KESSLER

CYBER RISK & INSURANCE
UPDATED 3RD EDITION (2021)

A SECURE FUTURE.

FOREWORD

If we look back at the situation five, just five, years ago, the question at the center of any advisory session was always the same: "What exactly could happen to us?"

Based on hundreds of discussions conducted with Swiss companies, it is now safe to say that corporate decision-making bodies are more than aware of the cyber risks lurking out there. Companies are familiar with the various scenarios, have quantified their cyber risks and insured any outliers. Working hand-in-hand with insurers, we have continually enhanced the products available, and insurers and brokers now settle a large number of claims. The learning curve was a steep one for all of us at times. In summary, our experience shows that Swiss companies have become more robust and, most importantly, are prepared in the event that something should happen.

Pascal Schweingruber
Member of the Executive Committee

In the 2020 fall session, the Councils adopted the new Swiss Federal Act on Data Protection (FADP). This has prompted us to issue a third updated edition of the Cyber Risk & Insurance publication to acknowledge the new legal aspects and share our experience in managing cyber risks.

I would like to thank the authors Simon Künzler (Risk Consulting), Melanie Koller (Legal), Nadine Janser (Special Risks), Simon Holtz (Property Insurance) and Patrick Dummermuth (Claims Advocacy) for their contributions and insights.

I hope that this publication gives you food for thought.

1
A PARTNERSHIP ON EQUAL TERMS

We help you create a cyber toolbox that makes your organization more resilient in the face of cyber attacks. This is an objective we can achieve thanks to our client-specific and holistic approach as well as analysis-based and hands-on technical and methodological skills.

BACKGROUND AND RISK EXPOSURE

Cyber attacks, the nature of which are constantly changing, find a fertile breeding ground in networked, complex and dynamic supply chains, information and communication infrastructures, the "Internet of Things" or "Internet of Everything" and, in particular, in what remains a careless approach to emails and the internet among employees. Digital innovations and developments, such as Industry 4.0, have opened up huge potential for rationalization and growth within organizations. On the other hand, they have also served to exacerbate the risk potential that was already significant to begin with. Overall, failures in the area of cyber resilience can compromise corporate governance and ultimately have serious financial and non-financial implications for a company. In this environment, cyber risks have to be analyzed comprehensively, evaluated and ultimately limited by taking suitable preventative and reactive measures.

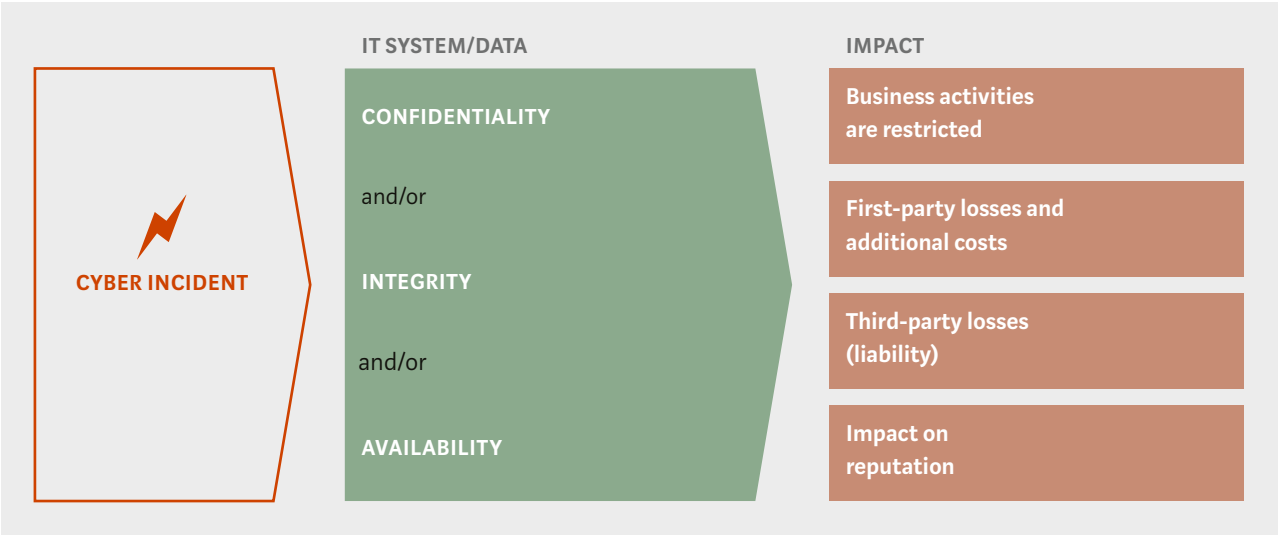
HOLISTIC UNDERSTANDING OF "CYBER"

Nowadays, most organizations are aware that cyber is an issue that not only has to be addressed by the IT department, but also needs to be embedded in a holistic enterprise risk management system. The human factor, and human user behavior, play a key role. This means that cyber is also a management and organizational topic and, as such, calls for a combination of technical, organizational, legal and financial measures. Knowing that there is no such thing as one hundred percent certainty, we recommend that measures be implemented transparently and as part of a continuous improvement process. Every organization should ensure that the organization can continue to function or normal operations can be restored as quickly as possible should a cyber incident occur.

CYBER RISK: WHAT IS IT?

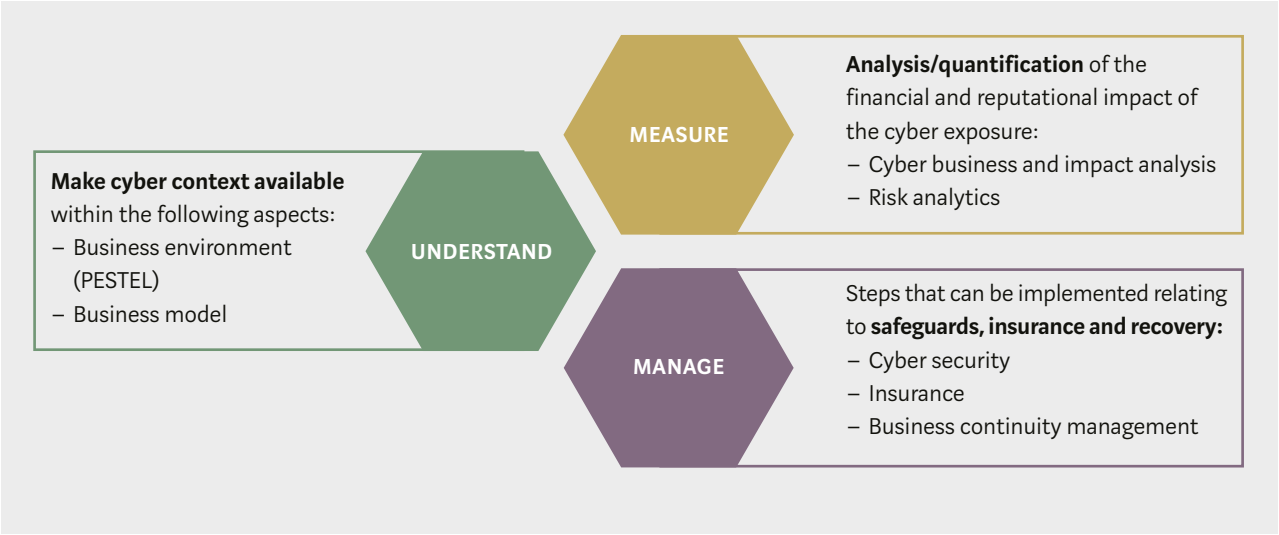
The risk relates to an attack on IT systems and/or a scenario in which data is compromised in terms of its confidentiality, integrity and availability. The impact can be of an operational, financial or non-financial nature, such as a serious loss of confidence among key stakeholders.

CYBER RISK



THREE-STAGE SOLUTION APPROACH

We use a three-stage approach to analyze the existing cyber risk.



