KESSLER

CYBER RISK SURVEY REPORT 2019
CYBER RISK FROM A SWISS PERSPECTIVE

SECURING THE COMPETITIVE EDGE.

CYBER RISK SURVEY REPORT 2019
CYBER RISK FROM A SWISS PERSPECTIVE

1	FOREWORD	5
2	ABOUT THE REPORT	6
3	FINDINGS AND COMMENTS	10
	3.1 SHARP RISE IN AWARENESS OF CYBER RISKS	10
	3.2 IMPORTANCE OF CORPORATE GOVERNANCE	12
	3.3 CYBER RISK MANAGEMENT: AN INDICATOR OF RISK AWARENESS	14
	3.4 SUPPLIER CYBER RISK MANAGEMENT	22
	3.5 CONTINUED INCREASE IN NUMBER OF CYBER INSURANCE POLICIES	24
4	EU GDPR STRENGTHENS CYBER RISK MANAGEMENT	28
	4.1 COSTS RESULTING FROM DATA PROTECTION VIOLATIONS	28
5	CONCLUSIONS	30

1 FOREWORD

INDUSTRY 4.0 BECOMING EVERYDAY LIFE

In the manufacturing industry in particular, companies are making increasing use of components from the Internet of Things, leading to a change in future security concepts. The dangers posed by the Internet of Things are currently underestimated. Automated coffee machines, smart lamps and photocopiers can represent gateways into a company network. No-one would try to suggest that smart coffee machines are more secure than business software developed by professionals. One aspect of cyber risk management is identifying weak spots in a company's operations in order to protect its most important assets and enable it to successfully achieve its corporate goals.

SUPPLIER CYBER RISK MANAGEMENT

The reliance on IT suppliers still tends to be neglected. Data and processes are outsourced for a number of reasons, but unfortunately we cannot entirely hand over responsibility for ensuring the confidentiality, integrity and availability of customer data. Liability issues are even more complex at an international level than in the national business environment. Companies today often have international value chains, requiring them to be highly disciplined with regard to the transparency of their reliance on suppliers. This transparency creates an understanding of the cyber risk exposure associated with the supply chain.

OUR SURVEY

In September 2018, we conducted a Switzerland-wide cross-sector survey that examined how companies deal with cyber risks and their potential dangers in their day-to-day activities. The survey also looked at the associated data protection risks. We invited all our international customers and other internationally active companies to take part in the «Cyber Risk Survey Report 2019 – Cyber Risk from a Swiss Perspective». We have now evaluated the results from the 387 responses for you and commented on the key findings.

SWITZERLAND IS NOT A PROTECTED ZONE

The results of the following report confirm once again that Swiss companies are also targeted by cyber criminals. I believe it is dangerous to conclude that Switzerland will continue to be unaffected by severe cyber damage in the future simply because it has escaped unscathed in previous years. Worldwide cyber incidents are too opaque, and the motives behind them too unpredictable.

We hope you enjoy reading the report and look forward to discussing your newfound cyber insights with you.

Melanie Koller
Legal Counsel Cyber Risk

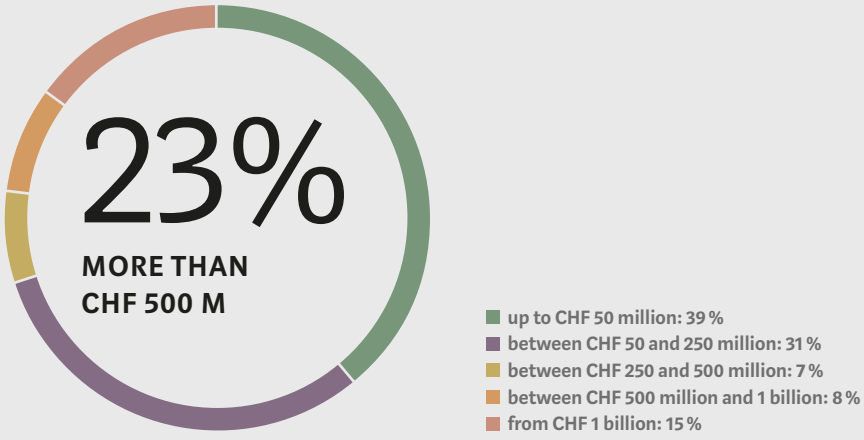
2
ABOUT THE REPORT

This report is based on the results of the Kessler survey on how our customers deal with cyber risks conducted in September 2018. The key findings from a Swiss perspective are summarized and commented on in the following pages.

387 international companies from all over Switzerland took part in the cyber risk survey. 29 % of the respondents were members of senior management teams or boards of directors, with the remaining 71 % of the surveys submitted by people in finance, risk management, IT, HR or legal departments.

