Cyber Threats to UK Institutions: Case Studies and Countermeasures

5653630

December 6, 2024

Contents

1 Executive Summary

This report addresses the increase in cyber threats against institutions in the British Isles, focusing on recent major attacks, such as those against universities and the British Library. The background sets the stage for the current cyber related issues universities have been facing. It details the attacks against Wolverhampton and Cambridge, underlining the operational disruption, reputational damage, and research setbacks. The analysis section introduces the ransomware group Rhysida, mentioning how they managed to steal data from the British Library and what likely methods were used. The attack graph illustrates the stages of the breach, mapped to the cyber kill chain. The report concludes by suggesting recommendations to mitigate future attacks against the British Library, such as implementing robust MFA to address credential theft and staff training to reduce phishing susceptibility.

Brilliant

2 Background

The rapid digitisation of university operations makes academic institutions increasingly lucrative targets for cyber criminals. With vast databases of sensitive information, universities have experienced a surge in cyber attacks. This trend has intensified since COVID-19, with universities increasingly incorporating remote learning into their programs with many institutions now offering online lectures, virtual lab sessions and hybrid degree programs to accommodate diverse learning needs. These advancements not only catered to students but also attracted malicious threat actors seeking to exploit vulnerabilities in complex and decentralised IT infrastructures, due to the growing number of endpoints. Attackers exploited multiple strategies to attack multiple vectors, including ransomware, phishing, and DDoS, (Department for Science, Innovation and Technology, 2023). As a result, 85% of higher education organisations have reported experiencing significant cyber security incidents (Thompson, 2024).

Among the universities impacted by cyber threats is Cambridge, which experienced a significant attack on February 19, 2024, carried out by the hacktivist group Anonymous Sudan. This group revolves around promoting political causes, particularly opposing the UK's support for Israel amid the ongoing Gaza conflict (Krebs, 2024), orchestrating a denial of service attack (DDoS) on the university, with varsity reporting that the attack affected access to student IT services such as CamSIS and Moodle (Coker, 2024).

This caused academic disruptions for students, as they were unable to access pre-recorded online lectures, communicate with their professors for critical matters, or submit assignments electronically via Moodle, resulting in heightened stress. The attack also disrupted academic activities, causing delays in ongoing research projects, including time-sensitive experiments funded by industry partners and other high-stakes researchers (Coker, 2024). These delays risk financial penalties from funding bodies and compromise the university's reputation as a reliable research partner, causing uncertainty and hesitation to work with the university for future projects and research. This is because studies suggest that cyber attacks erode credibility, making it harder for universities to secure funding and partnerships (Andersen and MoldStud Research Team, 2024) . Chronic underfunding exacerbates this issue, leaves institutions significantly behind private sector standards, creating inefficiencies and vulnerabilities undermining confidence among funding bodies and research collaborators (Rowsell, 2024).

These cyber threats are not limited to elite institutions; universities across the spectrum, including Wolverhampton, have also experienced significant impacts from cyberattacks, with one such incident in February attributed to the same group, Anonymous Sudan, previously mentioned in connection with the Cambridge attack. The group disrupted IT systems across all campuses, forcing staff and students to work remotely and obstructing services and lectures. These situations create much discord, which often causes students to express their frustration on social media platforms such as TikTok and Instagram shorts, causing the incident to go viral, amplifying negative perceptions and deterring prospective students. This can diminish public trust in the institution, potentially affecting enrolment and stakeholder confidence, reducing university income.

The problem was so severe that people speculated the issues could last up to six months (Lawson, 2024), creating a sense of prolonged uncertainty. This uncertainty affected both students and staff, who struggled to adapt to the disruption. Missed deadlines, stalled academic progress, and unreliable communication channels added to the stress, compounding the human impact of the cyber attack.

If these issues persist and universities fail to reinforce their defences, the consequences extending beyond academia, particularly in sectors like the NHS, which rely heavily on university-led research. For example, the collaboration between Oxford University and AstraZeneca led to the development of the first COVID-19 vaccine that went on to save millions of lives globally. Such challenges would also pose significant economic risks, as the UK's reputation as a global leader in education and research could deteriorate. This would make the country less attractive to international students, causing a shrink in the UK's economy, given that international students contributed approximately £41.9 billion to the UK economy in the 2021/22 academic year alone (Universities UK, 2023).

