# Cyber Resilience

Subjects: Computer Science, Information Systems

Contributor: Se-Ho Choi , Jaepil Youn , Kookjin Kim , Seongkee Lee , Oh-Jin Kwon , Dongkyoo Shin

Cyber resilience refers to an organization's capability to maintain its targeted performance despite a cybersecurity breach.

Cyber resilience cyberattack Internet

## 1. Introduction

Individuals are consistently connected to the Internet via diverse devices, including smartphones and Internet of Things (IoT) equipment, which are readily accessible. Cyberspace has evolved as an infrastructure, coexisting with people globally, reminiscent of the boundless nature of space. However, a fully reliable information protection system, adaptable to the swift shifts in infrastructure, has not been established. As a result, malicious activities persist in cyberspace. Furthermore, the magnitude and intensity of damages have been escalating, often bolstered by certain organizations and governments. Notably, entities, encompassing public institutions and private corporations, are confronted with tangible challenges when countering emerging, sophisticated cyber threats [1]. Since 2013, efforts have been undertaken by private companies to holistically incorporate and manage diverse security measures. These efforts involve perpetually countering cyberattacks and formulating and refining information protection policies through an information security management system (ISMS). Yet, the proficiency in real-time detection, analysis, and response to threats is found lacking [2].

In such a landscape, addressing every cyberattack within a limited time frame becomes unfeasible. The efficacy of investigation, analysis, and response largely hinges on the competencies of individual entities and organizations. For effective countering, a cyber-resilience strategy needs to be embraced, championed by a proactive and cohesive approach. Once a cyberattack is detected, standardized methodologies and procedures optimized for cyber defense are mandated across information security policy management, malicious code mitigation, and system recovery. Swift responses, facilitated by these measures, can curtail the proliferation of damage during system operation. Furthermore, achieving sustainable cyber resilience capable of reverting systems to their pre-attack state swiftly becomes feasible.

## 2. Cyber Resilience

Cyber resilience refers to an organization's capability to maintain its targeted performance despite a cybersecurity breach. At the World Economic Forum in Davos in 2012, cyber resilience was defined as the capacity of systems and organizations to endure cyber events, gauged as a blend of average downtime and recovery time [3]. This framework for cyber resilience is composed of five stages: identify, protect, detect, respond, and recover [4].

Cyberattacks are imminent threats, not merely distant possibilities. While it is widely held that maintaining updated software offers optimal information protection [3], the 2022 Ponemon report revealed that only 18% of cyberattacks resulted from software vulnerabilities. It is crucial to acknowledge that cyberattacks are executed across diverse platforms, and attackers continually innovate new means of breaching organizations; such intrusions have become routine [5].

Environments characterized by complexity and uncertainty, including cloud systems, IoT, blockchain, and globalized supply chain operations, are increasingly vulnerable to cyberattacks. An effective response necessitates the adoption of a proactive and cohesive cyber-resilience strategy. Notably, most breaches often go undetected internally and are brought to light only after being flagged by concerned organizations or the attackers themselves. Recognizing and swiftly responding to such cyberattacks using standardized protocols and reverting to a pre-attack state is paramount [3]. Consequently, cyber resilience is delineated as an organization's capacity to mitigate and recover from the detrimental impacts of both anticipated and unforeseen threats via defensive maneuvers in cyberspace [3].

The menace of cyber threats is not novel, but its magnitude and unpredictability are burgeoning daily. Detecting and thwarting cyberattacks proactively is challenging, and countering a specific cyberattack with established defense technologies is not straightforward [6]. Cyberattacks are evolving from isolated incidents to persistent, relentless campaigns. No singular remedy exists that is suitable for all infrastructures, and frequently, no unified approach prevails to defend against cyberattacks [7]. Rather than perpetually deploying security safeguards, enterprises ought to discern their paramount assets and evaluate their correlation with prevailing cyber-defense initiatives. A paradigm shift is warranted to propose strategies to stakeholders, underscored by cyber resilience, ensuring swift response and mission assurance.

