Cybersecurity and Law

2025 Nr 2 (14)

DOI: 10.34567/cal/215342

Phases of crisis management in cybersecurity

Fazy zarządzania kryzysowego w cyberbezpieczeństwie

Bartłomiej TEREBIŃSKI
Akademia Sztuki Wojennej
ORCID: 0000-0002-6124-9905
E-mail: b.terebinski@akademia.mil.pl

Abstract

The purpose of this article is to describe the essence of crisis management in the sphere of cybersecurity. The analyses undertaken revolve around legal provisions regulating the issues of crisis management taking place in cyberspace and a practical look at the individual phases related to crisis management in cybersecurity.

The activities related to describing the factual material and systematizing the conclusions from the conducted scientific considerations were possible thanks to the application of selected theoretical research methods. Analysis and synthesis allowed for the decomposition of the studied cyberspace crises into their component elements in order to identify their essence and diagnose the relationship between cybercrisis situations and phases of crisis management.

Cybersecurity crisis management can be divided into several key phases that help effectively respond to incidents and minimize their impact: preparation, detection, response, assessment of the effectiveness of actions taken in response to the crisis, and improvement.

The essence of cybersecurity crisis management is the systematic preparation for, response to, and recovery from digital incidents that may threaten an organization, its systems, and data. This process encompasses prevention, planning, and response to minimize the impact of cyberattacks and ensure business continuity.

Keywords
threat identification, response procedures, system isolation, data recovery, post-incident analysis

Streszczenie

Celem niniejszego artykułu jest opisanie istoty zarządzania kryzysowego w obszarze cyberbezpieczeństwa. Podejmowane analizy koncentrują się wokół przepisów prawnych regulujących zagadnienia zarządzania kryzysowego w cyberprzestrzeni oraz praktycznego spojrzenia na poszczególne fazy związane z zarządzaniem kryzysowym w cyberbezpieczeństwie.

Działania związane z omówieniem materiału faktograficznego i usystematyzowaniem wniosków z przeprowadzonych rozważań naukowych były możliwe dzięki zastosowaniu wybranych teoretycznych metod badawczych. Analiza i synteza pozwoliły na dekompozycję badanych kryzysów cyberprzestrzeni na elementy składowe, co pozwoliło na identyfikację ich istoty oraz zdiagnozowanie związku między sytuacjami cyberkryzysowymi a fazami zarządzania kryzysowego.

Zarządzanie kryzysowe w cyberbezpieczeństwie można podzielić na kilka kluczowych faz, które pomagają skutecznie reagować na incydenty i minimalizować ich skutki: przygotowanie, wykrywanie, reagowanie, ocena skuteczności działań podjętych w odpowiedzi na kryzys oraz doskonalenie.

Istotą zarządzania kryzysowego w cyberbezpieczeństwie jest systematyczne przygotowanie, reagowanie i odzyskiwanie po incydentach cyfrowych, które mogą zagrozić organizacji, jej systemom i danym. Proces ten obejmuje działania zapobiegawcze, planowanie i reagowanie w celu zminimalizowania wpływu cyberataków i zapewnienia ciągłości działania przedsiębiorstwa.

Słowa kluczowe

identyfikacja zagrożeń, procedury reagowania, izolacja systemów, odzyskiwanie danych, analiza poincydentalna

Introduction

Cyberspace is a sphere where the activity of both the public and private sectors has shifted. Not all tasks are performed using it, but certainly a significant number, and this number is constantly growing. On the one hand, cyberspace facilitates operations, but on the other, it is exposed to threats, which are increasingly burdensome for its users. Given that cyberthreats are a growing problem, constant protection of information and communication systems used by both the state and private entities, including citizens, is becoming essential. Due to their widespread use, legal standards must appropriately regulate issues related to their proper security, as well as taking appropriate actions in the event of damage caused by a cyberattack, including in the event of a crisis.

The aim of this research is to describe the essence of crisis management in the sphere of cybersecurity. The analyses undertaken revolve around legal provisions regulating the issues of crisis management taking place in cyberspace, where both national and European Union regulations were analyzed, as well as a practical look at the individual phases related to crisis management in cybersecurity.

Introduction to crisis management in the area of cybersecurity – legal approach

As indicated in the literature on the subject, ensuring security is the basic task of the state, international structures, and the European Union[1]. Crisis management is a key element of security, entrusted to public administration bodies at all levels in Poland. The development of new technologies and the use of cyberspace to provide numerous services mean that crises can generate threats in cyberspace, which are highly dynamic and diverse. Due to the intensity of cyber threats, particularly those occurring in strategic areas of state activity and in important economic sectors, special attention should be paid to crisis management in the cybersecurity environment. The intensity and scope of cybersecurity incidents, as well as the status of cyberattack recipients, are particularly important for the implementation of crisis management mechanisms. Critical infrastructure, which not only ensures the proper functioning of the state but also allows members of society to live normally and, above all, meet basic human needs, is of particular importance.

