DOI: https://doi.org/10.30837/EK.2024.002

Romanenkov Yu.,
Doctor of Technical Sciences,
Professor, Professor of Economic Cybernetics and
Management of Economic Security Department
Kharkiv National University of Radio Electronics
ORCID: https://orcid.org/0000-0002-6544-5348
Wei Wan,
student,
Kharkiv National University of Radio Electronics
ORCID: https://orcid.org/0000-0002-9524-4539
Siusiuk S.,
student,
Kharkiv National University of Radio Electronics
ORCID: https://orcid.org/0000-0001-8106-1523
Mazepa A.,
student,
Kharkiv National University of Radio Electronics
ORCID: https://orcid.org/0009-0006-9574-3174

NAVIGATING DIGITAL RISKS IN IT COMPANIES: CHALLENGES AND STRATEGIES FOR MITIGATION

IT companies play a central role in shaping and sustaining the digital economy, serving as both its backbone and drivers of innovation. These companies provide essential technologies, platforms, and services that facilitate the digitization of economic processes, enabling businesses and governments to operate more efficiently and effectively.

One critical contribution of IT firms is the development of digital infrastructure, such as cloud computing, data analytics, and cybersecurity systems. These technologies allow enterprises to scale operations, optimize decision-making, and safeguard sensitive information in an increasingly interconnected world. Moreover, IT companies spearhead innovation through advancements in artificial intelligence, blockchain, and the Internet of Things (IoT), creating new markets and transforming traditional industries.

In addition to technological innovation, IT companies foster digital entrepreneurship and economic inclusivity. Platforms provided by these firms lower entry barriers for startups and small businesses, enabling them to access global markets and compete on a level playing field. They also drive workforce development by generating high-skilled employment opportunities and offering training initiatives to address the digital skills gap.

However, the growing influence of IT companies also raises important challenges. Issues such as data privacy, market concentration, and unequal access to digital technologies require careful regulation to ensure the digital economy remains equitable and sustainable.

Key factors driving digital risks for it companies include [1]:

– *cybersecurity threats*: sncreasingly sophisticated cyberattacks, such as ransomware, phishing, and supply chain vulnerabilities, threaten IT companies by targeting critical infrastructure and sensitive data;

– *data privacy and compliance*: stricter regulations like GDPR and CCPA pose risks for companies that fail to comply with data protection standards, leading to financial penalties and reputational damage;

– *technological complexity*: rapid adoption of emerging technologies such as AI, IoT, and blockchain introduces vulnerabilities due to integration challenges, software bugs, and inadequate security measures;

– *third-party dependencies*: reliance on external vendors, cloud providers, and open-source software increases exposure to risks originating from supply chains and partner ecosystems;

– *rapid digital transformation*: accelerated digitalization in response to market demands can result in inadequate testing and rushed deployment of systems, heightening the likelihood of errors and breaches;

– *global connectivity*: the interconnected nature of IT operations expands the attack surface, exposing companies to risks across geographies and industries;

– *insider threats*: internal risks from employees or contractors, whether through malicious intent or negligence, can compromise systems and data;

– *geopolitical risks*: cross-border operations expose IT companies to risks stemming from regional conflicts, state-sponsored cyberattacks, and regulatory disparities.

By addressing these factors, IT companies can strengthen resilience and maintain operational integrity in the face of escalating digital risks.

A lot of researches investigated digital risks. Early studies (e.g., 2000s) explored cybersecurity risks in IT systems, focusing on vulnerabilities in software and networks. Key works addressed risk assessment frameworks, including the NIST Risk Management Framework and ISO 27001 standards. As IT operations expanded, researchers began analyzing operational risks such as system downtime, data loss, and third-party dependencies. Studies highlighted the financial and reputational impacts of these risks on IT companies.

Literature on compliance risks surged with the introduction of regulations like General Data protection regulation (GDPR, 2018) and CCPA (California Consumer Privacy Act – data privacy legislation that applies to most businesses that process the personal data of California residents. The CCPA gives California residents a certain amount of control over the personal data that businesses collect about them.).