A disparity in the evolution of defensive and offensive software has been highlighted by DARPA, as depicted in **Figure 1**. Due to the amplifying intricacy of the systems under safeguard, the complexity of software safeguarding a network has been observed to surge exponentially. However, the size of software code employed in a successful assault has remained relatively unchanged [8]. A defense system is mandated to counteract every conceivable attack, while attackers need only channel their efforts at the defense's most vulnerable point.

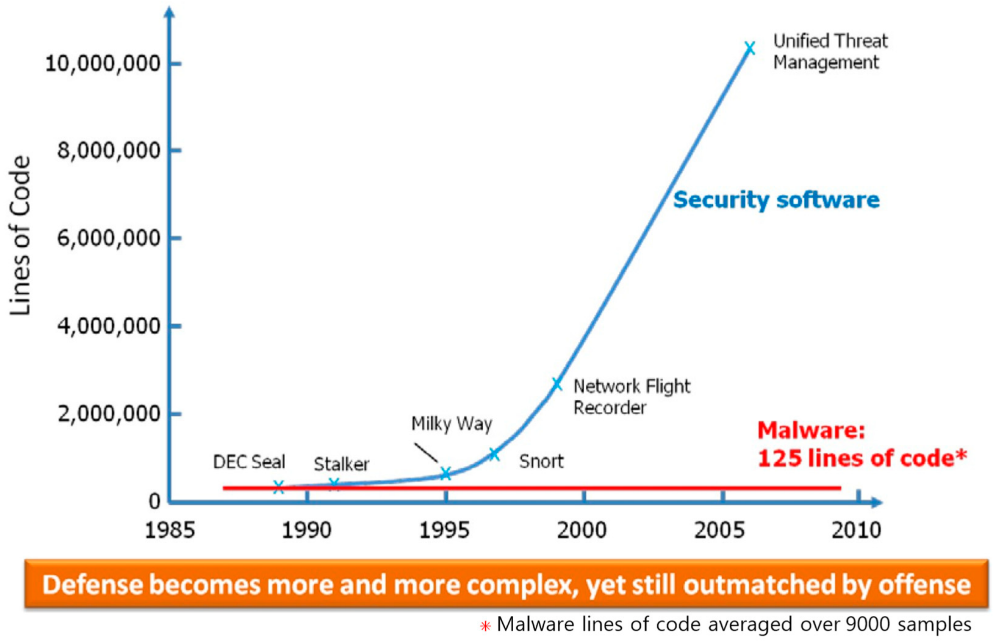

**Figure 1.** Size comparison of defensive and offensive software. Reprinted with permission from Ref. [8].

A system–theoretic process analysis for security through simulation (STPA-Sec/S) was proposed by Simone et al., marking a methodological bridge between STPA-Sec and quantitative resilience assessment grounded in simulation models. Once the systems–theoretic accident modeling and processes (STAMP) model, which addresses cyber threats and spots insecure controls within cyber–social technology systems, was expanded, it was posited that cyber resilience can be quantitatively determined based on systems–theoretic modeling [9].

Cyber resilience is characterized as an organization’s capacity to mitigate the adverse impacts of both foreseen and unforeseen threats via cyber-defense activities, aiming to revert to its pre-attack state in the minimal possible duration. Furthermore, cyber resilience is assessed contingent on the mean response time of the information protection apparatus and the quickest recuperation span following an information system disruption (**Table 1**).

**Table 1.** Application plan in cyber-resilience study.

| Study | How to Apply Cyber Resilience |
|---|---|
| Huang et al. [10] | Cyber resiliency is leveraged to uphold crucial functions and performance during vulnerability rectification. |
| Babiceanu et al. [11] | Restoration of software is approached from a security perspective, accentuating system responses to events. |
| Haque et al. [12] | Cyber resilience is qualitatively evaluated utilizing subjective survey techniques. |
| Ligo et al. [13] | Assessment of cyber resilience for autonomous entities is undertaken, barring recovery from outages. |
| Simone et al. [9] | Cyber resilience is applied based on cyberattack narratives, without giving precedence to |

| Study | How to Apply Cyber Resilience |
|---|---|
| | specific scenarios. |

## Cyberattack Response

Ponemon, an IBM-sponsored lab, specializes in analyzing the cost of data breaches. Between March 2021 and March 2022, incidents of cyberattacks across 17 industries including healthcare, energy, and finance in 17 countries and regions were studied. Situations where data were leaked through irregular channels were examined, with results presented in **Figure 2** [14].