Each EU Member State is required to designate or establish at least one authority responsible for large-scale cybersecurity incident and crisis management (a cybersecurity crisis management authority). Member States must provide these authorities with adequate resources to effectively perform their tasks. Such authorities must be embedded in national crisis management systems[2]. Polish lawmakers define crisis management as the activities of public administration bodies that constitute a component of national security management. This activity involves preventing crisis situations, preparing to take control of them (through planned actions), responding to crisis situations, and also addressing their effects and restoring critical resources and infrastructure[3].

Crisis management addresses crisis situations that have a significant negative impact on national security, often threatening the normal functioning of the state. It encompasses preventive, ongoing, and follow-up actions (including preventing future crises). A crisis situation has also been defined by law. According to Article 3, Section 1 of the Crisis Management Act, a crisis situation should be understood as a situation that negatively impacts the safety of people, significant property, or the environment, and that significantly limits the operations of relevant public administration bodies due to the inadequacy of available resources and resources. Therefore, a crisis situation threatens the operations of public administration bodies; however, these limitations must be significant and are caused by qualified threats, which include cyberattacks on IT systems.

In Article 9(2) of the NIS 2 Directive, the European Union legislator, in order to avoid a lack of response by the authorities responsible for cybersecurity crisis management to a cyber threat within the framework of crisis management (or an inappropriate, chaotic response), requires them to clearly indicate which of these authorities is to act as the coordinator of incident management and large-scale cybersecurity crisis management. According to Article 6(7) of the NIS 2 Directive,

[1] See more: M. Czuryk, Zarządzanie kryzysowe w obszarze cyberbezpieczeństwa, „Ius et Securitas" 2025, nr 1.

[2] Article 9(1) of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (OJ EU 2022 L 33, p. 80), hereinafter referred to as the NIS 2 Directive.

[3] Article 2 of the Act of 26 April 2007 on Crisis Management (Journal of Laws of 2023, item 122).

a large-scale cybersecurity incident is an incident that causes disruption at a level that exceeds the capacity of a given EU Member State to respond or that has significant impact in at least two Member States. Such an incident is therefore qualified. In the case of crisis management determined by its occurrence, the state's capacity to respond and the scope of its effects are taken into account. Article 9(3) of the NIS 2 Directive obliges each EU Member State to define the capabilities, resources, and procedures that can be used in the event of a crisis for cybersecurity purposes. States independently decide whether this will be a separate legal act or whether this matter will be incorporated into existing legal acts regulating crisis management and cybersecurity. In Poland, these are the act regulating crisis management and the act on the national cybersecurity system.

Each Member State is required, under Article 9(4) of the NIS Directive 2, to establish a national plan for response to large-scale cybersecurity incidents and crises, specifying the objectives and procedures for managing large-scale cybersecurity incidents and crises. This plan identifies, among other things: 1) the objectives of national preparedness measures and actions; 2) the tasks and responsibilities of cybersecurity crisis management authorities; 3) cybersecurity crisis management procedures, including their integration into the overall national crisis management framework, as well as information exchange channels; 4) national preparedness measures for taking action in response to threats, including exercises and training; 5) relevant public and private entities, as well as infrastructure; 6) procedures and arrangements between competent national authorities and institutions to ensure the effective participation of a Member State in the coordinated management of large-scale cybersecurity incidents and crisis management at European Union level and to ensure effective support from the EU Member State concerned for such coordinated management. Within three months of designating or establishing a cybersecurity crisis management authority, each Member State, pursuant to Article 9(5) of the NIS 2 Directive, shall notify the European Commission of the identity of its authority and shall notify it of any subsequent changes in this regard. Member States shall submit to the European Commission and the European Network of Cybersecurity Crisis Liaison Organisations (EU-CyCLONe) important information related to the requirements for large-scale cybersecurity incident management and crisis management (within three months of the date of adoption of the plans relating to these matters). However, Member States may refrain from sharing certain information to the extent that it is relevant to their national security. According to Article 10 of the Act on the National Cybersecurity System, an essential service operator develops, uses, and updates documentation regarding the cybersecurity of the information system used to provide the essential service. An essential service operator who is also the owner, sole possessor, or dependent possessor of facilities, installations, devices, or services that constitute critical infrastructure, and who has an approved critical infrastructure protection plan that includes documentation regarding the cybersecurity of the information system used to provide the essential service, is not required to develop documentation regarding the cybersecurity of the information system used to provide the essential service. Critical infrastructure (as one of the elements protected within the crisis management system) must be included in crisis planning for cyber threats. As indicated in Recital 70 of the NIS Directive 2, large-scale cybersecurity incidents and crises at the European Union level require coordinated action to ensure not only a rapid but also an effective response due to the high degree of interdependence between sectors and Member States. The availability of

networks and information systems that are resilient to cyber threats, as well as the availability, confidentiality, and integrity of data, are fundamental to the security of the European Union and to the protection of its citizens, businesses, and institutions (including public institutions) from incidents and cyber threats. This is also important for increasing the trust of individuals and organizations in the European Union's ability to promote and protect a global, open, free, stable, and secure cyberspace where freedoms and human rights, democratic principles, and the rule of law are respected.

