American Journal of Information Science and Technology
2025, Vol. 9, No. 2, pp. 148-154
https://doi.org/10.11648/j.ajist.20250902.17

SciencePG
Science Publishing Group

Research Article

Case Study: How T&S Survived a Ransomware Attack

Partha Majumdar*

Department of Computer Science, Kalinga University, Raipur, India

Abstract

This case study explores how Tools and Solutions (T&S), a small business, addressed and recovered from a major ransomware attack that jeopardised its operational continuity. The attack took advantage of significant weaknesses in the company's cybersecurity framework, including outdated software, a lack of adequate employee training, and missing regular backups. Consequently, vital business data got encrypted, operations were interrupted, and the organisation faced the tough choice of whether to pay the ransom or attempt data recovery. The study outlines the prompt crisis management actions taken by T&S, which included incident documentation, stakeholder communication, and data recovery through manual means. Additionally, it details the long-term cybersecurity improvements that followed, such as the adoption of cloud-based backup systems, the rollout of the Odoo ERP system, the application of the NIST Cybersecurity Framework, and the establishment of employee training programmes. By detailing each stage of the company's evolution, the case demonstrates how a small business built resilience through integrated policy reforms, infrastructure enhancements, and cultural shifts. The study also underscores important lessons regarding data redundancy, risk management, and organisational readiness. It offers a practical roadmap for small and medium-sized enterprises aiming to bolster their cybersecurity posture against increasing ransomware threats.

Keywords

Ransomware Incident Response, Cybersecurity Resilience in SMEs, Cloud-based Data Backup Strategies, NIST Cybersecurity Framework Implementation, Organisational Recovery After Cyber Attacks

1. Introduction

In the digital era, ransomware attacks are a growing threat, particularly targeting small and medium-sized businesses that often have inadequate cybersecurity measures [3, 12]. This case study highlights how Tools and Solutions (T&S), a small business, navigated a severe ransomware incident that threatened its operations and data security. The attackers infiltrated the company's systems, encrypting essential data and demanding a ransom for its recovery. The immediate consequences were devastating, disrupting key operations and halting business activities altogether. T&S exhibited the common vulnerabilities of small businesses: essential company data needing protection, yet insufficient cybersecurity measures in place [16].

The case starts by framing ransomware as a harmful strategy in which attackers encrypt an organisation's data and often threaten to make sensitive information public if their demands are ignored [8, 13]. T&S's situation illustrates the vulnerabilities faced by small businesses in today's increasingly perilous cyber environment [15]. At the onset of the attack, T&S found itself with limited options- attempting to unlock the encrypted files, contemplating ransom payment, or reconstructing data from scratch—each of which posed sig-

*Corresponding author: partha.majumdar@kalingauniversity.ac.in (Partha Majumdar)

Received: 23 April 2025; **Accepted:** 10 May 2025; **Published:** 16 June 2025

nificant risks and drawbacks [5].

T&S embarked on a mission to strengthen its cybersecurity posture, considering the crisis [18]. As a cloud provider, STC (Saudi Telecom Company) offered advanced security and backup services, establishing one of the strictest SOPs (Standard Operating Procedures) for routine data backups and restorations [7]. The company implemented the Odoo ERP system to enhance data management and security [4]. Realising that technical measures alone were not enough, T&S adopted a comprehensive cybersecurity framework by following the National Institute of Standards and Technology (NIST) guidelines [9]. This framework facilitated the classification and categorisation of functions, allowing the organisation to create a tailored ransomware profile to address its specific risks and vulnerabilities.

This case highlights the importance of preventive measures to prevent future attacks [10]. In response, T&S has implemented a comprehensive strategy that involves using antivirus software, consistently applying updates, blocking access to potentially dangerous websites, restricting personal device use on the corporate network, and mandating that only authorised applications are utilised [1]. Additionally, enhancing employee awareness and training has become a key element of their defence plan [6]. T&S's cybersecurity training empowers staff with the necessary knowledge and skills to identify potential threats, mitigate risky behaviours, and respond effectively during an incident, thereby cultivating a cybersecurity-oriented culture throughout the organisation [11].

