# Cyber Security Breaches & Legal Emergency Response

WOLF THEISS

Dr. Lukas Feiler, SSCP

Associate, Wolf Theiss Rechtsanwälte GmbH

# What to Do if a Breach Occurs Despite all Security Measures?

WOLF THEISS

- There is no such thing as “100% security”
  - People are not perfect and do make mistakes
  - Computer systems are not perfect and do contain vulnerabilities
  - Advanced Persistent Threats (APTs) may have more resources than your corporation
- Preparedness is key
  - Know your notification obligations vis-à-vis affected customers
  - Know what is needed to fulfill these obligations
  - Develop a clear policy on criminal prosecution of perpetrators and know what type of evidence is needed

# Data Security Breach Notification

- Statutory duty to notify – Data Protection Act 2000
  - All affected customers have to be notified if you learn that
    - your customers' data is systematically and seriously misused and
    - the customers may suffer damages
  - Customers have to be notified immediately in "appropriate" manner

# Data Security Breach Notification

- Statutory duty to notify – Telecommunications Act 2003
  - New breach notification obligation will be enacted later this year
  - Scope
    - Covers all providers of public communications services
    - Is triggered by *any* security breach affecting personal data (no “systematic and serious misuse”-requirement)
  - Data Protection Commission to be notified immediately
  - Customers have to be notified immediately

# Data Security Breach Notification

- Contractual duty to notify
  - Implied duty to prevent harm to the other contracting party
  - Breaches have to be notified if there is a risk of harm
  - Determining the limits of this duty
    - Implied duties are inherently vague
    - Duty should be regulated/limited by specific contractual provisions

# Crisis Communication after a Security Breach

WOLF THEISS

- How not to:
  - Claiming that no personal data was affected when indeed it was, thereby challenging hackers to publish data as proof
- Efficient crisis communication requires that you already know how to fulfill your notification obligations
  - What type of personal data is maintained by the corporation?
  - Is the data encrypted? If so, how strong is the encryption?
  - How sensitive is the data?

Most of these questions can be answered *in advance.*

# Criminal Prosecution & Evidence Collection

WOLF THEISS

- There should be a clear policy on criminal prosecution of hackers
  - Important decision that should not be postponed until a crisis situation arises
  - Can serve as an important deterrent measure
- Knowing what type of evidence is needed
  - What is needed to establish a computer crime?
  - How can this evidence be obtained?
  - Most technological solutions focus on detecting intrusions, not monitoring their effects

    → Additional monitoring/logging often needed

# (Legal) Cyber Security Emergency Response

WOLF THEISS

1. Preparation
   1a. Know your duties & develop criminal prosecution policy
2. Detection
   2a. Breach notification
3. Containment
   3a. Evidence collection
4. Eradication

5. Recovery

6. Follow-Up

# Thank you for your attention!

WOLF THEISS

# Contact Details

Dr. Lukas Feiler, SSCP

Wolf Theiss Rechtsanwälte GmbH
Schubertring 6, 1010 Wien

Tel: (+ 43 1) 515 10 5090
Fax: (+ 43 1) 515 10 665090

email: lukas.feiler@wolftheiss.com

www.wolftheiss.com