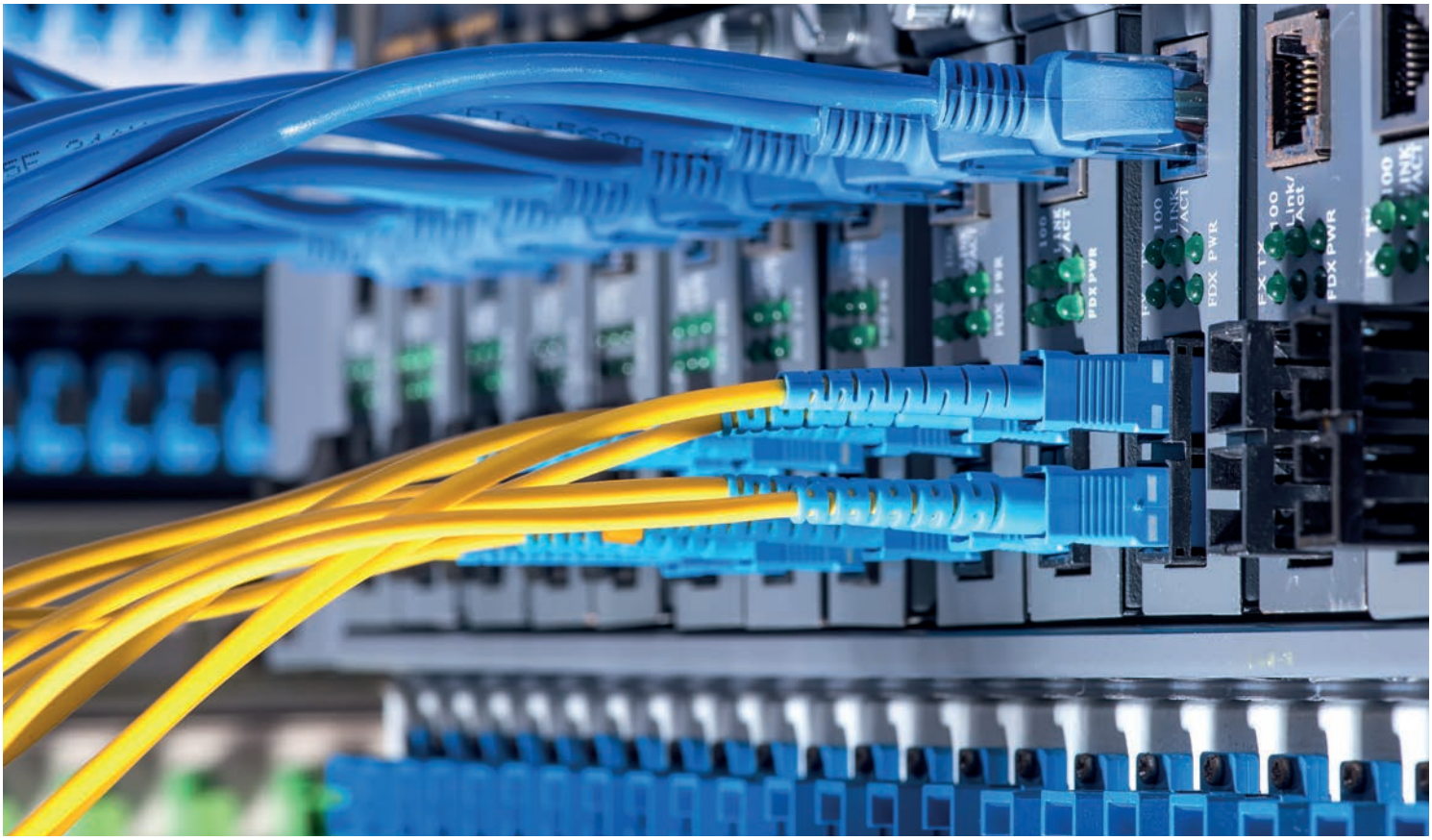
KESSLER

CYBER RISK SURVEY REPORT 2018
CYBER RISK FROM A SWISS PERSPECTIVE



SECURING THE COMPETITIVE EDGE.

CYBER RISK SURVEY REPORT 2018
CYBER RISK FROM A SWISS PERSPECTIVE

1
FOREWORD

DIGITALIZATION AS AN OPPORTUNITY

Digitalization has a fundamental impact on companies and their business and customer relationships. The Internet of Things has resulted in many convenience factors and new digital interfaces, however it has also led to the creation of many new points of attack.

Digitalization should be seen as an opportunity, but it should not cause companies to be exposed to disproportionately high risks. Valuable data and business processes must be identified and protected. The EU General Data Protection Regulation (EU GDPR) supports this approach and forms a justified basis for cyber risk management.

SUPPLY CHAIN MANAGEMENT AS A RISK FACTOR

The increasing use of outsourcing services may well reduce operating costs, however this is usually at the expense of data transparency, in particular in terms of where data is located and who ultimately has access to it. The failure of a centrally-managed IT system harbors serious calculable accumulation risks. Different operational areas/locations can thus be affected by a cyber attack simultaneously and in different ways, or attackers can obtain access to all the IT systems and software programs of different firms by attacking an IT provider. As the survey shows, companies often fail to include reliance upon suppliers in their internal cyber risk management process.

SURVEY BY MARSH

Our network partner Marsh carried out a global cross-sector survey in May 2017, which examined how companies deal with cyber risks and their potential hazards, as well as the associated data protection risks, as part of their daily business operations. We took part in the «Global Cyber Risk Perception Survey» and also invited all our international customers to take part. The results were published by Marsh at the end of February 2018.

IS THE SITUATION IN SWITZERAND IDEAL?

The threat situation in cyber space is set to continue in the years ahead. The digital world does not recognize Switzerland's borders, and the Swiss companies have begun to realize this. The report confirms that cyber risks are recognized to a certain extent, however there is a lack of targeted implementation.

Over the following pages, we have evaluated the results of the survey conducted by Marsh for Switzerland and have commented on the key findings.

We hope you enjoy reading this report and we look forward to discussing your newly-gained cyber insights with you.

Melanie Koller
Legal Counsel Cyber Risk

2
ABOUT THE REPORT

This report is based on the results of the «Global Cyber Risk Perception Survey» published by Marsh in February 2018. The key findings from a Swiss perspective are summarized and commented on over the next few pages.

