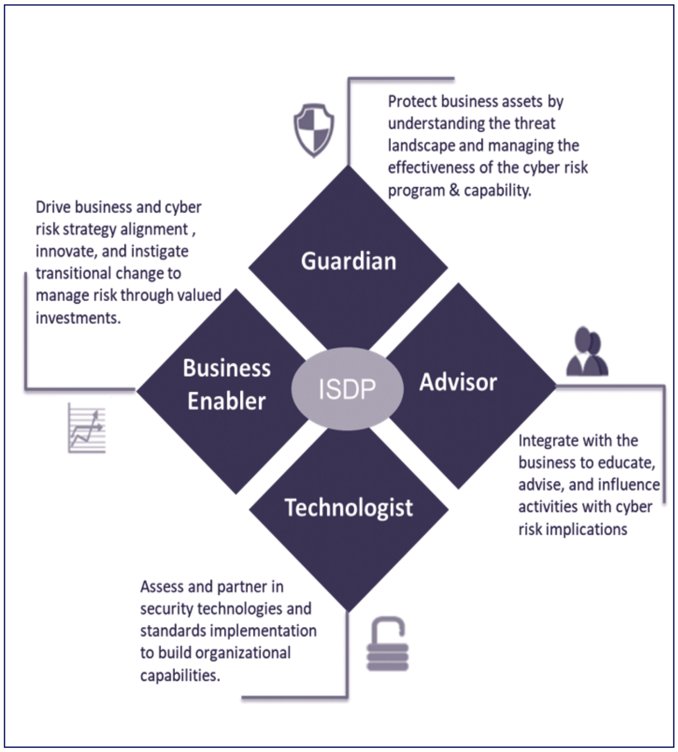
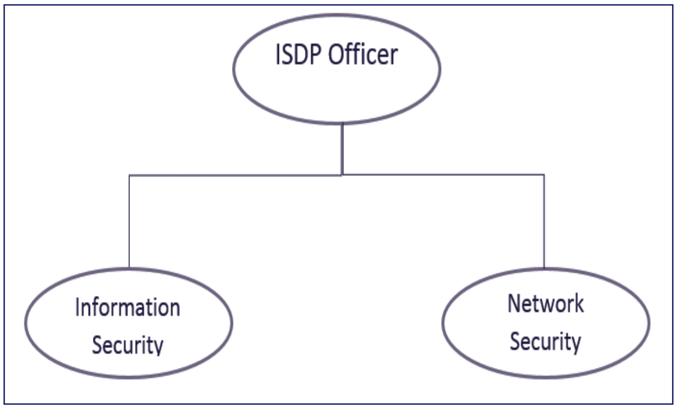


Fig-1b. Change in role of ISDP in today's context


Protect business assets by understanding the threat landscape and managing the effectiveness of the cyber risk program & capability.
Drive business and cyber risk strategy alignment , innovate, and instigate transitional change to manage risk through valued investments.
Guardian
Business Enabler
ISDP
Advisor
Technologist
Integrate with the business to educate, advise, and influence activities with cyber risk implications
Assess and partner in security technologies and standards implementation to build organizational capabilities.

There is an obvious change in scope of ISDP function because of the change in business environment and strategy. To address this, process and structure need to be changed in alignment with the business need. The process part is already modified by the business, changes in organisation structure needed to be done. The existing structure of ISDP (shown in Fig-2) consist of two verticals, Data Privacy and Network security. This existing structure was incapable of implementing the new processes and roles given to the department.

Fig-2. Existing Structure of ISDP

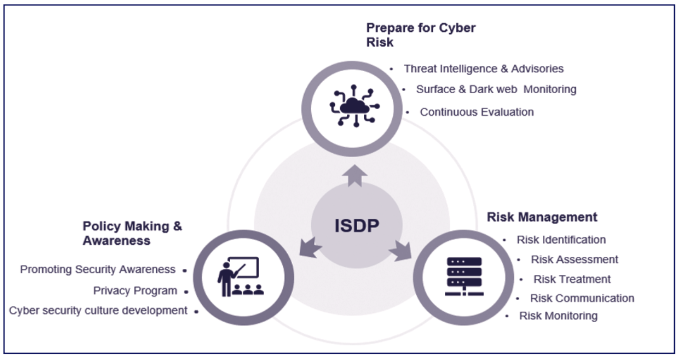


3. APPROACH FOR REVIEWING THE ORGANIZATION STRUCTURE OF ISDP

In the process of reviewing the organization structure, the primary focus or input required was to identify the framework which the division was adopting. Which will show the operating philosophy and major processes & practices involved.