This case study emphasises the extensive impact of ransomware on small businesses and the essential measures needed to alleviate these threats [14]. T&S's story of vulnerability and subsequent resilience highlights the importance of a thorough cybersecurity strategy that encompasses technology, policy, and education [17]. This serves as a vital lesson for organisations looking to bolster their defences against increasingly advanced cyberattacks [2].

2. Background and Context

T&S is a small business that found itself at the centre of a ransomware storm, exposing fundamental weaknesses in its cybersecurity framework. Like many other small businesses, T&S operated under the illusion that sophisticated cyberattacks were unlikely to target it. This false sense of security is typical among small businesses, which generally invest less in cybersecurity than their larger counterparts. However, hackers are more astute and view small businesses as attractive targets, as they possess valuable digital assets and often have inadequate security practices. The attackers infiltrated T&S's systems, encrypted critical data, and demanded a ransom for the release of the files.

The data stored by T&S was vital for carrying out its daily operations. This included sensitive client records, operational documents, and financial data, all crucial for ensuring business continuity. The ransomware attack disabled access to these resources and paralysed the company's operations. T&S's short-term survival and long-term reputation were at risk. Without immediate access to the necessary data, there was no established incident response plan. The course of action the company was considering included complex and challenging options: attempting to decrypt the files, paying the ransom, or manually recreating the company's data from scratch.

T&S's vulnerability stems from several common factors associated with small businesses. These include a lack of strong security measures, insufficient data backups, and inadequate training for employees on cyber risks. Furthermore, there were no automatic software updates or patches in place, leaving security gaps whenever a vulnerability was identified that could be exploited by an attacker. Additionally, the use of personal devices and unauthorised applications on the business network undermined the company's cyber defences. Such challenges are typical for organisations with limited capabilities and knowledge in cyber risk management.

T&S is simply another casualty of the rising cyber issues we face, particularly those affecting small businesses. Therefore, the most prudent course of action is to implement a comprehensive plan to safeguard against such attacks. For T&S, the incident served as a wake-up call, leading to a series of transformative changes in how it managed data security and operational resilience. This lays the groundwork for what the company ultimately pursued throughout its organisation to enhance its protection against future cyberattacks.

3. The Ransomware Attack

It began on what seemed to be a typical day in the office for T&S until a ransomware attack turned it into a full-scale disaster. The attackers infiltrated the company network through an unknown vulnerability, encrypting vital data and rendering core operational files inaccessible. The ransomware was detected after employees found themselves unable to open files and applications. Any attempts to access the file system triggered a chilling message from the attackers. A ransom demand was issued, accompanied by a warning that further attempts to unlock the files would jeopardise them, resulting in irreversible data loss. The attackers also issued an additional threat, suggesting that sensitive company data could be publicly disclosed or sold to competitors if their demands were not swiftly met.

The attack had an incapacitating effect immediately. Operations came to a standstill when T&S lost access to its primary databases, which contained everything from client records to financial data to project documentation. Internal communication deteriorated, and business continuity faced a significant threat. The company's executives were faced with a critical decision: either pay the ransom in hopes of regaining access to the encrypted data or explore alternative options, risking the permanent loss of some information. Once again,

without a proper incident response plan, the situation was evidently worsening over time.

The attacker exploited significant vulnerabilities in T&S's IT infrastructure. Chief among these was the absence of regular security updates and patches, which left exploitable gaps in the system. The company lacked a reliable data backup system and, therefore, had no means to quickly restore operations without paying the ransom. The absence of sufficient network monitoring allowed the attackers to carry out their activities until the encryption process was completed without detection. Inadequate access control policies, such as permitting external applications and personal devices on the enterprise network, heightened the risk by opening multiple attack vectors to the ransomware.

This attack made it clear that T&S needed to reconfigure its cybersecurity framework completely. The breaches exploited weaknesses in security frameworks, inadequate data handling policies, insufficient user training efforts, and the peril of operating solely under a vulnerability: surrender your information or face cyber-ballot blackmail. This underscored the necessity for a multi-faceted approach to digital security. The experience served as a wake-up call, prompting T&S to rethink its entire operational structure to protect itself from threats of this nature in the future. T&S needed to focus not only on addressing the immediate crisis but also on laying the groundwork for organisational resilience against the evolving landscape of ransomware attacks. The company's survival depended on implementing long-term preventive strategies.