1

PROJECT APPROACH

Thanks to the "Cyber Business and Impact Analysis" project approach, we help you understand, measure and manage cyber risks. One central element is the workshop that we organize with participants from various functional areas.

UNDERSTAND
Document analysis and interviews

- Desktop work
- Identifying potential exposures and vulnerabilities based on an analysis of the business environment and model
- Clarifying ICT dependencies
- Taking an inventory of physical and digital assets and infrastructures

MEASURE
Interdisciplinary workshop

- Developing cyber threat scenarios
- Evaluating and prioritizing the scenarios based on various cost parameters (risk matrix)
- Benchmark comparison
- Creating of a catalog of measures to improve the cyber toolbox

MANAGE
Cyber project report

- Summarizing project findings on the cyber threat situation
- Demonstrating the use of the holistic catalog of measures that has been prepared and provided
- Internal information/ communication
- Measures to raise awareness

2
CYBER RISKS

The term «cyber risk» is used in many different ways and refers to a number of risks connected with technology or with a company's information. In the insurance industry, cyber risks are defined as operational risks, generally meaning a loss of data or an IT/ICT disruption or malfunction that affects the confidentiality, availability or integrity of information or information systems.

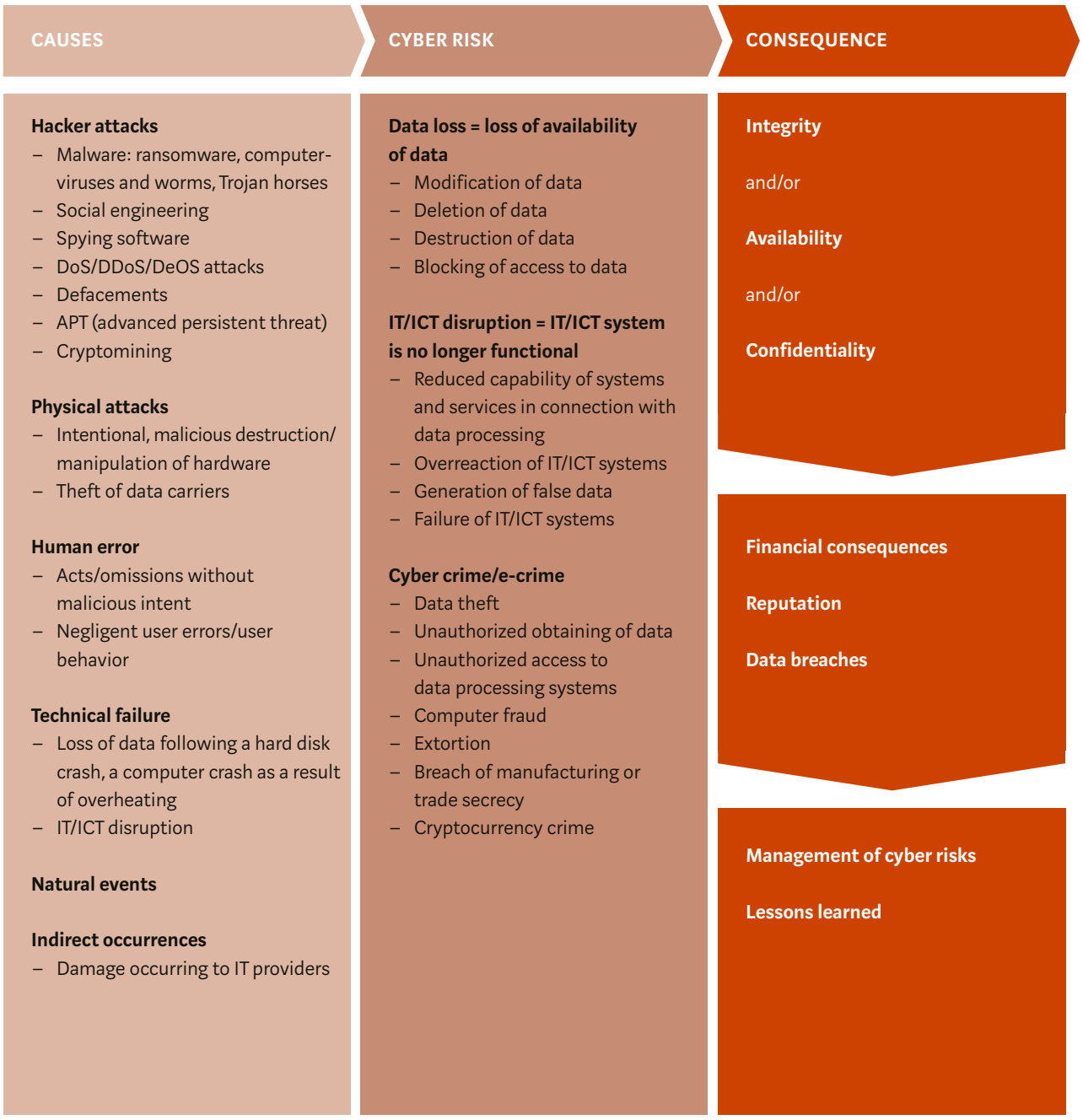
The cause-effect principle is a proven risk management tool and can be used to better understand a company's cyber risk landscape. Those who are familiar with the potential causes of worstcase scenarios at their company can institute targeted preventive measures with the help of a thorough cause analysis, and thus strengthen the overall IT technical and financial resilience of the organization.

Loss of data or an IT/ICT disruption can be attributed to either criminal or non-criminal causes (see page 10). According to the Swiss Criminal Code (StGB), criminal causes are usually criminal acts in and of themselves, independent of the resultant cyber risk (e.g. unauthorized obtaining of data for resale on the dark web in accordance with StGB 143 or unauthorized access to a data processing system for the purposes of espionage in accordance with StGB 143bis). Other criminal acts include the infiltration of an ERP system with malware and thus the manipulation of data integrity in accordance with StGB 144bis, or identity theft using the «fake president» fraud for the purpose of unlawful enrichment in accordance with StGB 147.

Above all, the increasing complexity of networked systems offers new opportunities to cyber criminals – including external third parties, current and former employees, competitors and even state organizations with various motives. Data which is worthless to one person can be extremely valuable to another. That's why companies are not safer from cyber criminals just because their management does not believe their data would be of much value to third parties. Anyone who wants to penetrate a system will find a way to do so, and thus a certain amount of inevitability has unfortunately become reality: there will never be any such thing as 100% cyber protection, and certainly not against a targeted attack (advanced persistent threat, APT).

2

CYBER RISK: CAUSE-EFFECT MODEL



2.1 FINANCIAL IMPACT

Cyber risk increases on a yearly basis, which is why close attention should be paid to assessing whether an organization can financially sustain the residual risk. An awareness of the financial risks can provide certainty in terms of financing. The losses caused by a cyber incident cannot be completely or conclusively quantified due to the lack of empirical data. These include:

FIRST-PARTY DAMAGE

- Cost of crisis management (IT forensics, legal advice, PR consultancy)
- Cost of notifying data subjects and authorities after a data loss
- Cost of data monitoring after a data loss
- Cost of processing requests for information
- Data protection fines
- Cost of restoring/replacing data and IT systems
- Cost of keeping IT systems up and running
- Cost of resuming business activities after an interruption to operations, incl. loss of profits
- Extortion payments and the related follow-on costs
- Loss of assets due to cyber fraud and social engineering, as well as related follow-up costs
- Cost of damage caused by external IT service providers
- Cost of enforcing your own rights that have been infringed by third parties (intellectual property)
- Defense costs in connection with regulatory proceedings
- Defense costs in connection with liability risks
- Cost of preventing or mitigating a potential liability risk
- Cost of determining the extent of the loss/damage
- Costs due to damage to your reputation

