Cybercrime and Data Breaches

PREVENTION

1. Has your company conducted a risk assessment?

1.1. Identify potential external and internal threats for your IT infrastructure and databases (e.g. hacker attacks, physical attacks, human errors, technical failure).

1.2. Identify and inventor sensitive and valuable data which require enhanced protection.

1.3. Analyze identified risks and distinguish between different kind and levels of risks taking into account the likelihood of occurrence and the severity of its consequences.

1.4. Include third parties (e.g. data hosting providers and subcontractors) in your risk assessment.

1.5. Locate weak points in your current risk management and control system to address them with adequate measures taking into account sector specific guidelines (e.g. FINMA Circular 2008/21). Involve top management into decision taking.

2. Based on the risk assessment, has your company implemented adequate organizational measures?

2.1. Set up cyber security and data processing policies defining the internal organization (in particular, the various responsibilities) and the implemented organizational and technical measures.

2.2. Set up an incident response team consisting of representatives from IT, legal & compliance, public relations & communications, regulatory affairs, HR and business operations.

2.3. Implement an incident response plan describing the reaction procedure and the responsibilities in the event of a supposed cyber security incident or data breach.

2.4. Define third parties' data protection and notification duties in service agreements and implement an emergency hotline (24/7) for them in case of cyber security incidents or data breaches.

2.5. Regularly inform and train employees in respect of potential cyber security threats and the correct behavior in the event of a supposed cyber security incident or data breach. Provide them with general principles to prevent incidents, clear guidelines of permitted data processing methods and reporting obligations, and regularly perform mock trainings to raise awareness.

Please note that this document is intended to convey general information only,
does not claim to be complete nor does it constitute legal advice.
Pestalozzi Attorneys at Law - Zurich, 15 March 2018

2.6. Implement an access matrix defining different access rights for business units and employees to databases based on the principle of least privilege (employees should only be granted rights they absolutely need).

2.7. Implement an appropriate management system for a regular risk reassessment, testing (simulated incidents) and amendment of the organizational and technical measures.

2.8. Consider to take out a cyber insurance against the financial consequences caused by cyber security incidents and data breaches.

3. Based on the risk assessment, has your company implemented state-of-the-art technical measures?

3.1. Protect physical access to buildings and IT infrastructure: limit number of persons with access; secure authentication and authorization; install alarm systems.

3.2. Protect access to data: limit access according to the access matrix; secure authentication and authorization; define a password policy and technically implement it.

3.3. Set-up secure remote access (e.g. RAS, VPN) from outside the organization: use two factor authentication and authorization.

3.4. Keep a database of all IT resources (hardware and software).

3.5. Segment your network into independent network zones.

3.6. Implement monitoring systems to rapidly detect cyber security incidents.

3.7. Implement multi-stage malware protection (anti-virus software, firewall, spam-filter, etc.).

3.8. Ensure automatic security updates for all elements in your IT infrastructure.

3.9. Anonymize or pseudonymize data to the extent possible.

3.10. Encrypt sensitive data, particularly when using cloud services and mobile devices.

3.11. Install logging mechanism to log all data access, input of new data, changes or deletions of data; keep secure log files; limit access to them and include them in backup system (log files are extremely important for following up a cyber security incident).

3.12. Define and regularly test backup and recovery procedure: define frequency of backups; save backup files independent of backed-up system (offline) and store them for a certain time period.

**Please note that this document is intended to convey general information only,
does not claim to be complete nor does it constitute legal advice.
Pestalozzi Attorneys at Law - Zurich, 15 March 2018**

REACTION

1. Has your company implemented an incident response team and plan describing the reaction procedure and responsibilities in the event of a supposed cyber security incident or data breach taking into account the following steps?

1.1. Detection and internal (or by third party) reporting of potential cyber security incidents or data breaches to responsible person/team.

1.2. Short period of initial investigation: gathering all relevant information; analysis and classification of incident; risk assessment; definition of objectives for first response.

1.3. Taking immediate actions to contain damage and to gather and preserve evidence (first response): blocking (and logging) of further unauthorized access, preventing spread of malware, etc.

1.4. Recovery of systems, data and connectivity, and validation that systems are operating normally again.

1.5. Decision about the necessity of a more thoroughly investigation and documentation of the incident.

1.6. Assessment whether and to whom (internal and external stakeholders) the incident should or must be reported.

- Internal communication to employees
- Information of concerned sub-contractors
- Notification to Federal Data Protection and Information Commissioner
- Notification to European Data Protection Authorities
- Information of affected individuals
- Notification to the Reporting and Analysis Centre for Information Assurance MELANI
- Notification to the Cybercrime Coordination Unit CYCO (Federal Office of Police)
- Notification to sector-specific authorities (FINMA, Federal Office of Communications, etc.)
- Information of the public

1.7. Assessment which legal actions against the perpetrator needs to be taken:

- Criminal complaints (e.g. for unauthorized obtaining or damage of data, unauthorized access to a data processing system, computer fraud, industrial espionage, breach of secrecies)
- Civil claims for injunctive relief and/or damages (e.g. due to breaches of contract, tort law, trademark and copyrights, data protection, unfair competition)
- Administrative remedies (e.g. request for blocking domains)

1.8. Carry out a post incident review and update organizational and technical measures.

Please note that this document is intended to convey general information only, does not claim to be complete nor does it constitute legal advice.
Pestalozzi Attorneys at Law - Zurich, 15 March 2018

2. Has your company already prepared standard documents related to the incident response plan such as the following?

2.1. Standard questionnaire and assessment system for initial investigation.

2.2. Overview of reporting obligations and standard notification and information letters to stakeholders.

2.3. Overview of possible legal actions.

2.4. List of external contacts (IT, PR, legal, etc.).

3. Has your company already prepared standard documents for your subcontractors?

3.1. Guideline summarizing the organizational and technical measures that must be put in place by subcontractors.

3.2. List of IT resources (hardware and software) that must be used by subcontractor.

3.3. Guidelines for further subcontracting.

Please note that this document is intended to convey general information only, does not claim to be complete nor does it constitute legal advice.
Pestalozzi Attorneys at Law - Zurich, 15 March 2018