Researchers emphasized the complexities of navigating legal landscapes in a globalized IT market.

Recent studies emphasize the rise of sophisticated cyber threats, including ransomware**,** phishing**,** and advanced persistent threats (APTs). Researches discussed economic models of cybersecurity investments and the costs of cybercrime. Studies analyze risks introduced by cloud computing**,** AI, and IoT, which increase attack surfaces and operational complexities. Research highlights how these technologies both mitigate and exacerbate digital risks.

A growing body of literature focuses on proactive approaches to mitigate risks, including cybersecurity frameworks, digital forensics, and predictive analytics. Industry-specific studies examine the role of cyber insurance in managing residual risks.

Recent works utilize quantitative models to measure digital risk exposure, combining financial, operational, and reputational dimensions. Studies advocate for integrating risk quantification into strategic decision-making for IT companies. Emerging areas include supply chain risks in IT, post-quantum cybersecurity, and AI-driven threat detection systems. Calls for interdisciplinary research combining technology, economics, and policy perspectives are prominent.

Digital risk broadly refers to the potential threats and vulnerabilities that arise from using digital tools, platforms and technologies. Assessing digital risk on the organizational level examines all of the negative consequences that can result from digital transformation. While going digital is critical to scaling a business, it also means relying more heavily on digital solutions [2]. Digital risks are unwanted and unexpected outcomes are a result of digital transformation, and they’re something that every organization will eventually need to learn how to manage if they want to survive [3]. To understand the nature of digital risks it is important to classify them. The main types of digital risks are represented at figure 1.

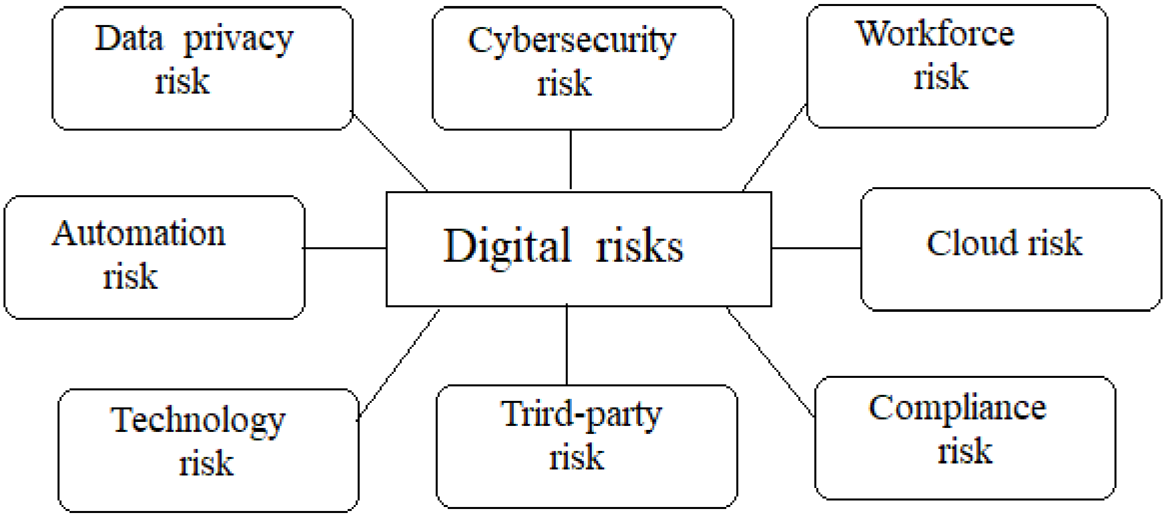

Figure 1 – Types of digital risks

Source: constructed by authors based on [2,3]

Nowadays IT-companies suffered all these risks cybersecurity risks (risk of a cyberattack), workforce risk (skill shortages and high employee turnover, risky behavior with data), cloud risk (Cloud outages), compliance risk (compliance requirements driven by new technology and the scope of data that company creates), third-party risk (supplier, vendor, contractor, or service provider), technology risk (potential unavailability of critical systems due to power failures, dependencies, and incompatibilities), automation risk (any potential risks posed by automation software), data privacy risk (data breaches).