More than 1,860 companies worldwide took part in the cyber risk survey; 386 of which are from Europe, including 178 (15 %) of our Swiss customers.

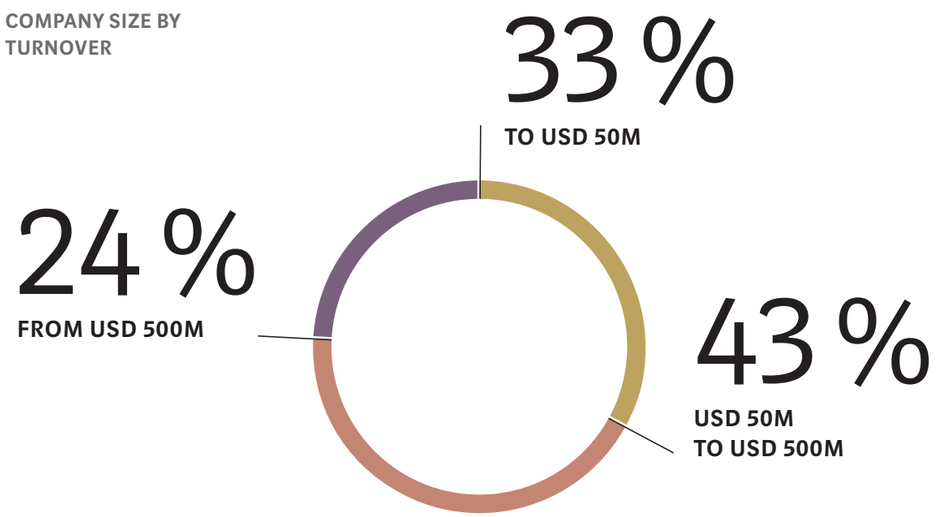
Out of the companies that took part in the survey, 33 % generate annual turnover of up to USD 50 million, 43 % generate turnover of USD 50 million and USD 500 million, and 24 % generate more than USD 500 million in turnover.

The Swiss companies that took part in the survey come from a wide variety of industries. The energy, electricity, supply and infrastructure sector was most heavily represented, accounting for a quarter of all participants. We were not surprised by this sector's interest in the survey, considering that in light of the current threat situation, critical infrastructures are among the top cyber attack targets.

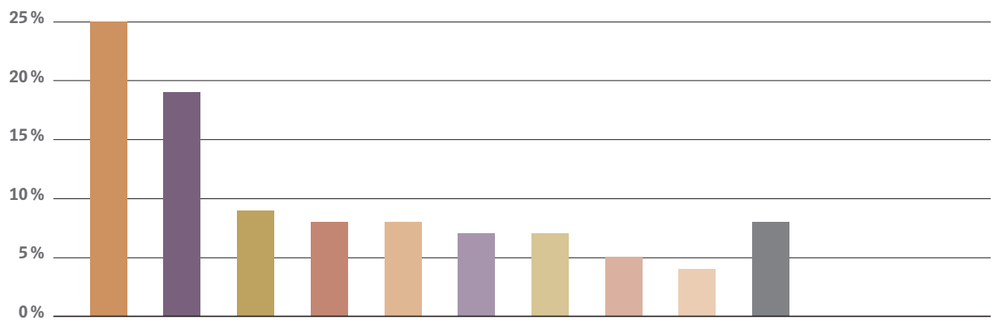
The key sales markets of the survey participants include Switzerland and Continental Europe as well as USA/Canada, UK/Ireland and Asia.

In our opinion, the diverse and extraordinarily high reliance of the survey participants upon digital tools and services is significant (text box on right). In this context, it is undisputed: cyber risk is not hype, in fact it is a causal consequence of today's digital economy.

COMPANY SIZE BY TURNOVER



SECTOR AFFILIATION



- Energy, electricity, supply and infrastructure: 25 %
- Industry: 19 %
- Healthcare: 9 %
- Finance industry: 8 %
- Communication, event, media: 8 %
- IT/ITC services: 7 %
- Public sector: 7 %
- Trade: 5 %
- Tourism: 4 %
- Other: 8 %

RELIANCE OF SURVEY PARTICIPANTS UPON DIGITAL TOOLS AND SERVICES

- One or more computers are connected to the Internet: 98 %
- Electronic processing and storage of employee files: 88 %
- Employees and third parties can connect their mobile devices to the company network: 87 %
- Electronic storage and/or management of customer data: 86 %
- Electronic processing of banking information: 75 %
- Electronic storage of supplier information: 74 %
- Cloud services: 54 %
- Electronic processing of employee or customer private health information: 31 %
- Electronic processing of credit card transactions: 28 %
- Entry of personal data (incl. cookies and similar tools) on a website: 25 %
- Electronic forwarding of personal data to suppliers or third parties: 24 %

3
FINDINGS AND COMMENTS

3.1 INCREASING AWARENESS OF CYBER RISKS

It is difficult to ignore cyber risks due to the constant media attention. The problem and the chance of being personally affected appear to be largely recognized. Nevertheless, considering the damage potential of cyber attacks, too little is being done.

This year's survey results confirm that companies now rank cyber risks among their highest risk management priorities (Figure 1). 56 % of Swiss companies already include cyber risks in their top five company risks (2016: 26 %). The rise of cyber risks into the top five company risks is due both to the increased media attention regarding cyber attacks, as well as EU GDPR that will come into effect on 25 May 2018, and the increasing awareness that it is impossible to guarantee 100 % IT security. The most extensive damage event is still to come, it is just a question of time. Increased awareness of cyber risks is by no means enough to prepare for a damage event. In our opinion, the gap between awareness of cyber attacks and the steps that are being taken to manage them is still wide. There is a clear need for action in this respect.

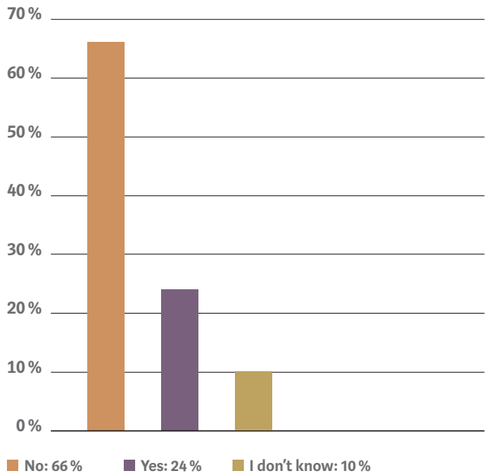
When asked whether their company had been a victim of a cyber attack during the last 12 months, 66 % replied with No, 24 % with Yes and 10 % with «I don't know» (Figure 2). In this respect, it can be assumed that a proportion of the 66 % of companies that answered No have not yet discovered that their company has been hacked. Malware is often only detected after many weeks or months, if indeed at all.