THIRD-PARTY DAMAGE

- Payment of third-party compensation claims following data privacy or security breaches
- Payment of claims for damages after a breach of privacy or offense against personal honor
- Payment of compensation claims following a breach or loss of third-party intellectual property
- Payment of compensation claims following a breach of competition, copyright and trademark law or a duty of confidentiality
- Payment of compensation or contractual penalties following a breach of contract

2

2.2 IT SUPPLY CHAIN RISK – WHO HAS AN EYE ON THE OVERALL PICTURE?

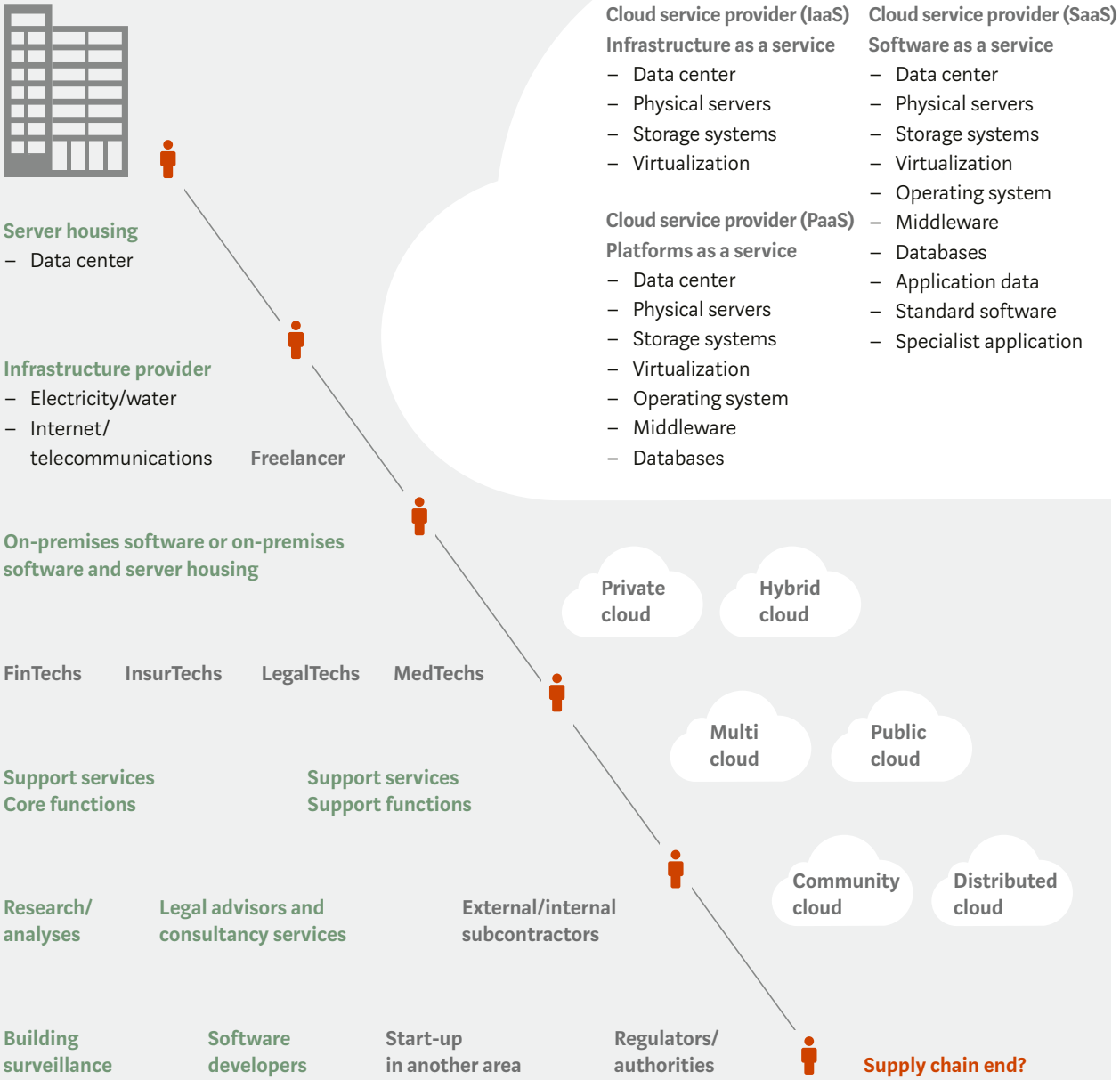
In today's digitally networked business environment, an IT system that runs smoothly is one of the most important prerequisites for a company's success. As services, systems, processes or facilities are outsourced, reliance on third-party companies increases. At the same time, the oversight of all the suppliers and the missing resources to ensure the ongoing assessment of cyber risk is lost.

Nowadays, investors, savvy clients or the supervisory authorities (such as FINMA or supervisory authorities for pension funds) are increasingly calling for the risk-based management of IT business partners. To ensure that the IT supply chain does not become/remain a black box for you and your key stakeholders, we recommend that you review IT suppliers based on your own needs.

- Which IT service providers are we dependent on? In which business area is data, and what kind of data, processed by whom (particularly sensitive personal data, sensitive production data, contractual conditions of major clients, strategic documents, etc.)?
- Which and how many employees of the IT service provider have access to our company's systems/can view this data?
- Which employees of the service providers have which administrator rights?
- How is the Service Level Agreement structured? Who is liable for what in the event of a network failure?
- Are we familiar with the key individuals and major cyber risks in the IT supply chain?
- Is the management aware of the financial impact of the relevant IT suppliers? What costs does the insurance policy cover?
- Who in our company has an overview of the aspects to be checked before a contract is signed with an IT service provider?

Graphic on the right: an average SME can have a good 20 to 50 IT service providers. The more international and the more digital the business model, the longer the IT supply chain. The human factor is known to be one of the biggest cyber/IT security weak points. Three aspects are important to know: Who belongs to our IT supply chain? Which employees of our own company and IT service providers are key to the success of our business model? And which key individual has which authorizations and which administrator rights? The answers can be used to develop targeted preventative measures or make a conscious decision on whether or not to assume a corresponding cyber risk.

WHO BELONGS TO OUR COMPANY'S IT SUPPLY CHAIN?



3
CORPORATE GOVERNANCE

Cyber security is a governance challenge. Questions associated with a great deal of uncertainty include: how do boards of directors structure their cyber security supervision and how do they interact with management on this key issue? Every time a loss occurs, the question arises as to whether the board of directors was, or should have been, aware of the existing cyber risks. The answers vary considerably from case to case and depend on the industry in question or on state-of-the-art data security safeguards. This is why every major cyber claim gives rise to the question as to whether the board of directors is liable for it. This makes conscious decisions all the more important.

3.1 DUTIES OF THE BOARD OF DIRECTORS

In connection with the enormous potential losses that can be caused by cyber risks, the increasingly complex duties incumbent upon the board of directors of a joint stock company are beginning to take center stage.

DELEGABLE DUTIES

The board of directors is the supreme executive body of a joint stock company, unless responsibility for managing the company has been delegated. When it delegates its duties, the board of directors is liable for damages caused by third parties if it cannot prove that it has exercised the requisite care in selecting, instructing and monitoring said third party (CO 716, para. 2 in conjunction with CO 716b, para. 1 in conjunction with CO 754, para. 2).

NON-DELEGABLE DUTIES

The full board of directors maintains complete responsibility for non-delegable and irrevocable duties of the board of directors. The inability to delegate duties is limited to finding and making decisions and making conscious decisions, although preparatory duties as well as the implementation of resolutions may be delegated to operational bodies.