4. Initial Response and Crisis Management

The moment T&S realised it was under attack, the company plunged into an immediate and overwhelming crisis. Initial steps involved coming to terms with the breach, such as assessing the extent of the damage and attempting to regain access to its encrypted data. IT staff contemplated unlocking the compromised file system with available tools and expertise. However, manual recovery proved futile. The attackers had employed advanced encryption algorithms that could not be broken without the decryption key. The company's executives then faced a difficult decision: to pay the ransom or not. The hackers had made it clear that if their demands were not met, the data would be lost forever or made public. However, even paying the ransom offered no guarantee that the attackers would restore access. Furthermore, that payment risked encouraging future attacks and exacerbating the wider ransomware epidemic.

T&S convened emergency meetings with stakeholders to discuss potential actions. The urgency was palpable. The company's operations were entirely broken, with key business processes effectively halted. Client services, internal communications, and project timelines were all severely disrupted. The company lacked a robust incident response plan, complicating efforts to organise under pressure. With no realistic path for a rapid recovery and growing concerns over reputational and financial repercussions from prolonged downtime, T&S began considering various options.

One alternative involved rebuilding the data from scratch, but this method presented significant challenges. Many of the company's records were irreplaceable or would necessitate weeks of painstaking effort to recreate. Without dependable backups, however, T&S found itself in a difficult position where neither recovery nor ongoing operations were immediately feasible. Moreover, time and company politics exacerbated the issue: the stakes associated with various solutions were well-known to all involved and were growing increasingly desperate by the minute.

Communication posed another critical challenge. Without access to essential systems, internal coordination became fragmented, and misunderstandings permeated an already chaotic environment. The absence of a centralised protocol for cyber crises left different departments to improvise their responses, often duplicating efforts or competing with one another. Meanwhile, external stakeholders—clients, partners, and others—began requesting explanations and assurances, which only intensified the pressure on the company's leaders.

Despite these challenges, T&S acted transparently and collaboratively. The group engaged cybersecurity experts to advise on risk mitigation and best practices for responding to a ransomware event. All the experts who consulted the company advised against paying the ransom and emphasised the importance of preserving the company's integrity and capacity to withstand future attacks. Simultaneously, T&S began implementing its damage-control strategies, including notifying relevant stakeholders of the breach, documenting the incident for forensic analysis, and initiating a plan to radically overhaul its cybersecurity framework.

Considering the costs of losing vital data, T&S decided to restore the missing information. To expedite this process, they hired data entry operators on an hourly basis. For the next four months, these operators diligently reconstructed the records from various sources. Although it was a resource-intensive undertaking, this approach enabled T&S to gradually regain stability, allowing it to recover the most essential data necessary for ongoing operations.

Although the attack revealed the company's lack of preparedness, it also ignited a collective effort to tackle the crisis. It served as a reminder of the vital need for a well-structured incident response plan, reliable data backups, and regular employee cybersecurity training to minimise the impact of cyberattacks. This established the foundation of T&S's long-term strategy to prevent ransomware attacks in the future.

5. Long-term Countermeasures and Preventative Steps

T&S realised that its cybersecurity framework required an

overhaul to prevent falling victim to another ransomware attack. The first strategic step was to partner with STC, a highly reputable cloud service provider offering numerous robust security and backup services. Drawing on STC's security expertise, T&S designed and implemented a strong infrastructure to safeguard sensitive data and enable rapid recovery in the event of a future cyber threat. These cloud-based solutions provided real-time monitoring, threat detection, and automated backups that minimised the likelihood of extended downtime.

T&S created a detailed draft of the data backup and recovery plan. The SOP (Standard Operating Procedure) outlines several written procedures on how to perform timely data backups, restore procedures, and maintain the integrity of stored data. This approach aimed to minimise data loss and ensure that the company could allocate time to restore operations in the event of further attacks. The SOP was part of the broader IT governance of the company and underwent periodic audits and updates to ensure alignment with emerging cybersecurity threats and best practices.