FIGURE 1

How much importance does your company attach to cyber risks?

FIGURE 2

Was your company a victim of a cyber attack during the last 12 months?



3

3.2 IMPORTANCE OF CORPORATE GOVERNANCE

The tendency for company management to take increasing responsibility for cyber risk management is very positive (2017: 34 %; 2016: 13 %). Nevertheless, in Switzerland the operational areas are still primarily responsible for cyber risk management. The disadvantages of this distribution of responsibility are usually only realized when the first cyber damage event occurs.

During the Big Data and Industry 4.0 era, it will increasingly be of interest whether managers incorporate potential cyber damage scenarios in their financial planning or whether they intentionally disregard them. In light of the fact that 56 % of Swiss companies include cyber risks in their top five risk management priorities (Figure 1), it is hoped that the responsibility for cyber risks will more frequently be assumed by the strategic management level in future.

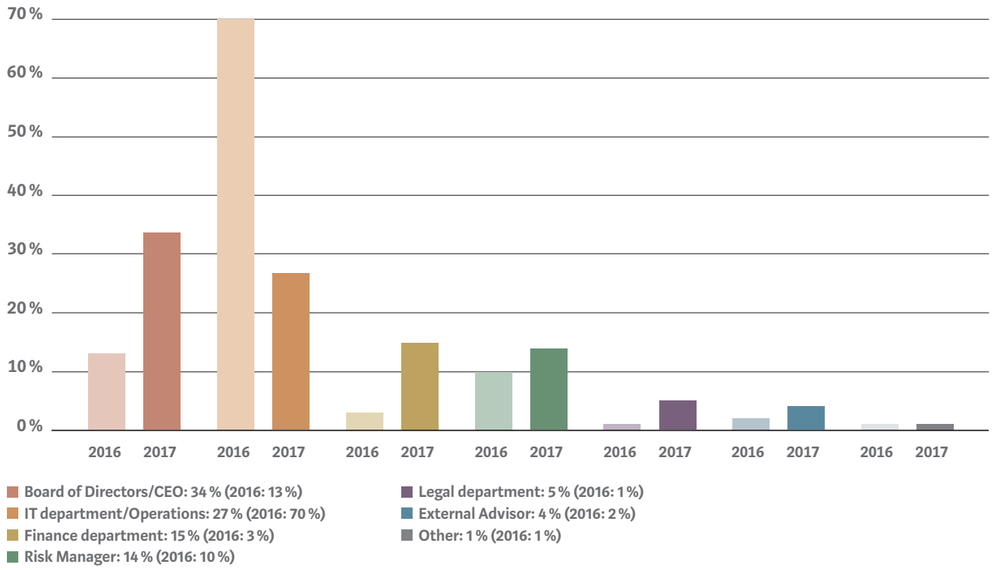
Regardless of whether or not the risk assessment is a legal obligation of the management report, company management are well advised to identify the risks to their company and to budget for them. In accordance with Murphy's Law, where anything that can go wrong will go wrong, cyber damage must always be accounted for, and how the damage is to be managed must be carefully planned by specialists.

In the event of bankruptcy or a cyber damage event that has a negative impact upon the balance sheet, by law action is taken first and foremost against the company management. The quantification of cyber damage scenarios that have not yet occurred is and shall remain – at least in the near future – the greatest challenge faced by companies and the global economy as a whole. It is precisely due to these incalculable cost factors that the rough budgeting of cyber risks is more important than ever. Cyber security due diligence and cyber insurance due diligence are also part of everyday operations in the M&A process. Nobody wants to purchase a pig in a poke.

Although company management teams are assuming greater responsibility for cyber risks than compared with the previous year, in Switzerland the primary responsibility still lies with the operational units. However, the first step has been taken, and today, it is at least no longer the IT department but rather the Finance and Risk departments that assume responsibility for cyber risks within the company (Figure 3). As a result of this redistribution at operational level, it is hoped that greater focus will be given to the financial sustainability of residual cyber risks.

FIGURE 3

Which of the following functional areas is primarily responsible for managing cyber risks?



3

3.3 CYBER RISK MANAGEMENT: WHAT ARE THE BENEFITS TO THE COMPANY?

The identification of cyber risks and the subsequent deliberate management of these risks appears to be a logical consequence in theory. However, in practice company management teams lack the time, knowledge and motivation to take a proactive approach towards the largely unknown «cyber risks» alongside the other company risks, and to bridge the gap between awareness and action. Cyber risks will not be eliminated over the years to come; instead companies need to be increasingly aware of their cyber exposure and improve the cyber resistance of their organization.

58 % of the survey participants have already quantified the financial impacts of an operational cyber incident (in 2016 this figure was 41 %). The results are satisfying and, in our opinion, demonstrate once more that cyber risks are increasingly being perceived as serions company risks (Figure 4).

Over half of the companies that quantify cyber incidents estimate the financial impacts at between USD 1 million and 10 million (Figure 5). In the SME sector, damage exceeding CHF 1 million is considered a threat to company existence. It is therefore even more astounding that the cyber prevention measures in relation to the mentioned damage potential are clearly lagging behind and, despite attractive insurance coverage and premiums, companies are generally slow at implementing cyber insurance solutions (Figure 6).

FIGURE 4

Have you estimated the financial impacts of a cyber incident at your company?