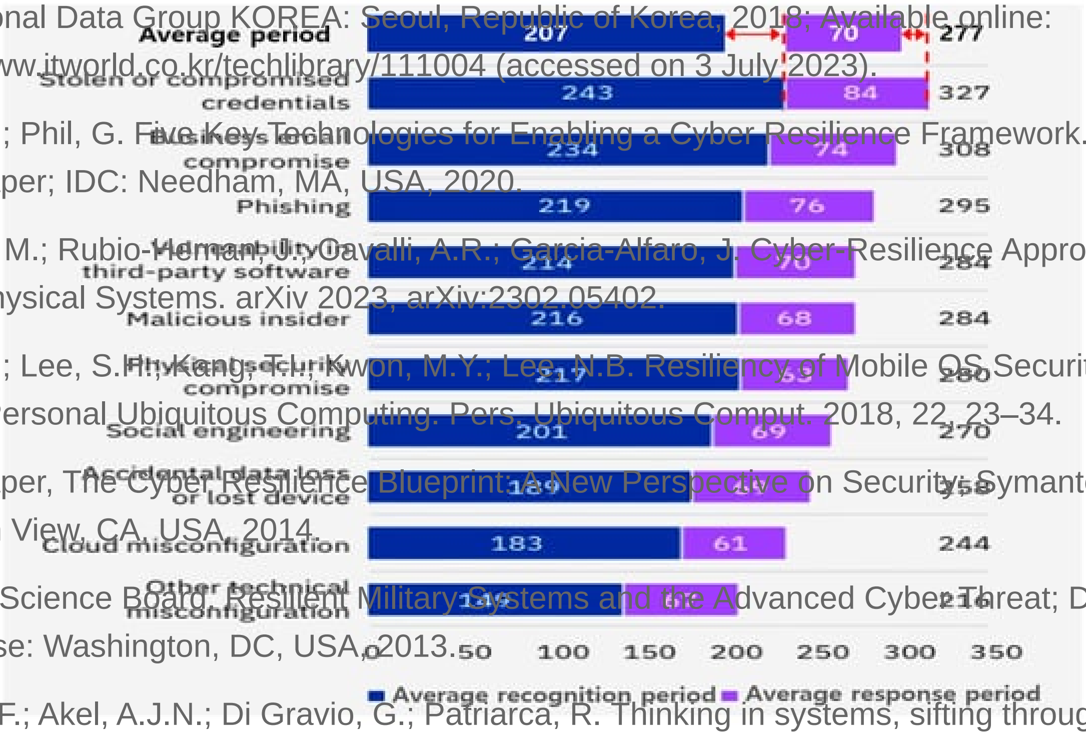

**Figure 2.** Time taken to recognize and respond to each type of attack. Reprinted with permission from Ref. [14].

Based on the survey, a cyberattack was recognized, on average, after 207 days, while a data breach was recognized and addressed in 70 days, leading to an entire life cycle of 277 days. For instance, if the initial cyberattack involving data leakage transpired on 1 January, 277 days up to 4 October were needed for recognition and response, indicating a lack of timely intervention [14].

In instances where cyberattacks leveraged stolen or compromised authentication data, 243 days were required for detection and an additional 84 days for response, totaling an extended period of 327 days. This duration is 18% longer than the typical time taken to detect and address a cyberattack. Cyberattacks executed via business emails were observed to have the second lengthiest life cycle for detection and response at 308 days. Moreover, attacks exploiting third-party software vulnerabilities took 284 days for detection and response, marking the fourth longest life cycle.

