# Table of Contents

**1 Summary** ........ 2

**2 Introduction** ........ 2

**3 Business Impact Analysis (BIA)** ........ 3

**3.1 Context: Assets, Data (PII/SPII), and Threat Landscape.** ........ 3

**3.2 Identification of Critical Business Functions.** ........ 4

**3.3 Analysis of Potential Business Impacts.** ........ 5

**3.4 Prioritization of Functions & Recovery Objectives (RTO, RPO).** ........ 5

**3.5 Relevant Data and Frameworks** ........ 6

**4 Incident Response Plan (IRP) based on the ransomware threat.** ........ 7

**4.1 Preparation.** ........ 7

**4.2 Detection and Analysis.** ........ 10

**4.3 Containment and Eradication. Recovery.** ........ 11

**4.4 Post-incident activity.** ........ 12

**5 Disaster Recovery Plan (DRP)** ........ 12

**5.1 Backup Strategy** ........ 12

**5.2 Recovery Strategy** ........ 13

**5.3 Testing and Validation of DRP** ........ 13

**5.4 Post-Recovery Actions and Improvements** ........ 13

**6 Information Security Best Practices** ........ 14

**References** ........ 14

# 1 Summary

Any cyber incidents, regardless of the cause of their occurrence in the context of ShopSmart Ltd., must be documented and controlled. Proactive preparation provides the best results in counteracting threats, allows to continue business processes and not to lose financial resources. Since ShopSmart Ltd. has a significant growth, an increase in the number of customers, and, accordingly, their trust, it is necessary to ensure the required level of cybersecurity protection of the company. A particular focus of this documentation is on the threat of ransomware, as it has proven to have a negative impact on the company's operations in the event of an incident. Therefore, this report is a planning document to improve the current protection of the company's operational processes from interruption, specifically addressing such critical points as: Business Impact Analysis (BIA), Incident Response Plan (IRP) based on the ransomware threat and Disaster Recovery Plan (DRP).

# 2 Introduction

The e-commerce sector in which the company operates faces a number of cyber threats that are constantly evolving and increasing due to the constant change in technology, including the impact of AI. Therefore, ensuring the security of the company's main assets, the sensitive information it receives, processes, stores, and transmits are important tasks that can determine the company's success. It is important to emphasize that since the company operates within the European Union, it is necessary to comply with a number of important regulations and standards, the main one is GDPR. The ransomware threats that the company has already faced are also regulated by the GDPR standard, so undoubtedly this plan requires significant emphasis from the steering committee. Therefore, this plan is designed to offer a comprehensive solution for ShopSmart Ltd to prepare for and recover from incidents, details of these operations and the persons responsible for these activities.
Among the list of threats that are particularly relevant to the e-commerce sector are ('Top 10 E-commerce Security Threats & Their Detailed Solution' 2025):

- Ransomware.
- Supply Chain and Third-Party Attacks.
- Distributed Denial of Service (DDoS).
- Phishing and Social Engineering.
- E-skimming.
- Credential stuffing and Account Takeover (ATO).
- Exploitation of Known Vulnerabilities (SQL injection, XSS and others).

Consequently, it can be argued that the number of threats relevant to e-commerce is quite large, so it should be emphasized that this area is one of the most popular areas for ransomware attacks, so it can be assumed that similar attacks like the one the company has already encountered may continue in the future. Therefore, the company should be prepared for cyber resilience ('Top 10 Major Cyber Attacks Targeting E-Commerce Industry' 2024).

# 3 Business Impact Analysis (BIA)

Business impact analysis is a process that should link each system involved in business operations to the critical functions it provides. This process is fundamental in terms of planning and taking into account emergencies such as incidents, etc. Therefore, BIA helps to identify the consequences if important systems and processes are disrupted, thereby prioritizing system elements and their impact on business continuity, which is particularly important in forming a recovery strategy and resource allocation (‘What is Business Impact Analysis?’ 2025).

## 3.1 Context: Assets, Data (PII/SPII), and Threat Landscape.

For an effective contingency plan, it is necessary to emphasize the organizational context of ShopSmart Ltd. The company operates in the European Economic Area and must comply with the following regulations: Payment Services Directive (PSD2), PCI DSS, GDPR and others. To improve the understanding of the current state of the organization, it is worth referring to the NIST CSF Maturity Model. Given that ISM practices are not yet finalized and continue to be modernized at the time of writing this report, as well as the presence of attacks that were not prevented in time, it can be assumed that the company is in a transitional phase between the initial stage (1) and development (level 2). The visualization is shown in Figure 1 (cinchws 2022).