3 Analysis

3.1 The Threat Actor: Rhysida

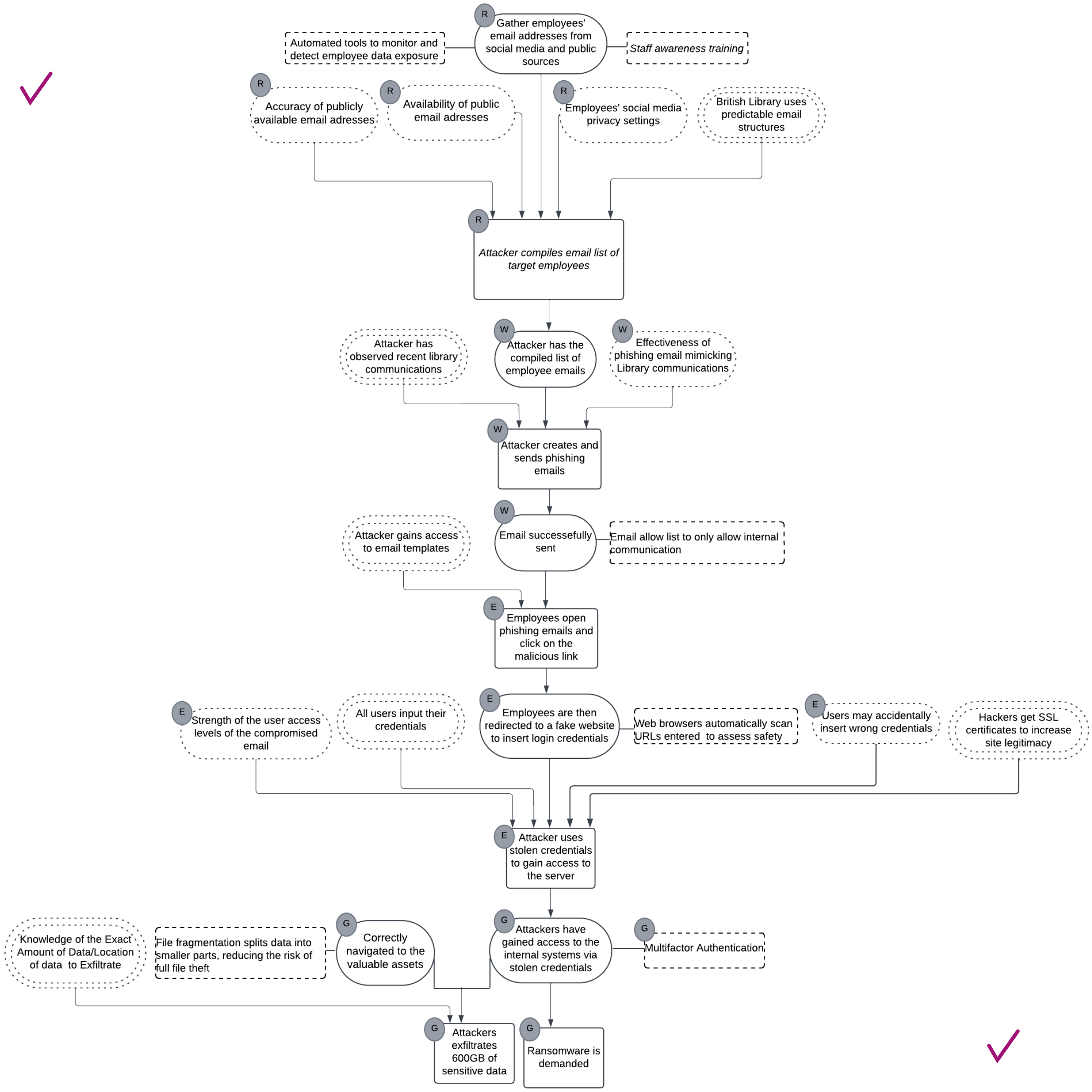
Rhysida is a ransomware group with a history of targeting high-profile institutions and organisations, particularly those maintaining large volumes of sensitive or valuable data. They emerged as a ransomware-as-a-service (RaaS) group, leveraging a profit-sharing model where tools and infrastructure are leased to affiliates (Cyber et al. Agency, 2023).

