NIEDERER KRAFT FREY

NKF Breakfast Workshop

Cyber Attacks in Switzerland and Lessons Learnt in 2019

Zurich — 27. February 2020

Table of Contents

Overview of Cyber Attacks in Switzerland

- Offix-Group
- Meier Tobler
- Crealogix
- Omya
- Auto AG Group in Rothenburg
- Digitec-Galaxus
- Hospital in Wetzikon
- Etc.

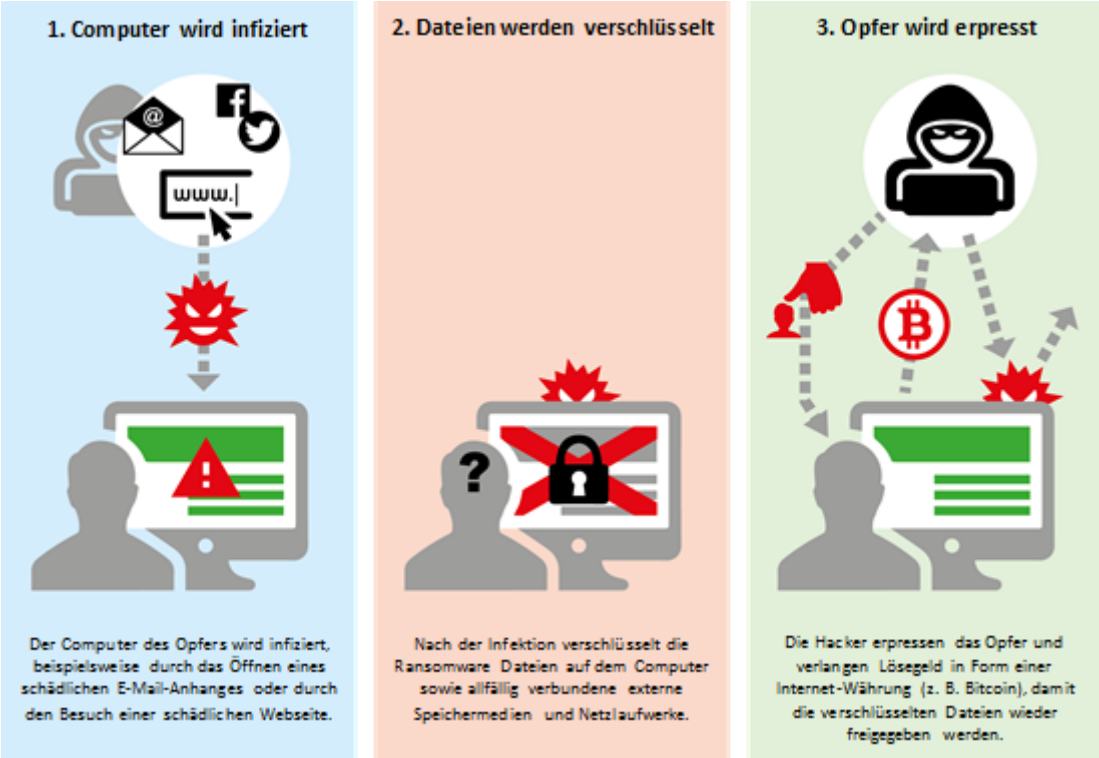
Note: only a tiny fraction of Cyber Attacks become publicly known

Possible Explanations

- Change of cybercriminals' focus away from B2C to B2B (=deeper pockets)
- Switzerland popular location for datacenters
- Switzerland has many EMEA headquarters
- Swiss companies massively underestimate the treat of cyber attacks and are not prepared
- Employee awareness training is not sufficient – attacks are 99% Spear-Phishing E-mails which employees open accidently
- No interest in implementing IT standards (e.g. ISO)
- Lack of effectiveness of law enforcement