According to prevailing doctrine, the following duties, among others, are considered to be non-delegable duties of the board of directors:

- Supervisory and strategy duties that aim to safeguard the interests of the company
- Risk assessment: As part of its management report, the board of directors must, among other things, assess the key business risks (CO 961c, para. 2, no. 2). In particular, this includes assessing current market risks, credit risks and supply risks as well as financial and operational risks, such as IT, security, product and legal risks, cyber risks as well as the future prospects of such risks. All companies legally subject to ordinary audits must prepare a management report (CO 961 in conjunction with 727).
- Decisions about the risk financing strategy and IT/ICT security strategy

CORPORATE GOVERNANCE – PREREQUISITES FOR MANAGEMENT DECISION

Non-delegable duties of the board of directors:
- Supervisory and strategy duties
- Assessment of key risks
- Decisions about the risk financing strategy or IT/ICT security strategy

Management decisions are based on:
- Appropriate and adequate information = all legal information relevant to specific decisions must be obtained
- Weighing up of all the advantages and disadvantages of alternative courses of action and their repercussions/ financial consequences

Are the prerequisites for a management decision met?

YES	NO
Management decision = conscious decision	Management decision ≠ conscious decision
Business judgment rule met	Business judgment rule not met
Even if the decision proves to be wrong, no breach of duty or liability under CO 754	Breach of duty or liability possible under CO 754

3

3.2 CONSCIOUS DECISION AND ITS RELEVANCE

The board of directors is liable to the company for carefully preparing, evaluating and implementing all decisions – but not for the success of these decisions. As such, a prudent and impeccable decision-making approach/process is the main focus here. This also applies to decisions on risk financing for the biggest risks and whether these risks should be self-financed or transferred.

CONSEQUENCES OF AN INCORRECT MANAGEMENT DECISION

In such a case, no breach of duty by the administrative bodies is deemed to have occurred if the management decision was based on appropriate and sufficient information and was made on the basis of a serious decision-making process. This includes having an appropriate and adequate process for obtaining all factual and legal information relevant to the specific decisions to allow the advantages and disadvantages of alternative courses of action and their repercussions/financial consequences to be weighed up thoroughly (see also BGer 4A_97/2013, cons. 5.2; BGE 139 III 26).

DIRECTORS AND OFFICERS LIABILITY (D&O LIABILITY) CO 754

Experts in the insurance industry point to the US and predict that, in future, cyber claims in Europe will increasingly be asserted under cyber and D&O insurance; this will have consequences for the consideration of cumulative risks, which are already taken into account by insurers and reinsurers during the underwriting process.

If management take inadequate security measures to prevent hacker attacks, or if said measures indirectly provide inadequate protection for their assets, the individual bodies can be held liable for this omission. From a legal point of view, lacking or inadequate cyber risk management or a non-conscious decision on risk financing may qualify as a breach of the duty of care or loyalty within the meaning of CO 717 and give rise to liability claims against a company's directors and officers under CO 754. Likewise, a deliberate or grossly negligent failure to comply with obligations under the EU GDPR, which require the implementation of certain security standards, may lead to stricter liability conditions for corporate governance.

In addition to members of the board of directors, all other people entrusted with management of the company are subject to D&O liability. These so-called de facto bodies carry out business-related duties of their own accord and have a decisive impact on the company's decision-making.

BUSINESS JUDGMENT RULE

Within the framework of directors and officers liability, the business judgment rule is assessed in accordance with CO 754. According to the formulation of the Swiss Federal High Court in its ruling 4A_74/2012, cons. 5.1, courts must exercise restraint in their retroactive assessment of business judgments if such judgments were made on the basis of a sound decision-making process that was based on an appropriate information basis and were free of conflicts of interest. A corporate management body only acts in breach of its obligations if a business decision is unjustifiable. For this reason, companies are well advised to make their business decisions consciously and document them fully.

EQUIFAX: LIMITS OF THE BUSINESS JUDGMENT RULE

Class actions filed after data security incidents due to a possible lack of cyber security result in companies or their responsible executive bodies being held liable. When it comes to assessing whether decision makers have complied with their due diligence obligations, the court will look for evidence showing whether the responsible individuals acted intentionally and competently, and identified and investigated alternatives to the conscious decision to accept the risks concerned.

The limits of the business judgment rule are illustrated by a very recent class action lawsuit against Equifax in early 2020: the plaintiffs claim that Equifax used the username "admin" and password "admin" to protect a credit dispute management portal, meaning that they chose a password that was a surefire way to get hacked. They claim that Equifax also left the keys needed to unlock the encryption of servers containing sensitive data on the same publicly accessible servers, making it easy to decrypt the data. These allegations will not make it easy for Equifax to prove that due diligence was exercised in a manner that was commensurate with the risk involved. The business judgment rule is of no help in a scenario like this either because, when it assesses whether the responsible individuals fulfilled their due diligence obligations or violated the business judgment rule, the court will look for evidence showing whether the decision makers acted intentionally and competently, and identified and investigated alternatives to the protective measure that was ultimately implemented. Those who basically ignore their responsibility for cyber security or recklessly expose the company to a risk in a quest to protect it will most likely not find a source of protection in the business judgment rule.

"NATIONAL STRATEGY FOR THE PROTECTION OF SWITZERLAND AGAINST CYBER RISKS 2018–2022" UNDERLINES THE IMPORTANCE OF CYBER RISKS

In Switzerland, various projects at federal level, such as the "National Strategy for the Protection of Switzerland Against Cyber Risks 2018–2022" or the expansion of the "Cyber Defense", show how essential cyber risks are and the priority that must be assigned to them. The fact that cyber and IT risks are universally present in both the private and public sectors means that they cannot be ignored. The larger and more system-critical a company is, the less ignoring or talking down the need for measures to prevent cyber risks is an option.

DOCUMENTATION OF BUSINESS DECISIONS

Business decisions and conscious decisions must be documented (CO 713, para. 3), as documentation such as the minutes of meetings of the board of directors may have to be produced as part of an evidence-gathering procedure (CPC 160, para. 1, let. b).

Based on the decision-making criteria, the advantages and disadvantages of different courses of action and their financial consequences must be documented. Reasons must be provided for the conscious decision. Corporate bodies that may be subject to conflicts of interest should not participate in the process for reaching a conscious decision.

4
WHAT DO DATA PROTECTION AND DATA SECURITY HAVE TO DO WITH CYBER RISK?

Practically every cyber incident results in the integrity, availability or confidentiality of personal and/or company data being breached. Consequently, every case of unintentional or unlawful destruction, loss, modification, disclosure or blocked access to data (business interruption) always raises the question as to which data protection laws and which other sector-specific laws are affected, and what regulatory measures or obligations result from them. While some data security breaches can be traced back to criminal cyber attacks, non-criminal causes such as technical IT faults or an email that was forwarded to the wrong recipient can just as easily result in data loss.

In today's business and legal environment, accountability and the resulting documentation of data protection measures is becoming increasingly important for company management teams. The documentation of the conscious decision regarding the implementation approach for, and the prioritization of, data protection obligations as well as the reasons justifying the strategy adopted based on the technical and organizational measures (TOM) implemented are another important factor.

The TOMs are to be implemented in line with the state of the art. The "state of the art" is an undefined and dynamic legal concept, but one subject to full judicial review, referring to the industry-specific security standards that are constantly subject to change. In the event of a cyber claim, the companies responsible have to prove that the TOMs they used are state of the art. "State of the art clauses" are also widely used in cyber insurance policies, and insurance cover can be denied or reduced if TOMs are not implemented in accordance with the state of the art.