In summary, cybersecurity threats can also trigger crisis situations. Therefore, it may be necessary to initiate crisis management measures, which may, among other things, result in restrictions on the exercise of freedoms and human rights. Restrictions on the exercise of constitutional freedoms and rights may be established, but only by statute and only when necessary in a democratic state governed by the rule of law for its security or public order, or to protect the environment, health, and public morals, or the freedoms and rights of others. However, such restrictions must not violate the essence of freedoms and rights. Effective crisis management in the area of cybersecurity requires cooperation, both at the international, European Union, and national levels. Such cooperation may involve exchanging information on cyber threats, cybersecurity incidents, experiences in cybersecurity crisis management, existing mechanisms in this area, as well as building infrastructure (even shared infrastructure) that allows for more effective combating of cyber threats, anticipating them, and minimizing their impact. According to Recital 13 of the NIS Directive, Member States should strive to ensure a high level of cybersecurity (especially given the intensity of cyber threats) and support the implementation of cybersecurity risk management measures. Cybersecurity governance, whether it concerns public or private activities, requires qualified personnel who not only possess appropriate knowledge of cybersecurity protection and the effectiveness of IT systems, but also the skills to apply this knowledge and effectiveness in practice. This staff will also have to take actions that, on the one hand, allow for the greatest possible access to services provided in cyberspace, and, on the other, protect against interference that disrupts the normal functioning of the IT systems through which these services are provided. Professional staff is the foundation for efficient cybersecurity management, regardless of the sphere in which it occurs[4].

Phases of crisis management in cybersecurity – introduction

Cybersecurity crises can have devastating consequences for organizations, ranging from financial losses and reputational damage to legal penalties and operational disruption. Effectively managing such crises requires a structured approach that guides organizations through the complex and often unpredictable digital threat landscape[5]. Despite the importance of rapid and coordinated responses, many organizations lack a comprehensive understanding of the structured phases that constitute an effective cybersecurity crisis management framework[6]. The phases of cybersecurity crisis management

[4] M. Karpiuk, W. Pizło, K. Kaczmarek, Cybersecurity Management – Current State and Directions of Change, „International Journal of Legal Studies" 2023, no 2.
[5] M. Bartock, J. Cichonski, M. Souppaya, NIST Special Publication 800-184, Guide for Cybersecurity Event Recovery, U.S. Department of Commerce 2016.
[6] J. Borky, T. Bradley, Protecting Information with Cybersecurity, „Effective Model-Based Systems Engineering" 2018, Sep, p. 345–404.

(primarily identification and preparation, followed by response and mitigation, and recovery and post-crisis analysis) create a comprehensive framework designed to minimize damage and facilitate rapid recovery. Each phase plays a key role in ensuring an organization's resilience to cyber threats, emphasizing proactive measures, rapid response, and continuous improvement. A detailed analysis of these phases provides a better understanding of how organizations anticipate, mitigate, and recover from cybersecurity incidents, strengthening their security posture and ability to withstand future threats. The first stage of cybersecurity crisis management focuses on identifying threats and vulnerabilities, which is crucial to establishing a robust defense mechanism. This involves implementing advanced detection tools, such as intrusion detection systems (IDS), security information and event management systems (SIEM), and real-time monitoring software, to identify suspicious activities or anomalies that may indicate a security breach. For example, many organizations use machine learning algorithms to recognize patterns that deviate from normal behavior, allowing for earlier detection of potential threats. Once threats are identified, a detailed risk assessment is conducted to assess the severity and potential impact of vulnerabilities. This assessment considers factors such as the likelihood of exploitation, the sensitivity of the data involved, and the potential for operational disruption. A notable example is how financial institutions regularly scan for vulnerabilities to prioritize remediation based on the risk level of the vulnerabilities detected. Based on this analysis, organizations develop comprehensive policies, procedures, and incident response plans that define roles, responsibilities, and communication channels during a crisis. These policies provide a roadmap, enabling organizations to respond effectively in the event of an attack. Training employees in security awareness and conducting simulated exercises further prepare organizations to quickly recognize and respond to threats, creating a culture of vigilance and preparedness.