Different Phases of Incident Management

Mainly Ransomeware Attacks in 2019

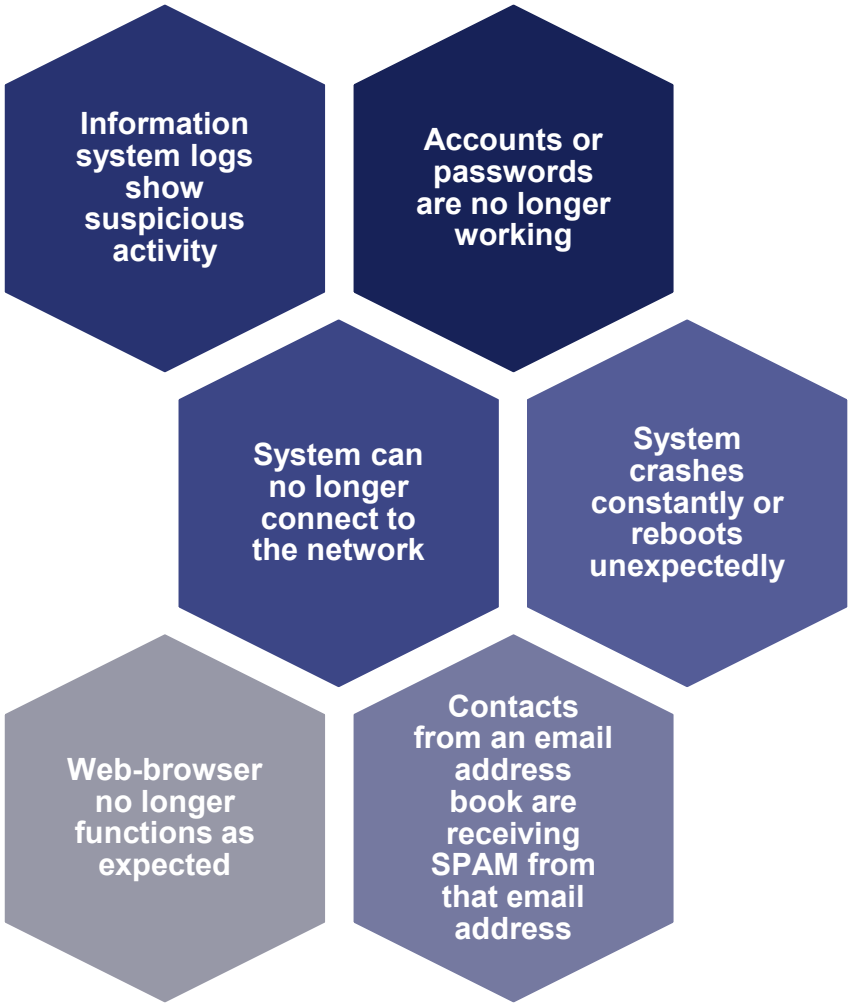


Source: NCSC

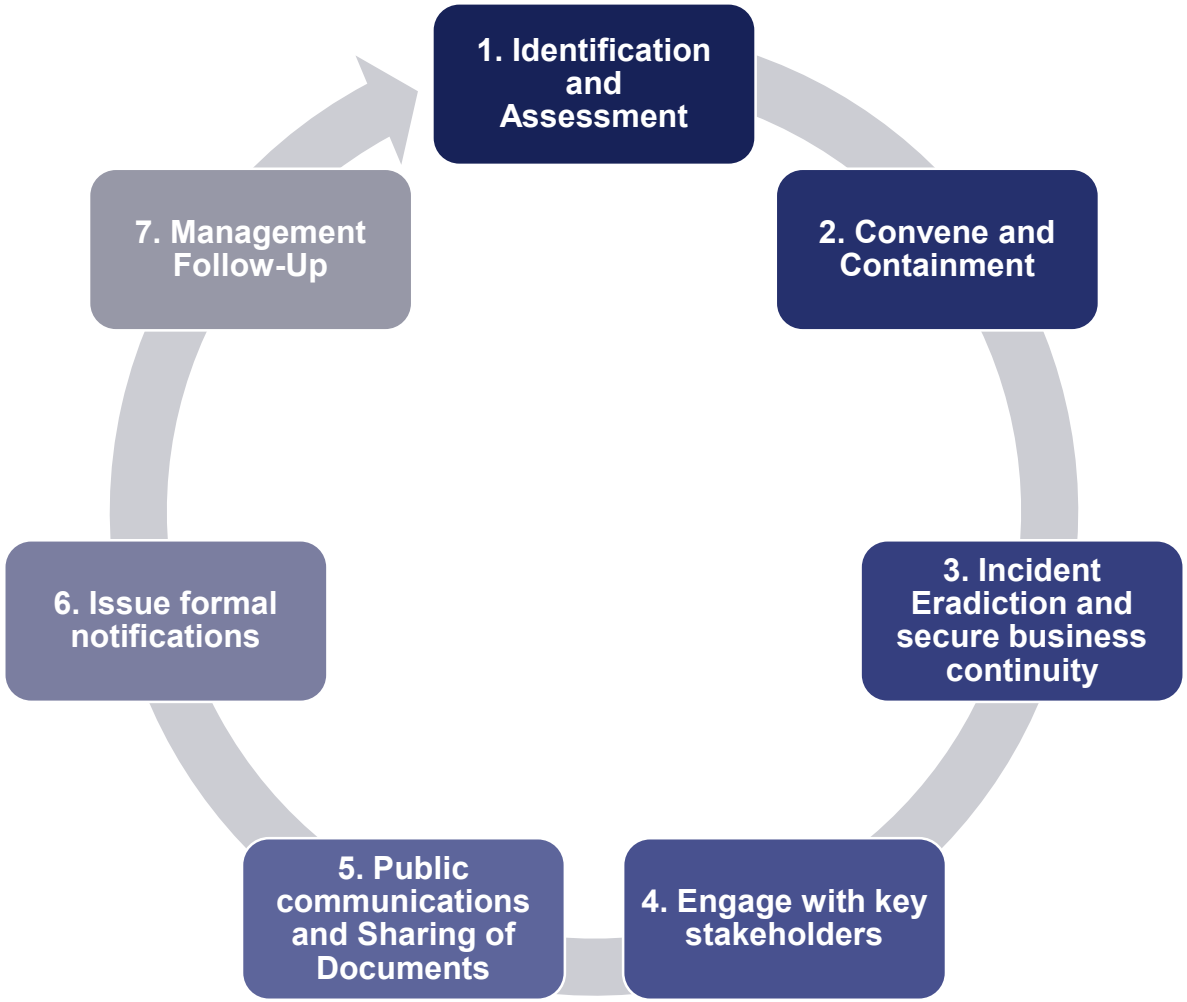
Different Phases

During Incident

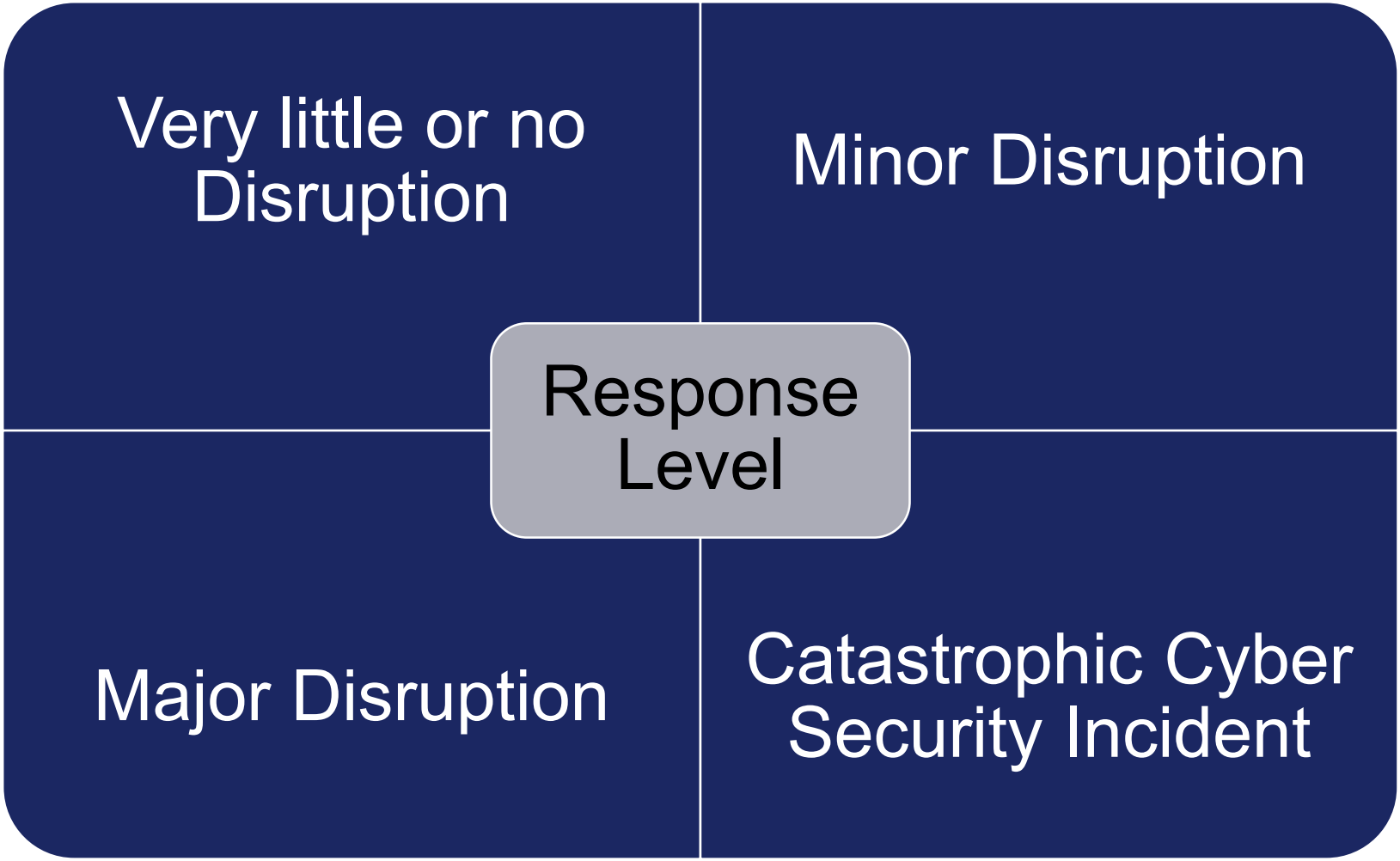
Signs of Cyber Attack



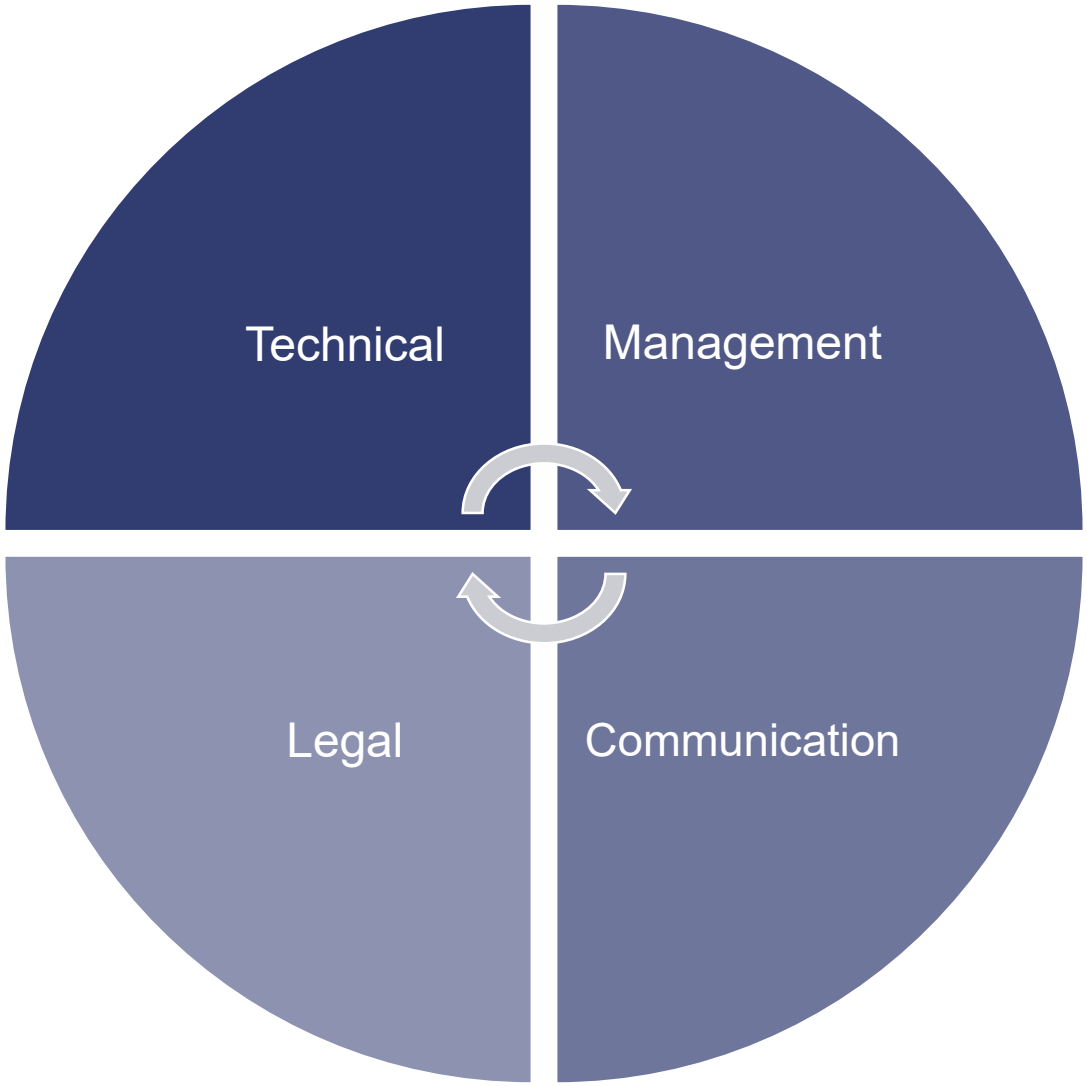
Phases of Management during Incident



Response Level depends on Impact



Four Classes of Incident Responses



