LEGAL AND ADMINISTRATIVE STUDIES, www.jlas.upit.ro.
e-ISSN: 2344-6900, ISSN-L: 1583-0772
Supplement 2025, pp. 794-805

THE THREAT OF CYBERATTACKS IN BUSINESS

Irina BENIA [1]
ORCID ^{ID}*:* https://orcid.org/0009-0005-3783-7255
E-mail: irinabenia1984@gmail.com
Tamara Sajaia[2]
ORCID ^{ID}*:* https://orcid.org/0009-0006-7851-3422
E-mail: tamirisaj@gmail.com
Afiliation: [1,2] Faculty of Law, Business, Humanities and Social Sciences X
Tbilisi Humanitarian Teaching University

Abstract: *This article examines the exposure of private businesses, particularly small and medium-sized enterprises (SMEs) to cyberattacks and the organizational measures that mitigate risk. A cross-sector survey of Georgian SMEs was conducted to assess awareness of cyber hygiene and the adoption of preventive controls during ongoing digital transformation. Results indicate strong recognition of the importance of cyber hygiene (100%) but limited competence in the field (66.7% report insufficient expertise) and low incident-reporting intent among employees. Managers (83.3%) view training as a decisive factor, yet two-thirds (66.7%) lack dedicated cybersecurity officers. Situating these findings within Georgia's National Cybersecurity Strategy (Resolution No. 482) and international indices such as the NCSI, the study argues for integrated programs that combine technical controls - access management, phishing simulations, and secure off-boarding with cultural initiatives focused on awareness and incentives. The paper concludes with policy and managerial recommendations tailored to SMEs. Global statistics further reveal that most cybercrimes target private businesses, which, on average, allocate less than $500 annually for cybersecurity measures, making them highly profitable targets for cybercriminals.*

Keywords: *cyberattack; cyber culture; cyber hygiene; cyber protection.*

Introduction

Although cyberattacks can serve various purposes—such as financial fraud, data breaches, or information manipulation—private businesses remain among the most at-risk targets. Small and medium-sized enterprises (SMEs) receive particular attention, as they are often the most vulnerable segment due to limited financial and technical resources. Research demonstrates that a significant proportion of cyberattacks stem from human error. Consequently, the human factor is widely regarded as the weakest link in cybersecurity. This vulnerability often manifests through phishing attempts, weak or reused passwords, and the use of unsecured networks and personal devices. Therefore, raising employee awareness and promoting a culture of cybersecurity are essential for strengthening an organization's overall defense posture. The aim of this study is to examine how Georgian companies ensure cybersecurity, to identify the preventive measures they employ, and to assess employees' awareness of such concepts as cyber culture and cyber hygiene. The intersection of digital transformation (DT) and cybersecurity has become a focal point for both researchers and practitioners. Saeed et al. (2023) argue that as organizations adopt new technologies, they inadvertently increase their vulnerability to cyber threats. The authors propose a staged cybersecurity readiness framework, which serves as a proactive approach for businesses to anticipate and mitigate potential threats during digital transformation initiatives. This framework emphasizes integrating robust cybersecurity measures from the outset, thereby safeguarding operations against disruption and data breaches (Saeed et al., 2023).

The threat of cyberattacks in business

As of December 15, 2024, Georgia holds the following positions in international cybersecurity and digital readiness rankings: 30th in the National Cybersecurity Index (NCSI), having previously ranked 44th between 2016 and 2023; 58th in the Global Cybersecurity Index (compared to 55th from 2016 to 2023); 68th in the E-Government

Development Index; and 67th in the Network Readiness Index. The country received its highest ratings in areas such as cybersecurity policy, personal data protection, and efforts to combat cybercrime. However, the lowest score was recorded in crisis management, with only 22% out of a possible 100%[1].