When an incident occurs, the immediate priority becomes containing the breach and preventing further damage. This involves activating an incident response plan, which typically includes steps such as isolating infected systems, disabling infected accounts, and blocking malicious traffic. For example, a company affected by a ransomware attack can immediately disconnect infected servers from the network to stop the malware from spreading. Quickly containing the attack minimizes the scope of damage and preserves evidence for forensic analysis. Communication is also crucial at this stage; organizations must promptly inform relevant stakeholders, including internal teams, external partners, regulators, and affected customers, to maintain transparency and comply with legal requirements. Effective communication is exemplified by the rapid issuance of public statements and coordination with authorities by large corporations such as Equifax following a data breach, which helped manage public perception. At the same time, organizations utilize their incident response teams (comprising IT specialists, cybersecurity experts, and legal advisors) to coordinate actions, analyze the attack vector, and determine the scope of the threat. This coordinated response ensures effective containment of the incident and sets the stage for subsequent remediation. Once the immediate threat is contained, the focus shifts to restoring normal operations and learning from the incident. Recovery involves repairing damaged systems, recovering lost or corrupted data from backups, and implementing additional security measures to prevent recurrence. For example, after a data breach, organizations often upgrade their firewalls, update access controls, and implement advanced endpoint protection tools. At this stage,

a detailed incident analysis is crucial; organizations investigate how the breach occurred, what vulnerabilities were exploited, and how effective the response was. This assessment often includes forensic investigations, interviews with affected personnel, and a review of system logs. The findings from this analysis are used to update security policies, response plans, and technological safeguards. An example is the WannaCry ransomware attack, which prompted many organizations worldwide to revise their patch management protocols and adopt more stringent cybersecurity standards. Furthermore, organizations must transparently communicate with stakeholders about the incident's resolution and the measures taken to prevent future crises. Continuous improvement is essential, and lessons learned from each incident should be incorporated into training programs and the security infrastructure, fostering a resilient cybersecurity environment that can adapt to evolving threats.

The phases of cybersecurity crisis management (from identification and preparation, through response and mitigation, to recovery and post-crisis assessment) provide a key framework for protecting organizational assets in the digital age. Each phase builds on the previous one, emphasizing the importance of proactive detection, rapid response, and continuous learning. By investing in comprehensive policies, advanced detection tools, effective communication, and iterative improvements, organizations can not only mitigate the impact of cybersecurity crises but also increase their overall resilience. As cyberthreats increase in complexity and scale, understanding and effectively implementing these phases becomes crucial for organizations seeking to protect their operations, reputations, and stakeholders. Ultimately, a well-structured crisis management strategy ensures that in the event of a cybersecurity incident, the organization will be prepared to respond quickly, recover efficiently, and emerge stronger.

Effective cybersecurity crisis management requires team collaboration, rapid response, and regular updates to procedures in response to evolving threats. Each phase of cybersecurity crisis management has its own specific aspects that are crucial for effective incident response. The literature[7] identifies the following general stages of effective crisis management:

1. Preparation – involves developing crisis action plans, which should be regularly tested and updated.
2. Response – rapid identification and assessment of the incident and initiation of appropriate procedures to minimize damage.
3. Recovery – focuses on rebuilding infrastructure and systems after the attack, as well as implementing improved security measures.
4. Analysis – after the crisis has ended, it is worthwhile to conduct a detailed review of the events to draw lessons for the future.

Properly implemented crisis management will not only help minimize losses but also build the organization's position as a leader in information security. This translates into trust among customers and colleagues, which is invaluable in today's rapidly changing digital environment. A more detailed presentation of each phase, adopted for further consideration, is as follows:

1. Preparation includes the following activities:

[7] https://excelraport.pl/index.php/2024/09/23/zarzadzanie-kryzysowe-w-cyberbezpieczenstwie-co-warto-wiedziec/ [access 20.11.2025].

- Developing policies and procedures – creating documentation that defines the rules of operation in crisis situations and the roles and responsibilities of team members;
- Training and exercises – regular training for employees to ensure they are aware of threats and know how to respond to incidents. Simulation exercises help to practically test plans;
- Risk management – assessing potential threats and assessing the risks associated with various cyberattack scenarios.

2. Detection includes the following actions:
- Monitoring and analysis – using network and system monitoring tools to detect suspicious activity. This may include IDS/IPS (Intrusion Detection/Prevention Systems), which help identify attacks;
- Data collection – analyzing logs and data from various sources (servers, applications, endpoints) to identify irregularities.

3. Response includes the following actions:
- Crisis response – taking rapid action to mitigate the effects of an incident, such as isolating infected systems or blocking network access;
- Communication – informing all stakeholders, including employees, customers, and the media, about the situation and the actions being taken.

4. Recovery includes the following activities:
- System restoration – the process of restoring data and systems to a normal state. This may include reinstalling software, restoring data from backups, and testing systems before restarting them;
- User Support – providing assistance to employees who may have difficulty returning to normal operations after an incident.

