SECTION: CYBERSECURITY AND RISK MANAGEMENT IN THE DIGITAL AGE

SECURING THE FUTURE

CZU: 004.056.5:005.334
DOI: https://doi.org/10.53486/csc2025.14

OHRIMENCO SERGHEI, Professor
Moldova Economics Academy, Chișinău, Republic of Moldova
osa@ase.md
ORCID ID: 0000-0002-6734-4321

BRADU NICHITA
Bachelor Cyber Security
Student of "IU International University of Applied Sciences ", Berlin, Germany
bradunichita.cs@gmail.com
ORCID ID: 0009-0004-7212-7278

Abstract. Cybersecurity is an information age chronic phenomenon, and enterprise is faced with more and more sophisticated cyber-attacks. Cybersecurity and risk management are also included since they quantify the economization of the cost of cybercrime, the value of good security mechanisms, and best practices to safeguard digital assets. Organizations can make themselves risk-proof and fortify their security position through adopting controls such as the CIA Triad and ISO 27005. Adopting an offensive security position, i.e., sophisticated technology and constant learning as a way of being one step ahead of anticipated cyber-attacks, has also been recommended in the report.

KEY WORDS: *hacker, cybersecurity, threats, digital age, security measures, risks.*

INTRODUCTION

Cyber security is safeguarding computer systems, networks, and data from any kind of malicious attacks. Opening business in the cyber world, malware attacks such as ransomware, phishing, and data stealing have been nightmare problems. Steps need to be taken for prudent steps of risk management to detect loopholes and reduce possibilities of such likely attacks before it becomes an issue.

The economic burden of cyber-crime is enormous.

The global economy lost a staggering $13.82 trillion to cybercrime up to 2028, the third-largest economy in the world behind America and China.

Increased sophistication of cyber-attacks necessitates multi-dimensional security solutions by way of technology intrusion, regulatory compliance, and compliance wherever on the web. This paper contends the evolving threat environment, cybersecurity best practice, and the degree to which developed risk models consider providing a firm cyber defense policy.

The Changing Cyber Threat Environment

Cybercrime is on the rise day by day, day by day more complex and harmful. The hackers are exploiting the capability of emerging technologies such as AI and machine learning to automate the attack, and thus it is hard to detect and filter. The most prevalent cyber-attacks are:

- **Ransomware:** Encryption of files by malware, and the hacker will request money in exchange for its release.

- **Phishing:** Deceptive messages or emails to get the users to provide sensitive information.
- **Data Breaches:** Infringement of sensitive data, resulting in loss of finances and reputation.

More value of cybercrime is a continuous parallel with investment in greater emphasis on spending in secure cybersecurity. None of the cybersecurity companies suffer losses, business interruption, and litigation.

Cybersecurity Best Practices and Frameworks

Strong cybersecurity posture rests upon security fundamentals. CIA Triad is a battle-hardened veteran which guarantees:

- **Confidentiality:** Prevention of unauthorized use of confidential data through encryption and access control.
- **Integrity:** Data integrity and consistency through protection of authorized changes.
- **Availability:** Service and data availability to authorized personnel when and where required.

Organizational security posture can be strengthened by staying compliant with best practices such as the below:

- Regular vulnerability scans and security audits.
- **MFA** hardening.
- Social engineering attack simulation against employees.
- **EDR** technology deployment for real-time threat detection and response against them.

Risk Management in Cybersecurity

Risk management in cybersecurity is the identification, analysis, and removal of the security threats so that the damage could be minimized. It includes the following steps:

- **Risk identification:** Identification of the potential threats and vulnerabilities in the IT system of an organization.
- **Risk Estimation:** Probability and likelihood of future risk of the identified risk.
- **Risk Mitigation:** Risk mitigation controls and security policy enforcement.
- **Monitoring Continuously:** Security policy update at regular time intervals and countermeasures to imminent threats.

International standards for risk management such as **ISO 27005** and **NIST Risk Management Framework (RMF)** utilized globally provide methodological tools for detection of cybersecurity threats and cost-optimality.

CONCLUSION

Increased intensity and sophistication of cyber-attacks require a fresh and dynamic approach to cybersecurity. Organizations require technological innovation, collaboration with regulators, and ethics in humans in order to be proof against cyberattacks. Organizations require security solutions based on AI, embrace the Zero Trust philosophy, and free the employees so that cybersecurity becomes second nature to them. Most critical to enable long-term security and resilience of digital assets will be ongoing investment in cybersecurity since the threat will persist in the digital economy. Companies can proceed to secure, de-risk, and create a future-proof digital tomorrow with best-of-breed cybersecurity architecture and best practice.

REFERENCES

1. Michael Houghton. 13 Top Strategic Cyber Security Trends to Watch Out For in 2024. 2023.
2. MacdonnelUlsch. CYBER THREAT! How to Manage the Growing Risk of Cyber Attacks. 2014.
3. Tushar Bhardwaj, Himanshu Upadhyay, Tarun Kumar Sharma, Steven Lawrence Fernandes. Artificial Intelligence in Cyber Security: Theories and Applications, 2023.
4. Yuri Diogenes, Dr. Erdal Ozkaya. Cybersecurity – Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals, Second Edition. 2019.
5. Charles J. Brooks, Christopher Grow. Cybersecurity Essentials: Making cybersecurity concepts and practices easy to understand. 2018.