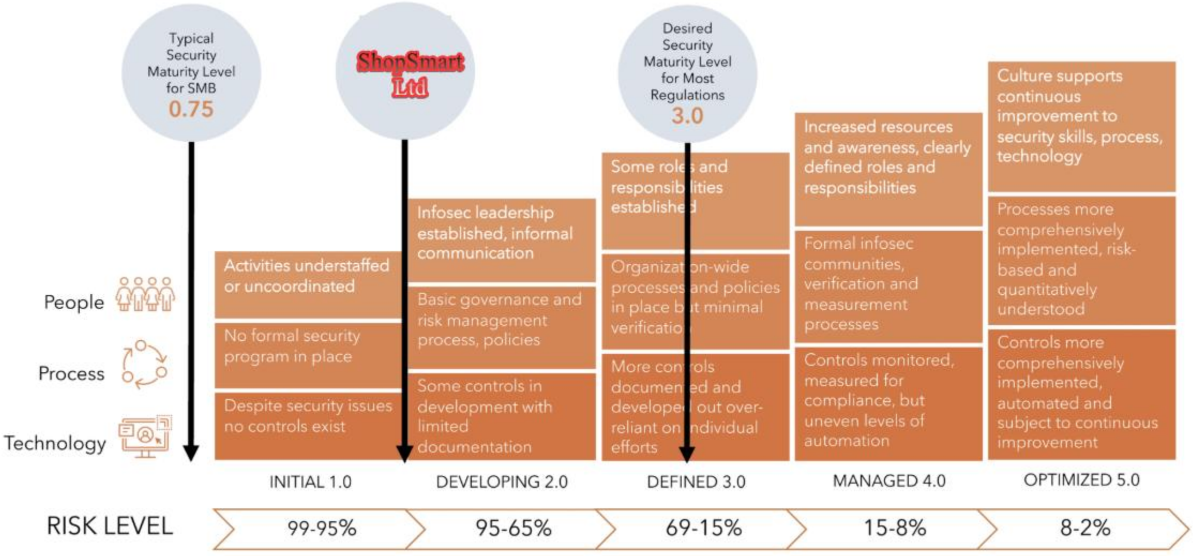
Typical Security Maturity Level for SMB
0.75
ShopSmart Ltd
Desired Security Maturity Level for Most Regulations
3.0
People
Process
Technology
Activities understaffed or uncoordinated
No formal security program in place
Despite security issues no controls exist
Infosec leadership established, informal communication
Basic governance and risk management process, policies
Some controls in development with limited documentation
Some role and responsib lities establishe
Organizat on-wide processes and policies in place b t minimal verificatio
More con rols documen ed and develope out over-reliant on ndividual efforts
Increased resources and awareness, clearly defined roles and responsibilities
Formal infosec communities, verification and measurement processes
Controls monitored, measured for compliance, but uneven levels of automation
Culture supports continuous improvement to security skills, process, technology
Processes more comprehensively implemented, risk-based and quantitatively understood
Controls more comprehensively implemented, automated and subject to continuous improvement
INITIAL 1.0
DEVELOPING 2.0
DEFINED 3.0
MANAGED 4.0
OPTIMIZED 5.0
RISK LEVEL
99-95%
95-65%
69-15%
15-8%
8-2%

Figure 1 The company is moving to improve the maturity of cyber security protection.

**Assets**. Knowing what assets the business operates with is essential to identifying potential targets for attack. The company heavily relies on digital infrastructure, including the website and application, databases with information necessary for order processing and business operations, gateways for processing electronic payments, customer communication tools, and data stored on a cloud service, as well as software including a CRM system for employee performance and an ERP system for financial tasks and product inventory. The company's assets also include the physical equipment of all departments, such as computers, laptops, etc. and network equipment.

**Data**. It should be emphasized that ShopSmart Ltd. processes large amounts of personal information (PII) on a daily basis, including the following: physical and email addresses, phone numbers, first and last names, and card financial information. It is worth noting that some of this data can be characterized as particularly sensitive (SPII) and, accordingly, must be reliably protected at all stages of interaction with it. Among other data, the company also processes operational data, including inventory, logistics information, and details of employees, business partners, and suppliers (‘PII (Personally Identifiable Information): E-Commerce Explained’ 2025).

**Threat Landscape.** Due to the dynamic nature of the business and data companies operate with, the retail sector and business services are among the most popular targets of ransomware attacks in 2023 and 2024, according to Cyberint (Duran 2025). The visualization is presented in Figure 2.