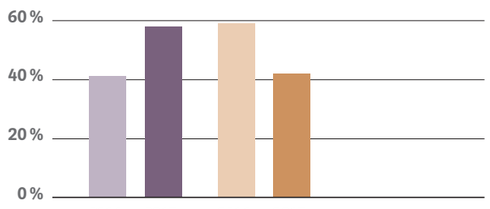
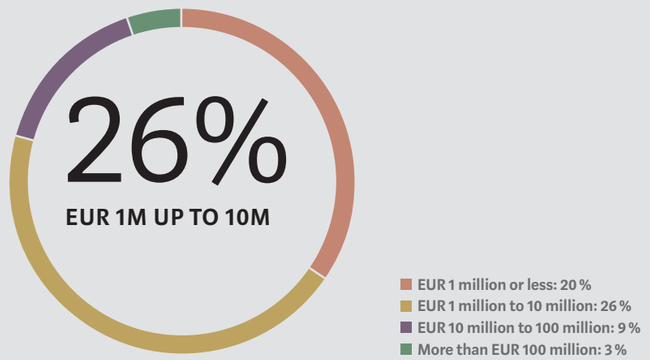


FIGURE 5

If your company has estimated the financial impacts of a cyber incident, what is the maximum potential loss value?



3

FIGURE 6

Which of the following steps has your company taken over the last 12 to 24 months as part of its cyber risk management process?

ASSESSMENT AND ANALYSIS
- Estimation of financial impacts of cyber incidents: 58 %
- Cyber security gap analysis conducted: 46 %
- Modelling of potential cyber loss scenarios: 25 %

SECURITY AND INSURANCE
- Encryption of the company's desktops and laptops: 54 %
- Multi-factor authentication for remote access to the company network: 45 %
- Penetration testing carried out: 41 %
- Cyber insurance taken out: 40 %
- Implementation of preventive measures for data loss: 39 %
- Improved vulnerability patch management: 31 %
- Reduced external system connectivity: 26 %
- Restructuring of existing cyber insurance or increase in coverage: 14 %

RESPONSE AND RECOVERY
- Introduction and improvement of social engineering awareness for employees: 69 %
- Development of a cyber incident response plan: 29 %
- Specific improvements for identifying cyber risk events: 25 %
- Organization of external support services (Legal, PR, IT Security): 12 %

No matter how subjective the perception of the survey respondents is, it certainly has an impact upon cyber risk management, in particular with regard to introducing or omitting preventive measures.

It is worth noting that around 40 % of the survey participants stated that they have taken out cyber insurance (Figures 6 and 12). In light of the relatively new cyber insurance market and the current premium volumes in Switzerland, we estimate the percentage of cyber insurance policies that have been taken out to be considerably lower. Rather, we assume that the 40 % of survey respondents either have not taken out any cyber insurance or mistakenly assume that the risks are covered in the existing insurance policies, or that individual coverage components with a reference to cyber incidents offer sufficient cyber coverage. Therefore, many companies are creating a false sense of security and as a result are tending to neglect the response and recovery measures (Figure 6).

Furthermore, the results in the area of response measures have led us to assume that 69 % of company social engineering preventive measures have been implemented. Due to the fact that most cyber risks are triggered in association with the human factor, this would be a very satisfying result.

With reference to our daily discussions with customers, this should however be interpreted with caution. The holding of one-off IT introductory events or simply informing employees of the latest phishing attempts, for example, are often considered social engineering awareness training. Despite all the numbers, we recognize however that companies are making far greater efforts to take a proactive approach towards the human factor as the weakest link in the cyber security chain. Human characteristics, willingness to help, good faith and curiosity represent the greatest vulnerabilities and thus the greatest risks among the workforce. Therefore, employees should receive training every year – one-off training usually does not offer long-term benefits.

3

Nowadays, the investment in an emergency response plan is one of the most crucial and most cost-effective preventive measures in the long term. Nevertheless, at least 61 % of the survey respondents stated that they have not developed an emergency response plan over the last 12 to 24 months (Figure 7). This is despite the average amount of damage as a result of a cyber incident being estimated as more than USD 1 million by most companies that estimated the worst case scenario (Figure 5). Companies largely justify the absence of a disaster plan by the presence of in-house cyber security/a firewall and the lack of know-how (Figure 8).

In many cases, technical IT measures with regard to cyber security are often overestimated: During times of increasing digital integration, and reliance upon third parties, neither state-of-the-art cyber security/IT security/firewall nor the lack of know-how justify the lack of an emergency response plan.

Few people are aware that cyber risks and natural disasters cause economic damage on a similar scale. If a Cloud provider should be put out of action, the total economic damage could equate to USD 50 to 120 billion, which is on a similar scale to the damage caused by Hurricane Sandy or Katrina (WEF Report 2018). The reliance upon key data and available systems is high, as is the level of damage, and yet little is being invested in preventive measures. The Not Petya attack on the Maersk shipping company in June 2017 was an expensive wake-up call. The 10-day interruption to business operations led to a 20 % decline in turnover, equating to total damages of at least USD 250 million. The costs would have been somewhat lower had a disaster recovery plan been developed beforehand.

THE BEST POSITIONED COMPANIES ARE THOSE THAT EXPECT AN ATTACK AND ARE PREPARED FOR IT.

Measures to combat cyber risks should not hinder business operations, instead they should offer special protection for vulnerable areas within the business. Those who are trained to deal with storm surges are best prepared, in the event of an actual storm, to deal with the waves in a skilful and calm manner.

FIGURE 7

Has your company developed an emergency response plan over the last 12 to 24 months to deal with cyber attacks?

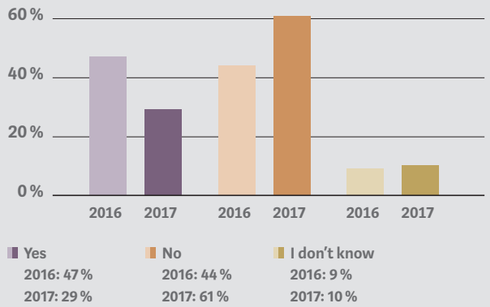
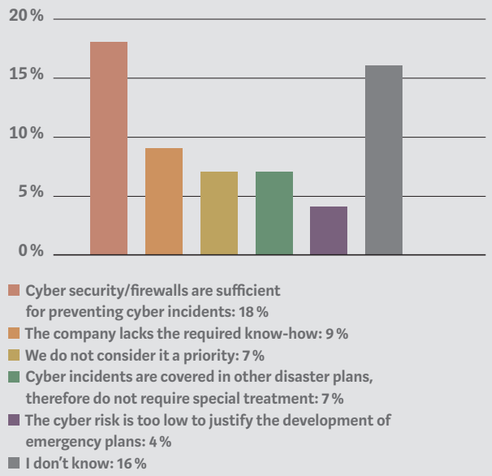


FIGURE 8

If your company has not developed an emergency response plan for cyber attacks, can you explain why?