Stakeholders

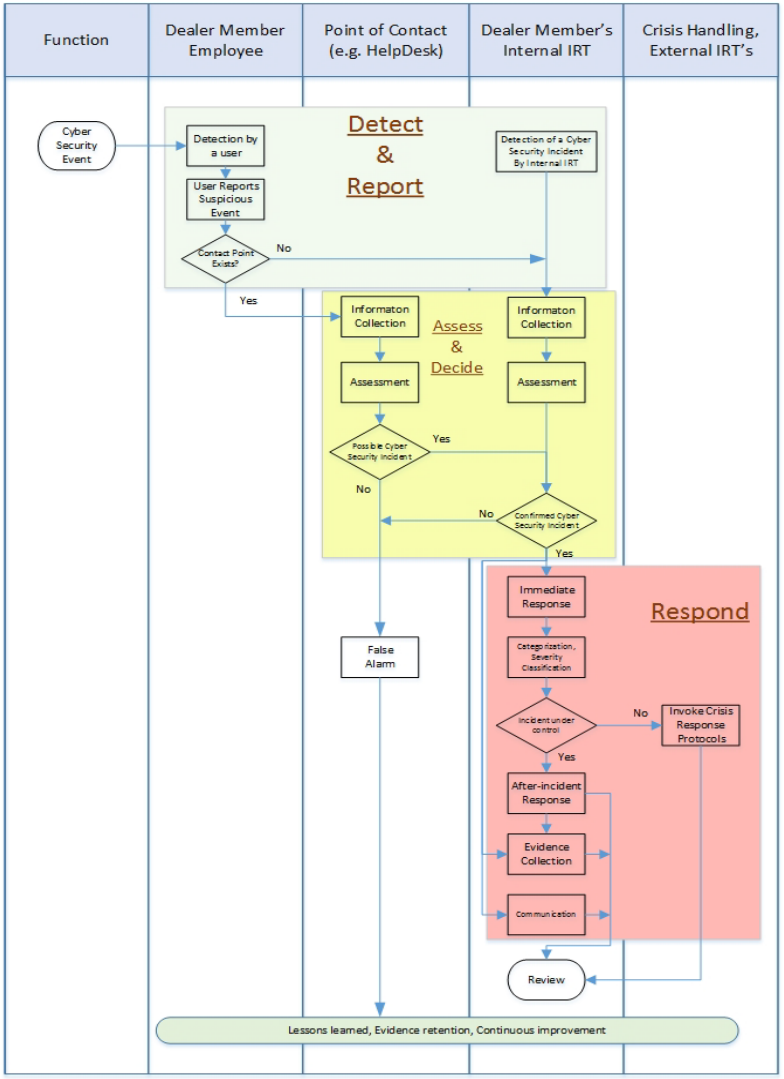
Primary Stakeholders	Secondary Stakeholders	Other Stakeholders
• Internal stakeholders (response team) • DPO • Customers/Clients/vendors/ suppliers • Employees • Group entities • Affected Individuals • Insurer	• Specialized security organizations (NCSC, FedPol) • Regulatory/ Supervisory Authorities • Privacy Commissions	• The Media • Federal/regional law enforcement • Voluntary information sharing organizations

Checklist During Incident

- ✓ Record the issues and open an incident report
- ✓ Convene the Incident Response Team
- ✓ Convene a teleconference with the appropriate internal stakeholders to discuss what must be done in order to restore operations
- ✓ Convene a management teleconference with the appropriate internal stakeholders in order to provide situational awareness to executive management
- ✓ Triage the current issues and communicate to executive management
- ✓ Identify the initial cause of the incident, and activate the specialists to respond to the current issues to restore operations
- ✓ Retain any evidence and follow a strict chain of evidence to support any needed or anticipated legal action
- ✓ Communicate to affected third parties, regulators, and media (if appropriate)