Additionally, T&S implemented the Oodu ERP system, which facilitates user-friendly data management and innovative company services. This ERP solution centralised control over critical business functions such as data storage, workflow automation, and access management. Oodu ERP introduced role-based access controls that restricted data visibility, ensuring that only individuals whose job descriptions required access to sensitive information could do so. The system also offered integrated security features, including encryption and activity logging, assisting the company in monitoring and addressing potential risks.

Employee education became a crucial element of the company's long-term strategy. To address these threats, T&S started holding regular training sessions to inform employees about phishing scams, tactics employed by potential ransomware, and practising safe online behaviours. The organisation aimed to reduce human error, a frequent contributor to successful cyber attacks, by fostering a culture of cybersecurity awareness.

Collectively, these measures have reshaped T&S's cybersecurity posture. Cloud-based services, RAID (redundant array of independent disks) technology, and robotic data management tools created a strong fortress against the evolving threats of cybercrime. The course of the attack illustrated not only the need for proactive initiatives but also the necessity of comprehensively addressing organisational resilience. These strategic initiatives enabled T&S to recover from the crisis and thrive in an increasingly digital and interconnected business landscape.

6. Cybersecurity Framework Implementation

T&S incorporated the NIST Cybersecurity Framework to enhance its defences against future ransomware attacks. Developed by the National Institute of Standards and Technology (NIST), this framework acted as a reference for establishing a comprehensive cybersecurity strategy. Recognising that the solution required a customised approach, T&S created a ransomware profile specifically tailored to its unique risk profile and business requirements.

The framework is organised around five key functions: Identify, protect, detect, respond, and recover. These functions can be further divided into categories and subcategories to guide the organisation's cybersecurity efforts. For instance, within the Identify function, T&S enhanced its asset management and risk assessment practices to gain a better understanding of its critical data and infrastructure vulnerabilities. The Protect function concentrates on access control, advanced antivirus solutions, and patch management. For the Detect function, T&S broadened its monitoring capabilities to identify abnormal or unauthorised activities across its network swiftly.

Organisational reforms were also necessary to fully implement the framework. T&S established standard operating procedures (SOPs) for regularly testing backup and recovery mechanisms to ensure data could be swiftly restored in the event of future attacks. The company restricted access to key systems, prohibited unauthorised applications, and did not permit personal devices on its network. An incident response plan was also instituted, adhering to industry best practices, such as conducting simulated responses and storing multiple backup copies of data.

Employee education became a cornerstone of this effort. T&S has expanded cybersecurity awareness across the organisation, training employees to be vigilant for potential threats, avoid dubious links, and adhere to security protocols. These initiatives were aimed at combating ransomware threats and educating employees on minimising risks and threats in real time.

Through these extensive measures, T&S bolstered its cybersecurity posture and substantially mitigated the risk of future ransomware attacks, establishing a foundation for ongoing digital resilience.

7. Preventative Strategies and Best Practices

T&S adopted numerous preventive measures and enhancements to its cybersecurity posture to guard against future ransomware attacks. Central to these initiatives was the consistent application of the latest security updates across all systems. By promptly patching known vulnerabilities, T&S mitigated the risk of exploitation by cybercriminals. The company also implemented robust antivirus software and configured its systems to block contact with known malicious sites. This combination of preventative strategies effectively reduced the attack surface available to cybercriminals.

Access control also became a crucial component of T&S's strategy. The entity restricted system access to those with the appropriate permissions and ensured users logged into standard accounts rather than elevated privileged ones, mitigating the risk of damage from a compromised account. The company's network was also secured to prevent unauthorised access through personal devices and applications.

To enhance the company's cyber resilience, T&S increased employee training. Recognising that human error was a significant contributor to successful cyberattacks, the company introduced new awareness training covering the full spectrum of cybersecurity threats. Staff were trained to identify phishing attempts, respond to suspicious links or files, and adhere to security protocols. Through ongoing drills and simulations, the staff was better equipped to respond appropriately to potential incidents.

T&S implemented a comprehensive backup and restore plan, enhancing preparedness. Multiple, regularly tested backups were created to facilitate rapid data restoration in the event of an attack. To ensure redundancy and fast recovery options, T&S stored these backups both on-site and in secure, off-site locations within a trusted service provider's cloud environment.