COSTS CONNECTED WITH BREACHES OF DATA PROTECTION LAW CAN BE ESTIMATED ON THE BASIS OF THE CORRESPONDING LAW AND ARE AT PRESENT LARGELY INSURABLE:

- Notifying the authorities or those affected
- Costs for regulatory proceedings
- Certain data protection fines
- Payment of third-party compensation claims following data privacy breaches, including legal and consulting fees during regulatory proceedings, data protection fines, costs of crisis management, reporting expenses

4.1 SWITZERLAND AND THE INFLUENCE OF THE EU: TOPICS FOR THE PERIOD LEADING UP TO 2022

On September 25, 2020, the Swiss Parliament adopted the amended Swiss Federal Act on Data Protection (FADP). COVID-19 meant that the procedure for the resolution of differences took longer than originally planned. Corresponding ordinances will be drawn up and submitted for consultation before the Act enters into force in 2022. The two-year transitional period that was originally planned and would have spared responsible companies from their obligations for the first two years has been scrapped. This makes it all the more important to plan the preparations for FADP compliance with specialists early on.

Furthermore, the European Commission's adequacy decision, which is designed to allow the unhindered transfer of data from the EU to Switzerland to continue, is still pending. Until a decision is taken, however, the current Commission decision of July 26, 2000 will continue to apply as it has no expiry date. The EU is not obliged to make this adequacy decision on the data protection legislation in Switzerland. The question therefore arises as to what political agenda the EU is pursuing with this decision. It is important to note that Switzerland will be considered a third country with adequate data protection for the EU until this decision is revised. With regard to the EU's political agenda, it is worth taking a look at the Schrems II judgment of July 16, 2020 in which the European Court of Justice declared the EU-US Privacy Shield to be null and void with immediate effect, meaning that the transfer of personal data from the EU to the US is no longer considered secure from a data protection law perspective. There is now a new requirement for additional contractual protection, which translates primarily into higher costs and additional work for the companies affected.

The impact of the Schrems II judgment is also being felt in Switzerland: although the Swiss-US Privacy Shield is valid until it is declared null and void by the Federal Supreme Court, the statement released by the Federal Data Protection and Information Commissioner (FDPIC), according to which the Swiss-US Privacy Shield is also said not to provide sufficient protection for data transfer from Switzerland to the US, could serve as a point of reference for a future court decision on the Swiss-US Privacy Shield. In this respect, Swiss companies that transfer personal data to the US are urged to keep an eye on the situation and take measures at an early stage if necessary.

4

4.2 COMPARISON OF REPORTING OBLIGATIONS SWITZERLAND/EU

Being aware of the existing data protection categories within a company helps it to assess what reporting obligations have to be observed in the event of a security breach. As a preventative measure and in order to keep the costs incurred following a data breach to a minimum, companies are advised to make certain preparations for a potential data breach.

	CURRENT LEGAL SITUATION IN CH **Federal Act on Data Protection (FADP)** In force: July 1, 1993 (1st revision 2008)	**FUTURE LEGAL SITUATION IN CH** **Amended FADP** Entry into force no earlier than 2022 (2nd revision)
Categories of data and related reporting obligations	– **Personal data (natural persons and legal entities)** – **Particularly sensitive personal data** Data concerning religious, ideological, political or trade union-related views or activities; data concerning health, the intimate sphere or the racial or ethnic origin; data concerning administrative or criminal proceedings and sanctions; data concerning social security measures.	– **Personal data (amended FADP Article 5a)** – **Particularly sensitive personal data (amended FADP Article 5c)** Data concerning religious, ideological, political or trade union-related views or activities; data concerning health, the intimate sphere or the racial or ethnic origin; genetic data; biometric data that uniquely identifies a natural person; data concerning administrative or criminal proceedings and sanctions; data concerning social security measures. – **Risk-based data protection: data whose processing poses significant risk to the personality or fundamental rights of the data subject.** The D-FADP is based on the potential risks of the data subject because the privacy of the data subject depends in large part on the activities of the responsible party and the order processor. It is assumed that the risk is substantial if a company is obligated to provide a data privacy impact statement. This is the case, for example, when there is substantial processing of particularly sensitive personal data or when large public areas are monitored systematically.
Notification obligation	**No** express statutory notification obligation	**Obligation to provide notification in the event of a breach of data security** which may lead to **substantial risk** to the personality or fundamental rights of the data subject **(amended FADP Article 24).** – **Controller's reporting obligation:** Federal Data Protection and Information Commissioner (FDPIC) to be notified as soon as possible. – **Processor's reporting obligation:** Controller to be notified as soon as possible. – **Controller's reporting obligation:** Natural person affected to be notified if this is necessary for their protection or if the FDPIC so requires (discretionary power).
Legal consequences in the event of a breach	**Criminal penalties:** Max. fine of CHF 10,000.00	**No fine** for breaches of notification obligation **Liability, claim for damages asserted by the data subject or further criminal sanctions outside the GDPR are possible.**

Important to know:
1. What happened? Which data categories are affected? 2. Who is responsible internally for making the notification?
3. Who do we report to? 4. How do we have to submit our report? 5. Within what period of time?

CURRENT LEGAL SITUATION EU/EEC
EU General Data Protection Regulation (GDPR)
Entry into force in the EU: May 25, 2018 / EEA: July 20, 2018

- **Personal data**
- **Special categories of personal data**
  Personal data that reveals racial or ethnic origin, political opinions, religious or ideological views, trade union membership as well as genetic information, biometric information that allows for clear identification of a natural person, data concerning health or details about the sex life or sexual orientation of a natural person.

- **Risk-based data protection: data whose loss poses a high risk to personal rights and freedoms.**
  The GDPR does not indicate the cases in which there is not a high risk to the personal rights and freedoms of the data subject, meaning that the risk has to be weighed up based on the potential impact of the breach of data confidentiality, integrity and availability. For example, in the event of a breach of the confidentiality of personal data resulting in damage for the data subject: theft of login details and purchase history at a provider, comprised health or payment information, marketing emails are sent in a manner that allows recipient to see all of the other recipients, etc.

Obligation to notify personal data breaches (GDPR Article 33)
- **Controller's reporting obligation:** Notification to the competent supervisory authority without undue delay and, where feasible, not later than 72 hours.
- **Processor's reporting obligation:** Notification to the controller without delay.

Obligation to notify in cases involving a "high risk" to the rights and freedoms of the data subject
- **Controller's reporting obligation:** Notification of the data subject without delay.

Fines following an infringement of the notification obligation (GDPR Article 83 (4))
Fines of up to EUR 10 million or up to 2 percent of the total worldwide consolidated annual turnover.

Liability, claim for damages asserted by the data subject or further criminal sanctions outside the GDPR are possible.

4

4.3 USING A TAILOR-MADE ACTION PLAN TO ACHIEVE FADP COMPLIANCE: STARTING WITH THE BASICS

4.4 CATALOG OF FINES IN THE AMENDED FADP

The amended FADP contains a more extensive criminal law section and also provides for tougher sanctions than those set out in the version of the FADP that is still in effect in the event that responsible executive bodies breach their obligations. The fines are increased to a maximum of CHF 250,000 and are primarily directed at the natural person in the company who is to blame (particularly the decision maker). In cases involving fines of up to CHF 50,000, the company itself may be ordered to pay the fine as an exception.

The Federal Data Protection and Information Commissioner (FDPIC) can only make recommendations but cannot impose fines. The authority to impose fines remains with the cantons. Only willful intent, and not negligence, is to be penalized. The option of criminal prosecution becomes statute barred after a period of five years (amended FADP Article 66).

The following catalog of fines gives a rough overview of the breaches of duty that can be penalized.

PRIVATE INDIVIDUALS ARE FINED UP TO CHF 250,000.