70 % of the companies surveyed generate annual turnover of up to CHF 250 million. A further 7 % generate between CHF 250 million and CHF 500 million, while the remaining 23 % generate more than CHF 500 million.

COMPANY SIZE BY TURNOVER



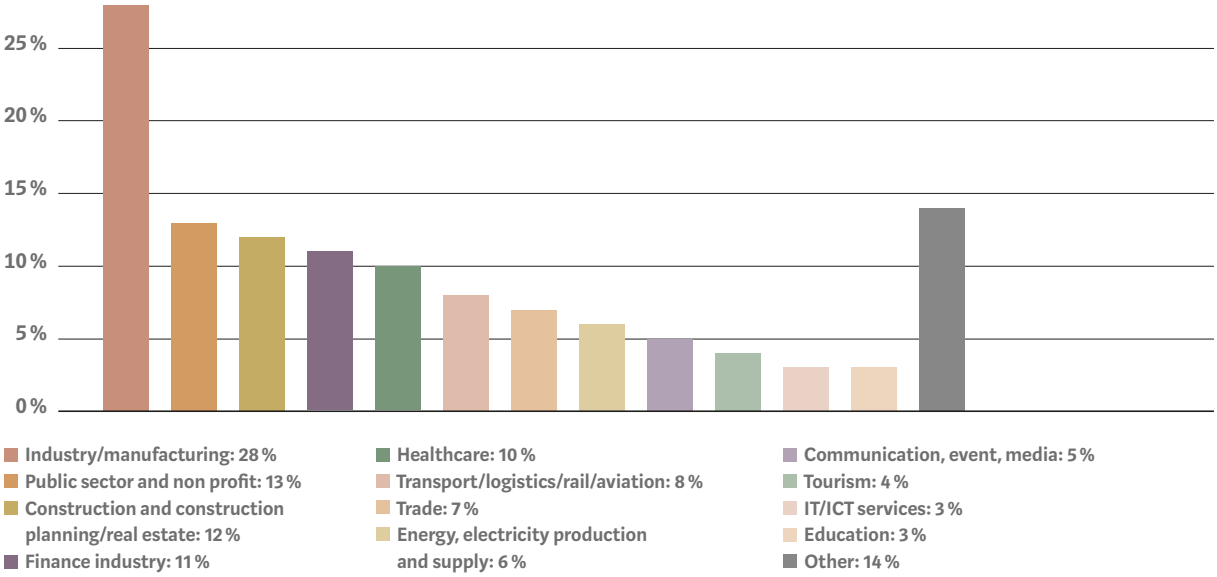
The industrial and manufacturing sector was most heavily represented, accounting for more than a quarter of all participants. We are not surprised that this sector was so keen to take part in the survey, as the fear of cyber-related business interruptions is driving companies to undertake a root-and-branch analysis of their cyber risks.

In addition to Continental Europe, the key sales markets of the survey participants include USA/Canada, Asia and the Middle East.

Like last year, the survey participants' extraordinarily high reliance on digital tools and external IT providers (text box p. 8) is extremely significant. The aspects cited are essentially the same as those in last year's Kessler Cyber Risk Report. We are seeing a striking increase in cyber risk awareness, however, with far fewer companies now allowing their employees and third parties to connect their own mobile devices to the company network. This development is also confirmed in our day-to-day discussions with customers.

2

SECTOR AFFILIATION



RELIANCE OF SURVEY PARTICIPANTS UPON DIGITAL TOOLS AND SERVICES

- One or more computers are connected to the Internet: 97 % (2017: 98 %)
- Electronic processing and storage of employee files: 71 % (2017: 88 %)
- Employees and/or contractual partners can connect their laptop and/or their mobile devices to the company network: 63 % (2017: 87 %)
- Electronic storage and/or management of customer data: 76 % (2017: 86 %)
- Electronic processing of banking information: 78 % (2017: 75 %)
- Electronic storage of supplier information: 67 % (2017: 74 %)
- Cloud services: 52 % (2017: 54 %)
- Holding of individually identifiable private healthcare information of employees or customers: 25 % (2017: 31 %)
- Electronic processing of credit card transactions: 32 % (2017: 28 %)
- Entry of personal data (incl. cookies and similar tools) on a website 26 % (2017: 25 %)
- Forwarding of personal data to suppliers or other third parties: 27 % (2017: 24 %)

3
FINDINGS AND COMMENTS

3.1 SHARP RISE IN AWARENESS OF CYBER RISKS

Cyber risks have come to the attention of companies' boards of directors and management, not least due to the omnipresent EU GDPR (General Data Protection Regulation) that came into effect several months ago. Given the extent of the potential damage, however, they are still not doing enough. Awareness is one thing, taking action is another.

