

BROCHURE

The World - Class Assignment Service

That you deserve

CONTACT US

 DrKhanhAssignmentService
 www.drkhanh.edu.vn
 (+84) 939 070 595 hoặc (+84) 348 308 628



Executive summary

This article provides a thorough analysis of TransTech's cybersecurity strategy and policy, focusing specifically on the organizational context, security governance frameworks, and fundamental principles. TransTech is a software company that specializes in the development of financial software solutions tailored to meet the particular needs of corporate entities. The business offers opportunities for remote work, encourages flexible working arrangements, and partners with Microsoft to grant access to Office 365 and Windows 10 software. The company provides a selection of connectivity options, including Wi-Fi and standard ethernet, alongside the implementation of routine data backup on external hard drives via the server computer. John has been assigned the duty of supervising server operations and provide IT assistance as required. The research employed the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CFT) as a methodology to assess the cybersecurity approach of TransTech.

The primary aim of the author is to construct Key Performance Indicators (KPIs) that are in accordance with the preferences of stakeholders and are especially pertinent to the field of cybersecurity. The Key Performance Indicators (KPIs) will be shown on a dashboard in order to facilitate accurate reporting of cybersecurity performance. The current investigation has established a collection of Key Performance Indicators (KPIs) with the objective of evaluating the effectiveness of cybersecurity measures. The collection of Key Performance Indicators (KPIs) indicated earlier was given to relevant stakeholders during interview sessions and later modified based on their stated preferences. The comprehensive aggregation of indicators and metrics serves as the fundamental basis for the eventual development of dashboards.

1. Introduction

This article presents a comprehensive examination of TransTech's cybersecurity strategy and policy, with a specific emphasis on the organizational backdrop, security governance structures, and underlying beliefs. TransTech is a software firm that focuses on developing financial software solutions specifically designed to cater to the requirements of corporations. The organization provides remote work options, promotes flexible working arrangements, and collaborates with Microsoft to provide access to Office 365 and Windows 10 software. The firm offers both Wi-Fi and traditional ethernet connectivity choices, while also implementing regular data backup on external hard drives through the server computer. John is tasked with the responsibility of overseeing server operations and providing IT support as needed. The study used the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CFT) as a means to evaluate the cybersecurity strategy of TransTech.

2. Cybersecurity strategic goals, initiatives, and business needs

2.1. The goals

The main goal is to ensure compliance with legal obligations, regulations, and industry standards in order to protect vital information assets and ensure adherence to relevant guidelines (Rodrigues et al., 2013). Lauter (1999) asserts that the prioritizing of compliance functions as a mechanism to ensure ethical business conduct and mitigate potential legal risks. The focus of the technique revolves around the reduction of cybersecurity events through the implementation of business continuity planning, the establishment of resilient response procedures, and the adoption of proactive preventative measures (Bandari, 2023). In order to address any financial, reputational, and operational repercussions, TransTech has the opportunity to cultivate a corporate environment that prioritizes the acquisition of cybersecurity expertise among its workforce. As stated by McCarthy (2021), this specific methodology equips employees with the necessary skills needed to establish and maintain a safe working environment.

TransTech's cybersecurity strategy entails the distribution of tasks and obligations across several hierarchical levels to enhance the efficiency and management of execution. The board of directors bears the obligation for providing financial aid, supplying strategic guidance, and enforcing accountability among top management with regards to cybersecurity measures (Neto and Chiarini 2021). The establishment of objectives and the alignment of essential policies with these aims are

the responsibilities of senior management leadership, overseen by Samuel. The individual identified as Samuel strongly supports the implementation of a comprehensive framework in relation to the governance of security. All employees have a duty to comply with security protocols, report any potential risks, and actively participate in continuous cybersecurity training and awareness programs. John is tasked with the responsibility of supervising the IT support and server operations.

