THE 10th ANNIVERSARY INTERNATIONAL SCIENTIFIC
PROFESSIONAL CONFERENCE
SECURITY AND CRISIS MANAGEMENT – THEORY AND PRACTICE (SeCMan)
- THE 10th ANNIVERSARY INTERNATIONAL FORUM
„SAFETY FOR THE FUTURE 2024" -
27th and 28th September 2024, Belgrade, Republic of Serbia

CRISIS MANAGEMENT AND CYBER SECURITY: KEY STRATEGIES FOR ADDRESSING DIGITAL THREATS

Samed Karovic[1a]
[1] Metropolitan University, Faculty of Management, Tadeusa Koscuska 63, Belgrade, Republic of Serbia, samed.karovic@metropolitan.ac.rs

Received: 19th August 2024
Accepted: 26th August 2024

Original scientific paper

Abstract: *Crisis management and cybersecurity are critical elements in addressing digital threats. In the current digital environment, many organizations face an increasing number of cyber threats that can seriously jeopardize their security and business stability. By analyzing existing threats, identifying vulnerabilities, and implementing appropriate countermeasures, successful crisis management and cybersecurity strategies become essential components in protecting against potential attacks.*

This paper explores and explains the strategies that organizations can apply to effectively manage crises caused by cyber attacks. By focusing primarily on preventive measures, early detection of vulnerabilities, and rapid incident response, organizations can enhance their ability to resist cyber attacks, thereby protecting their resources, data integrity, and reputation. The integration of comprehensive approaches to crisis management and cybersecurity becomes imperative to ensure business sustainability and continuity in today's digital environment.

Keywords: *Crisis Management, Cybersecurity, Digital threats, Strategies*

(Introductory lecture of the forum - work by invitation)

1. INTRODUCTION

In the modern digital age, where organizations and individuals are increasingly reliant on technology, cybersecurity has become one of the key aspects of overall security and data protection. Crisis management, as a discipline focused on identifying, planning for, and responding to crises, must include specific strategies to address cyber threats that can seriously compromise business operations, reputation, and public trust.

This paper focuses on understanding the concept of crisis management within the context of cybersecurity, identifying the key components that constitute an effective cybersecurity framework, and analyzing the strategies necessary for effectively confronting digital threats.

[a] ORCID: 0000-0001-5470-4650

By reviewing types of cyber threats and case studies of both successful and unsuccessful crisis management strategies in cybersecurity, the paper aims to provide a comprehensive insight into the importance of a proactive approach in protecting organizations in a digital environment.

2. FUNDAMENTALS OF CRISIS MANAGEMENT

When it comes to crisis management, it is important to emphasize that this discipline primarily deals with crises directly caused by human actions or those where human involvement has been a contributing factor. This primarily includes computer hacking, environmental pollution, kidnapping of executives, fraud, product counterfeiting, sexual harassment, and workplace violence. It is particularly important to note that crises caused by human actions are not inevitable and do not simply have to happen. Consequently, the public tends to be extremely critical of organizations responsible for their occurrence (Karovic, 2015).

Crisis management involves the intensification of resources and methods necessary for resolving the crisis, as well as the introduction of radical measures within the organization. If the focus is on crisis prevention, it is referred to as preventive or anticipatory crisis management. On the other hand, reactive crisis management refers to securing fundamental, existential variables after the crisis has occurred, characterized by clear objectives such as achieving a certain level of success (Karovic, 2015).

The elements present at every level of crisis management and crisis resolution (crisis management) are illustrated in Figure 1.