5. Post-Incident Analysis includes the following activities:
- Post-Mortem – conducting team meetings to discuss what happened, what actions were effective, and what could have been done better;
- Documentation – creating incident reports that provide detailed information about the incident and any conclusions drawn.

6. Improvement includes the following initiatives:
- Conclusions and Corrections – Based on post-incident analysis, changes to policies, procedures, and security tools are implemented;
- Education and Awareness – Continuing training and raising employee awareness of new threats and security best practices.

All of these phases are interconnected and should be part of a cyclical process that allows organizations to continuously improve their cybersecurity strategies. Effective crisis management not only mitigates the impact of incidents but also increases an organization's resilience to future threats.

Preparation phase in crisis management in cybersecurity

Given the growing number of cyber threats, adequate incident preparedness is becoming a key element of every organization's crisis management strategy. Before an incident occurs, it's crucial to identify critical assets and unusual points that could be potential attack targets. Creating an action plan that outlines steps to take in the event of an incident is the foundation of effective crisis management. Several key aspects should be considered as part of the preparation process:

- Risk Assessment – Regular audits and risk analyses help understand where the organization is most vulnerable to threats;
- Employee Training – Educating staff on security best practices, including phishing detection, is an essential element of incident protection;
- Communications Plan – Developing a crisis communication strategy that ensures transparency both internally and externally to manage information and minimize panic;
- Procedure Testing – Regular simulation exercises allow you to test the effectiveness of the action plan and its implementation in practice.

It's also worth investing in appropriate technologies that support attack protection. There are many tools available on the market that can help detect, respond, and monitor situations in real time:

- IDS/IPS Systems: Detecting and preventing network attacks;
- Vulnerability Analysis Software: Identifying weaknesses in IT systems;
- EDR Solutions: Monitoring and responding to threats on endpoint devices.

Creating a security culture is also crucial. When all team members are engaged in cybersecurity issues, the organization becomes a much more challenging target for potential attackers. Sharing responsibility for cybersecurity among all employees not only strengthens the organization's resilience but also engages the team in long-term data protection goals. By investing in education and security standards, it is possible not only to minimize the impact of potential attacks but also to build trust with customers and business partners. To increase the effectiveness of training, it is worth considering various methods of conducting it. Here are some examples:

- Webinars with experts – live meetings during which experts share their knowledge and experience;
- Attack simulations – practical exercises that allow employees to experience attack situations and learn effective defense strategies;
- Online courses – flexible programs that allow employees to learn at their convenience.

Given the growing threat of cyberattacks, risk analysis is becoming a key element of any cybersecurity crisis management plan. It allows organizations to effectively identify and assess potential threats, allowing them to better prepare for potential incidents. The basic stages of risk analysis can be divided into several key steps:

- Threat identification – understanding the vulnerabilities and weaknesses that cybercriminals can exploit;
- Impact assessment – analyzing the possible consequences of attackers' actions on the organization;
- Determining the likelihood of occurrence – estimating the likelihood of specific threats based on current trends;
- Developing a risk management strategy – creating contingency plans and security policies.

Implementing effective countermeasures based on risk analysis can yield numerous benefits:

- Minimizing damage – with appropriate preparations, organizations can reduce the impact of potential attacks;
- Resource optimization – by analyzing risk, security budgets can be better allocated;

– Building trust – customers and business partners will gain greater confidence that their data is properly protected.

All these actions, based on appropriate risk analysis, not only allow for the development of a stronger security infrastructure but also provide a foundation upon which further crisis management activities can be based. Good planning begins with long-term analysis and pre-natal preparation for future challenges, which provides hope for effective combating of cyber threats. Integrating IT teams with external experts becomes especially important in the face of dynamic threats. These specialists can offer a fresh perspective and access to advanced tools and technologies that can significantly increase an organization's resilience to cyberattacks. This collaboration not only increases the chances of successfully resolving crises but also fosters an atmosphere of trust and support. The ultimate goal is not only to defend against threats but also to build a security culture that grows stronger with each interaction.

Detection phase in cybersecurity crisis management

Early detection of cyber threats is a key element of effective crisis management. With the right tools and procedures, organizations can identify potential threats before they escalate into serious incidents. Several key aspects of this strategy are worth noting:

– Real-time response – thanks to advanced monitoring systems and data analysis, companies can immediately react to unusual behavior, significantly reducing potential losses;
– Security enhancement – regular threat analysis allows for the adjustment of security measures, ultimately leading to maintaining a high level of cybersecurity;
– Employee education – training the team in identifying suspicious activities and implementing best practices in IT security is crucial.