Their attack strategy typically begins with reconnaissance, collecting information about the organisation's internal systems, employee details, and network configurations. This intelligence enables them to craft targeted phishing emails, which are their most successful entry point. Research indicates that 20% of staff click on the malicious link, but an additional 13.4% proceed to give away their credentials, opening a gateway for further cyber attacks (Gundersen, n.d).

Once they gain access, Rhysida rapidly establishes persistence within the network, escalating privileges wherever possible. A key factor of their strategy involves exploiting vulnerabilities such as lack of Multi-Factor Authentication (MFA) or unmonitored remote access points. Rhysida's end goals are twofold: encrypting data to disrupt operations and exfiltrating it to create leverage for ransom demands. In many cases, they have threatened to release sensitive data online if their ransom is not paid, intensifying pressure on the victim (Cyber et al. Agency, 2023). Rhysida's attack on the British Library followed this pattern, amplifying the consequences of the attack and the pressure to meet their demands.

3.2 Attack Graph (Reconstructed Mapping)

✓


R
Gather employees' email addresses from social media and public sources
Automated tools to monitor and detect employee data exposure
Staff awareness training
R
Accuracy of publicly available email adresses
R
Availability of public email adresses
R
Employees' social media privacy settings
British Library uses predictable email structures
R
Attacker compiles email list of target employees
Attacker has observed recent library communications
W
Attacker has the compiled list of employee emails
W
Effectiveness of phishing email mimicking Library communications
W
Attacker creates and sends phishing emails
Attacker gains access to email templates
W
Email successefully sent
Email allow list to only allow internal communication
E
Employees open phishing emails and click on the malicious link
E
Strength of the user access levels of the compromised email
All users input their credentials
E
Employees are then redirected to a fake website to insert login credentials
Web browsers automatically scan URLs entered to assess safety
E
Users may accidentally insert wrong credentials
Hackers get SSL certificates to increase site legitimacy
E
Attacker uses stolen credentials to gain access to the server
Knowledge of the Exact Amount of Data/Location of data to Exfiltrate
File fragmentation splits data into smaller parts, reducing the risk of full file theft
G
Correctly navigated to the valuable assets
G
Attackers have gained access to the internal systems via stolen credentials
G
Multifactor Authentication
G
Attackers exfiltrates 600GB of sensitive data
G
Ransomware is demanded

✓

Figure 1: Attack Graph

3.3 Reconnaissance (R)

This phase focused on gathering intelligence about the Library's infrastructure and personnel to identify exploitable entry points. The initial stage involved collecting employees' email addresses from social media and public sources, particularly from individuals with low privacy settings. Once these addresses were obtained, attackers likely attempted to predict additional email addresses, assuming the British Library used a standardised email structure, before compiling a comprehensive list of target employees in order to maximise the chances of success in the targeted phishing campaign. Even though technical weaknesses played a role, human vulnerabilities of oversharing personal information online was the critical enabler during this phase. It is common practice for ransomware groups to collect publicly available information about staff from websites and professional directories, aligning with Rhysida's likely use of OSINT to enhance their targeting strategy (Flashpoint, 2023).

This can be seen in Figure 1, where Rhysida used OSINT techniques to gather not only employees email address, but also email patterns, job roles, and organisational hierarchies. This lack of privacy, combined with the attackers' ability to exploit predictable communication structures, allowed Rhysida to map potential entry points and move to weaponisation.

3.4 Weaponization (W)

This phase, as depicted in Figure 1, began with Rhysida compiling a list of targeted employee email addresses using publicly available sources. Data gathered during the reconnaissance phase enabled the attackers to craft targeted phishing emails. These emails were designed to closely resemble legitimate British Library communications by exploiting common email patterns and mimicking the Library's communication style. While the exact emails observed by Rhysida are unknown, phishing campaigns are commonly crafted by threat actors to deceive recipients into clicking on malicious links or opening infected attachments (Flashpoint, 2023). For instance, a phishing email with the subject line ”Online employee survey: What would you improve about working at the company?” sent by a fake HR department achieved a click conversion rate of 18% (Kaspersky, 2022).