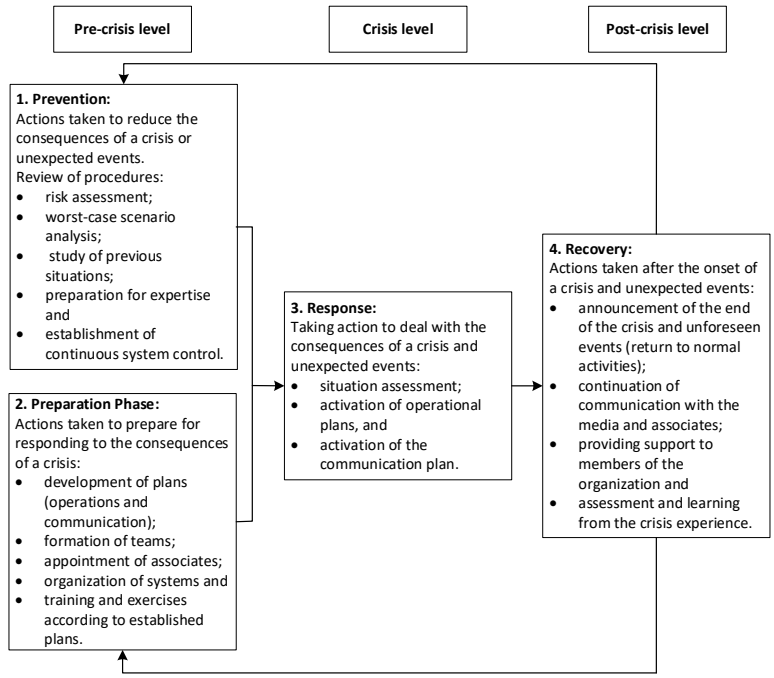

Figure 1: Levels of Crisis Management and Phases of a Crisis
***Source**: Samed Karovic, Krizni menadzment, Belgrade: Medija centar „Odbrana", p. 128.*

Crisis management encompasses various qualitative areas related to the specific type of crisis, primarily because it involves a multidisciplinary approach to resolving any type of crisis at

any level of occurrence. This means that crisis management involves a large number of people, the organization, and the ability to act in a coordinated and unified manner.

3. CYBERSECURITY AS AN ASPECT OF CRISIS MANAGEMENT

Cybersecurity can be defined as a set of practices, technologies, and processes designed to protect networks, devices, programs, and data from attacks, damage, or unauthorized access, with the purpose of ensuring the confidentiality, integrity, and availability of information. Simply put, cybersecurity refers to the process of protecting digital devices and network systems from various types of cyber attacks. These attacks pose a significant problem and a real threat, as they can compromise sensitive data and expose an organization to insecurity in the cyber world, which is never desirable (Nova.rs, 2024).

Ultimately, cybersecurity serves as a shield tasked with responding to various types of threats that may originate from the virtual world, such as malware, phishing, ransomware, as well as unauthorized access and data theft (USAF, 2024).

Crisis management and cybersecurity are interconnected through the need for proactive planning, rapid response, and effective recovery in the event of a cyber attack or threat. These relationships can be discussed through a comparative approach, which is illustrated in Table 1.

Table 1: Comparative Relationships Between Crisis Management and Cybersecurity

Relationships	Comparative Overview of Relationships	
	Crisis Management	**Cybersecurity**
1. Preventive Planning	Requires the development of response plans for various types of crisis situations, including cyber attacks.	Focuses on the prevention and protection of digital infrastructure from threats such as hacking, data theft, and ransomware attacks.
2. Rapid Response	Includes mechanisms for rapid response to crisis situations to minimize damage and ensure business continuity. In the case of a cyber attack, crisis management must quickly respond to isolate the threat, mitigate damage, and protect critical systems.	Enables rapid response to cyber threats through tools such as real-time threat detection, swift incident response, and malware removal. Quick action is crucial to prevent the escalation of an incident into a larger crisis.
3. Recovery and Restoration	Focuses on restoring normal business operations as quickly as possible after a crisis, including damage assessment, communication with key stakeholders, and the implementation of recovery plans.	Plays a key role in the recovery phase by ensuring that all infected systems are cleaned, data is restored from backups, and measures are implemented to prevent future attacks.
4. Training and Learning	Involves training employees to be prepared for appropriate responses during a crisis, including training on recognizing and responding to cyber threats.	Includes continuous education of employees on security practices, such as recognizing phishing attacks, proper password usage, and safe handling of sensitive information.
5. Communication	Includes clear communication with internal and external stakeholders during and after a crisis.	Requires a coherent communication strategy during a cyber attack, including informing users, partners, and regulatory bodies about the incident, as well as the measures taken to protect data and systems.

It can be concluded that crisis management and cybersecurity are closely interconnected in the goal of protecting an organization from cyber threats. While cybersecurity provides preventive and reactive tools for defending against cyber attacks, crisis management ensures that the organization is prepared to respond effectively to such threats and minimize their impact on business operations.

3.1. Key Components of Cybersecurity

When it comes to the key components of cybersecurity, similar to crisis management, it encompasses four critical processes: prevention, detection, response, and recovery. Each of these elements plays a crucial role in protecting organizations from cyberattacks and other security threats.

