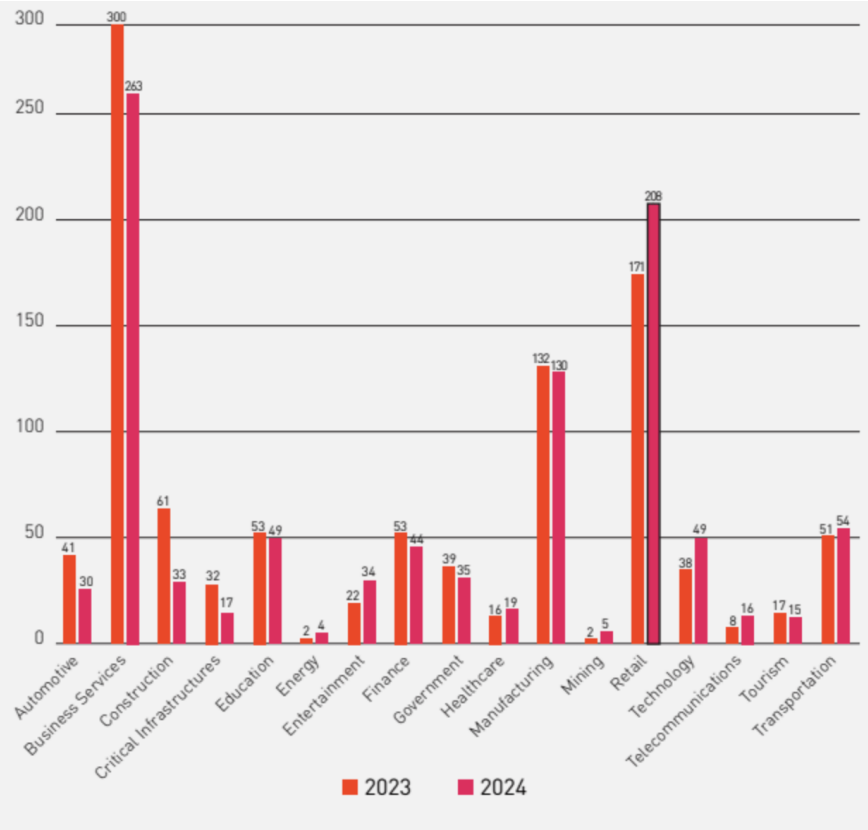
Contingency Plan

PAVLO BOKOVYI

Business Impact Analysis (BIA)

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.