Rhysida likely used open-source intelligence (OSINT) techniques to gather information about employee roles, email formats, and recent library communications, further refining their phishing emails to make them appear more authentic. Phishing attacks often target organisations by gathering publicly available details on previous data breaches or other discoverable information (Kaspersky, 2023).

3.5 Execution Phase (E)

This phase began when victims clicked on the phishing link sent by Rhysida. Studies show that the Education sector, which includes organisations like the British Library, has a phishing email click rate of 27.6%, making it one of the most targeted and vulnerable sectors (Smith, 2024). Once the victims clicked the link, as shown in Figure 1, they were redirected to a fake login portal closely mimicking the Library's official website. These phishing sites are specifically designed to look legitimate, exploiting visual similarities to deceive users into entering their login credentials without suspicion (Kaspersky, 2023).

Once directed to the fake page, users then proceeded to enter their details, with studies showing how 4% of users proceed to enter their login credentials on phishing websites, highlighting the effectiveness of these attacks despite low overall conversion rates (Luke Irwin, 2023) Rhysida likely improved this rate by using SSL certificates to enhance site legitimacy. Armed with these compromised credentials, Rhysida gained unauthorised access to the Library's internal systems. Using the credentials obtained from employees who entered their details, Rhysida likely escalated their access within the Library's network. This assumption is based on the typical modus operandi of ransomware groups, which often target users with higher-level permissions through further phishing or credential misuse tactics.

This escalation was further enabled by the lack of Multi-Factor Authentication (MFA) on the terminal server, a critical vulnerability in the Library's network. Initially installed in February 2020 to support remote work and external partnerships, this server was intended to ease access but ultimately created an exploitable entry point. Rhysida's ability to exploit these vulnerabilities highlights their deliberate and methodical approach. This ongoing activity, which began on October 25, suggests that the attackers were persistent in gaining and retaining access until the first complete detection on October 28, when a Technology Team member noticed network inaccessibility (British Library, 2024).

3.6 Goal Phase (G)

In the Goal phase, Rhysida achieved its primary objectives of data exfiltration and ransomware deployment, as illustrated in Figure 1. After escalating their access within the Library's network, the attackers exfiltrated 600 GB of sensitive data, including staff, user, and Library records from the Finance, Technology, and People teams. This data was targeted based on a deliberate selection process, likely informed by their knowledge of the exact location and value of the data to exfiltrate, as depicted in the attack graph. By focusing on high-impact assets, Rhysida maximised the operational and reputational damage to the Library. Rhysida also scanned files for sensitive keywords, prioritising both corporate and personal data to increase the leverage of their ransom demands.

Among the compromised data, 22 databases containing partial customer information used for marketing were forcibly backed up and removed, though more sensitive customer information was reportedly not included (British Library, 2024). The attackers demanded a ransom of £600,000, but the Library's refusal to pay led to further retaliation, with hackers offering to sell personal data on the dark web for 20 bitcoins (£596,459) (BBC, 2023).

The financial and operational repercussions of the attack were severe. To rebuild its digital services and improve security, the Library will need to allocate approximately £6 million to £7 million, representing 40% of its £16.4 million in unallocated reserves. This financial burden is nearly ten times the ransom amount initially demanded by the attackers. The funds will be directed towards addressing the crippling impact of the attack, which disrupted most of the Library's critical services and restricted access for researchers and other patrons (Uddin Thomas, 2024).

4 Recommendation

4.1 Multi-Factor Authentication (MFA)

The lack of MFA was a key vulnerability that allowed Rhysida to exploit the Library's network. Although MFA was in place for cloud applications, it was absent on critical internal systems like the terminal server, which was intended for trusted remote access. This meant that once the hackers entered the British Library terminal, they did not have to go through any secondary verification process, allowing them to compromise credentials without being detected. Implementing MFA would have been crucial at this stage, as it would not only have prevented unauthorised access but also alerted the Library's SOC analyst team, who could then provide an appropriate response. Studies back this as they show that enabling MFA blocks over 99.9% of account compromise attacks (Microsoft, 2019). Additionally, MFA prevents 96% of bulk phishing attacks, a tactic heavily relied upon by ransomware groups like Rhysida (Google, 2019). By requiring a second authentication factor, such as a biometric scan or one-time code, MFA renders stolen credentials useless, preventing lateral movement and escalation within the network.