Article 60: Breach of obligations to provide access and information or to cooperate, such as...
- Breach of/failure to fulfill the obligation to inform data subjects when collecting personal data (Article 19)
- Breach of/failure to fulfill the obligation to inform data subjects in the case of an automated individual decision (Article 21)
- Breach of/failure to fulfill the right of access by the data subject by deliberately providing false or incomplete information (Articles 25-27)
- Breach of obligations to cooperate by deliberately providing false information to the FDPIC in the course of the latter's investigation or deliberately refusing to cooperate (Article 49 para. 3)

Article 61: Violation of confidentiality obligation, such as...
- Violation of the principles regarding the cross-border disclosure of personal data (Article 16 para. 1, 2)
- Violation of obligations in the context of data processing by processors (Article 9 para. 1, 2)
- Failure to meet the minimum data security requirements (Article 8 para. 3)

Article 62: Violation of professional secrecy, such as...
- Anyone who willfully discloses secret personal data of which they have gained knowledge while exercising their profession that requires knowledge of such data
- Anyone who willfully discloses secret personal data of which they have gained knowledge in the course of their activities for a person bound by a confidentiality obligation or in the course of training with such a person

Article 63: Disregard of decisions
- Anyone who willfully fails to comply with a decision issued by the FDPIC or a decision issued by the appellate authorities

FINES OF UP TO CHF 50,000 CAN BE IMPOSED ON UNDERTAKINGS (ARTICLE 64).

4.5 DIGRESSION: US DATA PROTECTION LEGISLATION

A PATCHWORK QUILT OF LEGISLATION

There is no universally applicable data protection legislation in the US, unlike in Switzerland with the FADP or in the EU with the GDPR. Instead, the US has various data protection laws to protect the data of natural persons at national, state and regional level. In addition to or instead of these laws, one or more of the over 20 sector-specific data protection laws can be applied depending on the subject area, for example in the areas of finance, health or trade. The question as to how these laws compete with each other has to be examined on a case-by-case basis.

Unlike in Switzerland and the EU, data protection is not a fundamental right in the US, but rather falls under consumer protection law. This explains why the Federal Trade Commission, which is also responsible for supervision under competition and consumer protection law, is the body responsible for data protection in the US. The US does not have any independent data protection authority like Switzerland or the EU.

DATA BREACH NOTIFICATION

Data Breach Notification Laws are in place in all 50 US states. In the event of data loss or the accidental publication of data, the company that is affected by this sort of breach is obliged to notify the governments of the states concerned.

CALIFORNIA LEADS THE WAY IN DATA PROTECTION LAW

Of all the 50 states, California was the first state to enact a security breach notification law (California Civil Code section 1798.82) in 2002, making it a model state for data protection law with the California Consumer Privacy Act of 2018 (CCPA, in force since January 1, 2020). The scope of the CCPA is limited to the State of California and gives consumers the right to access and erase personal data held by companies. The law also obliges companies to provide consumers with adequate data security. Due to the extraterritorial effect, companies that do not have any physical presence in California can also fall under the scope of the CCPA.

1. Requirements for the scope of application of the CCPA

- Collection of personal information from California residents; and
- Company does business in California; and
- Alternatively: annual revenue of over $25 million or processing of data from more than 50,000 people or devices, or more than 50% of annual revenue is generated from the sale of consumer data.

2. Risks for companies

Fines of between $2,500 and $7,500; being confronted with civil class actions and damages payments of between $100 and $750 per affected consumer and per incident or corresponding to the actual damage incurred, whatever is higher; legal proceedings also for foreign companies if covered by the CCPA.

3. Effectiveness of the CCPA

The law's effectiveness is called into question because there are no obligatory safeguarding procedures or sanctions for non-compliance and the monetary fines are low, especially in comparison with the GDPR.

5
INSURABILITY OF CYBER RISKS

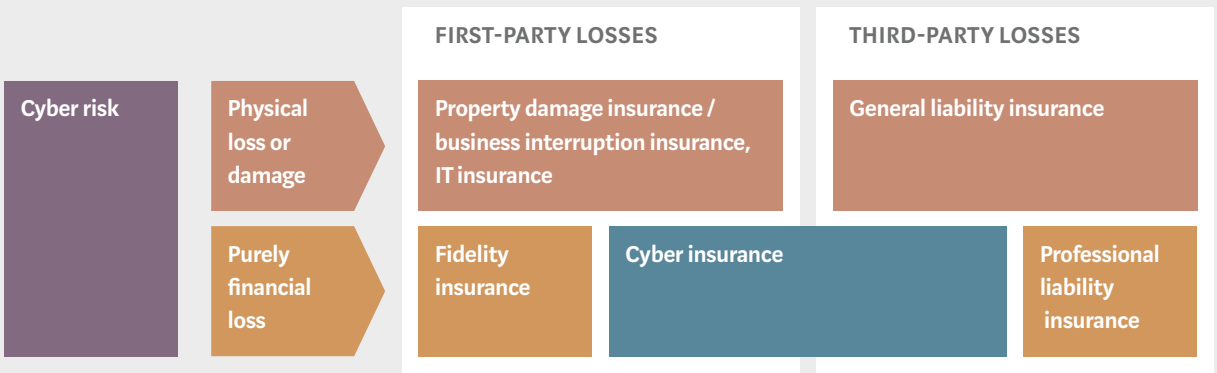
Insuring cyber risks poses new challenges for the insurance industry. Risks such as fire, property and business interruptions are subject to natural risk distribution. It is unlikely that hundreds of major fires will break out on the same day in Switzerland. However, cyber risks can spread virally and damage many companies simultaneously. In some cases, this could result in a cumulative risk for insurers that is difficult to calculate and for which multiple insured risks covered by the same insurer may be affected by a single loss event.

As a result, the insurance industry has developed special cyber insurance policies that can cover key components of a company's cyber risk. By concentrating cyber risk in a separate insurance solution with its own underwriting process, insurers can develop a sound understanding of the risk. Clients on, the other hand, receive a comprehensive insurance solution focused on cyber risk.

In order to better control accumulation risk, insurers have recently started to offer no or only limited insurance cover for cyber risks in conventional insurance policies. Despite this development, the scope of cover is not yet set out transparently in all policies. Policies with what is known as silent cover (silent cyber) still exist. This is why coordination with conventional insurance policies remains a challenging process and one that is essential in order to avoid gaps in cover. Our cyber specialists carry out a comprehensive gap analysis for each and every one of our clients.

The graphic below shows how cyber insurance can be placed in the context of conventional insurance policies. Typically, cyber insurance covers purely financial loss and combines first-party and third-party losses.