## Recuperation Times

1. Government of the Republic of Korea. National Cyber Security Master Plan; Government of the Republic of Korea: Seoul, Republic of Korea, 2019; p. 2.
2. Kim, K.H. Overview of Information Security Management System Certification System and Development Direction; Korea Internet & Security Agency: Seoul, Republic of Korea, 2017; pp. 3–7. Available online: https://m.blog.naver.com/ntower/221003396724 (accessed on 3 July 2023).
3. Ryu, J.G. Respond to Cyber Security Incidents That You Don’t Know When Not If; IDG Summary, International Data Group KOREA: Seoul, Republic of Korea, 2018; Available online: https://www.itworld.co.kr/techlibrary/111004 (accessed on 3 July 2023).
4. Frank, D.; Phil, G. Five Key Technologies for Enabling a Cyber Resilience Framework. In IDC White Paper; IDC: Needham, MA, USA, 2020.
5. Segovia, M.; Rubio-Hernan, J.; Cavalli, A.R.; Garcia-Alfaro, J. Cyber-Resilience Approaches for Cyber-Physical Systems. arXiv 2023, arXiv:2302.05402.
6. Lee, S.K.; Lee, S.H.; Kang, T.I.; Kwon, M.Y.; Lee, N.B. Resiliency of Mobile OS Security for Secure Personal Ubiquitous Computing. Pers. Ubiquitous Comput. 2018, 22, 23–34.
7. White Paper, The Cyber Resilience Blueprint: A New Perspective on Security; Symantec: Mountain View, CA, USA, 2014.
8. Defense Science Board. Resilient Military Systems and the Advanced Cyber Threat; Department of Defense: Washington, DC, USA, 2013.
9. Simone, F.; Akel, A.J.N.; Di Gravio, G.; Patriarca, R. Thinking in systems, sifting through simulations: A way ahead for cyber resilience assessment. IEEE Access 2023, 11, 11430–11450.
10. Huang, Y.; Huang, L.; Zhu, Q. Reinforcement learning for feedback-enabled cyber resilience. Annu. Rev. Control 2022, 53, 273–295.
11. Babiceanu, R.F.; Seker, R. Cyber resilience protection for industrial internet of things: A software-defined networking approach. Comput. Ind. 2019, 104, 47–58.
12. Haque, M.A.; Shetty, S.; Krishnappa, B. ICS-CRAT: A cyber resilience assessment tool for industrial control systems. In Proceedings of the 2019 IEEE 5th IEEE International Conference on Big Data Security on Cloud (BigDataSecurity), High Performance and Smart Computing (HPSC) and Intelligent Data and Security (IDS), Washington, DC, USA, 27–29 May 2019; pp. 273–281.
13. Ligo, A.K.; Kott, A.; Linkov, I. How to measure cyber-resilience of a system with autonomous agents: Approaches and challenges. IEEE Eng. Manag. Rev. 2021, 49, 89–97.
14. Ponemon Institute. Cost of a Data Breach Full Report 2022; IBM Security: Armonk, NY, USA, 2022; pp. 14–18.

Recuperation time is employed as a functional damage assessment metric within combat damage assessment. It designates the period necessary to either restore or replace the functionality of a specific target. Both the shortest feasible (minimum) and the most realistic extended (maximum) times to regain lost functionality are determined. Furthermore, a combat damage assessment may incorporate a judgment on recuperation time contingent on the target’s processing objective and accessible intelligence. For instance, while full restoration of a particular target’s capabilities might be projected to take 10 days, achieving 50% of its original functions could require a minimum of 2 days. In specific scenarios, satisfactory performance might be sustained even with just half of the original functionalities restored [15].

15. Chairman of The Joint Chiefs of Staff Instruction 3162.02, Methodology for Combat Assessment; U.S. Joint Chiefs of Staff: Washington, DC, USA, 2019; p. C-7.

Retrieved from https://encyclopedia.pub/entry/history/show/111281