Due to The European Union Agency for Cybersecurity (ENISA) report of Cyberthreats during 2024, Threats against availability (DDoS) and Ransomware ranked at the top during the reporting period. Geopolitics continued to be a strong driver for cyber malicious operations. A notable trend is the increasing similarity between State-nexus actors and alleged hacktivist activities. There was a rise in data compromises leading up to 2021 and although this trend remained relatively stable in 2022, it began to increase once more in 2023 and showed signs of maintaining this momentum in 2024 [4].

Here are some examples of digital risks realization, based on [5-8].

In 2017, ransomware attacks like WannaCry and NotPetya drew global attention by causing widespread disruption to major companies and organizations. These cyberattacks exploited vulnerabilities in systems and networks, temporarily crippling operations. The types of attacks range widely, targeting everything from personal information to confidential industrial data, with consequences including identity theft, financial fraud, blackmail, ransom demands, and even infrastructure disruptions like power outages.

Many of these attacks are preventable, as they often exploit well-documented and known vulnerabilities. Proper system maintenance, timely updates, and robust security protocols are critical to mitigating such risks and reducing the impact of cyber threats.

In October 2013, Adobe reported a significant cyberattack on its IT systems, leading to the theft of sensitive data from 2.9 million accounts. Compromised information included login credentials, passwords, names, and credit card details with expiration dates. Later investigations revealed a file online that raised the total number of affected accounts to 150 million, though only 38 million were active. Hackers exploited vulnerabilities in Adobe’s security practices, particularly the encryption of passwords instead of the recommended hashing method. While the stolen banking data remained secure due to robust encryption, a more alarming consequence was the theft of 40GB of source code for Adobe products. This breach posed significant risks to the company’s intellectual property and product security, amplifying concerns beyond customer data theft. This case underscores the critical importance of adhering to best practices in password management and securing sensitive operational data to mitigate the risks of cyberattacks.

In April 2011, Sony's PlayStation Network (PSN) suffered a major cyberattack that exposed the personal data of 77 million users, including banking details of thousands of players. The breach forced Sony to shut down PSN, Sony Online

Entertainment, and Qriocity services for a month. To address the fallout, Sony provided $15 million in compensation to affected users, in addition to covering legal fees and refunding customers whose accounts were exploited.

The attack exploited a well-known vulnerability in Sony's network, which had not been addressed. Unencrypted data and a simple SQL injection allowed hackers to access the information with ease. This incident highlighted critical lapses in Sony's cybersecurity measures, emphasizing the need for proactive vulnerability management and robust data protection protocols.

In August 2014, cybersecurity firm Hold Security disclosed that a Russian hacker group known as «CyberVor» had stolen 1.2 billion sets of login credentials and passwords from 420,000 websites worldwide. This breach potentially gave the hackers access to 500 million email accounts. The attack leveraged botnets programmed to scan websites for vulnerabilities, focusing on exploiting SQL injection flaws to gain unauthorized access to databases. This large-scale operation highlighted significant weaknesses in website security across a wide range of industries.

In 2014, Yahoo! announced it had suffered a cyberattack in 2014 that affected 500 million user accounts constituting the largest massive hacking of individual data directed against a single company. Names, dates of birth, telephone numbers and passwords were stolen.

A major outage disrupted in 2020 Google services globally, impacting users and businesses relying on Google Cloud. This incident highlighted the risks of over-reliance on cloud infrastructure.

Uber in 2016 and 2022 suffered from Ransomware Attack. Hackers accessed sensitive user data, and Uber concealed the breach instead of reporting it. Company received regulatory penalties and reputational harm. The sum of losses for Uber was $148 million.