The necessity of merging cybersecurity with digital transformation is further supported by the findings of Browne et al. (2015), who emphasize the importance of Cyber Threat Intelligence (CTI) in enhancing organizational resilience. Their proposed framework encompasses a knowledge base, detection models, and visualization dashboards, equipping businesses to identify and respond to potential security breaches effectively. This integrated approach is crucial as organizations increasingly rely on digital solutions, creating new avenues for cyber threats (Browne et al., 2015).

The goals and objectives of national cybersecurity can be found in Resolution of the Government of Georgia No. 482 on the approval of the National Cybersecurity Strategy of Georgia for 2021-2024 and its action plan[2].

The main directions for protection and prevention from cyber attacks are clearly visible here. The main aim of cybersecurity is to build a strong cyber culture within our society and organizations, and to enhance our ability to tackle cyber threats effectively. This includes educating schoolchildren and students about safe online practices, raising awareness among society and organizations about cyber risks, and ensuring safe and reliable functioning in cyberspace.

Second goal emphasizes the importance of enhancing collaboration between the public and private sectors. This involves using communication platforms to share information about current trends, best

[1] NCSI (E-Governance Academy), "Georgia – National Cybersecurity Index Profile," *National Cyber Security Index* (2024), https://ncsi.ega.ee/country/ge/1011/#details

[2] Government of Georgia, "Resolution No. 482: National Cybersecurity Strategy of Georgia 2021–2024 and Action Plan," *Matsne.gov.ge* (2021), https://matsne.gov.ge/ka/document/view/5263611?publication=0

practices, and cyber threats. Additionally, it aims to encourage the adoption of international standards and to support research activities in the field of cybersecurity.

Third goal highlights the need for robust human resources and technical support to develop cyber capabilities. This includes enhancing the knowledge and skills of specialists in the field and bolstering national cyber capabilities through adequate technical support.

Fourth goal focuses on enhancing Georgia's role as a secure player in the global cybersecurity landscape. This involves improving access to information about cyber threats, increasing international support and cooperation, and participating in cyber trainings and exercises. Additionally, it aims to strengthen partnerships through bilateral and multilateral exchanges of knowledge and experience.

Understanding the primary areas of national cybersecurity, along with its aims and purposes, should be considered within the business sector. This includes every organization, irrespective of its scale, be it small, medium, or large.

According to Cybersecurity Ventures, global cybercrime expenses for companies are projected to reach approximately $10.5 trillion annually by 2025, rising from $3 trillion in 2015. This represents a year-over-year growth rate of 15 percent (Embroker, 2024).

With more of the workforce working remotely during the pandemic, more people are connected to the internet than ever before. This has created an ideal environment for cybersecurity threats to grow[1].

Industry 4.0, characterized by the integration of IoT and cloud computing, has transformed manufacturing processes but also expanded the attack surface for cybercriminals (Wang et al., 2021). The vulnerabilities present in factory environments necessitate the establishment of effective cybersecurity guidelines tailored to this new

[1] PA Consulting, "What Is Cyber Security Culture and Why Does It Matter for Your Organisation?" *PA Consulting Insights* (2023), https://www.paconsulting.com/insights/what-is-cyber-security-culture-and-why-does-it-matter-for-your-organisation

industrial landscape. By addressing the specific challenges faced by Industry 4.0, businesses can proactively implement strategies to safeguard their operations against evolving cyber threats (Wang, Zhu, and Sun, 2021, pp. 11895–11910).

Cybercrime, which includes everything from theft or embezzlement to data hacking and destruction, is up 600% because of the COVID-19 pandemic. Nearly every industry has had to embrace new solutions and it forced companies to adapt quickly.

Cyber-attacks on all businesses are becoming more frequent, targeted, and complex. According to Accenture's Cost of Cybercrime Study, 43% of cyber-attacks are aimed at small businesses, but only 14% are prepared to defend themselves.

According to data from the Ministry of Internal Affairs of Georgia, between January 1 and March 31, 2024, a total of 169 incidents involving unauthorized access to computer data and/or systems for financial purposes were recorded. Of these, 57 cases (44.77%) were resolved, while the remaining 112 remain under investigation.