CYBER RISK FROM THE PERSPECTIVE OF THE INSURANCE INDUSTRY



5

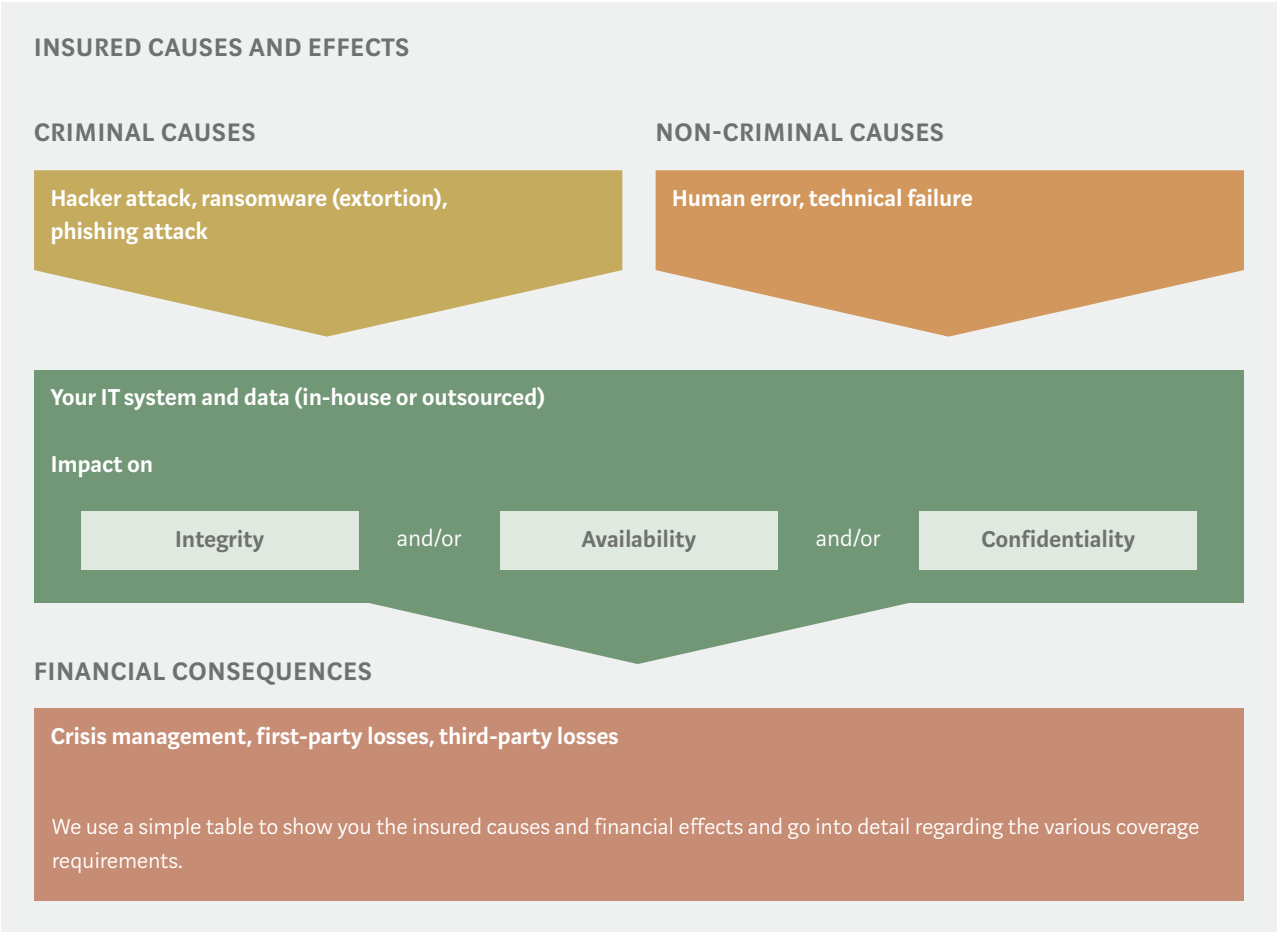
5.1 CYBER INSURANCE: INSURABLE LOSSES

Not all insurers offer the same insurance cover under the same cover modules. Based on the analysis of your company's cyber risk, we assess the different products offered by various insurers for you.

The graphic on the right shows the scope of the cover.

- Crisis management comprises the services provided by the insurer via external partnerships in the areas of IT forensics, legal advice and PR consultancy.
- Insurance includes first-party losses (business interruption and additional costs) as well as third-party damage. First-party losses refer to the costs incurred due to a cyber incident. Third-party losses refer to the assumption of justified claims for damages as well as defense against unjustified claims.

The extent to which the providers insure the causes and financial implications set out in the graphic forms part of the negotiations conducted by Kessler. The same applies to the scope of cover for IT outsourcing.


INSURED CAUSES AND EFFECTS
CRIMINAL CAUSES
NON-CRIMINAL CAUSES
Hacker attack, ransomware (extortion), phishing attack
Human error, technical failure
Your IT system and data (in-house or outsourced)
Impact on
Integrity
and/or
Availability
and/or
Confidentiality
FINANCIAL CONSEQUENCES
Crisis management, first-party losses, third-party losses
We use a simple table to show you the insured causes and financial effects and go into detail regarding the various coverage requirements.

5

5.2 FIDELITY INSURANCE

For the insurance industry, purely financial losses resulting from social engineering are not actually cyber risks because the perpetrators' actions do not involve any intervention in the IT system. Fidelity insurance can provide cover for these risks.

Whereas cyber insurance recognizes any sort of hacker attack as an insured cause, not all the financial implications of these attacks are insured. Social engineering offenses are one well-known example: data recovery costs arising from the spread of viruses after a phishing attack are covered by cyber insurance. The direct financial loss in the form of a fake bank transfer, on the other hand, is either not insured at all or is only covered to a limited extent. There are two reasons for this.

Firstly, the majority of attacks like these take place without any intervention in an IT system but by only using emails with forged sender addresses. In these emails, business partners report changes in bank account details or alleged notifications from banks are used to ask the recipient to update their login data using a link. In other cases, attackers make phone calls in which they pretend to be a client, a member of IT support or the CEO. Secondly, from the perspective of the insurance market, fidelity insurance is already an insurance solution that protects the company's balance sheet against IT-based criminal acts and insures the purely financial losses arising from these acts.

So it is worth checking carefully whether your insurance requirements also include a separate fidelity insurance policy. After all, the shift towards working from home and the associated changes in work processes and access rights to company IT create an environment that is much more susceptible to IT-based criminal acts. But not all policies insure losses like these. This is because the main risk insured is unlawful personal enrichment by an employee.

5.3 PROPERTY AND BUSINESS INTERRUPTION INSURANCE AND TECHNICAL INSURANCE

Property insurers have reacted to the increasing number of cyber claims by adapting their terms and conditions or making them more specific. Today's policies no longer include silent cyber coverage, meaning that there is no confusion about what is and is not insured. The insurance cover for cyber-related property damage is explicitly described in the policy. The way in which the cover is implemented varies considerably from insurer to insurer.

In general, there has to be physical damage to property that must then be responsible for business interruption losses. Data itself does not constitute "property", meaning that it cannot be damaged for the purposes of this insurance. If, however, the data medium on which the data is stored is damaged or destroyed, such as due to a fire, the costs of recovering the data from a back-up will be reimbursed. No indemnity, however, will be provided for the data itself.

A targeted cyber incident can, for example, trigger a fire that destroys an IT system, a production machine or even a building. In the worst case, this can, in turn, lead to a business interruption. In such cases, the property and business interruption insurance will cover the damage because the fire caused damage to property.

The same applies if a key supplier becomes unavailable. This could be a company's electricity supplier or IT service provider, for example. Property damage insured under the company's own policy as part of its CBI cover must have been incurred by the supplier. The reason for the power cut or the outage experienced by the IT service provider must be something like a fire. The mere unavailability of electricity or data due to a cyber incident that has encrypted important data, for example, does not constitute damage to property.

There are also technical insurance policies that include electronics and machinery insurance. Although the insured events are typically defined a little more broadly in these policies due to the all-risk approach, the general requirement of physical damage to property also applies here. This means that the mere fact of an IT system or piece of machinery not working due to a cyber incident is not covered by the insurance.

6
FROM CYBER INCIDENT TO INSURED CYBER EVENT

One in four cyber insurance policies already has a claims history. This also steepens the learning curve for the companies and experts concerned. Insurers have made continuous improvements to crisis management and claims handling and can now show policyholders how effective the preventative measures can be. Kessler supports you throughout the entire process to ensure efficient claims handling.