Proper use of tools (SIEM, IDS/IPS, antivirus) and early threat detection strategies allows not only to minimize risk but also to build trust among customers and business partners. Organizations that demonstrate a proactive approach to cybersecurity are better able to adapt to the changing threat landscape, which translates into their long-term success. A wide range of tools enables not only threat identification but also analysis and rapid response. Thanks to these technologies, organizations can manage risk more effectively. Key technological solutions in this area include:

– Multi-layered detection systems – the use of advanced algorithms that analyze network traffic allows for the identification of suspicious behavior in real time;
– Artificial intelligence (AI) – the use of AI in data analysis enables the prediction and identification of new threats based on previous attacks;
– Cloud data analysis – collecting and processing data on cloud platforms provides quick access to information and increases collaboration between teams.

It is also worth noting the importance of automation, which allows for:

– Accelerated response – automatic detection and classification of incidents minimizes response time to threats;
– Resource savings – automation allows security teams to focus on more complex issues, increasing operational efficiency.

Investing in monitoring technologies can be crucial to building a stronger security infrastructure. To minimize risk, organizations should continually update their systems and procedures to ensure they are not only effective but also resilient to critical threats.

Response phase in cybersecurity crisis management

Effective cybersecurity crisis management requires not only a rapid incident response but also preparation. A key element is the creation and implementation of a contingency plan. Here are some important steps that can help transform a crisis into a learning and development opportunity:

- Risk assessment – regularly analyzing the vulnerabilities of systems and data and identifying potential threats;
- Employee training – raising team awareness of cyber threats and implementing incident response procedures;
- Contingency plan testing – conducting cyberattack simulations to assess the effectiveness of procedures and the team's capabilities in a crisis;
- Technical support – maintaining contacts with cybersecurity experts who can assist in emergencies.

When an incident occurs, it's crucial to maintain composure and focus on rapid action. It's important to implement the following principles:

- Incident Identification – quickly determining the source of the threat and the scope of the problem;
- Crisis Communication – informing relevant stakeholders and, if necessary, customers about the situation and actions being taken;
- Patching and Restoration – quickly taking corrective action and restoring systems to normal operating condition.

In any crisis, regardless of its source, communication plays a key role in managing recovery processes. In the context of cybersecurity, clear and effective communication can determine the future fate of an organization. Properly constructed communication not only builds trust but also mobilizes resources for a rapid response. In the case of cyber incidents, the following elements become particularly important:

- Transparency – it is crucial that stakeholders, including employees and customers, are kept up-to-date on the situation and actions being taken to resolve the problem;
- Timeliness – a rapid response to incidents increases the chances of minimizing losses. Delays in communication can lead to speculation and uncertainty;
- Consistency – all messages should be consistent with the previously established strategy and avoid conflicting information that can cause confusion.

Every organization can benefit from proven strategies that will strengthen its resilience to cybersecurity threats and, most importantly, maintain trust with customers and partners. Documenting and reporting incidents are essential elements of cybersecurity crisis management. Properly executed, they can significantly impact response effectiveness and future learning. There are several key steps to consider in this process:

- Incident Identification – The first step is to detect and precisely define the nature of the incident. It is important to gather as much information as possible at this stage to allow for further analysis;
- Incident Categorization – Once the incident is identified, it should be categorized according to its impact on the organization and risk level to tailor remediation actions accordingly;
- Documentation of Events – All relevant details should be carefully documented, including the time of the incident, the individuals involved, and the measures taken in response. This will facilitate subsequent analysis;
- Damage assessment – Assessing the potential damage, both financial and reputational, to the organization is an important step. This will help formulate a strategy for further action;
- Report development – Based on the collected data, a detailed report should be created, containing all key information and recommendations for preventing similar incidents in the future.

It's worth emphasizing that documentation and reporting should be considered an integral part of organizational culture. Regular training and simulations can significantly impact a team's preparedness to effectively respond to incidents. By fostering a proactive approach, organizations can not only minimize negative impacts but also learn from mistakes, which contributes to increased security in the long run.

Recovery phase in cybersecurity crisis management

After a cyberattack, proper preparation and swift action are key to increasing the chances of fully restoring system functionality. Every organization should have a developed action plan to minimize damage and restore normalcy as quickly as possible. It's worth focusing on several key aspects:

- Situation Assessment – Immediately after an incident, the security team should thoroughly assess its scale and nature. It is essential to understand which systems were affected and what data may have been compromised;
- System Isolation – It is important to isolate compromised systems from the rest of the infrastructure to prevent further spread of the threat. This may include disconnecting them from the network, shutting down servers, or locking user accounts;
- Data Recovery – In the event of data loss, using backups is crucial. Regular data backups allow for rapid recovery and minimize operational downtime;
- Threat Remediation – Once the source of the attack is identified, a thorough malware scan should be conducted. Using appropriate threat remediation tools is essential to restoring system security;
- Monitoring and Analysis – After remediation is complete, it is important to implement close system monitoring to detect any suspicious activity. Analyzing the root causes of the attack will help adapt the preventative strategy.