It is noteworthy that the number of registered cybercrime cases has declined by 29.3% compared to the same period in 2023. According to the Ministry of Internal Affairs, 239 cases were recorded in the first quarter of 2023, with 107 of them (44.77%) successfully resolved).[1]

Not only does a cyber-attack disrupt normal operations, but it may cause damage to important IT assets and infrastructure that can be impossible to recover from without the budget or resources to do so. Addressing these cybersecurity challenges requires a combination of user awareness, security practices, and technology solutions. Organizations and individuals must remain vigilant and actively protect themselves from evolving cyber threats.

Organizations face the challenge of personal data, financial data, proprietary information, and intellectual property being compromised

[1] https://www.bpn.ge/article/126634-rogoria-kiberdanashaulis-statistika-sakartveloshi/

when cybercriminals launch cyberattacks, leaving them vulnerable to exploitation by fraudsters.

Cybercriminals launch frequent and vigorous attacks against small businesses, as well as medium and large enterprises. These hackers focus on exploiting hundreds, if not thousands of small businesses at once. Because small businesses typically have less robust technology security, lower threat awareness, and limited time and resources to maintain cybersecurity, they are especially vulnerable. The size of the business does not deter hackers because they will win anyway. Even the smallest businesses may conduct significant financial transactions or have extensive customer data that regulations such as the General Data Protection Regulation (GDPR) require protection. In addition, small businesses often partner with larger corporations, providing hackers with an opportunity to attack these larger organizations.

The most common types of attacks on small businesses include:

- Phishing/Social Engineering: 57%
- Compromised/Stolen Devices: 33%
- Credential Theft: 30%

Some industries face a higher vulnerability to cyberattacks, especially those that are closely integrated into people's daily lives. Companies that store confidential or personal information are prime targets for hackers. For example, banks and financial institutions that store credit card information, bank account information, and customer data are particularly vulnerable. Similarly, medical facilities with medical records, clinical trial data, and information about patients such as Social Security numbers and billing information are being targeted. In addition, corporations that contain product concepts, intellectual property, marketing strategies, customer and employee databases, and contract deals are at risk. Institutions of higher education that contain enrollment data, academic records, financial records, and personal data such as names, addresses and payment information also attract cyber threats.

A recent Global Application and Network Security report found that the average cost for organizations to recover from a major cyberattack has surpassed $1 million.

To protect itself, a company needs to create a cybersecurity strategy, and this strategy must be built into the company's overall risk management plan, which considers all possible business risks, which is associated with significant costs. Statista Market Report's revenue in the Cybersecurity market is projected to reach $162 billion in 2023. It is expected to show an annual growth rate from 2023 to 2028 of 9.63%, resulting in a market volume of $256.50 billion by 2028.

Given the statistics and the looming threat of cyber-attacks on private businesses, it makes sense that there should be systems in place to protect against such attacks and minimize the damage they cause. Since the private sector often owns critical infrastructure, it's crucial for them to be actively involved in detecting, preventing, investigating cybercrimes.

United Nations Security Council Resolution 2341 (2017) states that each country should identify its critical infrastructure within its borders. Many critical infrastructure sites, like those supporting industrial processes, use off-the-shelf software. This choice brings cost savings, ease of use, and enables remote control and monitoring from various locations. However, it also opens them up to greater risks of computer network-based attacks when connected to intranets and communication networks.

As mentioned, there are both internal threats, like cybercrimes by employees or managers, and external threats, like suppliers or customers. Surprisingly, when cybercrimes happen, businesses and organizations often hesitate to involve law enforcement.

