Cybersecurity and the Law Seminar

A practical walk-through of the legal landscape, enforcement, management liability and discussions on potential real-world situations

Zurich — 25 September 2018

What can you expect today?

Cybersecurity Breach – academic issue or real Threat?

Cybersecurity Breach – academic issue or real Threat?

- British Airways
- Delta
- Air Canada
- Carphone
- Digitec
- EOS
- Groupe Mutuel
- Abbott Laboratories
- Industrial control systems / IoT

Why?

- Sheer pleasure of technical challenge
- Concrete financial interests
- Blackmailing

  → Uber case

- Threatened cyber attack (DDoS)

Consequences for your Company?

- Financial damage
- Management capacity
- Reputational loss
- Claims
- Sanctions (?)

Practical Example – Data Theft by Employee

Conclusions

- Prevention
- TOMs
- IT / data breach response planning
  - People
  - Measures

→ Good governance

Some sources

- MELANI

https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte.html

- FEDPOL

https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/cybercrime.html

Legal Framework and Enforcement

Legal Framework – Overview

- International Law:
  - Cybercrime Convention
  - Cloud Act
- National Laws
  - Swiss Criminal Code, SCC
  - Swiss Data Protection Act
  - Corporate Governance: Swiss Code of Obligations (716a CO)
  - Ordinance on the Preservation of Corporate Books (retention), Ordinance on Internet Domains, Financial Market Supervision Act, etc.
- Legislatory Developments Federal Council and Federal Offices
  - NCS Strategie Cyber Risks 2018-2022
  - Strategy Digital Switzerland

Legal Framework – Criminal Law I

- Criminal Law (Swiss Criminal Code, SCC)
  - Unauthorised obtaining of data art. 143 SCC (electronic theft)
  - Unauthorised access to a data processing system art. 143bis SCC (Hacking)
  - Damage to data art. 144bis SCC (Denial-of-service attacks; ransomeware)
  - Computer fraud art. 147 SCC (theft of identity)
  - Breach of secrecy or privacy through the use of an image-carrying device (art. 179^{quater} SCC)
  - Obtaining personal data without authorisation (art. 179^{novies} SCC)
  - Industrial espionage (art. 273 SCC)
  - Breach of postal or telecommunications secrecy (art. 321ter SCC)

Legal Framework – Criminal Law II

- Criminal Law - Connection with other offences
  - Fraud (art. 146 SCC)
  - Extortion (art. 156 SCC)
  - Offences against Personal Honour and in Breach of Secrecy or Privacy (art. 173 et seqq. SCC)
  - Forgery (art. 251 et seqq. SCC) (phishing)
  - Corporate Criminal Liability (art. 102 SCC)

Actions before, during and after Incident

- Actions before incident
- Actions during or immediately after incident
- Actions after incident / enforcement

Actions before Incident – Preventive Measures

- Technical and organisational measures (art. 7 DPA / art. 8 and 9 Ordinance DPA)
  - Implement technical measures (authorisation; transmission; back-up; access)
  - Implement organisational measures (IT-security policies; IT-security policy for employees; privacy policies; retention policy; awareness & training)
  - Set up task force / Appointment of external service providers
- Limit liability risks with third parties (contractual measures)
- Cyber risk insurance
- ISO certification