3

As in the previous year, most Swiss companies feared an interruption to business operations. Reputational damage is the second-greatest threat, followed by data/software damage and breach of customer information. These are followed by extortion/ransomware, disruption/interruption of industrial systems or other operational technology, liability towards third parties due to a system breach, loss/theft of intellectual property, contingent business interruption (supply chain) as well as physical property damage and/or bodily injury (Figure 9).

Cyber-related business interruption is, in our opinion, with good reason the most feared risk in the whole of Europe (Figure 9); the extent of the damage and the various damage scenarios remain an unpredictable surprise and are influenced by a number of factors, including whether the arrangement of the IT systems is centralized or decentralized, which and how many IT service providers are involved and what back-up concept is in place etc. The place of jurisdiction and the applicable law can also have a major influence upon the costs in terms of damage to the company or third parties.

In terms of reputation, the reporting obligation as part of EU GDPR will play an interesting role: As a result of the hitherto «affordable» data protection penalties in Switzerland and Europe, companies would previously have accepted a fine in order to keep quiet the details of a hacker attack on their customer database and thus protect their reputation.

It remains to be seen how the threat of high fines resulting from EU GDPR will actually be modelled in legal practice. One thing is clear: the cost-benefit decision «Can we/do we want to pay a fine or can we afford damage to our reputation?» will require companies to implement new strategies with regard to transparency matters and cost considerations.

The breach of customer information might, in light of EU GDPR and other European data protection laws or laws relating to data privacy – as far as the scope of the damage is concerned – be a second major area of uncertainty. This is not only resulting from the breach of customer information and the associated reporting obligations for those concerned or the authorities, but rather due to the threat of high fines (up to 4 % of the consolidated global annual turnover or EUR 20 million; GDPR Art. 83) following a violation of the EU GDPR. In addition, a data protection investigation procedure initiated by an EU authority can generate further costs in the area of first-party damage. These costs are currently difficult to quantify.

FIGURE 9

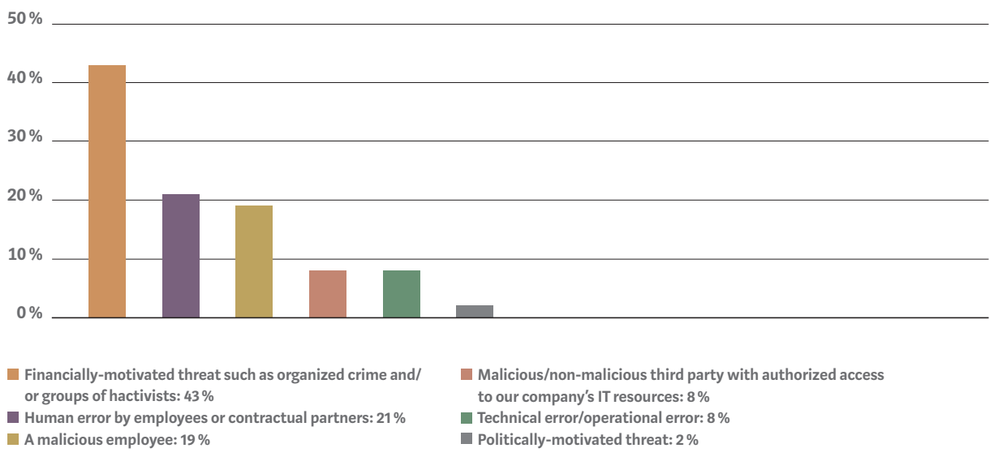
Which cyber attack scenarios represent the greatest threat to your company?

	Italy	France	Spain	Portugal	Germany	Switzerland	Romania	Belgium	Benelux
Business interruption	69 %	83 %	84 %	81 %	75 %	86 %	82 %	60 %	63 %
Data/software damage	71 %	83 %	53 %	54 %	17 %	53 %	59 %	47 %	52 %
Reputational damage	46 %	42 %	53 %	51 %	25 %	57 %	41 %	60 %	63 %
Breach of customer information	40 %	42 %	32 %	49 %	33 %	52 %	47 %	47 %	52 %
Liability to third parties resulting from a system breach	34 %	42 %	37 %	27 %	17 %	30 %	29 %	13 %	24 %
Disruption/interruption of industrial systems or other operational technology	34 %	33 %	32 %	41 %	33 %	33 %	29 %	27 %	33 %
Extortion/ransomware	31 %	33 %	42 %	51 %	25 %	37 %	29 %	43 %	41 %
Loss/theft of intellectual property	26 %	17 %	21 %	24 %	50 %	22 %	47 %	37 %	33 %
Contingent business interruption (supply chain)	20 %	33 %	32 %	35 %	25 %	17 %	29 %	30 %	30 %
Physical property damage and/or bodily injury	6 %	25 %	16 %	5 %	8 %	11 %	12 %	13 %	9 %
Other	34 %	33 %	32 %	41 %	33 %	34 %	29 %	27 %	33 %
I don't know	3 %	0 %	5 %	0 %	0 %	2 %	0 %	0 %	0 %

3

FIGURE 10

With regard to a cyber attack that delivers destructive malware, which threat actor concerns you the most?



Malware is malicious software that is developed to damage a computer user. The inexpensive hacker tools and increasing trend for «let's share knowledge» support the spreading of malware through inexperienced IT users. The waves of cyber attacks in June 2017, led by the crypto Trojan horses WannaCry, Petya and NotPetya, not only demonstrate the risks posed by cyber criminals but also further highlight the IT monoculture that facilitates cyber crime, which is endemic in Europe. The tendency for companies to deploy similar software, security programs and IT infrastructure opens up the door for successful cyber attacks in other organizations (Sigma Report 1/2017, SwissRe).

The discussion regarding the issue of the most-feared threat actors in relation to malware infection (Figure 10) often leads to emotionally-charged discussions when we are talking to our customers. Why is this? Unlawful access to company systems is often the fault of the employees. They are the weakest link in the cyber security chain. Humans are difficult to predict due to their emotional nature (see also comment regarding Figure 6). Even long-serving, loyal, older or younger, well or poorly-established employees can, without any prior indication, develop criminal intentions towards their employer following certain events, or well-trained employees can be tricked by a specially tailored phishing e-mail. Many people are aware of this problem. Nevertheless, in many cases our customers find it difficult to incorporate their employees in the residual cyber risk debate as being the most frequent active or passive initiators of a cyber risk incident. In our opinion, an important step would be for the residual risk to be incorporated objectively and without emotional connotations in the cyber risk analysis in connection with potentially-criminal or easy-to-manipulate employees. We estimate residual cyber risk of a human nature at no less than 50 %.