One example of non-disclosure of information about a data leak is the case of Yahoo Inc. Yahoo Inc. faced a significant data breach incident, leading to a 3% drop in its share price and a loss of about US$1.3 billion in market value. Moreover, during negotiations to sell its business to Verizon, Yahoo had to accept a 7.25% discount on the deal, amounting to a reduction of $350 million. Additionally, due to delayed disclosure of the breach, Yahoo was fined $35 million by the US Securities and Exchange Commission.

The private sector has the manpower, money, and tech know-how to investigate cybercrimes, and they can lend a hand to national security, law enforcement, and other government bodies in cybercrime cases. To boost countries' ability to tackle cybercrimes, numerous international public-private partnership projects have been launched. For instance, INTERPOL's Cyber Fusion Centre collaborates with both law enforcement and industry cybersecurity experts to gather and share important intelligence with key players. At the national level, mechanisms for public-private partnerships are also emerging. In the US, the National Cyber Forensics and Training Alliance (NCFTA) unites cybercrime specialists from government, academia, and private sectors to detect, minimize, and fight cybercrime. In Japan, they established a structure like NCFTA called the Center for Combating Cybercrime, as part of a public-private partnership. In Europe, the 2Centre project involves cooperation between law enforcement, education, and private businesses. It began with national centers in Ireland and France and later expanded to other countries like Greece, Spain, Belgium, Estonia, Lithuania, Bulgaria, and England. In Georgia Cyber-crimes are usually investigated by the Cyber Crime Unit of the Home Office. This unit is responsible for handling various cyber-crimes including hacking, identity theft, online fraud, and other cyber-crimes. In addition, the State Security Service of Georgia may also be involved in the investigation of cybersecurity threats that pose a threat to national security.

Let's go back to companies dealing with cyber-attacks and cybersecurity. It's crucial for them to develop a strong risk management culture. Business leaders must prioritize building awareness about cybersecurity among their teams to ensure that any risk management plan stands a chance of success and remains effective in the long run.

The relationship between corporate social responsibility (CSR) actions and cybersecurity vulnerabilities has emerged as a significant theme in the literature. Talesh (2018) highlights how superficial CSR initiatives can unintentionally attract cybercriminals, particularly when companies face pressing social issues. This relationship underscores the importance of aligning social performance with genuine operational integrity, as a tarnished public image can exacerbate a firm's vulnerability to cyberattacks (Talesh, 2018, pp. 417–440).

The effectiveness of cybersecurity and the strength of security measures heavily rely on the awareness and actions of all employees within a company. Cybercrime stats reveal that 95% of the time, attackers succeed due to human error, carelessness, or trust. Data protection officers (DPOs), chief information security officers (CISOs), and security decision makers shoulder the responsibility of safeguarding sensitive information. Since hackers know companies have security experts, they often resort to tricking less informed employees into granting access to networks and systems, a tactic known as "phishing" or "social engineering" scams.

A survey was conducted among representatives of small businesses operating in various sectors. The analysis revealed that all respondents (100%) acknowledged the critical importance of cyber hygiene and the need for a prompt and appropriate response to cyberattacks. However, 66.7% indicated a lack of competence in the field, while 86% reported that their employees possess an insufficient level of knowledge regarding cyber hygiene and cybersecurity culture.

Additionally, 60% of managers emphasized that cyber hygiene and cybersecurity awareness are vital components of their company's overall security. While many employees claimed to be aware of cybersecurity risks and processes, their responses to simulated scenarios raised concerns. When asked how they would react to receiving a suspicious email or a potentially malicious link, 40% stated they would either ignore it or avoid opening the link, 20% admitted they would not recognize it as a threat at all, and notably, none reported they would escalate the issue to management.

Despite these challenges, most managers (83.3%) acknowledged that effective protection depends heavily on educating and training staff, and they highlighted the importance of regular training sessions and seminars. Nonetheless, due to the high costs associated with maintaining dedicated cybersecurity personnel or services, 66.7% of small businesses still lack a designated cybersecurity officer or relying on self-management of threats, if the smaller scale of their operations reduces their risk exposure.