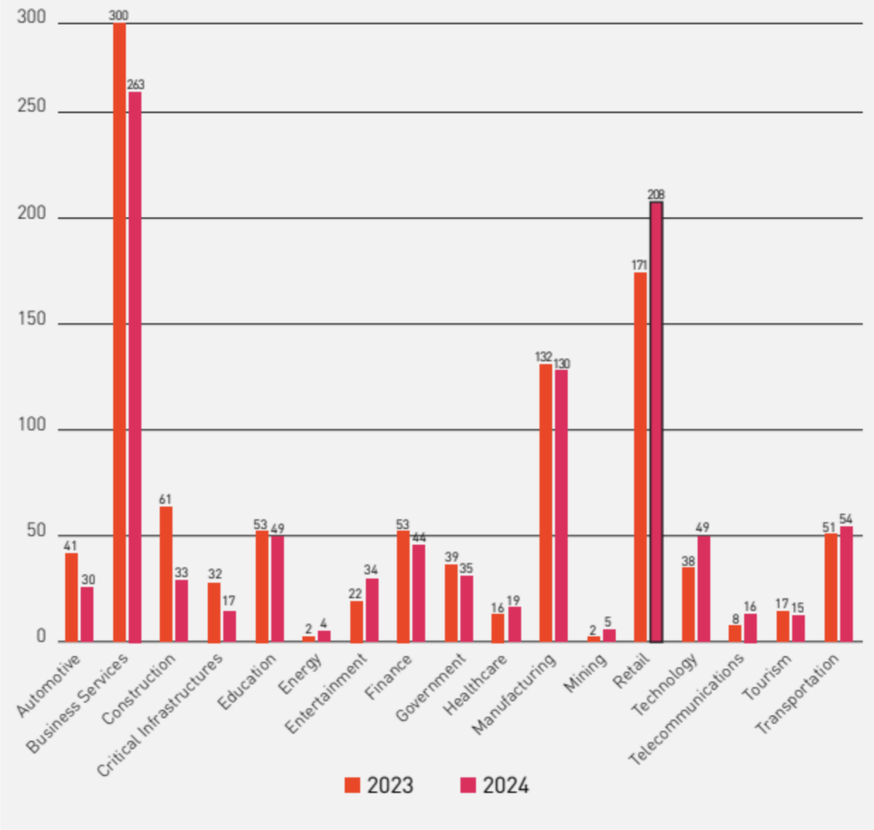

Figure 2 Targets of ransomware attacks in 2023 and 2024

Therefore, the risks of ransomware threats in 2025 for the e-commerce sector can be assessed as very high, with a high impact, which leads to the focus on ransomware threats as one of the main threats for which protection and recovery procedures should be provided. Among other threats, DDoS attacks can be expected as well, which can often be caused by the consequences of competitors' actions. Attacks on the company's website and or application are also possible (such as XSS, SQL injection and other CVE exploits) - since this is the first point of contact between the company and its customers, it can be expected that attackers will want to attack it.

### 3.2 Identification of Critical Business Functions.

Since ShopSmart Ltd has a clearly defined business niche and model, the following functions are crucial to the company's operation (Deepika 2022):

- Functioning of the main web sales platform - support of the application or the main website for the process of receiving orders from customers.
- Payment processing - which involves the secure processing of all transactions that take place within the company.
- Order fulfillment - management of orders from customers, data related to these orders, logistics control, etc.
- Customer data management - involves the secure management of data, including PII and SPII.

- ERP system operation - tracking the movement of products within the company and business partners, tracking the availability of product stocks, and entering and reading other operational data (e.g., payment status, etc.).
- Service Desk - customer support, in particular in case of problems, questions about the product, warranty claims, etc.
- CRM system operation - tracking metrics and key parameters of staff performance, plan implementation, and compliance with standardized work processes (ticketing is a system for sales).
- Network infrastructure - access of all employees to all necessary tools and data within the office and cloud environment.

## 3.3 Analysis of Potential Business Impacts.

Disruption of any of the business functions described above could have the following serious consequences.

**Financial potential impact.**

- Direct loss of sales revenue during the downtime.
- Costs incurred in responding to and recovering from the incident (including hiring external experts or overtime).
- Potential ransom payments in the case of ransomware (not recommended).
- Fines due to regulations - GDPR and other standards.
- Increased cost of business insurance as a result of serious business interruption.

**Operational implications.**

- Inability to process customer orders.
- Delays and deviations from the normal work schedule, and, accordingly, logistical delays in the delivery of goods to the final recipient.
- Errors in the calculation of products, and potential discrepancies in the quantity of goods in fact and in the system (especially important if there is still a physical store).
- Loss of process control and access to key metrics in the CRM system.
- The need for urgent redistribution of human resources with the risks of overtime and a reduction in the level of working atmosphere.

**Reputational losses.**

- Potential loss of a significant number of customers in case of interrupted delivery times or customer data leakage.
- Potential negative PR in social media or news.
- Deterioration of the company's image.
- Reduced ability to grow and acquire new customers

## 3.4 Prioritization of Functions & Recovery Objectives (RTO, RPO).

Given the potential impact, critical business functions should be prioritized for recovery. To ensure transparency in controlling these processes, Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) should be used (‘BIA Business Impact Analysis: Tutorial & Best Practices’ 2025).It should be noted that these indicators should be set within balanced, clear limits, failure to comply with them may lead to the uncontrollability of the process. An example of the boundaries is shown in Figure 3 (‘Establishing RPO and RTO Targets for Cloud Applications | AWS Cloud Operations Blog’ 2022).

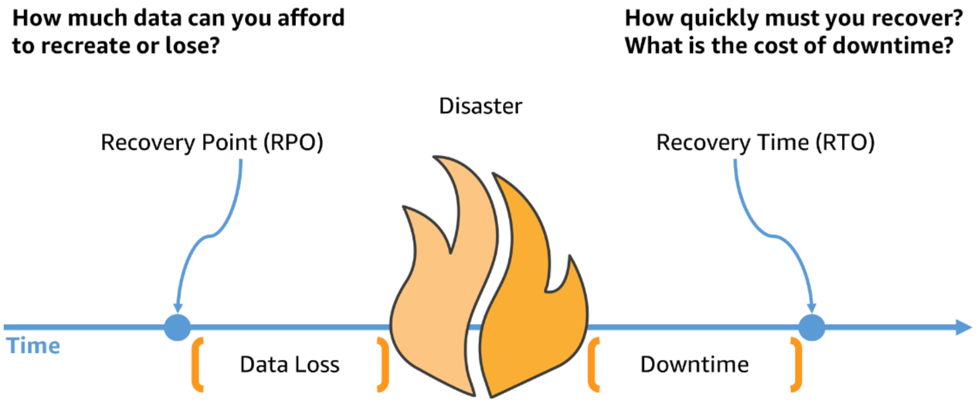
How much data can you afford to recreate or lose?
How quickly must you recover? What is the cost of downtime?
Disaster
Recovery Point (RPO)
Recovery Time (RTO)
Time
Data Loss
Downtime