These preventive practices, combined with a commitment to continual learning and system fortification, refined the T&S infrastructure to resist a multitude of threats. The company's management acknowledged that no system can be entirely impervious to cyber threats, but that a proactive, multi-layered strategy can significantly reduce the risk and impact of future ransomware incidents. This emphasis on cyber hygiene demonstrated T&S's determination to protect its operations and stakeholders from emerging threats.

8. Results and Impact

It marked the dawn of a new era for T&S, a transformation ignited by the implementation of comprehensive cybersecurity protocols. The company's system maintenance, access control, and employee training have significantly enhanced system reliability. Formerly vulnerable systems, often due to outdated software and insufficient monitoring, now operate with greater stability and reduced risk. Thanks to proactive patch management and advanced security tools, malware has failed to infiltrate the network.

Significant advancements in data security also took place. T&S effectively minimised the risk of unauthorised access by implementing strong access controls, restricting administrative privileges, and applying multi-layered protection, which includes antivirus software and network security measures. Data backups were secured, routinely tested, and stored redundantly across multiple platforms, instilling confidence that critical business data could be swiftly restored in the event of an attack.

Another glaring strength was operational resilience. Rather than merely reacting to potential threats, this organisation maintained a continual state of readiness. This approach was bolstered by awareness programmes that educated staff to assume the role of the first line of defence, resulting in a decrease in incidents of human error. The nature of incident simulations, coupled with a clearly defined incident response plan, also enabled the organisation to swiftly contain and mitigate the impact of a breach when it occurred.

Collectively, these changes enhanced T&S's resilience to ransomware and other cyber threats, establishing the foundation for a sustainable security strategy. Clients, stakeholders, and others trusted the company more to protect sensitive information and ensure business continuity. The crisis not only strengthened T&S's resilience but also positioned the company as an exemplar of cybersecurity best practices within its industry. Currently, the company's focus is on incremental improvement and adaptation to the rapidly evolving cyber threat landscape.

9. Lessons Learned

The ransomware attack on T&S uncovered three vital lessons about adequately preparing for cybersecurity incidents. The primary lesson is that data backup and regular testing of the recovery process are essential. Importantly, T&S lacked dependable backups, compelling it to make the difficult decision to rebuild its data from scratch, a lengthy and expensive undertaking. This underscored the significance of redundancy and proactive strategies for disaster recovery.

A second key lesson was the significance of employee education and awareness in preventing cyberattacks. T&S discovered that many security breaches exploit human error, such as clicking on phishing links or mishandling sensitive information. Organisations should prioritise cybersecurity awareness from day one, conducting regular training sessions to ensure employees are equipped to identify and mitigate threats. This precautionary measure has become one of the greatest safeguards against future attacks.

Access control and system hardening were also crucial lessons from the attack. Strict access permissions and regular software updates minimise vulnerabilities that hackers could exploit. This significantly strengthened T&S's ongoing defence against a constantly evolving onslaught of threats, especially given their continual efforts to limit unauthorised access and ensure frequent software patching.

Other organisations, particularly small and medium-sized businesses, can adopt these lessons to strengthen their cybersecurity framework. With virtually no security infrastructure, small businesses can become appealing targets. However, by implementing robust security measures, such as antivirus software, regular updates, access controls, and backup solutions, these businesses can significantly reduce their risk of an attack. Finally, preparing and practising incident response plans can enable a rapid and efficient response to any security incident, resulting in minimal downtime and loss of revenue.

Ultimately, the experience imparted a lesson in cybersecu-

rity to T&S, viewed both as an ongoing process and as a balancing act involving risk, decision-making, and adaptation. No organisation is free from cyber threats. Nevertheless, a proactive, multi-layered defence strategy can mitigate an attack. This approach serves as a model for other businesses to emulate, emphasising the notion that resilience is rooted in preparation and continuous vigilance.

10. Conclusion

The T&S data breach reminds us of the importance of a proactive and comprehensive cybersecurity strategy. In the modern digital landscape, where cyber threats constantly evolve, organisations must adopt a proactive stance. Cybersecurity is not merely a technological challenge; it should be an integral part of the enterprise that melds technology with organisational policy and ongoing education for long-term resilience.