NKF

Example of Event and Incident Flow Chart



Template for Incident Report

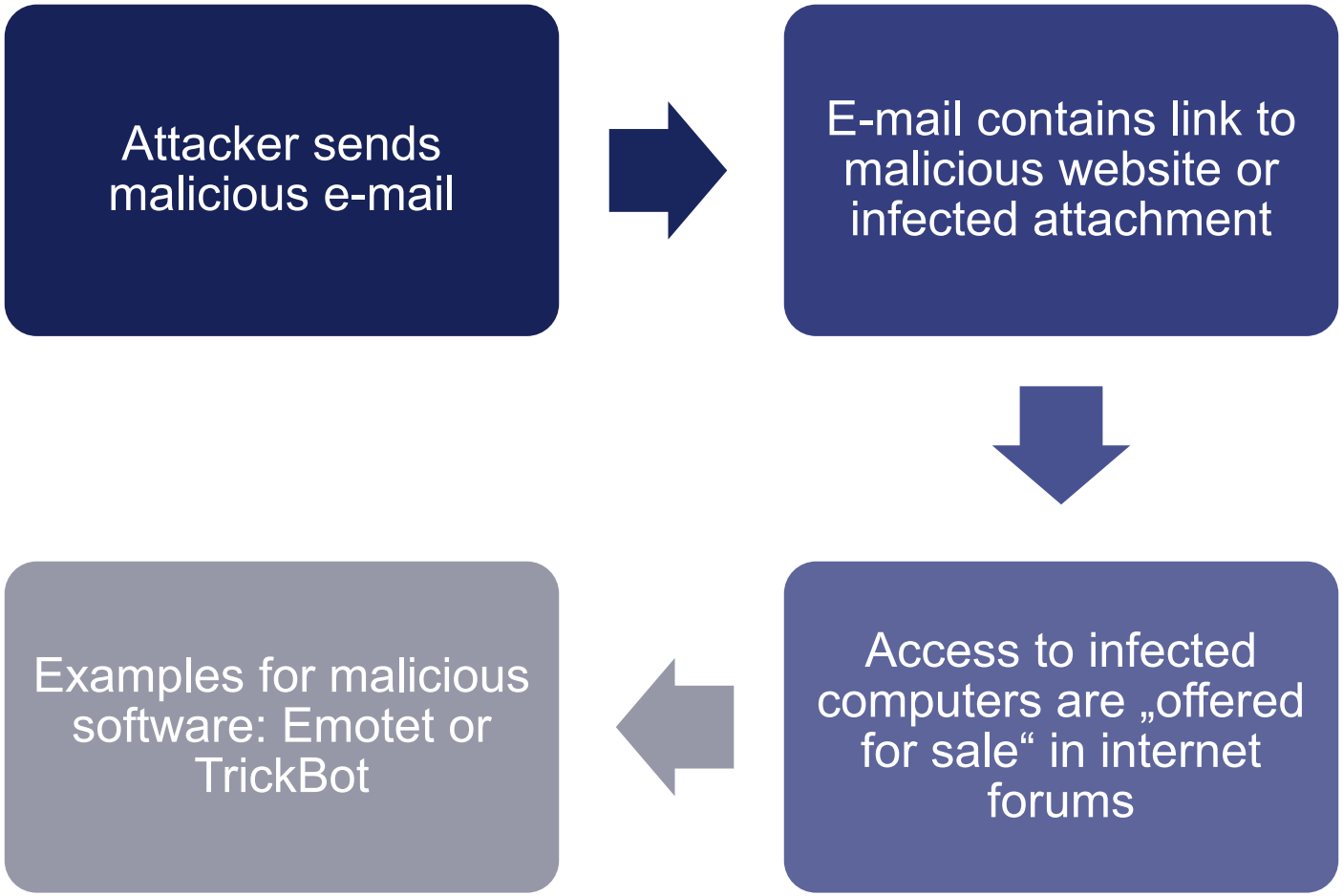
- Incident Current Assessment
- Background
- Summary Conclusion
- Breach Factor Assessment
- Legal Notification Requirements
- Communication Plan
- Remediation
- Incident Response Activities
- Takeaways/Lessons
- Open items