Figure 3 RPO and RTO limits ('Establishing RPO and RTO Targets for Cloud Applications | AWS Cloud Operations Blog' 2022)

**The following prioritization** is suggested:

1. The application and website for online sales, payments and transaction processing is the highest priority.
2. Handling orders and internal databases, in particular with PII and SPII, is also a high priority as it is critical for many tasks.
3. ERP system
4. CRM system and order logistics coordination.
5. Service desk
6. Other functions

**The Recovery Time Objective (RTO)** metric defines the maximum allowable period during which a feature can be unavailable to the business. Examples of RTOs for ShopSmart are (data to be confirmed with the governance team) :

- The main online sales platform as well as the application: up to 1-4 hours.
- Order processing and database: up to 4-8 hours.
- ERP or CRM systems: up to 8-12 hours Service desk: up to 24 hours.

**Recovery Point Objective (RPO)** is a metric that defines the maximum acceptable amount of data loss measured over time. Examples of RPOs in the context of ShopSmart Ltd. are (exact numbers need to be agreed with the governance team):

- Transaction data from customers - as close to real-time as possible up to 15-30 minutes (depending on the method).
- Customer database updates: less than 1 hour.
- ERP system data updates: up to 1-2 hours.
- Website content (prices, product availability, etc.): up to 10 minutes.

## 3.5 Relevant Data and Frameworks

The BIA covers a variety of data needed to identify critical functions, assess impact, and set RTOs and RPOs. All these data are necessary input parameters for the development of a proper Incident Response Plan (IRP) and Disaster Recovery Plan (DRP). The described BIA aligns with the requirements and principles described by NIST, in particular, NIST SP 800-34, which is responsible for Contingency Planning (Swanson *et al.* 2010). Also, the described points correspond to the ISO 27001 standard, which is used in the European Union.

# 4 Incident Response Plan (IRP) based on the ransomware threat.

This section describes a plan for responding to incidents using a CSIRT (Computer Security Incident Response Team) structure (‘NCSC: CSIRT-IE’ 2025). It is expected to use the NIST SP 800-61 framework, in particular, proactive measures, policy development, use of tools - SIEM and EDR, training sessions, etc. NIST identifies 4 key phases in the incident response procedure, as shown in Figure 4.

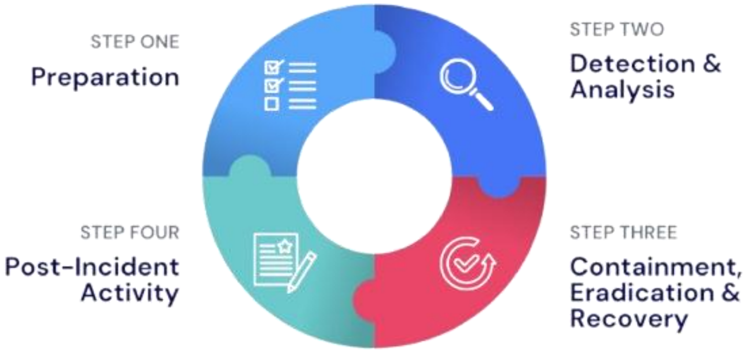

Figure 4 The NIST incident response life cycle (‘What is Incident Response?’ 2023)

## 4.1 Preparation.

The success of an incident response is directly proportional to the quality of the preparation phase, as balanced actions, clear procedures and reporting lead to predictable results. The main goal of the preparation phase is to create a controlled environment during the incident itself. This phase is especially important for such a threat as ransomware, as in this case, the speed of response can determine the percentage of infrastructure that will be infected, as well as the likely impact of the attack on backup data that should not be available to attackers in any case. It is important to understand that all strategies and techniques that will be implemented during the preparation phase of an incident can potentially be known to attackers, so it is important to include a cybersecurity awareness program for all personnel as part of proactive measures. For the incident response team, it is imperative to include the study of MITRE's ransomware attack techniques. In particular, one of the key techniques is T1490 Inhibit System Recovery, which essentially consists of encrypting the company's backup data and or modification of backup tools, therefore leaving the company no chance to quickly restore data and, accordingly, business processes (‘Inhibit System Recovery, Technique T1490 - Enterprise | MITRE ATT&CK®’ 2025). The documentary part of the preparation phase is also necessary and consists of creating and adjusting documentation as necessary. It includes, in particular, an Incident Response Policy that regulates the tactical and strategic attitude to incidents, while an Incident Response Plan defines specific actions to be taken. Since the company can scale and change the business context, it is important to have a strategic documented vision of what to do in the event of an incident. As for the procedures, it is worth emphasizing the need to have designated rooms for communication (or a dedicated online platform) in the event of an incident, and a storage facility for evidence. It is necessary to ensure the availability of backup resources for the incident - hot site, clean system images, and cloud solutions.

**Roles and Responsibilities. CSIRT.** A critical step in the preparation phase is to form a response team (CSIRT) in advance and to have a clear division of responsibilities. This group is key to the response to an incident. It is also important to note that the main responsibilities of the team are incident management, but as noted earlier, it is important to follow proactive protection. Thus, special attention is given to the first phase according to NIST, the team's tasks are shown in Figure 5 (‘Guidebook_for_new_CSIRT_employees_EN_09032023.pdf’ n.d.).