Attackers exploited vulnerabilities in Microsoft Exchange servers, affecting over 250,000 organizations globally in 2021. This was widespread data theft and operational disruptions.

Each example illustrates different facets of digital risks IT companies encounter and the critical measures needed to mitigate such threats.

Many companies nowadays use proactive approaches to counterfight risks. Proactive approaches focus on identifying, assessing, and addressing potential risks before they materialize. Proactive risk mitigation not only minimizes the likelihood of digital threats but also ensures that organizations are better prepared to handle incidents effectively. Key approaches include:

– *cybersecurity frameworks*. These structured frameworks provide a systematic approach to manage and reduce cybersecurity risks. Key elements of cybersecurity frameworks usually include: risk assessment, policies and procedures (developing clear security and incident response protocols), Implementation of control (technical measures such as firewalls, intrusion detection systems, and access controls), monitoring (using tools to detect and respond to threats in real time). Example of such cybersecurity framework is represented by ISO/IEC 27001 (International standard for information security management systems). The benefits of using cybersecurity framework is that it provides a comprehensive and scalable approach to cybersecurity and enhances compliance with regulatory and industry standards;

– *digital forensics* that involves collecting, preserving, and analyzing electronic data to investigate security incidents and prevent future occurrences. It includes incident response (readiness plan to handle breaches effectively), data collection (ensuring secure acquisition of digital evidence from affected systems), Analysis and Reporting (identifying attack vectors and malicious actors using forensic tools), and lessons learned, using insights from forensic investigations to enhance security measures. The benefits of digital forensics are the follows: it strengthens investigative capabilities and supports compliance with legal and regulatory requirements;

– *predictive analytics* that leverages data, statistical algorithms, and machine learning techniques to anticipate and mitigate risks before they occur. Main characteristics of predictive analytics are: Threat Intelligence (collecting and analyzing global threat data to predict potential attacks); anomaly detection (using machine learning to identify unusual patterns in network traffic or user behavior); Risk Scoring **(**quantifying risks to prioritize mitigation efforts). To detect potential threats predictive analytics uses AI-powered tools like SIEM (Security Information and Event Management) and UEBA (User and Entity Behavior Analytics) Real-time dashboards to monitor and visualize risk metrics. It enables faster and more accurate risk identification and reduces response times by preemptively addressing vulnerabilities.

Besides these proactive methods companies also use cyber insurance and create risk-shaping partnerships.

Cyber Insurance provides financial protection against losses resulting from cyber incidents. Policies typically cover costs associated with data recovery, business interruption, legal liabilities, and regulatory fines. For IT companies, cyber insurance is particularly valuable in managing residual risks that remain after implementing technical and organizational security measures. Furthermore, insurance providers often offer risk assessment services, enhancing an organization's overall cybersecurity posture. However, the challenge lies in accurately pricing premiums, which requires a detailed understanding of evolving threat landscapes and a company’s specific risk profile.

Risk-Sharing Partnerships involve collaboration between multiple stakeholders, such as IT firms, insurers, governments, and industry associations, to distribute the financial and operational burdens of cyber risks. These partnerships leverage collective resources and expertise to build robust defenses and facilitate faster recovery from cyber incidents. For instance, industry consortia may share anonymized threat intelligence, reducing individual companies’ exposure to attacks. Governments may also play a role by offering cyber risk frameworks or financial incentives to support such initiatives.

Together, cyber insurance and risk-sharing partnerships provide IT companies with a multi-layered approach to managing cyber risks. While insurance offers financial resilience, partnerships foster collective risk mitigation, enabling organizations to better navigate the complexities of the digital landscape. However, the success of these strategies depends on transparent communication, robust data-sharing mechanisms, and alignment of goals among stakeholders. As cyber threats continue to grow in sophistication, these approaches will remain critical components of a comprehensive risk management framework in the IT sector.