BEFORE THE EVENT

CYBER INCIDENT

Develop a cyber risk management process
- Identify, protect, detect, react and ensure continuous monitoring
- Review liability clauses in contracts with clients, suppliers and IT service providers
- Check dependencies on suppliers and IT service providers
- Implement preventative measures, such as training sessions to raise awareness among employees
- Make a conscious decision in favor of internal or external financing of cyber incidents

Create an incident response plan, business interruption plan and disaster recovery plan
- Identify experts in the fields of IT forensics, legal advice and PR consultancy
- Rehearse situations in which IT systems are not available or cannot be trusted for a number of days or weeks, and set up alternative communication channels
- Test plans on a regular basis and evaluate results

INSURED CYBER EVENT

Preparatory measures
- Identify and contract experts from the fields of IT forensics, legal advice and PR consultancy and conduct onboarding meetings

Be familiar with the ins and outs of the insurance policy
- Communicate the emergency number to the individuals involved
- Comply with contractual obligations (e.g. reporting obligations in the event of an aggravation of risk)

	CYBER INCIDENT	INSURED CYBER EVENT
DURING	**Materialization of cyber risk** – Data loss – IT/ICT fault – Cyber crime/e-crime **Immediate measures** – Consult the incident response plan – Consult defined experts in the fields of IT forensics, legal advice and PR consultancy – Initiate and coordinate the defined measures (see also notifications) – Ensure ongoing documentation of the cyber incident regarding the course of events leading up to its occurrence and costs **Notifications** – Check the statutory reporting obligations or voluntary notification to authorities and data subjects – Involve the police to secure evidence – Check the obligation to notify employees, the media and/or ad-hoc disclosure obligations	**Immediate measures** – Dial the emergency number: experts in the fields of IT forensics, legal advice and PR consultancy are consulted – Report the cyber incident immediately to Kessler and/or the insurer and continue close cooperation **Further measures** – Have expenses approved by the insurer in advance – Comply with the obligations to mitigate the damage – Identify and involve experts for damage quantification purposes early on – Case settlement with the insurer: submit documents to facilitate an assessment of the facts of the case and allow the insurance cover to be verified; obtain possible advance payment
AFTER	**Lessons learned** – Validate the services provided by the experts in the fields of IT forensics, legal advice and PR consultancy that were involved in the matter – Review the incident response plan, business interruption plan and disaster recovery plan	**Lessons learned** – Validate the services provided by the insurer(s) as well as the experts in the fields of IT forensics, legal advice and PR consultancy that were involved in the matter – Check the selected limit of indemnity and deductibles

7
THE TWO-PHASE PROCESS

For your individual cyber insurance solution, you will be assisted by our Cyber Team which specializes in cyber risk management and cyber insurance. It has extensive expertise and relevant practical experience. In the interests of our clients, we regularly coordinate with our network partner Marsh, which develops global cyber insurance solutions. For your cyber insurance needs, we recommend a two-phase process, although it is of course possible to start with phase 2 immediately.

7.1 PHASE ONE: CYBER RISK DIALOGUE

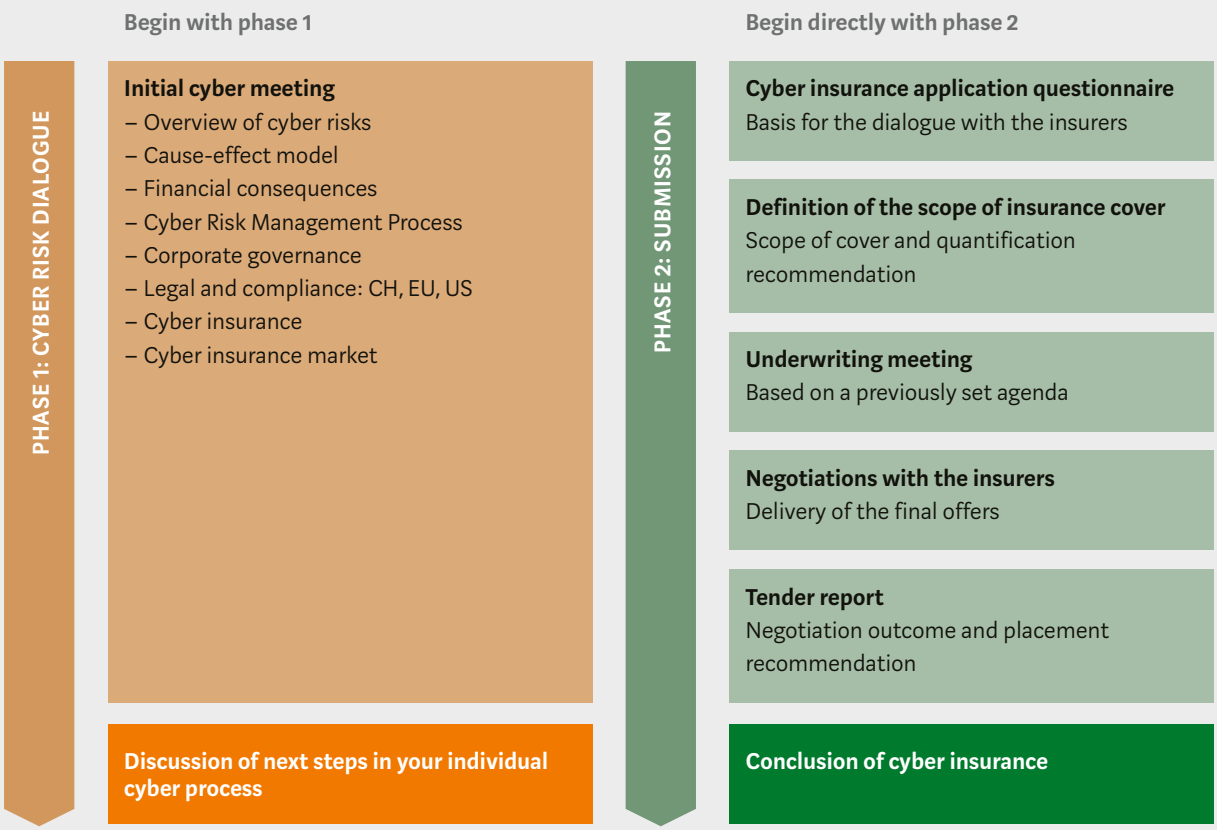
As part of risk management and with the purpose of promoting optimal corporate governance at your company, we meet with you to discuss your company- and sector-specific cyber risks, the associated internal organizational and information processes, and the constantly changing legal aspects, in particular in relation to Switzerland, the EU and the US. This serves as a basis for us to plan the next steps.

7.2 PHASE TWO: OBTAINING BINDING OFFERS

We recommend starting negotiations with three leading suppliers. After receiving the cyber insurance application questionnaire, we will work together to determine the scope of insurance you are looking for and then start the tender process. Prior to the offer phase, the selected insurers require information specific to your company regarding the company's structure and business environment, IT organization, maturity of the IT security systems and risk management. This information is usually provided verbally in a presentation or conference call. This step is followed by individual negotiations.

The insurers then prepare binding offers. The results are summarized in the Kessler tender report and discussed with you in person. This provides the basis for the decision to take out cyber insurance. Weighing up the costs and benefits of cyber insurance is a decision on the type of risk financing. In our opinion, the requirements of corporate governance (business judgment rule) are also fulfilled by making a conscious decision to include the "cyber" risk in the company's risk management process.

THE TWO-PHASE PROCESS
CONDUCT A DETAILED RISK DIALOGUE IN ORDER TO MAKE A CONSCIOUS DECISION



ABOUT KESSLER

Kessler is the leading Swiss enterprise specializing in comprehensive risk, insurance and pension fund consulting. We advise over 1,000 medium-sized and large Swiss companies from the service, trading and manufacturing industries, as well as the public sector. Thanks to our expertise in each of these economic sectors, our highly qualified staff and our leading market position, we contribute significantly to the long-term success of our clients. As a reliable partner, we inspire our clients and open up new perspectives through the safe and successful management of risks. Founded in 1915, Kessler has 300 employees working at its headquarters in Zurich and its other sites in Basel, Bern, Geneva, Lausanne, Lucerne, Neuchâtel, St. Gallen and Vaduz. As the Swiss partner of Marsh since 1998, we are part of a network with specialists in all areas of risk management and great experience in handling global insurance programs. Marsh, the world's leading insurance broker and risk advisor, operates in more than 130 countries and is part of Marsh & McLennan (NYSE: MMC).

Further information can be found at
www.kessler.ch, www.marsh.com, www.mmc.com.

KESSLER & CO Inc.
Forchstrasse 95
P. O. Box
CH-8032 Zurich
T +41 44 387 87 11
www.kessler.ch

Marsh Network