Prevention is the first and most important element of cybersecurity, focusing on proactive measures that organizations take to prevent potential attacks or unauthorized access to systems and data. The goal of prevention is to minimize risks and eliminate vulnerabilities before they can be exploited. Prevention includes: access management (involves strict control of access to information and systems through authentication, authorization, and the use of Identity and Access Management (IAM) tools); encryption (the use of encryption to protect sensitive data during transmission and storage to prevent unauthorized interception and access); updates and patches (regularly updating software and systems with the latest security patches to eliminate known vulnerabilities); firewall and antivirus software (implementation of firewalls and antivirus software to filter malicious traffic and protect against malware); employee training (educating employees on cybersecurity best practices, including recognizing phishing attacks and using strong passwords).

Detection refers to an organization's ability to identify and recognize potential security incidents or suspicious activities in real-time. Effective detection enables a quick response and minimizes the impact of an attack. Key components of detection include: Intrusion Detection Systems (IDS): (systems that continuously monitor network traffic and identify suspicious activities or intrusion attempts); Security Information and Event Management (SIEM): (tools that collect and analyze data from various sources to identify threats and anomalies); Logging and Monitoring: (setting up systems to log and monitor activities within networks and systems to detect unusual actions that may indicate an attack); Behavioral Analysis: (using analytics and artificial intelligence to detect deviations in user or system behavior that may signal malicious activities).

Incident response encompasses all actions taken after a security incident is detected, with the goal of minimizing damage and impact on the organization. A swift and efficient response can significantly reduce the consequences of an attack. Key components of incident response include:Incident Response Plan (IRP): A plan that outlines detailed steps to be taken in the event of different types of incidents, including responsible individuals and resources. Incident Response Team (IRT): A specialized team responsible for managing incidents, including experts from IT, cybersecurity, legal, and communications fields. Isolation and Threat Elimination: Rapid isolation of affected systems or network segments to prevent the spread of the threat and taking measures to remove malicious software or restore systems.

Communication: Effective internal and external communication during the incident to ensure that all relevant stakeholders are informed and to avoid unnecessary panic or misinformationRecovery refers to the processes that ensure an organization can return to normal operational status after an incident. This process includes restoring systems to an operational state, analyzing the cause of the incident, and implementing measures to prevent future attacks. Key components of recovery include: Disaster Recovery Plan (DRP): (a

recovery plan that outlines the steps to restore systems and data after a major incident, including the use of backups and redundant systems); Root Cause Analysis: (Post-Incident Analysis) (a detailed analysis of the cause of the incident to identify vulnerabilities that allowed the attack and implement corrective measures); System Restoration: (restoring systems from backups and verifying data integrity before bringing them back online); Enhancing Security Measures: (based on the root cause analysis and recovery process, organizations implement additional security measures to prevent similar incidents in the future).

Thus, these elements together form a practical approach to cybersecurity that enables organizations not only to protect themselves from attacks but also to recover quickly and efficiently in case an attack occurs.

3.2. The Types of Cyber Threats

As Ivana Hrcak pointed out, "… a cyber attack represents a type of attack that can target entire information systems, infrastructure, computer networks, or even personal computers. The attacker can be an anonymous individual, a hacker group, an organization, or even a sovereign state. The goal of the attack is to gain access to the data or functions of a particular computer system with the intention of theft, alteration, or extortion. Such attacks have multiple negative effects. In addition to the loss or theft of important data, organizations that are targeted face significant financial losses and reduced user trust" (Hrcak, 2022).

What needs to be emphasized is that cyber attacks are almost always based on combinations of different infiltration skills and the management of malicious software, which can be extremely simple and routine to use, but also very complex and demanding. This text will only illustrate two simple threats: Ransomware and Social Engineering.

In the Introduction to Cybersecurity, it is highlighted that "…ransomware functions like kidnapping, but instead of a person, sensitive data is kidnapped. Once ransomware is activated on a computer system, it encrypts or blocks access to the data on that system, then demands a ransom from the victim in exchange for unlocking access. It's important to dispel the misconception that ransomware activates immediately after gaining access to a computer system. Sometimes, it can wait for months, gathering information on how to spread most effectively and cause the greatest possible damage" (USAF, 2024).