4.2 Staff Training

Regular training sessions, complemented by phishing simulations, can help employees identify malicious emails, reducing the likelihood of falling victim to similar attacks in the future. Data indicates that organisations without any training or phishing simulations often see 30% or more of their users likely to fall for phishing emails. However, after implementing regular training and frequent phishing simulations, this rate can drop to around 5% within a year (KnowBe4, 2023).

This highlights the effectiveness of tailored interventions in mitigating one of the most common entry points for ransomware groups. Training staff on common forms of social engineering attacks, such as phishing, through immersive labs enables organisations to significantly reduce risk. This approach also cultivates a cyber security conscious workplace, positioning employees as a vital defence against future threats. Had such training been implemented at the British Library, staff would have been better equipped to identify and report suspicious emails, likely preventing Rhysida's attack entirely.

4.3 Strengthen Network Monitoring

The absence of robust network segmentation allowed Rhysida to escalate its attack after gaining initial access. Implementing network segmentation can significantly limit the lateral movement of attackers by dividing the network into smaller, isolated segments. In the context of the British Library, segmentation could have isolated the department's individual databases, such as the finance and research databases, from general user access. This is to ensure that even if one database gets compromised, access to the other one remains restricted due to them being on different networks.

This isolation would have forced Rhysida to overcome additional barriers, increasing the likelihood of detection and reducing the overall impact of the breach as segmentation improves monitoring capabilities, making it easier to detect suspicious activities and respond effectively to potential breaches (Wickramasinghe, 2023) . The British Library should have implemented this by prioritising high-value assets for immediate isolation, which are often the primary targets in ransomware attacks, such as sensitive staff records and financial databases.

Glossary

Ransomware: A type of malicious software designed to block access to a computer system or data until a ransom is paid.

Phishing: A social engineering attack that tricks individuals into providing sensitive information, such as usernames, passwords, or financial details, by impersonating a trusted entity.

Reconnaissance: The initial phase of a cyber-attack, during which attackers gather information about the target to identify vulnerabilities.

Weaponisation: The phase in a cyber-attack where attackers create tools, such as malware or phishing emails, to exploit the target's vulnerabilities.

Execution: The phase where attackers deploy their tools or methods to gain access to the target system.

Data Exfiltration: The unauthorised transfer of data from a system, often conducted during or after a cyber-attack.

Multi-Factor Authentication (MFA): A security mechanism that requires users to provide two or more verification factors to access a system, making it harder for attackers to gain access using stolen credentials.

Open-Source Intelligence (OSINT): Information gathered from publicly available sources, such as social media, websites, and directories, for use in reconnaissance.

Social Engineering: A technique used by attackers to manipulate individuals into revealing confidential information or performing actions that compromise security.

Credential Theft: The act of stealing login credentials, such as usernames and passwords, to gain unauthorised access to systems.

Terminal Server: A server that provides remote access to users, often used for administrative or technical purposes.

Denial-of-Service (DoS) Attack: An attack that overwhelms a system, server, or network with traffic, rendering it inaccessible.

References

- Department for Science, Innovation and Technology, 2023. *Cyber Security Breaches Survey 2023: Education Institutions Annex.* Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023-education-institutions-annex (Accessed: 15 November 2024).

- Thompson, R., (2024). *Further and higher education institutions suffer weekly cyberattacks.* [online] NWCRC. Available at: https://www.nwcrc.co.uk/post/further-and-higher-education-institutions-suffer-weekly-cyber-attacks#:~:text=3%20min-,Further%20and%20higher%20education%20institutions%20suffer%20weekly%20cyber%20attacks,in%20the%20past%20few%20years. [Accessed: 18 November 2024].

- Krebs, B. (2024). *Sudanese brothers arrested in AnonSudan takedown.* Krebs on Security, 17 October. Available at: https://krebsonsecurity.com/2024/10/sudanese-brothers-arrested-in-anonsudan-takedown/ [Accessed: 18 October 2024].

- Coker, J. (2024). *Universities Recovering from DDoS Attack.* Infosecurity Magazine. Available at: https://www.infosecurity-magazine.com/news/universities-recovering-ddos-attack/ [Accessed: 28 November 2024].