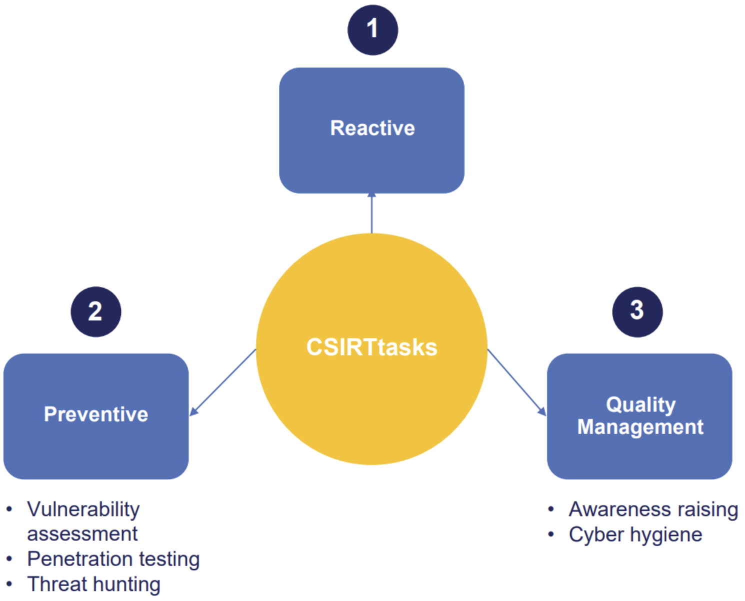

Figure 5 CSIRT tasks.

Various models can be considered, and a hybrid model is suggested as having a balanced approach in terms of cost and effectiveness (‘What is a CSIRT (Computer Security Incident Response Team)?’ 2025).The breakdown of the structure and role of the response team in case of the ransomware attack is shown in Table 1.

| Role | Responsibilities during a ransomware incident | ShopSmart employee or External partner. |
|---|---|---|
| Incident Manager | Coordination, decision-making (including analysis of buyout decisions), resource allocation, communication with management and stakeholders, and ensuring plan adherence. | CISO or CIO |
| Technical Lead | Leading technical analysis (root causes, strain of ransomware), managing containment/eradication activities, overseeing the technical team, and providing technical updates. | CTO, CISO. |
| Security Analysis | Initial alert triage, logs/monitoring tools (SIEM/EDR), incident classification, evidence collection, threat analysis, and technical lead support. | Security Analyst |
| Forensics Specialist | Collecting, preserving (chain of custody), analyzing digital evidence (images, memory); data | External Partner |

|  |  |  |
|---|---|---|
|  | recovery; supporting investigations. |  |
| Communications Lead | Manage internal/external communications (to stakeholders, business partners, regulators, media); | PR |
| Legal Specialist | Advising on legal/regulatory obligations (GDPR and others), legal liability, handling of evidence, legality of ransom payments, and analysis of communications. | External Partner |
| Awareness program | Introducing awareness of the ransomware threat to employees at the stage of preparation for an incident | SAO, CISO. |
| IT Operations | Provides technical response (isolation, remediation, restoration from backup), access to the system/network and information, and communication with IT teams. | IT operations staff, system and network administrators |
| Executive management | Provides strategic guidance, approves major decisions, and supports the CSIRT. | CEO or board members |

Table 1 Roles and responsibilities

A visual representation of the command is shown in Figure 6.