3.1 ISWP Framework of an Indian Steel Company

Fig-3. ISDP Framework Evolving



From the framework (shown in Fig-3), the major job categories of the department can be categorised into three,

- **Prepare for Cyber Risk:** Commit to and invest resources and tools on the front end of risk to prevent from cyber-attacks. Continuously evaluate the assets, monitor the external environment, identify trends and sentiment going on, advise the respective business regarding the same etc.
- **Risk Management:** Identify the areas which are most prone to cyber risk and assess whether the controls and safeguards have in place, keep the risk below the level of risk appetite. Cyber risk assessment should also include activities like IT penetration testing and implementing filtering systems for suspicious and/or external e-mails.
- **Policy Making & Awareness:** Make sure you have policies related to information security and data privacy are clear, well communicated, and understood by every employee. With cyber-attacks on the rise, it's simply not worth it to take unnecessary risks because even a single employee could end up causing a lot of financial damage.

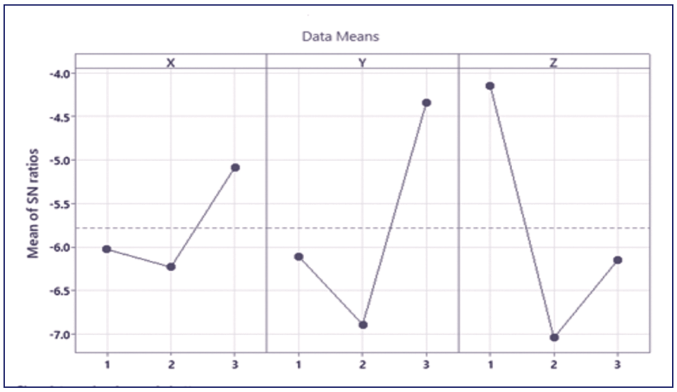
1.2 *Structured way to build organization designing*

The current organisation structure (shown in Fig 2.) of ISDP department was not aligned with the implementation of the framework mentioned in Fig-3. The identification of the framework shown above facilitates designing an organisation structure. The verticals in the organisation structure represent the job families (in this case three job families) of the function. The strength of each vertical will be decided on the workload of the respective vertical. As the technology is changing continuously within a short period of time, whether to develop the competency inhouse or outsource to third party is a business decision, and this will also influence the strength of each vertical.

4. CONCLUSION: FINAL ORGANIZATION STRUCTURE OF ISDP

With the above consideration mentioned above, final structure of the organisation for ISDP is formulated and shown in Fig-4.

Fig-4. Proposed Structure of ISDP



Post covid, remote working and technology involvement in the business function has increased, which makes the data system more vulnerable for cyber-attacks. Therefore, a robust IT infrastructure and governance mechanism and a supporting organisation structure is a must for every organisation. It should be noted that, as the technology integration advances, business requirement and framework will also change, and this organisation structure might not be suitable for such scenario. Therefore, it is advised to revisit the organisation structure for ISDP function more frequently.

REFERENCES

[1] Chung, L., Subramanian, N. (2007), "Bridging the gap between enterprise architectures and software architectures." Science of Computer Programming 66 (2007), 1-3.

[2] Giachetti, R. (2012), "A Flexible Approach to Realize an Enterprise Architecture." Procedia Computer Science 8 (Aug. 2012), 147-152.

[3] Malone, T.W., Weill, P., Lai, R.K., D'Urso, V.T., Herman, G., Apel, T.G., Woerner, S.L. (2006), "Do Some Business Models Perform Better than Others?", MIT, 4615-06 (May 2006).

AUTHORS

Sachin M S, Productivity Services Department, Human Resources Management, Tata Steel, Jamshedpur

B N Bhagat, Productivity Services Department, Human Resources Management, Tata Steel, Jamshedpur

Sharath Kumar, Productivity Services Department, Human Resources Management, Tata Steel, Jamshedpur

Shri Rama Shanker Singh, Productivity Services Department, Human Resources Management, Tata Steel, Jamshedpur
Email: ramashanker.singh@tatasteel.com / Mob. 9234567849

Ramesh Kumar R, Information Security and Data Protection, Tata Steel, Jamshedpur