Threat Landscape

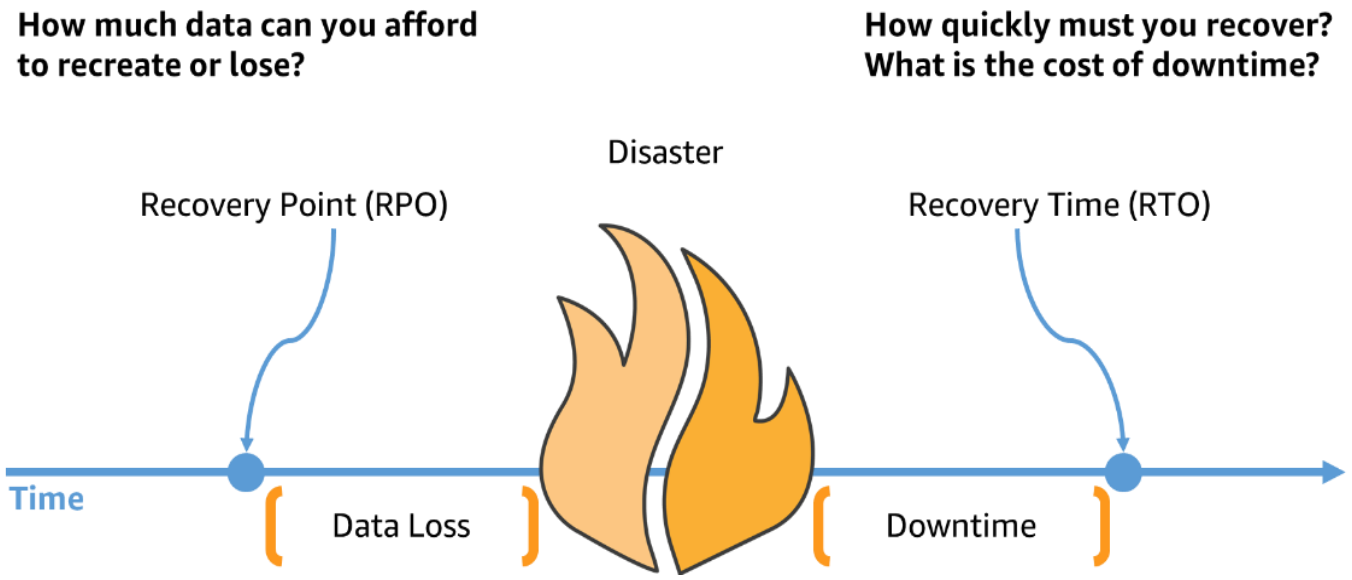


Due to the dynamic nature of the business and data companies operate with, the retail sector and business services are among the most popular targets of ransomware attacks in 2023 and 2024. Therefore, the risks of ransomware threats in 2025 for the e-commerce sector can be assessed as very high, with 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

Critical Business Functions

- 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.

Prioritization of Functions & Recovery Objectives (RTO, RPO)



Prioritization

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 systems.
4. CRM system and order logistics coordination.
5. Service desk.
6. Other functions.

(RTO) and (RPO)

RTO:

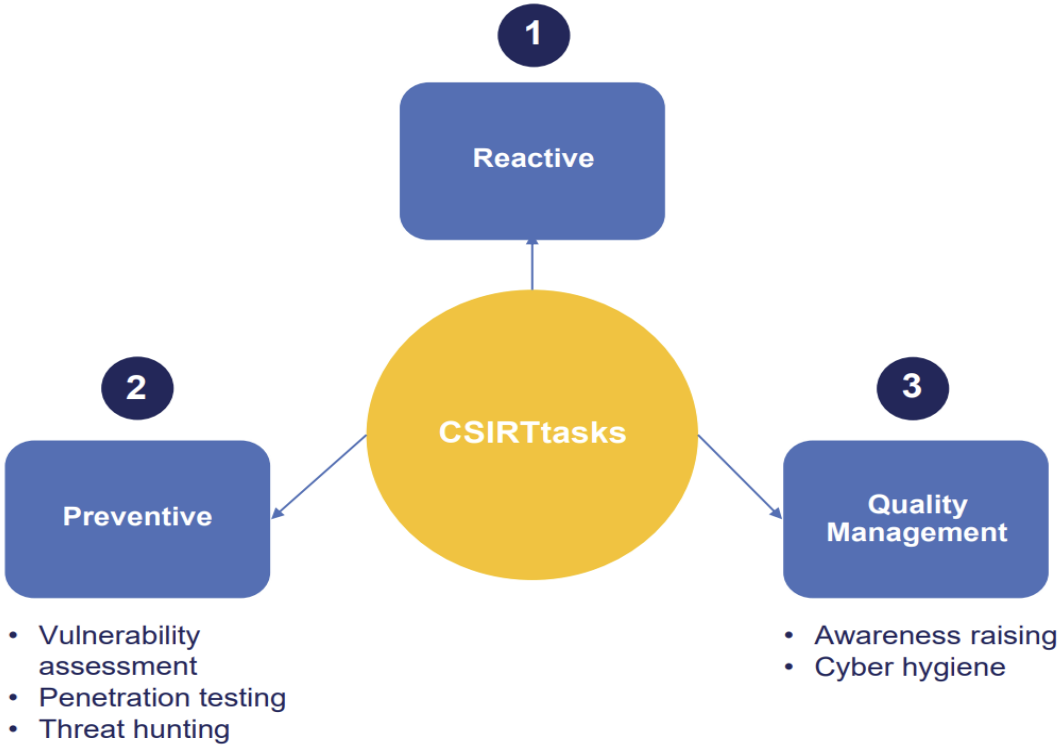
- The main online sales platform as well as the application: up to 1-4 hours.
- Order processing and database: up to 4-8 hours.
- ERP or CRM systems: up to 8-12 hours Service desk: up to 24 hours.