Several prominent IT companies have implemented cyber insurance and risk-sharing partnerships to manage digital risks effectively:

– Cloudflare has partnered with cyber insurers to offer customers reduced premium rates and enhanced coverage by integrating robust security solutions with their insurance offerings. This collaboration simplifies the insurance process and reduces risk for customers;

– SentinelOne and Chubb formed an integration partnership to share data on cybersecurity health, helping clients secure lower premiums and better protection. Such partnerships streamline renewals and incentivize proactive cybersecurity measures;

– Amazon Web Services (AWS) has partnered with cyber insurance providers like Cowbell Cyber. This collaboration allows customers to share AWS security postures with insurers via AWS Security Hub, expediting insurance quotes and enabling better terms.

These examples demonstrate how IT companies and insurers leverage risk-sharing partnerships to enhance resilience, reduce costs, and encourage better cybersecurity practices.

The rapid expansion of the IT sector, driven by advancements in digital technologies, has brought unprecedented opportunities and challenges. Among these challenges, digital risks-ranging from cyberattacks and data breaches to system failures and regulatory non-compliance-pose a significant threat to organizations. A complex systematic approach is critical to managing these risks effectively, ensuring both resilience and sustainability.

A complex systematic approach recognizes that digital risks are interconnected and multifaceted, requiring holistic management strategies. Unlike traditional risk management, which often focuses on isolated threats, this approach emphasizes the interdependencies among various technological, operational, and organizational factors. By addressing these interdependencies, companies can better anticipate potential vulnerabilities and mitigate cascading failures.

Key components of a systematic approach include risk identification, assessment, mitigation, and continuous monitoring. Advanced analytical tools, such as artificial intelligence and big data analytics, enable organizations to detect patterns and predict emerging risks. Moreover, the integration of risk management into strategic decision-making ensures that digital resilience becomes a core organizational priority.

Collaboration across departments and with external stakeholders, including regulators and cybersecurity experts, is also essential. Such collaboration fosters information sharing and coordinated responses to complex threats. Additionally, regular training and awareness programs empower employees to recognize and respond to digital risks effectively.

In the IT sector, where innovation and speed are paramount, neglecting a systematic approach to digital risk management can result in substantial financial, reputational, and operational losses. Conversely, a well-implemented strategy enhances an organization’s ability to innovate securely, maintain trust, and achieve long-term success.

References

1. Deloitte. Managing risk in digital transformation. URL: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-managing-risk-in-digital-transformation-1-noexp.pdf.

2. Proofpoint. What is digital risk? https://www.proofpoint.com/au/threat-reference/digital-risk.

3. Bevin L. 10 common types of digital risks. ZenGRC. 31.05.2024. URL: https://www.zengrc.com/blog/common-types-of-digital-risks/

4. The European Union Agency for Cybersecurity (ENISA) Threat Landscape 2024. September 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

5. Techmonitor. The biggest cyberattacks of 2023. 4 December, 2023. URL: https://www.techmonitor.ai/technology/cybersecurity/biggest-cyberattacks-2023?cf-view.

6. Outpost 24. The top 10 list of the biggest cyberattacks. 11 July, 2023. URL: https://outpost24.com/blog/top-10-biggest-cyberattacks/.

7. Canalys. An RSAC 2024 takeaway: cyber insurance partnerships take on new forms. URL: https://www.canalys.com/insights/cyber-insurance-partnerships.

8. Elliot M. Why Companies Are Partnering With Insurance to Maximize Risk Management Know-How. Risk&Insurance. 9 Sept., 2019. URL: https://riskandinsurance.com/why-companies-are-partnering-with-insurance-to-maximize-risk-management-know-how/.

9. Babenko V., Romanenkov Yu., Yakymova L., Nakisko A. Development of the model of minimax adaptive management of innovative processes at an enterprise with consideration of risks. *Eastern-European Journal of Enterprise Technologies*. 2017. Vol. 5. No. 4 (89). pp. 49-56.