



Risk-!n 2025

Cyber Risks Decoded

Philippe DOERKS & Roberto GROSSO CIPONTE

A2F Cybersécurité
Route de la Pâla 129
1630 Bulle

Speakers



Philippe DOERKS



- Design of personalised training programmes..
- Responsible for the InfoSec Masters program at Unige (University of Geneva).
- Expertise in trainings, PM, Cybersecurity & LPD (Swiss data protection law).

Roberto GROSSO CIPONTE



- Expert in business continuity, risk, and crisis management with over 20 years of experience in the FMCG, financial and pharma industry.
- Certified PECB & BCI accredited trainer. & Lecturer at the University of Geneva.

Objectives (1/2)



1. Even though we have very little time today, the objective of this session is to highlight the importance of practicing your various business continuity and crisis scenarios.
2. Simply because there are no reputational or financial consequences, if an exercise doesn't go well, it does not matter.
3. However, in a real-life situation, the impact on you and your company could be tremendous or even lead to a disaster.

Objectives (2/2)



Today's table top exercise (TTX) objectives are:

- 1) Identify the incident(s) and understand its / their nature.
 - Assess the effectiveness of **business continuity** and **crisis governance** in response to an outage at a critical **third-party** IT services provider.
- 2) Restore systems and services to normal operation.
 - Discuss risk **tolerance and prioritization** criteria on how to **restore services** and balance operational recovery with **regulatory compliance** and **reputational** considerations.
- 3) Communicate
 - Identify gaps in compliance, reporting obligations, and third-party coordination.
- 4) Lesson learned
 - Share lessons learned and your best practices related to resilience planning and communication strategies.

Ground Rules



- The scenario is fictional and not derived from current intelligence but is deemed plausible based on current threats.
- Work with the scenario. Assume normal safeguards have failed.
- There is no "hidden agenda" or trick questions.
- This exercise is neither a regulatory nor supervisory activity.
- Comments made during the exercise are not for attribution.
- State your name and organization when participating in the discussion.

Interactivity



- Connect to Votamatic (QR code)

Votamatic.unige.ch

- Verify connections

- Start TTX

Swiss Operations & Cybernetics GmbH (SOC)



Company Overview

- **Headquarters:** Fribourg, Switzerland
- **Industry:** Financial IT Services
- **Established:** 2017
- **Core Services:** IT Infrastructure Management, Secure Transaction Processing, Cybersecurity Solutions, “Swiss” Cloud Solution
- **Company Description:** Swiss Operations & Cybernetics GmbH (SOC) is a leading third-party service provider specializing in IT infrastructure and transaction services for the Swiss financial industry. With headquarters in Fribourg, SOC is a trusted partner for numerous Swiss banks and insurance companies, ensuring secure and efficient processing of financial transactions, data storage, infrastructure management and is also the provider of the Swiss Cloud.
- **Role in the Financial Sector:** As an integral part of Switzerland's banking ecosystem, SOC manages critical IT functions and transaction flows, providing seamless and secure operations for clients in the highly regulated financial sector. SOC's services include real-time transaction monitoring, secure data handling, and regular security updates in line with Swiss banking standards.

Initial Incident Notification and Public Disclosure



Friday 22nd November 13:00

- Swiss Operations & Cybernetics GmbH (SOC), a critical IT services provider for Swiss financial institutions, appears on a well-known cybersecurity website as the latest victim of a ransomware attack.
- Shortly after the article is published, SOC sends an email notification to its clients, acknowledging that they have shut down certain services due to a potential issue under investigation. The clients are informed that SOC is proactively working to understand and contain the problem.

Friday 22nd November 18:00

- In response to the ongoing investigation and emerging concerns, SOC decides to shut down all its services and disconnects all client systems.
- The Cyber Hub's Operational Command Structure (CHOCS) releases a preliminary report indicating that SOC's environment has been severely compromised.
- There is no confirmed evidence that client systems (therefore their data) have been directly affected yet. The CHOCS recommends that all institutions review their security posture and prepare for potential impacts.

Inject – Transition to a Clean Cloud Environment



Date / Time

Sunday 24th
November
18:00

Event / Details

SOC proposes a transition to a temporary clean cloud environment.
Clients must decide whether to reconnect critical systems amid uncertainty around the original compromise.

Discussion Questions



- How should institutions **evaluate third-party proposed mitigation solutions** before reconnecting critical services?
- **What business continuity triggers** should be used to decide between reconnecting or activating fallback solutions?
- How does this situation impact your **risk appetite and tolerance levels**?
- How should **internal governance structures** (e.g., risk committees, C-level briefings) be activated during such a decision?
- What **regulatory and reporting requirements** must be considered when reconnecting or remaining disconnected?
- What are your **third-party risk management obligations** (under FINMA, ISO, etc.)?

Votamatic results



Possible next steps for you...



- Personalise exercise in line with your business
- A normal table top exercise should last at least 3-4 hours up to one working day.
- Inject samples which could be used in this exercise are:

Description	Objective
Forensic investigators confirm compromise of administrative credentials used to manage client environments.	Test decision-making around containment actions, client notifications, and escalation paths.
Major news outlets report the breach, mentioning several financial institutions by name without confirmation	Evaluate crisis communication, reputational risk management, and alignment between institutions and SOC messaging.
A client detects unusual outbound network traffic from systems previously managed by SOC.	Assess incident detection, investigation, and escalation procedures; evaluate assumptions about system trustworthiness.
Discovery that SOC's subcontractor for backup services is also compromised.	Test supply chain risk management practices and reassess data recovery strategies.
FINMA mandates immediate regulatory reviews of institutions using third-party IT providers.	Stress-test regulatory readiness, documentation practices, and internal governance structures.



Thank you for your participation!

If you have any more questions please contact us under

info@a2f.ch