2.2. The business needs

The above process, when being applied to Trantech company, would produce the Information Security Maturity Model as follow:

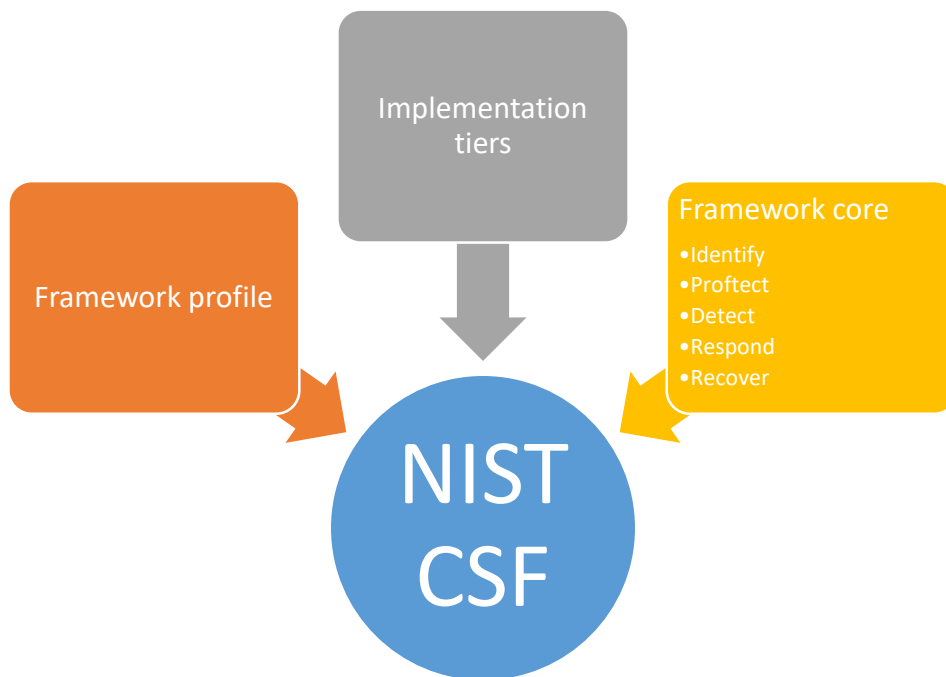
Table 2-1: Identified business needs of Trangia company

	Performance	Management	Establishment	Optimization
People	The execution of general people capabilities can be carried out by an individual, while their specific parameters may not be clearly delineated.	The personnel competencies are regularly accomplished within certain subsets of the organization, but exhibit inconsistency when considering the company as a whole.	The identification, assignment, and training of roles and tasks are conducted throughout the entirety of the company.	The implementation of proactive measures to enhance performance and allocate resources in response to organizational changes and the assimilation of internal and external knowledge.
Process	The execution of general process skills can be carried out by an individual, albeit their specific parameters and boundaries are not clearly delineated.	Sufficient protocols that have been duly recorded inside a certain segment of the institution.	Organizational policies and processes are established and standardized. Policies and procedures play a crucial role in facilitating the alignment between an organization's strategic objectives and its operational activities.	Policies and procedures undergo updates in response to organizational modifications, while lessons gained from both internal and external sources are documented.
Technology	Individuals have the option to utilize established technical procedures that are generally available.	A subgroup of the organization is responsible for explicitly identifying and defining technical mechanisms. The implementation of technical requirements has been established.	The purpose and objective are clearly delineated, ensuring the selection of appropriate technology and its effective deployment. The organization ensures that the suitable technology is applied in each subset of the organization.	Technical mechanisms are systematically enhanced in response to organizational changes and the assimilation of knowledge gained from both internal and external sources.

3. Cybersecurity program development

The Framework serves as a supplementary component to an organization's risk management process and cybersecurity program, rather than serving as a substitute for both. The firm has the ability to utilize its existing procedures and exploit the Framework in order to find potential areas for enhancing and effectively communicating its handling of cybersecurity risk, all while adhering to established industry norms (Christopher et al. 2021). In the absence of a pre-existing cybersecurity program, an organization might utilize the Framework as a point of reference in order to develop one (Couch 2023).

In order to accommodate the distinct cybersecurity requirements of companies, there exists a diverse range of methodologies for leveraging the Framework. The responsibility for determining the application of the decision is with the implementing entity. As an illustration, a particular business may want to employ the Framework Implementation Tiers as a means of expressing its envisioned risk management strategies.



NIST Cybersecurity Framework



Figure 3-1: NIST CFT framework

The Core facilitates the dissemination of cybersecurity actions and outcomes throughout the business, enabling effective communication from top-level executives to those involved in implementation and operations (Luengo et al. 2023). It achieves this by presenting industry standards, rules, and practices in a comprehensive way. The Framework Core has five Functions that operate simultaneously and continuously: Identify, Protect, Detect, Respond, and Recover. When taken into account together, these Functions offer a comprehensive and strategic perspective on the life cycle of an organization's management of cybersecurity risk (Zahid et al. 2023).