Lessons Learnt During Incident Management

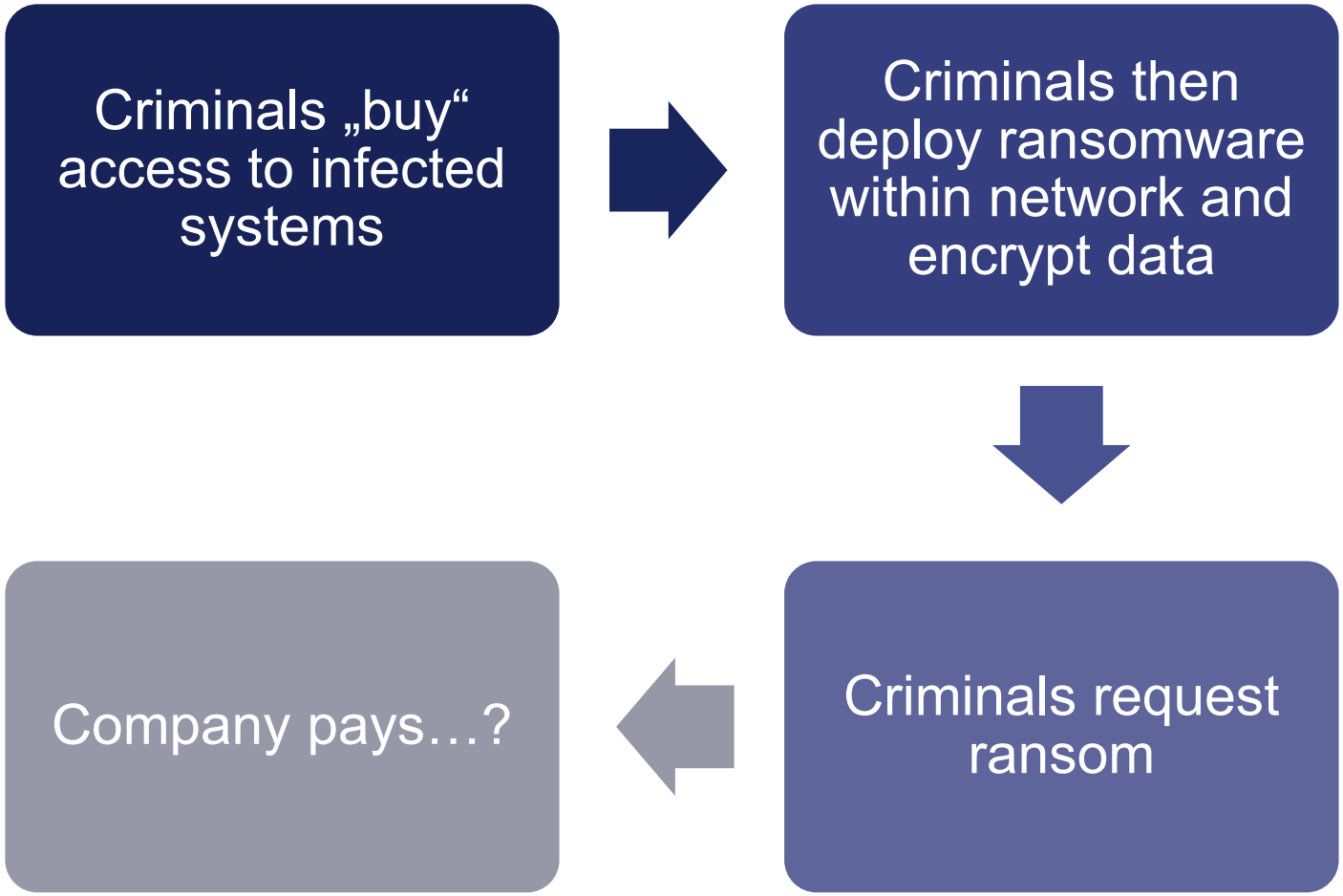
- Time is of essecense in the first 24 hours
- Go offline
- Cooperate with police and other cybersecurity organizations
- If forensic teams are not delivering, do not be afraid to exchange
- Holistic approach: communication is key, but has legal impact on many areas:
  - Force major clauses in customer/client contracts
  - Insurance coverage
  - Litigation
- Divide forensic report in two parts: forensic analysis and recommendations
- Talk to other impacted companies

Precautionary Measures

How does Ransomware get installed?



How does Ransomware get installed?, cont.



Laws and Standards

Art. 7 Swiss Data Protection Act

Art. 8 and 9 Swiss Data Protection Ordinance

Art. 32 GDPR

ISO 27001

Organizational Measures

Assess effects of IT failure on your business	Identify IT assets critical for ongoing business	Define work around solutions in case of IT failure
Create incident response team including relevant points of contact	Create incident response plan including reporting process	Implement and test incident response plan

Organizational Measures, cont.

Train employees on breach awarness, employee responsibility and reporting process

Keep knowledge base on security threats updated (e.g. MELANI cyber-incident releases)

Assess risk associated with company information publicly made available on website

Ensure security throughout entire life cycle of IT assets up to disposal

Define appropriate password policy, use two factor authentication

Technical Measures

Use appropriate Virus protection

Protect corporate network with firewalls

Ensure regular data backups, ensure back-ups are stored offline

Ensure log files are kept for every critical system. Review log files for suspicious entries

Separate networks where possible/ appropriate

Technical Measures, cont.