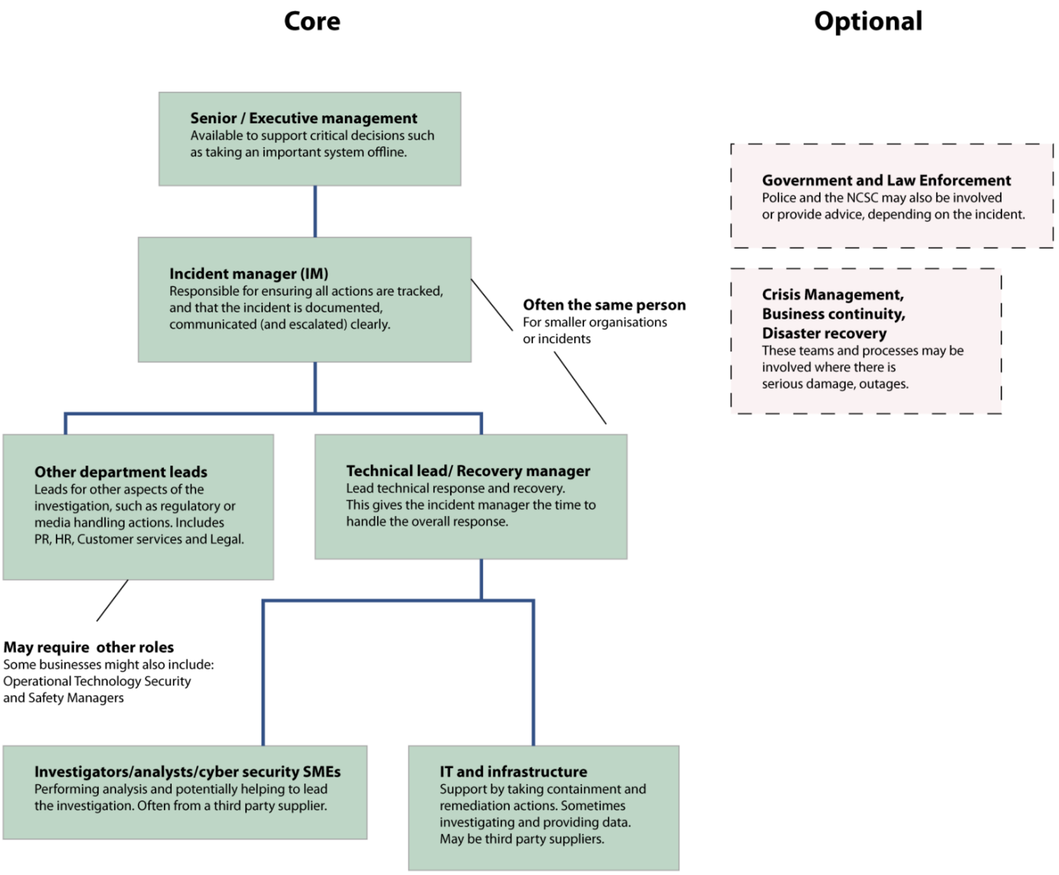
Core
Optional
Senior / Executive management
Available to support critical decisions such as taking an important system offline.
Incident manager (IM)
Responsible for ensuring all actions are tracked, and that the incident is documented, communicated (and escalated) clearly.
Often the same person
For smaller organisations or incidents
Other department leads
Leads for other aspects of the investigation, such as regulatory or media handling actions. Includes PR, HR, Customer services and Legal.
Technical lead/ Recovery manager
Lead technical response and recovery. This gives the incident manager the time to handle the overall response.
May require other roles
Some businesses might also include: Operational Technology Security and Safety Managers
Investigators/analysts/cyber security SMEs
Performing analysis and potentially helping to lead the investigation. Often from a third party supplier.
IT and infrastructure
Support by taking containment and remediation actions. Sometimes investigating and providing data. May be third party suppliers.
Government and Law Enforcement
Police and the NCSC may also be involved or provide advice, depending on the incident.
Crisis Management, Business continuity, Disaster recovery
These teams and processes may be involved where there is serious damage, outages.

Figure 6 CSIRT team (‘Build: A cyber security incident response team (CSIRT)’ 2025)

**Communication Plan.** To ensure clear interaction between all members of the response team and other employees, the following communication is suggested.

- CSIRT: Use secure primary and backup channels (e.g., chat, phone). Update information and make calls regularly.
- Employees: Share clear, relevant information through the primary or, if unavailable, an established backup communication channel. Consult on safe actions as needed. Direct media to the Communications Manager. In case of any In the event of any signs of a ransomware attack, immediately notify the cybersecurity analyst, whether or not the current work task is in progress.
- Management: Provide regular updates on status, impact and key decisions.
- Affected individuals (customers): if disclosure and notification is required under the GDPR, inform them without undue delay, using plain language. It is necessary to explain the breach, the data involved, the likely consequences, the actions taken by ShopSmart, and recommendations. The channel should use available tools if they have not been compromised, including email and social media.

## 4.2 Detection and Analysis.

**Incident Detection.** Effective control of the consequences of incidents and their causes begins at the stage of early detection, as it is key to limiting the spread and impact of ransomware. Detection methods include the following options:

- Automated alerts: SIEM systems compare logs to detect suspicious encryption activities or known ransomware indicators;
- EDR notifications about malicious processes of various file modifications;
- Anti-virus program notifications to detect known malware signatures.

- Anomalies experienced by users: employees may report a lack of access to files or incorrect system operation, and a ransomware window may appear;
- CIT monitoring and resurfacing are allowed to detect IoC indicators associated with an attack, including ransomware. This step is valid as a detection when there are no direct notifications from company tools about the threat (which may indicate an attack right now).
- Security Analysts are responsible for analyzing information coming from SIEM, IDS, IPS, SOAR and WAF systems. False positive alerts must be recognized from true positive alerts in order to avoid initiating a false response to an incident and using CSIRT resources. In particular, such actions should be performed by analysing signatures.

**Escalation**. Confirmed incidents according to the attack and/or compromise indicators, according to the instructions, should be prioritized based on severity and impact (according to the BIA). A confirmed incident, in particular a ransomware attack that impacts critical business functions, requires immediate escalation to the full CSIRT as described in Table 1.

**Legal obligations.** The company has to notify users about data breaches and other issues that are stipulated by regulatory requirements within a specified period of time.

According to the GDPR, if personal data is compromised, i.e. accessed or leaked, the notification requirements apply within 72 hours. Notification of affected individuals without undue delay (‘Breach Notification | Data Protection Commission’ 2025).

The NIS2 Directive provides for an early warning within 24 hours of receiving the information and 72 hours of notification of the incident itself (‘NIS 2 Directive, Article 23: Reporting obligations’ 2025).

### 4.3 Containment and Eradication. Recovery.

In this phase, the main task is to localize the ransomware and prevent further encryption or lateral movement across the company's infrastructure. The speed of countermeasures is crucial, so it is necessary to act immediately, regardless of current business processes.