- Andersen, G. MoldStud Research Team, 2024. *The Effects of Cyber Security Breaches on University Reputations and Admissions.* MoldStud. Published 7 February. Available at: https://moldstud.com/articles/p-the-effects-of-cyber-security-breaches-on-university-reputations-and-admissions [Accessed: 28 November 2024].

- Rowsell, J., (2024). *Funding crisis 'puts universities at higher risk of cyberattacks'.* [online] Times Higher Education. Available at: https://www.timeshighereducation.com/news/funding-crisis-puts-universities-higher-risk-cyberattacks [Accessed: 29 November 2024].

- Lawson, E. (2024). *University of Wolverhampton disrupted as IT systems go down.* BBC News, 21 February. Available at: https://www.bbc.co.uk/news/articles/cgrlljz2pv5o [Accessed: 18 October 2024].

- Universities UK, (2023). *International students boost UK economy.* Available at: https://www.universitiesuk.ac.uk/latest/news/international-students-boost-uk-economy (Accessed: 25 November 2023).

- Cybersecurity and Infrastructure Security Agency (CISA), (2023). *Joint CSA #StopRansomware: Rhysida.* [online] Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a [Accessed: 17 November 2024].

- Gundersen, G.M. (n.d). *1 in 5 employees click on phishing email links.* CyberPilot Blog. Available at: https://www.cyberpilot.io/cyberpilot-blog/does-phishing-training-work-yes-heres-proof#:~:text=1%20in%205%20employees%20click%20on%20phishing%20email%20links&text=The%20results%20showed%20that%20a,the%20employees%20submitted%20their%20credentials (Accessed: 4 December 2024).

- Flashpoint. (2023). *The Anatomy of a Ransomware Attack.* Available at: https://flashpoint.io/blog/the-anatomy-of-a-ransomware-attack [Accessed: 29 November 2024].

- Kaspersky. (2022). *Phishing emails that employees find most confusing.* [online] Available at: https://www.kaspersky.com/about/press-releases/best-bite-kaspersky-reveals-phishing-emails-that-employees-find-most-confusing [Accessed: 5 December 2024].

- Kaspersky. (2023). *Phishing attacks: defending your organisation.* [online] Available at: https://www.kaspersky.co.uk/resource-center/preemptive-safety/phishing-prevention-tips [Accessed: 1 December 2024].

- Smith, G., (2024). *Phishing statistics.* [online] StationX. Available at: https://www.stationx.net/phishing-statistics/ [Accessed: 1 December 2024].

- Luke Irwin. (2023). *50 phishing stats you should know.* [online] Available at: https://www.itgovernance.co.uk/blog/51-must-know-phishing-statistics-for-2023 [Accessed: 1 December 2024].
- British Library. (2024). *British Library Cyber Incident Review.* Available at: https://www.bl.uk/home/british-library-cyber-incident-review-8-march-2024.pdf [Accessed: 14 November 2024].
- BBC. (2023). *British Library hack: Customer data offered for sale on dark web.* Available at: https://www.bbc.co.uk/news/entertainment-arts-67544504 (Accessed: 2 December 2024).
- Uddin, R. and Thomas, D. (2024). *The British Library to drain 40% of reserves after cyber attack.* Financial Times. Available at: https://www.ft.com/content/4be5d468-0cc3-4881-a5fb-b5d0163de93e [Accessed: 14 November 2024].
- Microsoft Security Blog. (2019). *One simple action you can take to prevent 99.9 percent of attacks on your accounts.* Available at: https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/ [Accessed: 1 December 2024].
- arXiv.org. (2024). *How effective is multifactor authentication at deterring cyberattacks?* Available at: https://arxiv.org/pdf/2305.00945 [Accessed: 1 December 2024].
- KnowBe4. (2023). *Data confirms the value of security awareness training.* Available at: https://www.knowbe4.com/hubfs/Data-Confirms-Value-of-SAT-WP_EN-us.pdf [Accessed: 5 December 2024].
-
- Wickramasinghe, S. (2024). *What is Network Segmentation? A Complete Guide.* Available at: https://www.splunk.com/en_us/blog/learn/network-segmentation.html [Accessed: 5 December 2024].