Ensure all system/security updates are regularly installed

Use appropriate spam filters to block harmful e-mails/ attachement/ macros

Limit usage rights to what is required for relevant tasks

Ensure encryption of sensitive data, in particular on mobile devices

Ensure proper authentication in case of remote access

Notification of Authorities

Does Ransomware Attack trigger «Data Breach» that is to be notified?

- Usually ransomware „only“ encrypts data/system
- causes loss of availabilty of data and business interruption
- does not causes access to (personal) data and/or misuse of (personal) data
- but one cannot definitely conclude that incident is unlikely to result in a risk to the rights of data subjects
- therefore notification recommended on a precautionary basis

NKF

Notification Duties

Be prepared

Clarify notification duties before something goes wrong

Be aware: effects of cyber attacks not limited to data breach

Distinguish between notification duties under data protection and other laws

Distinguish between notification duties in CH and abroad

Notification Duties in Switzerland

Data protection law

- No mandatory notification duty
- Voluntary notification to MELANI (Reporting and Analysis Centre for information Assurance)
- Current legal system under review

Sector specific rules

- Mandatory reporting obligations in various sectors
- Not cyber specific
- e.g.
  - Art. 11/22 KEG (Kernenergiegesetz)
  - Art. 23 LFG(Luftfahrzeuggesetz)
  - Art. 8 StromVG (Stromversorgungsgesetz)
  - Art. 29 FINMAG

Notification Duties in the EU

Data protection

- Mandatory notification duties
- Duty to notify supervisory authority Art. 33 GDPR
- Duty to notify data subjects Art. 34 GDPR

Sector specific rules

- Mandatory reporting obligations
- Not necessarty cyber-specific

Notification Duties in other Jurisdictions

Data protection

- Possibly mandatory notification duties including:
- Duty to notify authorities, e.g. Canada
- Duty to notify data subjects, e.g. Canada

Sector specific

- Possibly mandatory notification duties
- Not necessarily sector specific
- e.g. tax authorities in Brazil

Do Swiss Companies have to notify in the EU?

What about GDPR?

- Yes, in two cases:
  - Establishment in Union Art. 3 (1) GDPR "processing of personal in the context of the activities of an establishment in the Union"
  - Targeting data subjects in Union Art. 3 (2) GDPR "processing of personal data of data subjects in the Union by controller/processor not in the Union, where processing activities are related to (i) offering of goods/services to data subjects in the Union or (ii) monitoring of their behaviour in the Union"

Specific Issues for Group of Companies headquartered in Switzerland

Can group benefit from one-stop-shop principle under Art. 56 GDPR

Which would be the „lead supervisory authority“ according to Art. 56 GDPR?

Lead supervisory authority is the authority of „main establishment“

Main establishment is „place of central administration in the Union, unless decisions on data processing are taken in another establishment in the Union“ Art. 4 (16) GDPR

NKF

Specific Issues for Group of Companies headquarterd in Switzerland, cont.

On 21 January 2019 CNIL imposed financial penalty of EUR 50 m against Google LLC

Google‘s European headquarters are located in Ireland

CNIL did not consider such headquarters as „main establishment“ in Union under GDPR

CNIL did not consider European headquarters to have decision-making power on processing operations

CNIL thus denied the Irish DPA to be the lead authority and imposed fine on Google LLC (U.S.)

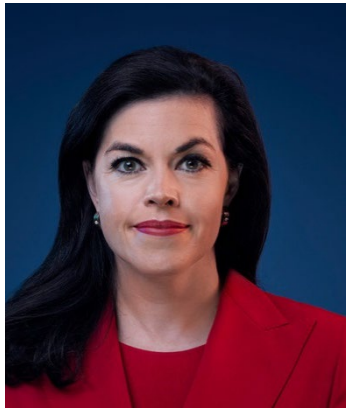
Conclusions for Group of Companies headquartered in Switzerland

- If Swiss headquarter has decision making power for processing operations one-stop-shop principle not applicable
- Nofifications to be made in each EU jurisdiction where data breach occured
- Exposes group to risk of accumulation of fines
- CNIL decision critized, but still to be considered
- Does appointment of representative according to Art. 27 GDPR change assessment?

Q&A

THANK YOU

Your Contacts



Clara-Ann Gordon
clara-ann.gordon@nkf.ch
D +41 58 800 84 26

Dr. Andras Gurovits
andras.gurovits@nkf.ch
D +41 58 800 83 77