Practices such as regular system updates, antivirus software, and secure access controls form the foundation of any cybersecurity strategy. However, these tools must be backed by organisational policies to ensure that best practices are adhered to across all functions. By establishing clear data access protocols for managing backups and incident response procedures, you create a framework within which employees and systems operate, designed to both guard against and respond to cyberattacks.

Cultivating a culture of cybersecurity within the business is essential. T&S's experience demonstrates that employee education is generally the first line of defence against threats such as phishing and social engineering. Ongoing training, simulations, and security exercises empower employees to identify and respond effectively to risks, significantly reducing the likelihood of human error affecting the enterprise's defences.

The T&S case also demonstrated that cyber resilience is not a lifetime achievement award but an active discipline requiring ongoing awareness and flexible readiness. Organisations must remain vigilant as new threats arise, continuously assess their security posture, and invest in upgrades to stay one step ahead of attackers. Every business can protect itself against the growing ransomware threat by combining the latest technical solutions with straightforward policies and a culture of preparedness.

T&S's experience should remind organisations everywhere that cybersecurity is not just an IT issue—it is an essential component of business continuity. A well-prepared organisation can minimise the impact of cyberattacks, safeguard vital data, and ensure that operations remain secure in an increasingly hostile digital environment.

Abbreviations

ERP	Enterprise Resource Planning
IT	Information Technology
NIST	National Institute of Standards and Technology
RAID	Redundant Array of Independent Disks
SME	Subject Matter Expert
SOP	Standard Operating Procedure
STC	Saudi Telecom Company
T&S	Tools and Solutions

Author Contributions

Partha Majumdar is the sole author. The author read and approved the final manuscript.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] Abawajy, J. H. (2014). User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 33(3), 237-248. https://doi.org/10.1080/0144929X.2012.708787

[2] Alharthi, S., Cerotti, D., & Rajarajan, M. (2020). Cyber security risk assessment for SMEs: A novel approach. International Journal of Critical Infrastructure Protection, 29, 100339.

[3] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78, 544-546. https://doi.org/10.1016/j.future.2017.07.060

[4] Duan, Y., Faker, P., Fouchereau, F., & Thomas, H. (2012). Overcoming ERP project obstacles: The role of integrative risk management. Industrial Management & Data Systems, 112(4), 484-500.

[5] Egele, M., Scholte, T., Kirda, E., & Kruegel, C. (2017). A survey on automated dynamic malware-analysis techniques and tools. ACM Computing Surveys (CSUR), 44(2), 6-42. https://doi.org/10.1145/2089125.2089126

[6] Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. Heliyon, 3(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

[7] Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1), 5. https://doi.org/10.1186/1869-0238-4-5

[8] Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). Cutting the Gordian knot: A look under the hood of ransomware attacks. International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, 3-24. Springer. https://doi.org/10.1007/978-3-319-20550-2_1

[9] National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). NIST.

[10] Nguyen, K., Nwokedi, S., & Gajbhiye, A. (2017). Mitigating cybersecurity risks for small businesses: Recommendations and strategies. Journal of Small Business Strategy, 27(2), 71-84.

[11] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165-176. https://doi.org/10.1016/j.cose.2013.12.003

[12] Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. International Management Review, 13(1), 10-21.

[13] Scaife, N., Carter, H., Traynor, P., & Butler, K. R. (2016). Cryptolock (and drop it): Stopping ransomware attacks on user data. 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS), 303-312. https://doi.org/10.1109/ICDCS.2016.46

[14] Shinde, P., & Patil, S. (2020). A review on ransomware attack: Evolution, defence and challenges. International Journal of Computer Sciences and Engineering, 8(4), 132-138.

[15] Small Business Trends. (2019). Ransomware is most common malware threat for small business. Journal of Small Business Cybersecurity Research, 3(2), 10-18.

[16] Verizon. (2021). 2021 Data Breach Investigations Report. Verizon Enterprise Solutions.

[17] von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

[18] Wangen, G., Hallstensen, C., & Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness. International Journal of Information Security, 17(6), 681-699. https://doi.org/10.1007/s10207-017-0382-0