Maintaining organizational business continuity after an incident occurs is crucial. This requires a thoughtful approach and the implementation of effective strategies. In the face of cybersecurity incidents, it is crucial to ensure that the company can continue its operations while minimizing losses and downtime. To effectively manage business continuity in the context of cyberthreats, it is worth implementing the following steps:

- Risk analysis – identifying potential threats and their impact on the company's operations;
- Contingency plan – developing a detailed incident response plan that defines procedures and responsibilities;
- Employee training – conducting regular cybersecurity training to increase team awareness and preparedness;
- Plan testing – conducting incident simulations to help verify the effectiveness of the contingency plan;
- Procedure updating – regularly reviewing and updating procedures in response to changing threats.

Establishing an appropriate IT infrastructure that allows for rapid recovery after an attack is also crucial:

- Data Backup: Regular data backups that can be quickly restored in the event of an attack;
- System Monitoring: Implementation of monitoring systems that detect irregularities and activities in real time;
- Network Resilience: Use of cloud solutions and redundancy to minimize the risk of downtime.

With proper preparation and strategic planning, organizations can not only survive cybersecurity incidents but also emerge stronger and more resilient. Transparency in operations and communication with stakeholders can significantly support the recovery process in the face of crisis.

Post-incident analysis phase in cybersecurity crisis management

The post-incident analysis phase is a key element of comprehensive cybersecurity crisis management, providing a structured approach to understanding what happened, why it happened, and how to strengthen defenses. The goal of this phase is to uncover the root causes of a cybersecurity breach, assess the effectiveness of incident response actions, and implement lessons learned to increase resilience. As cyberattacks become more complex, organizations that neglect this reflective process risk recurring security vulnerabilities and a loss of stakeholder trust. Therefore, a detailed, methodical post-incident analysis is essential to strengthening an organization's cybersecurity posture and ensuring continuous improvement of incident management protocols.

The primary goals of the post-incident analysis phase are focused on gaining a comprehensive understanding of the breach and its consequences. Identifying the root causes of a cybersecurity incident is crucial; this includes tracing the attack vector, pinpointing the vulnerabilities exploited, and understanding the motivations behind the breach. For example, investigating whether the attack was the result of outdated software, weak passwords, or social engineering tactics helps organizations address specific vulnerabilities. Furthermore, assessing the effectiveness of incident response actions is crucial. This includes verifying whether detection mechanisms were timely, response actions were appropriate, and communication channels were functioning efficiently. An incident in which an organization only detects the breach after a significant delay highlights the importance of rapid detection and response protocols.

Furthermore, lessons learned from each incident form the basis for process improvements, such as refining incident response plans, updating security controls, or enhancing employee awareness training. The ultimate goal is to translate analysis findings into concrete actions that reduce the likelihood of similar incidents occurring and thus strengthen a proactive security culture. Effective post-incident analysis relies on a number of key components and systematic processes that ensure thorough investigation. Data collection and evidence retention are fundamental, especially when forensic analysis is required; organizations must secure logs, network traffic captures, and infected files to ensure their integrity for legal and investigative purposes. For example, using write-locks during data collection prevents the modification of digital evidence.

Incident documentation is equally important, including creating detailed timelines that chronologically track the attack and conducting impact assessments to quantify operational, financial, and reputational losses. Documenting these elements not only aids in understanding the situation but also provides crucial information for legal proceedings or insurance claims. Techniques such as fault tree analysis or Ishikawa diagrams can be used to identify the root cause. These tools facilitate structured exploration of potential causes by breaking complex incidents into manageable components, revealing hidden vulnerabilities or process errors. For example, an Ishikawa diagram can illustrate how technical flaws, human errors, and procedural gaps all contributed to a breach, enabling targeted corrective action[8]. Despite the critical importance of post-incident analysis, organizations face numerous challenges that can hinder comprehensive review. One significant obstacle is overcoming delays in documenting incident detection and response, which can result in incomplete data and hinder accurate analysis. For example, if a breach goes undetected for weeks, crucial evidence may be lost or compromised, making it difficult to accurately reconstruct the attack timeline. Furthermore, maintaining objectivity and accuracy can be difficult when organizations are under pressure to resume normal operations or protect their reputation. When management prioritizes rapid recovery over detailed investigation, analysis can be superficial, leaving hidden vulnerabilities unaddressed. To address these challenges, best practices include implementing automated tools that streamline data collection and threat detection, such as security information and event management (SIEM) systems, which provide real-time insights and reduce manual effort. Integrating threat intelligence improves contextual understanding of attacks, enabling analysts to identify emerging tactics and adapt defenses accordingly. Furthermore, fostering an organizational culture that values transparency and continuous learning fosters honest assessment and open communication during post-incident reviews, ultimately leading to more effective and actionable conclusions. Crisis response plans should also incorporate post-incident reviews to help understand what went well and what needs improvement.