4. Performance metrics and KPI

4.1. Designing prioritized and traceability map

Table 4-1: Priorities of Trantech company

Category	Description
The development and testing environments are distinct entities that are independent of the production environment. The management of remote access is conducted.	The implementation of comprehensive testing environments enables the execution of test cases without apprehension of causing harm to the production environment.
	Establish a method for monitoring remote access to the production system. Restrict remote access to restricted functions only to authorized individuals. The primary objective is to establish agreements and ensure the verification of security measures for establishing links with external systems.

Individuals who possess privilege possess a comprehensive understanding of the obligations and responsibilities associated with their privileged status. The protection of data-at-rest is ensured.	This proposal aims to provide a set of well-defined cybersecurity awareness and training protocols for privileged users, specifically targeting developers. The objective is to outline a comprehensive framework that clearly delineates acceptable and undesirable actions within the working context.
The management and protection of physical access to assets is effectively implemented.	Develop and execute protocols that outline the steps for encrypting all personally identifiable information (PII) data throughout the whole Amazon Web Services (AWS) infrastructure.
The process of planning and testing for response and recovery is carried out in collaboration with suppliers and third-party providers.	This request pertains to the establishment, documentation, and execution of protocols inside the Access Control Policy framework, specifically focusing on delineating roles and duties associated with physical access.
The protection of data throughout its transmission is ensured.	The objective is to define and develop formal protocols that outline the processes for response, recovery planning, and testing in collaboration with suppliers and third-party providers.
	It is advisable to incorporate a contractual clause mandating third-party suppliers/partners to promptly inform the contracting party in the event of a prospective or real security incident or data security breach.
	Develop and execute protocols that delineate the appropriate methods for transferring data.

4.2. KPI designs

Table 4-2: KPI and NIST framework

	Identify	Protect	Detect	Respond	Recover
	Total auditing realized	% of IT budget for IS	% non-compliance with policies	% benchmark met	Recover Recovery time objective (RTO)
	Maximum tolerable downtime (MTD)		% non-compliance with norms & laws		Recovery point objective (RPO)
Strategic	Level of maturity		#reported incidents		RTO <MTD % incident impacts analysed
	% of approved security plans				% of learning from incidents
	Time invested in security awareness				% of critical assets in recovery plans

					Frequency of continuity tests
Tactical	# of antimalware software used	% of up-to-date malware protection	# of inactive user IDs	Respond phase of security controls	
	% of systems covered by access management	% of systems treating integrity, availability and confidentiality	Vulnerabilities per product	Time from incident to implementation of initial response	
	% of departments covered by the awareness program	% of tests of emergency plans	Total vulnerabilities by business units	Time from incident to completion of response	
	% of employees with user (root) rights	Last security update of software systems	Business unit severity level		
	Risk tolerance level	#of updates of the security policy	% of non-compliance with policies	#/% of incidents a day that require countermeasures	
	<i># of employees that followed trainings</i>	% of computers protected by antivirus software	#false identification /authorization attempts	% of planning actions implemented	
Operational	<i>#of systems that are being monitored</i>	% of computers protected by antivirus software	# of incidents due to bringing infected removable media	Total of incident responses	
	Open/closed status for reported events	Time between patch release and installation on system	# of incidents due to browsing malware infected websites	Prioritizing of response actions	
	#of hours spent on security trainings	% of systems with password policies	Value of MIN: # of malware incidents	% incidents solved	
		#of stopped viruses on network gates	#of files that should be deleted		
	Risk level		#of security alerts per period		
	Success rate	% of systems fully patched			
	# access requests	% of systems that can			

# of critical alerts	potentially be patched % of system without controls
----------------------	---

5. Reporting and communication

Our preferred mode of communication would be a dashboard that encompasses key performance indicators (KPIs) and performance measures of superior quality. One of the goals and deliverables established at the outset of this thesis is the formulation of a user-friendly dashboard that can be easily used by the stakeholders. Our study will be focused on investigating methods for the development of a user-friendly dashboard, with a particular emphasis on incorporating this objective into the design process. In general, our dashboard incorporates many elements as shown below:

- **Aesthetic Appeal:** The dashboard should possess visual attractiveness and be visually pleasant to the user. Effective design integrates elements of strength, practicality, and minimalism while also presenting an aesthetically beautiful visual composition.
- **Comprehensibility:** It is important for a dashboard to arrange information in a coherent and intelligible manner. This encompasses the arrangement of the whole dashboard, including both the composition of its components and the sequential placement of visualizations. Moreover, the need of reading and comprehending lengthy explanations should be deemed unnecessary. However, it is crucial to include explanations in order to facilitate comprehension of the dashboard. The absence of accompanying language, labels, or instructions in data may lead to misinterpretations and misunderstanding.
- **Customizability:** The inclusion of adaptable features inside the dashboard is crucial in order to cater to the diverse needs and preferences of various users. Flexibility refers to the capacity of a system to effectively adapt and accommodate the unique characteristics and variances among individuals. Various users exhibit interest in certain metrics. The inclusion of a customizable dashboard provides users with the ability to search for and choose information that aligns with their own interests. The seamless ability to customize the dashboard facilitates an engaged stance in comprehending information and accommodates individual choices in proficiency levels. One prevalent approach of achieving customizability in a

dashboard is via the use of data filters, which serve to delineate the specific scope of the data being shown.

6. Conclusion

The objective of the thesis was to address the fundamental issue of inadequate provision of reliable cybersecurity reporting for management. The organization seeks to implement a dashboard that offers a comprehensive depiction of cybersecurity vulnerabilities and associated operations. The management seeks to efficiently identify the areas of cybersecurity systems or processes that require improvement and determine the appropriate strategies for enhancing them. The author's objective is to establish Key Performance Indicators (KPIs) that are aligned with the preferences of stakeholders and are specifically relevant to cybersecurity. These KPIs will be shown on a dashboard to ensure precise reporting of cybersecurity performance. In the present study, a set of Key Performance Indicators (KPIs) has been identified for the purpose of assessing the performance of cybersecurity. The aforementioned set of Key Performance Indicators (KPIs) was presented to pertinent stakeholders during interview sessions and subsequently revised in accordance with their expressed preferences. The ultimate compilation of indications and metrics is the foundation for the eventual creation of dashboards.

7. Bibliography

Christopher SJ, Ellisor DL and Davis WC (2021) 'Investigating the feasibility of ICP-MS/MS for differentiating NIST salmon reference materials through determination of Sr and S isotope ratios', *Talanta*, 231:122363, doi : [10.1016/J.TALANTA.2021.122363](https://doi.org/10.1016/J.TALANTA.2021.122363).

Couch AN, Sharp J and Davidson JT (2023) 'Assessing the effectiveness of the NIST DART-MS Forensics Database and Data Interpretation Tool for designer drug screening with alternative instrumentation', *International Journal of Mass Spectrometry*, 483:116964, doi: [10.1016/J.IJMS.2022.116964](https://doi.org/10.1016/J.IJMS.2022.116964).

Luengo E (2023) 'Further analysis of the statistical independence of the NIST SP 800-22 randomness tests', *Applied Mathematics and Computation*, 459:128222, doi: [10.1016/J.AMC.2023.128222](https://doi.org/10.1016/J.AMC.2023.128222).

da Silva Neto VJ and Chiarini T (2021) 'Technological progress and political systems: Non-institutional digital platforms and political transformation', *Technology in Society*, 64:101460, doi: [10.1016/J.TECHSOC.2020.101460](https://doi.org/10.1016/J.TECHSOC.2020.101460).

Zahid S et al. (2023) 'Threat modeling in smart firefighting systems: Aligning MITRE ATT&CK matrix and NIST security controls', *Internet of Things*, 22:100766, doi: [10.1016/J.IOT.2023.100766](https://doi.org/10.1016/J.IOT.2023.100766).

Laufer WS (1999) 'Corporate liability, risk shifting, and the paradox of compliance', *Vand. L. Rev.*, 52: 1341

JPC Rodrigues J, de la Torre I, Fernández G and López-Coronado M (2013) 'Analysis of the security and privacy requirements of cloud-based electronic health records systems', *Journal of medical Internet research*, 15(8):186, 10.2196/jmir.2494

Bandari V (2023) 'Enterprise Data Security Measures: A Comparative Review of Effectiveness and Risks Across Different Industries and Organization Types', *International Journal of Business Intelligence and Big Data Analytics*, 6(1):1-11, <https://orcid.org/0000-0003-4185-3985>

McCarthy K (2021) *Cybersecurity Awareness Training Methods and User Behavior*, Doctoral dissertation, Utica College.

Stoneburner G, Goguen A and Feringa A (2002) 'Risk management guide for information technology systems', *Nist special publication*, 800(30):800-30.

Kim L (2022) *Cybersecurity: Ensuring confidentiality, integrity, and availability of information*, Nursing Informatics: A Health Informatics, Interprofessional and Global Perspective.