Actions during or immediately after Incident

Unauthorised access to company's data

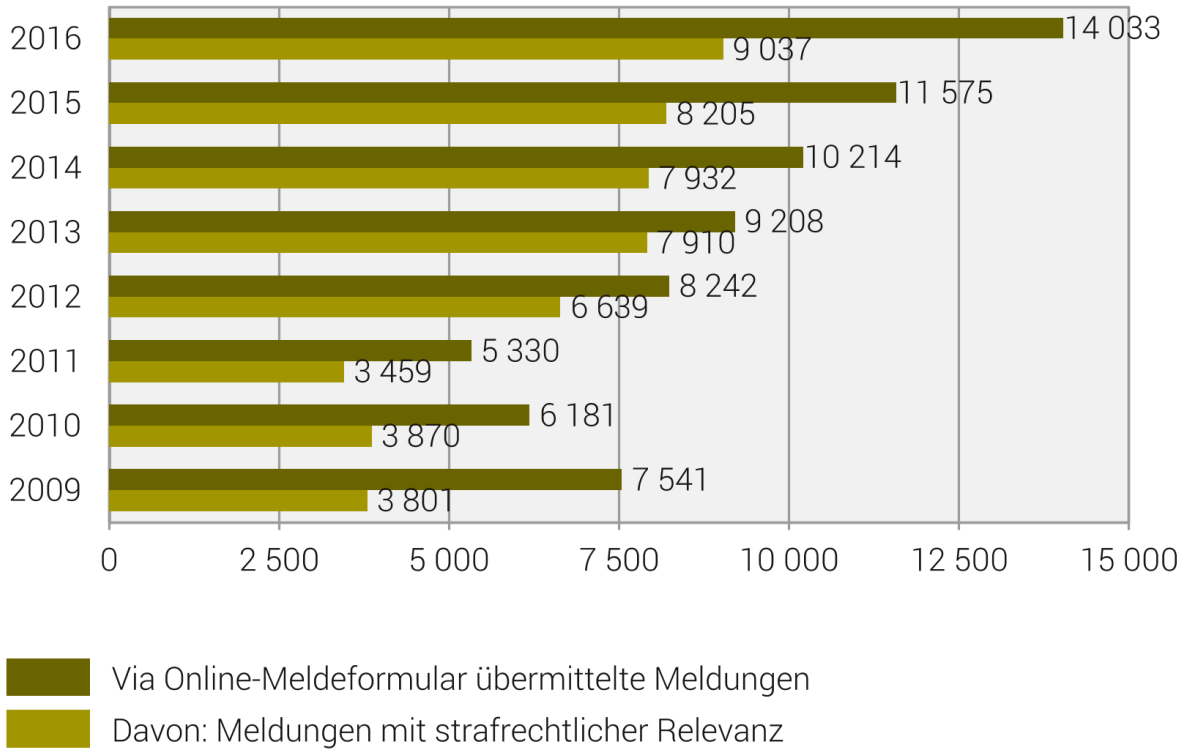
– Identify and analyse	URGENT
– Stop / Contain	URGENT
– Restore / Mitigate	URGENT
– Notify data protection authorities	URGENT
– Notify cyber security insurance	URGENT
– Review / Remediation	Do not forget

Actions after Incident – Notifications

- Notification / Report to MELANI
- Notify Cybercrime Coordination Unit Switzerland (KOBIK)
- Notify data subjects
- Notify third parties

Cybercrime Development

Anzahl an fedpol übermittelte Meldungen einschliesslich jener mit strafrechtlicher Relevanz, 2009-2016



Quelle: jahresbericht fedpol

Actions after Incident - Enforcement

- Enforcement
  - Criminal complaint
  - Civil procedural law measures (filing a claim, requesting precautionary measures)
- Practical problems
  - Official offences vs. offences prosecuted on complaint
  - Identifying offender
  - Place of jurisdiction
  - Cooperation in international law enforcement

Liability of Board Members and Management

Duties and Liabilities of Board (in general)

- "Monistic" Concept
  - As opposed to dualistic concept (Germany, France)
  - Board of Swiss Co responsible for supervision and management (unless delegated)
- Statutory catalogue of duties of Board
  - Broad scope of (non-transferable) responsibilities:
    - Ultimate management
    - Organization
    - Accounting, financial controls and planning
    - Appointment / removal of management
    - Supervision of management
    - Business report / shareholders' meeting
    - Notification of judge

Corporate Governance and Delegation of Duties

- Corporate Governance
  - Swiss Code of Best Practice / SWX Directive / Foreign Regime
  - Specific Guidelines for the Regulated Sectors
  - No specific guidelines for cybercrime risks
- Delegation of Duties
  - Principle: “Core duties” are non-transferable and may not be delegated
  - Exceptions:
    - The preparation, implementation and supervision of decisions of Board (delegated e.g. to Committees of Board)
    - The day-to-day management, if Board uses due care re selection, instruction, supervision of managers
    - Even if the Board delegates the fulfillment of certain duties to a management, the Board remains responsible

NKF

Liability

- Liability of Board Members
  - Board Members are liable for damage caused by intentional or negligent breach of duties
  - Joint and several liability, but dependent on degree of negligence
  - Who can sue (when)
    - Shareholders (going concern)
    - Creditors (in bankruptcy)
    - Company (going concern)
- Excursion:
  - Directors and Officers' Liability Insurance
  - Cybersecurity Insurance