**Containment.**

- **Isolation** -Network isolation, which involves immediately disconnecting the affected devices (servers, workstations) from the network. If multiple systems are affected, the entire network segment must be shut down at the switch level. To coordinate actions, use mobile communication or a pre-agreed secure communication channel such as Signal.
- **Segmentation** - it is necessary to use topological solutions like existing network segmentation, such as virtual local area networks, to control the spread. If necessary, create temporary LANs.
- **Blocking C2 communication** - modify firewall rules to block traffic to detected ransomware servers.
- **Account deactivation** - disable user and service accounts that are found to be compromised or used for distribution.
- **Protect backups** - as mentioned earlier, this is one of the techniques of attackers, so ensure that backups are stored offline and are securely protected from attackers.

**Eradication.** It is necessary to remove all elements of the ransomware presence and any mechanisms for saving or reproduction.

- It is necessary to identify the strain and check the decryptors, analyze the records made by the ransomware and encrypted files to identify the type of program that attacks the company.

- It is essential to notify the law enforcement authorities of the local jurisdiction of the country where the company operates and, if necessary, request assistance in decrypting the data (if the company cannot solve this on its own, for example, it is an unknown new form of ransomware).
- Ransomware removal should be done with specialized tools, for example, Trend Micro, Thor Premium Home, Emsisoft, etc (‘Ransomware Removal: Is it Possible to Remove Ransomware?’ 2025).
- Eliminate the cause of the infection - it is necessary to accurately find and eliminate the primary factor of infection - it could be a phishing email to an employee, the use of CVEs, etc.

**System recovery** - in the case of heavily infected systems or if the process is too time-consuming, a simpler method may be to clean and fully restore the OS. Any return to the initial state of the network without localization and segmentation should be done only if there is confidence that the threat has been overcome and completely eradicated, so if in doubt, it is better to turn to OS recovery.

### 4.4 Post-incident activity.

After the incident is successfully resolved, steps should be taken to improve the work of the response team  for the future and to work on mistakes, in particular:

- Analyze the mistakes made and their causes.
- Document all actions taken and compare them with the original incident response plan.
- Write conclusions about the effectiveness of the documentation and propose changes (if necessary).
- Analyze the communication between the team members and propose changes if necessary.

## 5 Disaster Recovery Plan (DRP)

The Disaster Recovery Plan (DRP) provides for actions to be taken in the event of critical threats such as ransomware, and procedures for recovering IT systems and business functions (Editor 2025).

### 5.1 Backup Strategy

Efficiently executed backups are the key to countering ransomware (Bevin 2023).

- The frequency of backups is determined by the RPO defined in the BIA (as described in section 3.4).
- Data related to customer financial transactions should be copied in near real-time, especially during business hours when orders can be placed every minute.
- Less critical data (e.g., team performance indicators for one business day) can be backed up daily in the evening.
- A rule is to collect at least 3 copies of data on 2 or more types of media, with at least 1 copy stored on an external environment, such as the cloud or an offsite server.
- A hybrid approach should be used, i.e., local backups stored on a separate device for quick recovery if necessary and in compliance with the RTO (described in section 3)
- At least one copy of the main data, including SPII and PII, should be protected from intruders by using exclusively offline storage or features such as S3 Object Lock

**Backup security.**

- Encrypt backups - transit and permanent, thus making it difficult to access the data.
- Strict control of access to data - the principle of zero trust policy and minimum privileges.

- Mandatory MFA for backup administrators.
- Logical and or physical isolation of network backup segments
- Qualitative selection of backup tools, taking into account the RTO and RPO set by BIA.

### 5.2 Recovery Strategy

- Prioritized recovery: Restore systems in the order prescribed by the BIA (Section 3.4) from the highest priority functions (e.g., website, payment gateway, databases).
- Mapping application interdependencies -understand and account for dependencies (e.g., the technical database must be restored before the website).
- Restore components only in the correct order.
- Recovery methods: Use established methods, such as restoring from verified clean backups to a rebuilt/cleaned infrastructure.
- Secure recovery - ensure that the root cause of the vulnerability is fixed before recovery.
- Use isolated recovery networks to prevent reinfection.
- Verify backup integrity before using it.
- Thoroughly test restored systems and applications to confirm functionality and data integrity.

### 5.3 Testing and Validation of DRP

The DRP should be regularly reviewed for effectiveness and compliance with RTO and RPO objectives. In particular, quarterly and annual tests should be conducted. It is also mandatory to test after any significant system changes.

The main types of tests are:

- Regularly testing the recovery of individual files/systems.
- Checklists - reviewing the plan documentation.
- Simulation exercises (discuss hypothetical scenarios) and response steps without actual changes to the system. Resources can be used as CISA Tabletop Exercise Packages (‘CISA Tabletop Exercise Packages | CISA’ 2025).
- Parallel tests - activating the recovery environment in isolation using data replication.
- Full disruption/recovery tests - Simulation of a real disaster, requires approval from the management team before execution.
- Documentation - Capture test actions, results, issues, and metrics.

### 5.4 Post-Recovery Actions and Improvements

- After successful disaster recovery, focus on what can be improved, corrected, and implemented.
- Conduct a meeting with the CSIRT and stakeholders to analyze the incident and response.
- Documentation of lessons learned.
- Documentation of chronology of events.
- Update plans as necessary.
- Implement technical or procedural changes to address the root cause and prevent recurrence
- Improve a cybersecurity awareness program based on lessons learned.

# 6 Information Security Best Practices

This plan is based on best practices in the field of information security and is aligned with a generally accepted framework to ensure a robust and secure approach to cybersecurity resilience. Key practices integrated into the plan include the following points.