When it finally activates, the "kidnappers" are in a position to blackmail the victim and extort money under the threat of permanently denying access to the data, deleting it, or making it public, which brings with it a host of other legal complications. The ransom is usually demanded in bitcoins or other cryptocurrencies to more effectively avoid money tracking, and the ransom amount varies from a few hundred to several thousand dollars (USAF, 2024). The decision to pay the ransom should be carefully considered, as there is no guarantee that the victim will actually receive the decryption key or that the attackers will not release the stolen confidential data to the public. Generally, agreeing to the attackers' demands is an open invitation for them to target you again.

The most common file formats of email attachments that contain ransomware are .zip, .doc, .xls, and .pdf. However, it's important to keep in mind that ransomware can be present in any attachment format, so it's crucial to be cautious when opening messages and downloading attachments from unknown sources.

Social engineering refers to manipulating human behavior to trick the victim into downloading and activating malware or disclosing sensitive information. For example, attackers may pose as technical support staff, pretending to help the victim resolve a computer issue, while actually

trying to convince the victim to unknowingly download a malware file. The same situation can occur in the physical world—attackers might attempt to access servers and other network equipment under the guise of authorized service personnel or plant a USB flash drive in a visible location containing malicious software, with the goal of having the flash drive end up in the victim's computer.

On the other hand, social engineering is increasingly utilizing deepfake technology, which allows the manipulation of visual and audio materials in real-time. By using deepfake filters, attackers can disguise their physical appearance and voice during video calls, making them appear as someone the recipient knows or a person of authority whom they trust.

It is important to remember that cybercriminals are social chameleons and will always find ways to exploit emerging technologies for malicious purposes.

4. KEY STRATEGIES FOR CONFRONTING CYBER THREATS

The purpose of strategies for dealing with cyber threats is to provide comprehensive protection for an organization from potential cyber attacks, minimize the risk of data damage or loss, and ensure a quick recovery of business operations after an incident. In this context, the following strategies are discussed: prevention and preparation, response to cyber attacks, communication during a cyber crisis, and post-attack recovery and analysis.

The second strategy pertains to responding to cyber incidents and requires timely and effective responses to minimize the harmful effects of attacks. It includes the formation of a crisis management team and the development of recovery plans.

Effective communication during a cyber crisis is crucial for maintaining trust and minimizing panic. It encompasses both internal and external communication. Employees must be promptly informed about the incident, with clear instructions on what actions to take, how to protect their data, and how to report suspicious activities. External communication focuses on key partners, clients, and the public, who need to be informed about the incident through press releases, website announcements, and other communication channels.

The strategy of recovery and post-incident analysis focuses on returning to normal business operations and learning from previous incidents to enhance cybersecurity. It includes restoring business to normal and analyzing the attack (incident). This analysis should cover technical aspects (e.g., how the attack was carried out, which vulnerabilities were exploited).

When comparing the aforementioned strategies with crisis management, specifically the phases of crisis resolution, they fully reflect the phases of crisis management and are compatible with crisis resolution. This demonstrates how inseparable crisis management is from cybersecurity and how they intertwine with each other.as well as procedural shortcomings (e.g., whether employees responded in a timely manner).

5. CHARACTERISTIC CASES OF SUCCESSFUL AND UNSUCCESSFUL CRISIS MANAGEMENT STRATEGIES IN CYBERSECURITY

a) Successful case

Royal Mail Ransomware Attack (2023) - United Kingdom (Alliance, 2023)

Attack Description: Royal Mail was the target of a cyberattack in January 2023. International parcel and letter delivery through Royal Mail’s postal branches was completely halted. The attackers, the LockBit ransomware group associated with Russia, demanded a large ransom in exchange for a decryption key. Reportedly, ransom notes were printed on special papers after the hackers encrypted devices used for international shipping. Allegedly, the organization

refused to comply with the ransom demand, which some believe was in the millions. The attackers then threatened to release the stolen and encrypted data online.

Response Strategy: The UK's National Cyber Security Centre (NCSC), along with other agencies, quickly became involved in crisis management, providing support and guidance for the response. Due to timely actions and good coordination, the impact of the attack was minimized, and services were quickly restored.

Lessons Learned: An effective response to a cyberattack requires rapid problem identification and coordination with relevant institutions, which can significantly mitigate the consequences of the attack.

b) Unsuccessful case

Prospect Medical Holdings Ransomware Attack (2023) - United States (Kapko, 2023)

Attack Description: In August 2023, Prospect Medical Holdings, a company managing hospitals and healthcare centers in the US, was targeted by a ransomware attack. The system was forced to switch to manual operations, leading to patient redirection and the shutdown of some operations.