3

3.4 RISK ASSESSMENT OF IT SUPPLIERS

In order to focus upon their core competencies, an increasing number of companies are outsourcing their IT and information systems. Besides the obvious benefits, outsourcing is always associated with risks. Valuable data and business processes must be placed in good hands, which is why the IT provider must be selected with great care. Outsourcing is a matter of trust.

IT outsourcing means that, on the basis of a contractual relationship, internal operational tasks are handed over, such as applications, infrastructure, processes, personnel or individual IT maintenance tasks. Clear benefits of outsourcing are increased efficiency and effectiveness as well as low costs. The downsides, such as losing control of the data, lack of isolation of the different data processing operations from other cloud users, compliance risks, lock-in effects and access of overseas authorities to data are often weighted more heavily, but surprisingly are often accepted without much resistance (exceptions include financial institutions, which thus have less choice due to the stricter regulations imposed by the Federal Financial Supervisory Authority or FINMA).

OUTSOURCING IS A MATTER OF TRUST.

A targeted attack upon an IT supply chain is lucrative. By attacking the IT provider, an attempt is made, for example, to control various organizations at the same time, which can result in extensive cyber damage. The liability risks are usually passed onto the customer to the extent permitted by law. In this respect it is important to be aware that even leading telecommunications companies only offer a certain level of IT security/cyber security under optimal service level conditions, and cannot ultimately protect a company against loss of liquidity or even bankruptcy. The greater the dependency upon external service providers, the greater the importance of integrating the failure of such providers in the operational cyber risk management process. Figure 11 provides some interesting figures in this respect.

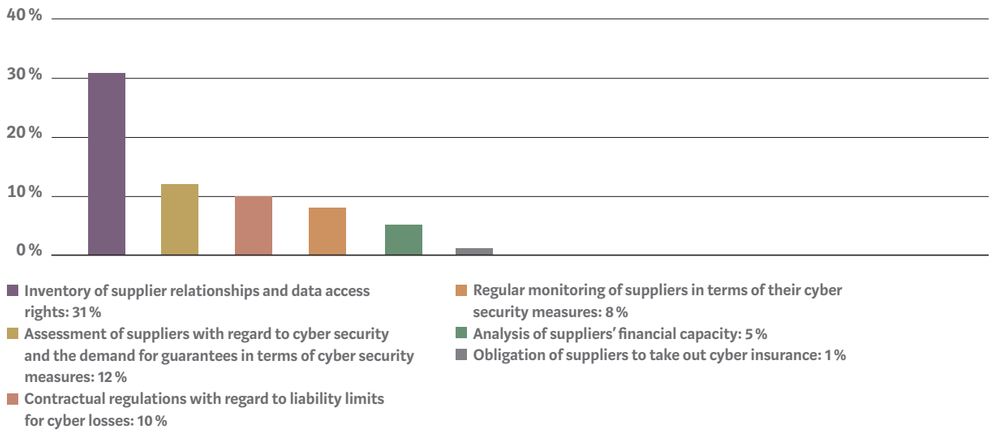
33 % ASSES THEIR SUPPLIERS WITH REGARD TO VULNERABILITY TO CYBER RISKS. 46 % DO NOT ASSESS THEM. 21 % DO NOT KNOW.

Meanwhile, 33 % of companies assess their suppliers with regard to vulnerability to cyber risks; in 2016 this figure was 20 %. This result demonstrates significant progress compared with last year.

However, Figure 11 shows that there is room for improvement in terms of the approach that companies take towards assessing their IT suppliers. Therefore, the assessment of suppliers with regard to their cyber security, the requirement for guarantees for sustained cyber security and monitoring, contractual agreements with regard to liability limits for cyber-related losses, analysis of the suppliers' financial capacity and the suppliers' obligation to take out cyber insurance are some of the rare provisions.

FIGURE 11

What steps is your company taking to assess and manage the cyber risks arising from your suppliers and other third parties?



3

3.5 CONTINUED INCREASE IN NUMBER OF CYBER INSURANCE POLICIES

The cyber insurance market is continuing to grow as a result of new cyber risks, while the companies themselves are also changing. The better companies identify their cyber security vulnerabilities and needs, the easier it is for them to decide upon the financing strategy: Cyber insurance can never replace preventive measures, however in the event of a damage incident it is aimed at preventing the threat to the balance sheet and income statement as well as the loss of liquid assets.

Since the wave of cyber attacks took place in mid-2017, besides at large corporations there is also increasing interest in cyber insurance policies among SMEs. For our Swiss customers, the focus of their cyber insurance is still upon the coverage of cyber-related business interruption. Currently and before the direct impact of the EU GDPR that enters into force on May 25, 2018, due to the lack of European jurisdiction and legal issues relating to the enforcement of fines, which has not yet been fully defined, it is difficult to estimate whether EU GDPR will have a noticeable influence upon the increase in the number of cyber insurance policies that are taken out in Switzerland as a result of higher insurable cost risks in the areas of data protection fines, notification costs and regulatory legal costs.

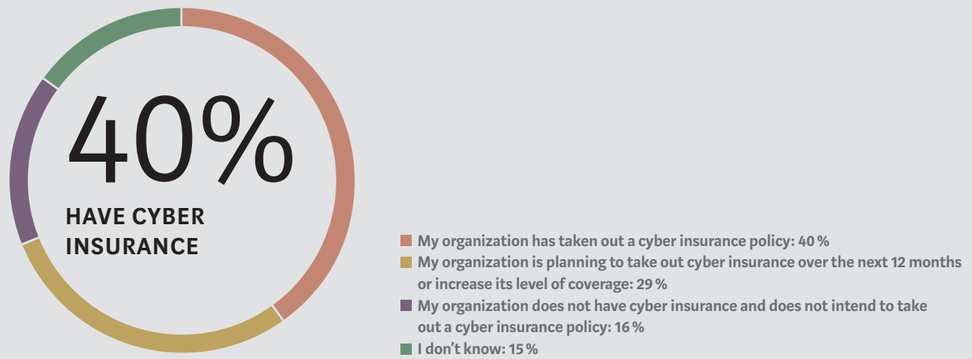
According to the survey, 40 % of our customers have taken out cyber insurance, while 29 % are planning to take out suitable insurance over the next 12 months or increase the existing level of cover (Figure 12).