It is important to remember that the human factor is characterized by significant vulnerability. Employees, often unintentionally, can become the weakest link in the security chain. Therefore, it is critical to develop a culture of cybersecurity awareness to root out not only bugs but also active insider threats.

Strategies to effectively increase cybersecurity awareness include:

Interactive training modules that simulate real cyber threats. These may include phishing simulations, role-playing scenarios, and gamified training;

Regular communication, creating a constant communication channel for updates, tips, and news on cybersecurity;

Recognition and reward. Implementation of a recognition and reward system for employees who comply with cyber hygiene rules. Publicly recognizing their efforts can create a positive culture.[1]

When an employee leaves, it's crucial to swiftly revoke their access to sensitive data as a preventive measure. Following this, monitoring employees' actions within the organization becomes essential. Transparency within the company facilitates the early detection of potential threats, enabling prompt action to mitigate them.

Conclusions

The points discussed above highlight the importance of cultivating a strong cybersecurity culture. But what does this mean? It involves employees' attitudes, knowledge, norms, and values regarding cybersecurity—shaped by an organization's goals, structure, policies, and leadership.

A strong cybersecurity culture recognizes that people—not just technologically are critical to security. It's essential to create an environment where employees are informed and prepared to serve as the first line of defense.

[1] https://www.linkedin.com/pulse/how-do-you-make-employees-aware-cyber-security-thesecurityco

Cyberattacks are constant and evolving. However, by adopting best practices, building a resilient cybersecurity culture, and staying alert to new threats, businesses can significantly reduce their risk. Cybersecurity is not a one-time task—it requires ongoing attention. Prioritizing ensures not only your organization's safety but also contributes to a more secure digital ecosystem.

References

BPN.ge. (2024). როგორია კიბერდანაშაულის სტატისტიკა საქართველოში? [What are the cybercrime statistics in Georgia?]. *Business Press News.* https://www.bpn.ge/article/126634-rogoria-kiberdanashaulis-statistika-sakartveloshi

Cobalt.io. (2024). Top Cybersecurity Statistics 2024: With around 2,220 Cyberattacks Each Day. *Cobalt Blog.* https://www.cobalt.io/blog/cybersecurity-statistics-2024

DataProt. (2024). Cyber Security Statistics – Everything You Need to Know. *DataProt Blog.* https://dataprot.net/blog/cyber-security-statistics/

Embroker. (2024). 2024 Must-Know Cyber Attack Statistics and Trends. *Embroker Blog.* https://www.embroker.com/blog/cyber-attack-statistics/

Government of Georgia. (2021). Resolution No. 482: National Cybersecurity Strategy of Georgia 2021–2024 and Action Plan. *Matsne.gov.ge.* https://matsne.gov.ge/ka/document/view/5263611?publication=0

NCSI (E-Governance Academy). (2024). Georgia – National Cybersecurity Index Profile. *National Cyber Security Index.* https://ncsi.ega.ee/country/ge/1011/#details

PA Consulting. (2023). What Is Cyber Security Culture and Why Does It Matter for Your Organisation? *PA Consulting Insights.* https://www.paconsulting.com/insights/what-is-cyber-security-culture-and-why-does-it-matter-for-your-organisation

Saeed, S. et al.. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. *Sensors (Basel, Switzerland),* 23. https://doi.org/10.3390/s23167273

Talesh, S. A. (2018). Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as 'Compliance Managers' for Businesses. *Law & Social Inquiry,* 43, 417–440. https://doi.org/10.1111/lsi.12303

The Security Company. (2023). How Do You Make Employees Aware of Cyber Security? *LinkedIn Pulse.* https://www.linkedin.com/pulse/how-do-you-make-employees-aware-cyber-security-thesecurityco

Wang, Z., Hongsong, Z., & Limin S. (2021). Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. *IEEE Access,* 9, 11895–11910. https://doi.org/10.1109/ACCESS.2021.3051633