Media monitoring and public opinion analysis are also crucial elements of reputation management. Regularly examining company mentions online and in traditional media allows for early detection of potential problems and rapid response.

[8] https://inzynierjakosci.pl/2017/12/diagram-ishikawy/, (access 21.11.2025).

Cybersecurity crisis management improvement phase

Education about potential cybersecurity threats is crucial for effective crisis management. In today's complex world of information technology, the risk of cyberattacks affects not only companies but also individual users. Proper preparation for potential incidents can significantly improve network security. Educational activities that should be implemented include:

- Employee training – regular courses and workshops related to threat recognition;
- Technology use guidelines – principles for safe use of the internet, email, and social media;
- Attack simulations – exercises that help understand how a cyberattack works and its consequences.

Building public awareness through various communication channels is crucial. In this context, it's worth emphasizing the importance of:

- Social media – the rapid and widespread reach of information allows for ongoing information about threats;
- Educational portals – websites offering resources and tools for learning about cybersecurity;
- Collaboration with non-profit organizations – initiatives to increase awareness of threats among various social groups.

Testing and simulations play a key role in effective crisis management, particularly in the area of cybersecurity. Conducting regular simulations allows organizations to better prepare for potential threats and incidents, which translates into longer-term resilience. In this context, several important aspects are worth noting:

- Scenario realism – creating scenarios that are realistic and likely to occur allows teams to train in situations that are close to real-world situations, increasing their preparedness for real-world challenges;
- Evaluating the effectiveness of operations – simulations enable the assessment of current crisis management procedures, identifying strengths and weaknesses. This allows the organization to make necessary adjustments;
- Increasing awareness – conducting tests increases team awareness of potential threats and reinforces the importance of adhering to security policies;
- Team as a foundation – joint exercises help build team synergy and a better understanding of team members' roles and responsibilities during crises.

Investments in modern technologies are a key element of security strategies, especially in the area of cybersecurity. Rapid technological development and growing online threats force companies to adapt their approach to risk management. Properly allocating resources to innovative solutions can not only minimize the consequences of potential attacks but also contribute to the long-term success of the company. It's also worth considering how technology investments impact a company's competitiveness. Organizations that utilize modern solutions can gain an advantage over their market rivals, attracting the attention of customers and business partners. Ultimately, appropriate investments in technology not only build an organization's resilience to cyber threats but also foster an atmosphere of trust among customers and colleagues.

In the long run, this can lead to the development of innovative products and services that meet market expectations and increase customer satisfaction.

Summary

In general, cybersecurity crisis management can be divided into several key phases that help effectively respond to incidents and minimize their impact. Preparation includes developing crisis management plans and procedures, as well as training personnel and testing security systems. Collaboration with other organizations and institutions to exchange information about threats is also crucial. Detection is the result of monitoring systems to identify potential threats and incidents. It requires the use of analytical tools to analyze data and detect anomalies. Incident response is immediate action in response to an identified threat.

This involves isolating infected systems to prevent further spread of the threat. Communication with stakeholders, including employees, customers, and the media, is crucial here. Recovery activities then follow, which involve restoring systems to a normal state after the incident and analyzing the incident to understand its causes and effects. Following an incident, the effectiveness of the actions taken in response to the crisis must be assessed, as well as lessons learned to improve future responses. Finally, refinement involves implementing changes to strategies and procedures based on the findings from the post-incident analysis. Continuous improvement of crisis management plans and security systems remains crucial.

Literature

Bartock M., Cichonski J., Souppaya M., NIST Special Publication 800-184, Guide for Cybersecurity Event Recovery, U.S. Department of Commerce 2016.

Borky J., Bradley T., Protecting Information with Cybersecurity, „Effective Model-Based Systems Engineering” 2018, Sep 9.

Czuryk M., Zarządzanie kryzysowe w obszarze cyberbezpieczeństwa, „Ius et Securitas” 2025, no. 1.

Diagram Ishikawy, https://inzynierjakosci.pl/2017/12/diagram-ishikawy/.

Karpiuk M., Pizło W., Kaczmarek K., Cybersecurity Management – Current State and Directions of Change, „International Journal of Legal Studies” 2023, no 2.

Zarządzanie kryzysowe w cyberbezpieczeństwie, https://excelraport.pl/index.php/ 2024 /09/23/zarzadzanie-kryzysowe-w-cyberbezpieczenstwie-co-warto-wiedziec/

Act of 26 April 2007 on Crisis Management (Journal of Laws of 2023, item 122).

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (OJ EU 2022 L 33, p. 80), hereinafter referred to as the NIS 2 Directive.