MANAGING THE RISK OF FINES IS ALSO ON THE COMPANY MANAGEMENT'S AGENDA, AS IS THE CONSCIOUS DECISION ABOUT THE RISK FINANCING STRATEGY.

We are very surprised at the high percentage of 40 % of companies that have cyber insurance, based upon the cyber placement orders that we are entrusted with as a broker and also in light of the current market situation for independent cyber insurance. We suspect that the term «cyber insurance» is interpreted in different ways, for example that some of the survey respondents assume that implicit cyber coverage is included as part of a standard product, or that individual cyber coverage components in conventional insurance products are interpreted as cyber coverage.

FIGURE 12

How is your company currently positioned with regard to cyber insurance protection?



3

FIGURE 13

If your company has cyber insurance or would like to extend its coverage, what are the drivers behind this?

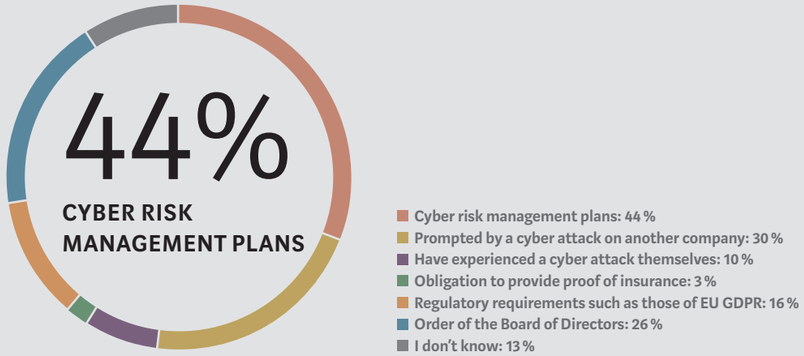
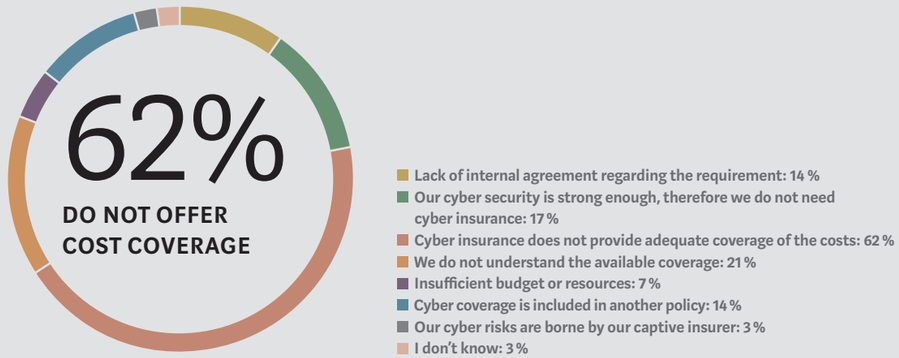


FIGURE 14

If your company has not taken out cyber insurance, what are the reasons for this?



It is understandable why almost half of the 40 % or so of survey respondents that already have cyber insurance or are considering increasing their level of coverage specified that the current cyber risk management plan is a driver behind this (Figure 13). After all, those who deal closely with cyber risks and potential subsequent damage quickly realize that an interruption to business operations lasting several hours can result in considerable financial losses.

If potential cyber worst case scenarios are not quantified, cyber damage remains a total surprise for the company management. Companies are ill-advised to rely upon the principle of hope when it comes to preventing the liability of the management bodies, for instance as a result of insufficient IT security measures or suitable monitoring. In this respect, it is understandable why, in their own interest, boards of directors appear to be adopting a top-down strategy for their cyber risk financing strategy (see also Figure 13).

31 % of Swiss companies do not have cyber insurance and do not intend to take out a cyber insurance policy, or they do not have a suitable plan (Figure 12). The main reason specified for this is insufficient coverage of costs (62 %) (Figure 14).

There is a clear need for advice, considering the results shown in Figure 14. For non-experts, it is difficult to differentiate between the different coverage components offered by the insurer and the required criteria of the diverging risk assessments. Each insurer speaks its own language, which is why it is not advisable to take out a standard policy without consulting a cyber specialist and without carefully examining the market. The needs of each customer must be determined individually and each cyber insurance policy is accordingly unique. The cyber worst case scenario should not be excluded from the coverage.

4
EU GDPR AS AN OPPORTUNITY TO STRENGTHEN CYBER RISK MANAGEMENT

4.1 CAUSE AND IMPACT OF EU GDPR COMPLIANCE

Although EU GDPR is perceived by many Swiss companies as both cost and time-intensive, and thus obstructive to their business, it is at least having one positive impact: Companies are more or less being forced to examine cyber risks and optimize management of them.

The costs that arise in connection with data protection law violations can be calculated and to a large extent can (still) be insured. The conscious decision to implement EU GDPR to a suitable degree is, in our opinion, also on the company management agenda, as is the conscious decision about the risk financing strategy of top risks.

Out of the companies surveyed that are subject to EU GDPR, in mid-2017 only 6 % admitted to being fully compliant with the EU GDPR regulations, while 51 % were developing a plan to comply with EU GDPR in accordance with their EU exposure. The fact remains that 43 % of Swiss companies either do not have a plan to integrate EU GDPR into their company, or they do not know where their company stands with regard to implementation of EU GDPR (Figure 15).

Considering the efforts that are required to comply with the EU GDPR provisions to some extent, it is assumed that companies will engage in a further larger wave of implementation for EU GDPR compliance during the final weeks before EU GDPR comes into force (on 25 May 2018) or by the latest at the time of the first final judgements regarding fines. It is clear that, as a result of the threat of sanctions stipulated in Article 83 of EU GDPR, Swiss companies may be faced with considerable liability risks.