- Risk Management Method: Using the BIA (Section 3) and risk assessment (in accordance with NIST SP 800-30) to identify, analyze and prioritize risks, which is the basis for all subsequent planning and control steps.
- Alignment with the NIST regulatory framework: Adoption of the NIST Cybersecurity Framework (CSF) 2.0 framework (Control, Identify, Protect, Detect, Respond, Recover) and the NIST SP 800-61r incident response lifecycle (Nelson 2025).
- Preventive controls: Emphasize the preventive measures that were identified during the preparation (Section 3.4), such as robust patch management, strict access control (least privilege, MFA), network segmentation, user training, and secure backups.

# References

Bevin, L. (2023) Developing an Effective NIST Disaster Recovery Policy and Template [online], *ZenGRC*, available: https://www.zengrc.com/blog/disaster-recovery-policy-template/ [accessed 14 Apr 2025].

BIA Business Impact Analysis: Tutorial & Best Practices [online] (2025) available: https://drata.com/grc-central/risk/bia-business-impact-analysis [accessed 12 Apr 2025].

Breach Notification | Data Protection Commission [online] (2025) *Breach Notification | Data Protection Commission*, available: https://www.dataprotection.ie/organisations/know-your-obligations/breach-notification [accessed 14 Apr 2025].

Build: A Cyber Security Incident Response Team (CSIRT) [online] (2025) available: https://www.ncsc.gov.uk/collection/incident-management/creating-incident-response-team [accessed 13 Apr 2025].

cinchws (2022) ‘Are you prepared to defend your law firm against cyberthreats?’, *Strategic Technology Solutions*, available: https://stspartner.com/are-you-prepared-to-defend-your-law-firm-against-cyberthreats/ [accessed 11 Apr 2025].

CISA Tabletop Exercise Packages | CISA [online] (2025) available: https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages [accessed 14 Apr 2025].

Deepika (2022) ‘What is Ecommerce Business & What are eCommerce Functions?’, *Nimbuspost*, available: https://nimbuspost.com/blog/what-is-an-ecommerce-business-and-its-functions/ [accessed 12 Apr 2025].

Duran, N.K. and J.F. (2025) Europe Retail Threat Landscape 2024 [online], *Cyberint*, available: https://cyberint.com/blog/threat-intelligence/europe-retail-threat-landscape-2024/ [accessed 11 Apr 2025].

Editor, C.C. (2025) Disaster Recovery Plan (DRP) - Glossary | CSRC [online], available: https://csrc.nist.rip/glossary/term/disaster_recovery_plan [accessed 14 Apr 2025].

Establishing RPO and RTO Targets for Cloud Applications | AWS Cloud Operations Blog [online] (2022) available: https://aws.amazon.com/blogs/mt/establishing-rpo-and-rto-targets-for-cloud-applications/ [accessed 12 Apr 2025].

Inhibit System Recovery, Technique T1490 - Enterprise | MITRE ATT&CK® [online] (2025) available: https://attack.mitre.org/techniques/T1490/ [accessed 13 Apr 2025].

NCSC: CSIRT-IE [online] (2025) available: https://www.ncsc.gov.ie/CSIRT/ [accessed 13 Apr 2025].

Nelson, A. (2025) *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile*, NIST SP 800-61r3, National Institute of Standards and Technology, Gaithersburg, MD, available: https://doi.org/10.6028/NIST.SP.800-61r3.

NIS 2 Directive, Article 23: Reporting Obligations [online] (2025) available: https://www.nis-2-directive.com/NIS_2_Directive_Article_23.html [accessed 14 Apr 2025].

PII (Personally Identifiable Information): E-Commerce Explained [online] (2025) *ThoughtMetric*, available: https://thoughtmetric.io/define/pii-personally-identifiable-information [accessed 11 Apr 2025].

Ransomware Removal: Is It Possible to Remove Ransomware? [online] (2025) *Fortinet*, available: https://www.fortinet.com/resources/cyberglossary/ransomware-removal [accessed 14 Apr 2025].

Swanson, M., Bowen, P., Phillips, A.W., Gallup, D., and Lynes, D. (2010) *Contingency Planning Guide for Federal Information Systems*, NIST SP 800-34r1, National Institute of Standards and Technology, Gaithersburg, MD, available: https://doi.org/10.6028/NIST.SP.800-34r1.

Top 10 E-Commerce Security Threats & Their Detailed Solution [online] (2025) available: https://www.getastra.com/blog/knowledge-base/ecommerce-security-threats/ [accessed 11 Apr 2025].

'Top 10 Major Cyber Attacks Targeting E-Commerce Industry' (2024) *SOCRadar® Cyber Intelligence Inc.*, available: https://socradar.io/top-10-cyber-attacks-targeting-e-commerce-industry/ [accessed 11 Apr 2025].

What Is a CSIRT (Computer Security Incident Response Team)? [online] (2025) available: https://www.techtarget.com/whatis/definition/Computer-Security-Incident-Response-Team-CSIRT [accessed 13 Apr 2025].

What Is Business Impact Analysis? [online] (2025) *Splunk*, available: https://www.splunk.com/en_us/blog/learn/business-impact-analysis-bia.html [accessed 11 Apr 2025].

What Is Incident Response? [online] (2023) *AI Security Automation*, available: https://swimlane.com/blog/incident-response/ [accessed 13 Apr 2025].