Response Strategy: The response was slow and inadequate. The hospitals were not sufficiently prepared for this type of attack, resulting in significant operational disruptions and jeopardizing patient safety.

Lessons Learned: The lack of adequate preparation and crisis management plans can lead to severe consequences. Regular staff training and the enhancement of crisis plans are necessary to ensure resilience against such attacks.

c) Cases in Serbia

Although specific details about cyberattacks in Serbia are not often publicly disclosed, there has been an increase in ransomware attacks and data theft cases. For example, in recent years, there have been attacks on both public and private institutions, where organizations were often forced to upgrade their security strategies after the attacks. In one case, the lack of effective crisis management resulted in a loss of customer trust and significant financial losses.

Attack on Telekom Srbija - April 12, 2022.

Characteristics: Telekom Srbija became the target of a DDoS (Distributed Denial of Service) attack on April 12, 2022, which lasted for several hours. The goal of the attack was to overwhelm the network, preventing users from accessing the internet and services.

Consequences: The attack caused intermittent disruptions in internet services across Serbia, affecting the operations of many businesses and the daily lives of citizens. Telekom Srbija had to take urgent measures to mitigate the attack and restore normal network functioning.

Elektroprivreda Srbije (EPS) was targeted by a cyberattack aimed at the IT infrastructure that manages the distribution of electricity. The attack involved compromising server systems and encrypting data using ransomware.

Consequences: Although there was no disruption in the electricity supply, the attack caused significant difficulties in network management and data recovery. EPS had to deploy additional resources to restore systems and enhance cybersecurity.

Attack on JKP Vodovod Novi Sad - June 21, 2023.

Characteristics: The Public Utility Company Vodovod Novi Sad became the target of a cyberattack that resulted in the temporary loss of access to operational systems and databases. The attack involved malicious software that disrupted the functionality of the water supply network management system.

Consequences: The attack led to interruptions in service delivery to citizens, including water supply disruptions in certain parts of the city. It took several days to restore the systems to normal operation, which incurred additional costs and caused dissatisfaction among customers.

Through these examples, it can be seen that the key components of successful crisis management in cybersecurity are a swift response, coordination with relevant institutions, and adequate organizational preparedness through regular training and the enhancement of security protocols. Failure in these aspects can lead to significant operational and reputational losses for an organization.

6. CONCLUSION

Given the increasing frequency and sophistication of cyber threats, effective crisis management in the field of cybersecurity has become an indispensable part of any organization striving for long-term stability and the protection of its interests. An analysis of key strategies for dealing with digital threats shows that successful crisis management depends not only on technical preparedness but also on the organization's ability to quickly and adequately respond to threats, ensure business continuity, and restore the trust of its users and partners.

By studying characteristic cases, this paper highlights the importance of an integrated approach to crisis management and cybersecurity, where proactivity, education, and continuous risk assessment stand out as key factors for success. Only by combining these elements can organizations build resilience against cyber threats and ensure a secure digital future.

REFERENCES

Alliance, C. M. (2023). Royal Mail Ransomware Attack Timeline. Retrieved from https://www.cm-alliance.com/cybersecurity-blog/royal-mail-ransomware-attack-timeline. (Accessed on August 18, 2024, at 17:25)

Hrcak, I. (2022). What Are Cyber Attacks and What Types of Attacks Exist? Retrieved from https://mint.rs/blog/bezbednost/sajber-napad/. (Accessed on August 13, 2024, at 14:20)

Kapko, M. (2023). Ransomware Attack on Prospect Medical Holdings Impacts Hospitals Across 4 States. Retrieved from https://www.cybersecuritydive.com/news/ransomware-hospitals/690130/. (Accessed on August 10, 2024, at 16:15)

Karovic, S. (2015). Crisis Management. Belgrade: Media Center "Odbrana". ISBN 978-86-335-0439-3

Nova.rs. (2024). Cybersecurity: The Key to Protection in the Digital Age. Retrieved from https://nova.rs/vesti/drustvo/sajber-bezbednost-kljuc-zastite-u-digitalnom-dobu/. (Accessed on August 13, 2024, at 17:15)

USAF. (2024). Introduction to Cybersecurity. Retrieved from https://www.preduzmi.rs/uvod-u-sajber-bezbednost/. (Accessed on August 13, 2024, at 14:15)20