Nevertheless, the positive effect of EU GDPR must not be ignored. Companies are more or less being forced to improve their ability to manage risks and to respond to risks that occur within the daily-changing cyber risk landscape, in order to ultimately also ensure better protection of personal data. For example, EU GDPR includes the obligation to process personal data in such a way that reasonable security is guaranteed, which includes preventing unauthorized access or use of personal data and also of the devices that are used to process the data. Therefore, the company responsible for processing the data or the company processing the order (e.g. IT provider), must assess the risks associated with personal data and must introduce measures to minimize these risks (EU GDPR 32). In the event of infringement of various regulations, EU GDPR sets out clear rules regarding the conditions for imposing administrative penalties: In future, high monetary fines can be imposed upon companies if they do not inform their customers of an event where their personal data has been compromised, for example, or if they only notify them as a result of external pressure.

Everyone knows that a suitable emergency response plan for a defined risk is one of the most effective cost-reducing measures (take, for instance, fire drills that are widely practised among the entire workforce). It is therefore surprising that only 23 % of the companies surveyed have developed a response plan to deal with data protection violations (Figure 16).

EU GDPR does not oblige companies to implement an emergency response plan for cyber incidents, however it does require that they inform the supervisory authorities within 72 hours of a data security incident being detected. It goes without saying that companies with an emergency action plan will be better positioned with regard to this notification deadline than companies without a plan. If the costs resulting from cyber incidents are to be minimized from the very start, the cost/benefit decision (costs/internal efforts versus reduction of extent of damage in the event of an emergency) must be taken prior to the first cyber attack.

Against all reason: The company management is free to pursue a risky path and thus consciously refrain from taking any IT security precautions. It would appear that managing the risk of fines as a result of EU GDPR is also on the company management agenda, as is the conscious decision about the risk financing strategy of top risks. Due to the hitherto affordable data protection fines, it can be assumed that Swiss companies would previously have accepted a fine in order to keep quiet the details of a hacker attack on their customer database and thus protect their reputation, rather than inform the persons concerned or the authorities. This practice will change with the introduction of EU GDPR and in any case during the second revision of the Swiss Federal Data Protection Act.

FIGURE 15

What progress has your organization made in terms of preparing for EU GDPR compliance?

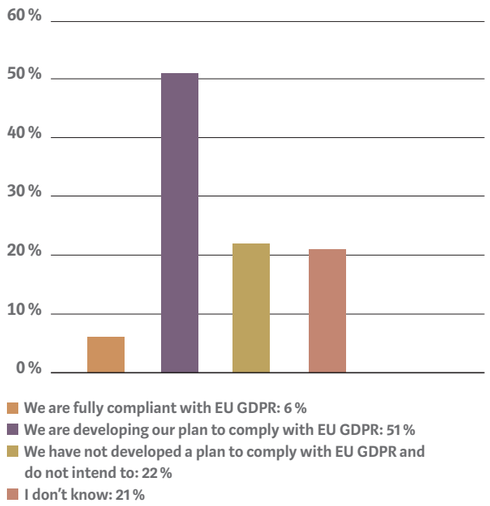
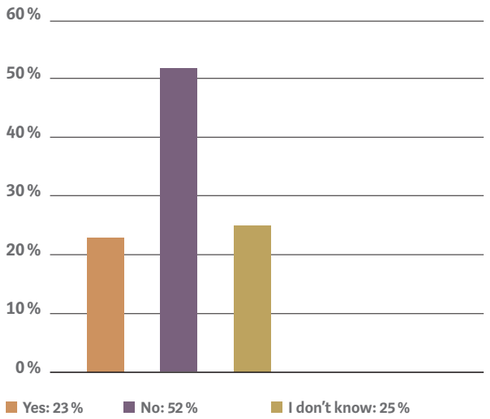


FIGURE 16

If your company is subject to EU GDPR, have you developed a response plan with regard to data protection violations, which includes, for example, notifying the EU supervisory authorities of an EU GDPR violation within 72 hours?



5
CONCLUSIONS

FINDINGS

The advancement of digital business models is leading to data traffic volumes that are difficult to manage, an incredibly high amount of digital data and thus an increase in cyber risks. Many companies lack the practical know-how to address and sensibly deal with these challenges.

Cyber risks are complex and harbor the risk of considerable cumulative losses, therefore consideration must be given to the company's own cyber risks and also those of the IT, raw materials and sub-component suppliers in the supply chain, as part of operational risk management. The initial effort for sensibly managing cyber risks is time-intensive, generates costs and, in addition to the other company risks that must also be taken seriously, it is undoubtedly laborious.

One thing is clear: In light of advancing digitalization, cyber risks are here to stay. This makes it all the more important for targeted cyber risk management that does not obstruct business operations, but rather strengthens the cyber resistance of the companies and the Swiss economy.

It is also evident that the operational management of cyber risks is individual to each company and depends heavily upon the risk aversion of the company management.

And last but not least, companies that see EU GDPR as an opportunity to rethink their operational cyber risk management will deal with the subject of data protection more constructively, rather than seeing it as a burdensome obligation.

NEED FOR ADVICE

Managing the residual cyber risk is challenging. We have identified that there is also a need for advice with regard to the assignment of responsibility for cyber risks within the company, and the localization and analysis of cyber risks. Furthermore, there is an increasing need for advice on the implementation of suitable, diversified preventive measures. Besides the diversified preventive measures, cyber risk management also includes additional risk financing strategies that are adapted to the financial capacity and risk insurance policy.

Do you have any questions? Arrange a personal consultation:

Helmut Studer
Member of the Executive Committee
helmut.studer@kessler.ch
T +41 44 387 87 17

Melanie Koller
Legal Counsel Cyber Risk
melanie.koller@kessler.ch
T +41 44 387 88 39

ABOUT KESSLER

Kessler is the leading Swiss enterprise specializing in risk, insurance and pension fund consulting. Due to the know-how and experience of our staff, the innovative strength as well as due to our market position, we create added value in a sustainable manner for our clients from all parts of industry (i.e. service, trading and manufacturing companies). Our excellent reputation combined with our financial success form the foundation of our long-term future as an independent family enterprise. Founded in 1915, Kessler has 275 employees working at the headquarters in Zurich as well as at further sites in Aarau, Basle, Berne, Geneva, Lausanne, Lucerne, Neuchâtel, St. Gallen and Vaduz. As the Swiss partner of Marsh, we are part of a network with specialists in all areas of risk management and experienced in handling global insurance programs. Marsh, the world's leading insurance broker and risk consultant, operates in more than 100 countries and is part of Marsh & McLennan Companies whose share is traded on the New York, Chicago and London Stock Exchanges (ticker symbol: MMC).

Further information can be found under
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