Duties in a Cybercrime Context I

- Expected Awareness from Board:
  - Cybersecurity no longer an “IT issue”, but an enterprise-wide risk management issue
  - Board should understand the legal and regulatory implications of cyber risks
  - Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the Board meeting agenda
  - Board should set the expectation that management will establish an enterprise-wide risk management framework with adequate staffing and budget
  - Board Management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach

Duties in a Cybercrime Context II

- Board should perform the following general tasks:
  - Review and approve an IT strategic plan that aligns with the overall business strategy
  - Promote effective IT governance
  - Oversee processes for approving the institution's third-party providers
  - Oversee and receive updates on major IT projects, IT budgets, IT priorities, and overall IT performance
  - Oversee the adequacy and allocation of IT resources for funding and personnel
  - Approve policies to escalate and report significant security incidents to the Board
  - Hold management accountable for identifying, measuring, and mitigating IT risks

Duties in a Cybercrime Context III

- Independent, comprehensive and effective coverage of IT audits:
  - Board and senior management are responsible for ensuring that the company's system of internal controls operates effectively
  - Board should ensure that written guidelines for conducting IT audits have been adopted
  - Board or its audit committee is responsible for reviewing and approving audit strategies (including policies and programs), and monitoring the effectiveness of the audit function

Duties in a Cybercrime Context IV

- Board should establish and approve risk-based policies to govern the outsourcing process:
  - Ensuring each outsourcing relationship supports the company's overall requirements and strategic plans
  - Ensuring the company has sufficient expertise to oversee and manage the relationship
  - Evaluating prospective providers based on the scope and criticality of outsourced services
  - Tailoring the enterprise-wide, service provider monitoring program based on initial and ongoing risk assessments of outsourced services
  - Notifying its primary regulator regarding outsourced relationships, when required by that regulator

Civil Liability I

- General comments:
  - Board Members must carry out their duties and responsibilities with due care and duly safeguard the interests of the company
  - Several and joint liability, unless a particular damage s attributable to such Board Member based on its own default and the circumstances of the case (e.g. CIO with regard to IT)
  - Liability is the same for all Board Members irrespective of their nationality
  - Board Member is personally liable to the company, as well as to the individual shareholders and the creditors for damages caused intentionally or negligently by breach of its duties
  - Lack of practice, lack of time or lack of knowledge does not excuse
  - Abstaining from vote is also no excuse

Civil Liability II

- Board Member is liable if the following preconditions are met:
  - Position and activity as a Board Member
  - Breach of Duty
  - Negligent or willful conduct
  - Damages
  - No exculpation and causality
  - Right to assert liability claims
  - Burden of proof

Criminal Liability

- Board Members and any other person managing a company may be held liable for criminal offenses committed in their function
- If a criminal offense is committed within a legal entity and in the conduct of its business and if, due to a lack of organization, no particular person can be held liable for such on offense, then the legal entity is fined
- In general, not only the Swiss Penal Code contains criminal law provisions. A number of other statutes are relevant as well, such as statutes on taxation, social security and unfair competition
- Unless explicitly provided for otherwise by a particular legal provision, an offender is only punished for an offense committed intentionally

Consequences of Breach of Duty in Practice?

- Principle: company liable for any damages
- However… internal finger pointing:
  - Removal from Board?
  - Termination of Employment Agreement?
  - Claim by company or shareholders against Board Members or Management (depending on the case)?
  - Criminal complaint against Board Members, Management or Head Compliance/Head IT?
  - Claiming D&O insurance coverage for director's and officers' liability?
  - Claiming insurance coverage for cybercrime incidents?
  - Validity of company indemnifications for Board Members or Management?

Limiting the Risk

- As a minimum, Board may wish to take the following practical steps:
  - Employ (or engage) a dedicated cybersecurity expert, a person qualified to brief and train the board of directors regularly
  - Carefully formulate a robust policy on cybersecurity which is constantly monitored and reviewed, forming part of the governance framework, and record all consideration and action taken
  - Ensure the company has adequate insurance and that the board of directors understand the extent and limits of the policy
  - Agree contingency measures for during and after an attack and be prepared to respond to an attack with a detailed plan which has been tested (incident response plan)
  - Testing and monitoring network security
  - Anti-malware software
  - Staff training

THANK YOU

Your Contacts

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

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

Victor Stancescu
victor.stancescu@nkf.ch
D +41 58 800 82 29

Niederer Kraft Frey Ltd Bahnhofstrasse 53 CH-8001 Zurich T +41 58 800 80 00 F +41 58 800 80 80 nkf.ch