RPO:

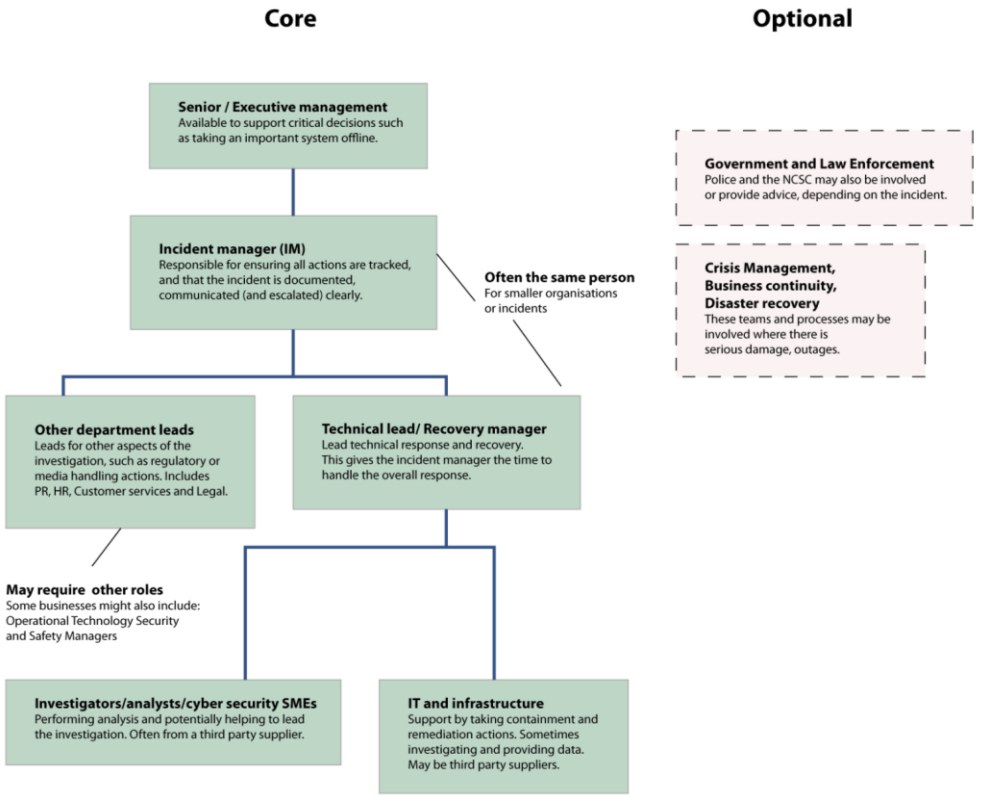
- Transaction data from customers - as close to real-time as possible up to 15-30 minutes (depending on the method).
- Customer database updates: less than 1 hour.
- ERP system data updates: up to 1-2 hours.
- Website content (prices, product availability, etc.): up to 10 minutes.

Incident Response Plan (IRP)

Roles and Responsibilities. CSIRT.



Roles and Responsibilities. CSIRT.



Disaster Recovery Plan (DRP)

- The frequency of backups is determined by the RPO defined in the BIA
- 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.

Disaster Recovery Plan (DRP)

- 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.

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.

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 the 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.

Best Practices

- Risk Management Method: Using the BIA 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 such as robust patch management, strict access control (least privilege, MFA), network segmentation, user training, and secure backups.

Thank you for your attention!