

# Banking Case Study

## Kentbank d.d. - Incident Response Plan Testing

### ■ The Problem

**Kentbank d.d.**, (hereinafter referred to as the **Bank**) a prominent financial institution headquartered in Zagreb, Croatia, is a SWIFT service user required to comply with the **SWIFT Customer Security Controls Framework (CSCF)**. A critical component of this framework is **Control 7.1: Cyber Incident Response Planning**, which mandates the development, annual review, and biennial testing of a cyber incident response plan to ensure timely recovery of critical business operations following a cybersecurity incident.

Recent risk assessments and threat intelligence revealed an increase in cyberattacks targeting financial institutions, underscoring the importance of robust preparation. Given that payment transaction services through the SWIFT infrastructure are essential to the Bank's operations, the need to test and validate their incident response plan became a priority.

### ■ The Solution

To address these challenges, the Bank used the **Cyber Conflict Simulator (CCS)** to create a digital replica of its ICT infrastructure, business processes and human resources, including critical systems supporting SWIFT payment services. This virtual environment allowed for the simulation of:

- **Cyberattack scenarios:** Including service unavailability (availability), data theft (confidentiality), and unauthorized data modifications (integrity).
- **Business impacts:** Categorized into financial losses and client attrition.

A realistic attack scenario was designed based on tactics, techniques, and procedures (TTPs) used by criminal groups targeting financial institutions. This simulation closely replicated a sophisticated cyberattack, enabling the Bank to test its readiness under realistic conditions.

### ■ The Results

#### Enhanced Preparedness:

- The exercise involved the Bank's ICT incident response team, technical staff, development engineers, the CISO, heads of sectors (e.g., payment transactions and SWIFT services), and senior management.
- Participants engaged via CCS interfaces replicating real-life business conditions and communicated through the simulator's message module, supporting text, voice, and document sharing.
- The accelerated simulation timeline compressed activities spanning four days into a one-day exercise, maximizing efficiency while maintaining realism.

## Key Outcomes:

### *Technical Skill Development:*

- Technical teams faced high-pressure attack scenarios, enabling them to test and refine incident response plans.
- Participants practiced decision-making under uncertainty and learned advanced defense techniques integrated into CCS.
- Newly acquired skills proved effective when some were applied in mitigating a real cyberattack weeks later.


### *Operational Resilience:*

- The Bank institutionalized incident response testing as a core component of its digital operational resilience strategy, ensuring continuous improvement and readiness for emerging threats.

### *Business and Management Insights:*

- Senior management and business leaders gained a clear understanding of the potential impacts of cyberattacks on payment services and overall operations.
- Based on exercise findings, risk assessments were updated, and new security protocols were implemented for processing SWIFT messages.

By utilizing CCS for realistic simulation and testing, the Bank significantly improved its cyber incident response capabilities, minimized operational risks, and strengthened trust with its clients and stakeholders.



„Conducting the exercise was extremely useful. All functionalities are surprisingly well-conceived. The greatest benefit of conducting the exercise is gaining experience in managing the response to a cyber incident, similar to a flight simulator. Repeated exercises achieve an efficient and optimal response for specific types of cyber events.“

Srećko Bartol, CISO Kentbank d.d.

“We have been conducting CCS exercises for several years now, and we find them extremely useful and plan to continue doing them in the future. Besides the training and practicing reactions to unforeseen situations, we also gain insight into our weaknesses which allows us to improve, enhance the system, improve procedures, and strengthen where necessary. CCS provides a different level of experience and reality and is therefore a much higher quality test than some other methods. Moreover, not to be overlooked, no one has to be forced to do it because, thanks to the simulator and the way the exercise is conducted, it is all more fun than an obligation and work.“

Franjo Prjić, ICT Director Kentbank d.d.

“A useful exercise and good training to see how prepared we are for unforeseen situations. Through the exercise, we always get new ideas on where to raise the level of system security. The application is quickly 'caught' and then the interesting part begins. The attack scenarios are realistic and challenging each time, and we are already thinking about what the next one might be.“

Branimir Ivošević – ICT Infrastructure  
Department Manager Kentbank d.d.