The results of this year's survey confirm once again that companies rank cyber risks among their highest risk management priorities (Figure 1). 76 % of Swiss companies include cyber risks in their top ten company risks, with 39 % of those surveyed even placing them in their top five. But cyber risks are not the only risks that our customers had to deal with in 2017 and 2018. In addition to the trade war between the USA and China, which is having a major impact on many sectors, Brexit and new legislation such as the EU GDPR also caused a great deal of instability and uncertainty for companies in 2018.

Cyber risk awareness alone is not enough when it comes to tackling and minimizing these currently still opaque threats. To ensure compliance with the law on directors' and officers' liability pursuant to Article 754 of the Swiss Code of Obligations (CO), even companies that are not subject to mandatory auditing are well advised to document their cyber risk exposure in their management report in accordance with Article 961c CO and initiate appropriate preventive measures. Awareness alone is not enough.

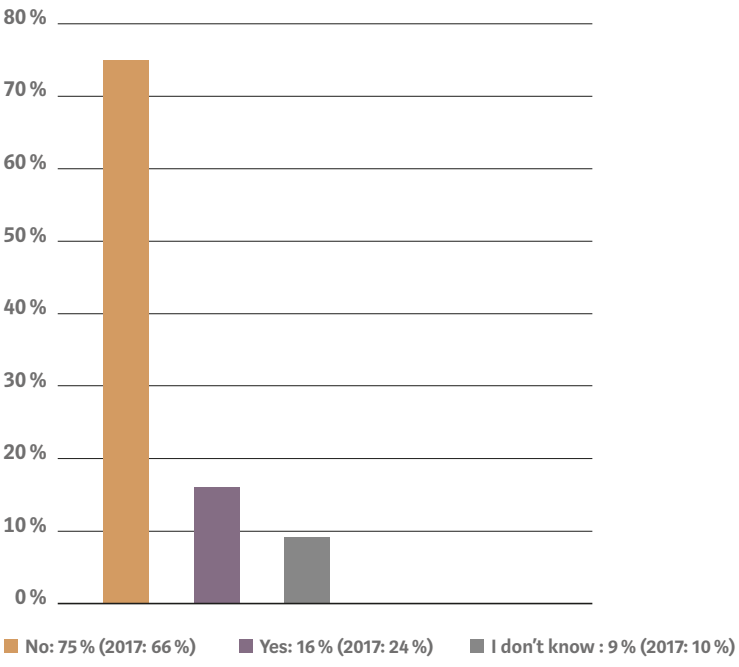
FIGURE 1

How much importance does your company attach to cyber risks?

When asked whether their company had been a victim of a cyber attack during the last 12 months, 75 % replied No, 16 % Yes and 9 % I don't know (Figure 2). This result is not surprising, as the latest findings put the global average detection time for malware at 99 days – if it is detected at all. Malware is only detected after 106 days on average in Europe, for example, rising to as many as 172 days in the Middle East, Asia and Africa. As such, it is once again reasonable to assume that some of the 75 % of companies who responded No in September 2018 have not yet discovered that their company was hacked in the last few months. This is a major problem that is recognized worldwide, and lots of research is being done into possible ways of drastically reducing the time it takes to detect infiltrated malware. The shorter the period between the introduction and detection of malware (known as the breach detection gap or dwell time), the smaller the financial impact for companies.

FIGURE 2

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



3

3.2 IMPORTANCE OF CORPORATE GOVERNANCE

A company's directors and officers can ultimately be held personally liable for cyber damage for which they are responsible. As a result, company management and not the IT department is responsible for ensuring that its operations are resistant to new cyber threats.

The results in this year's report demonstrate similar characteristics to those seen in the previous year: IT departments are still responsible for cyber risk management in the majority of companies (64 %). Management assumes responsibility for cyber risks in just 12 % of the companies surveyed. These results give us cause for concern.

Companies need to be innovative to keep pace with new technologies. Risks and opportunities must always be weighed up, and the correct security precautions must meet the security requirements required to achieve a company's strategic goals. The EU GDPR has helped raise awareness of operational cyber risks. In this age of big data, Industry 4.0 and artificial intelligence, company management teams that do not set out a conscious strategic and financial approach for dealing with cyber risks will face unpleasant questions if a cyber damage event occurs.

From a legal point of view, non-existent or inadequate cyber risk management may in some cases be deemed to constitute a breach of the duty of care or good faith as defined in Article 717 CO and may lead to a company's directors and officers being held liable pursuant to Article 754 CO.

Irrespective of this, a company's management is well advised to identify and quantify the biggest risks to its company. In accordance with Murphy's Law, where anything that can go wrong will go wrong, major cyber incidents must always be anticipated and plans for managing them drawn up carefully with the aid of specialists.

FIGURE 3

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

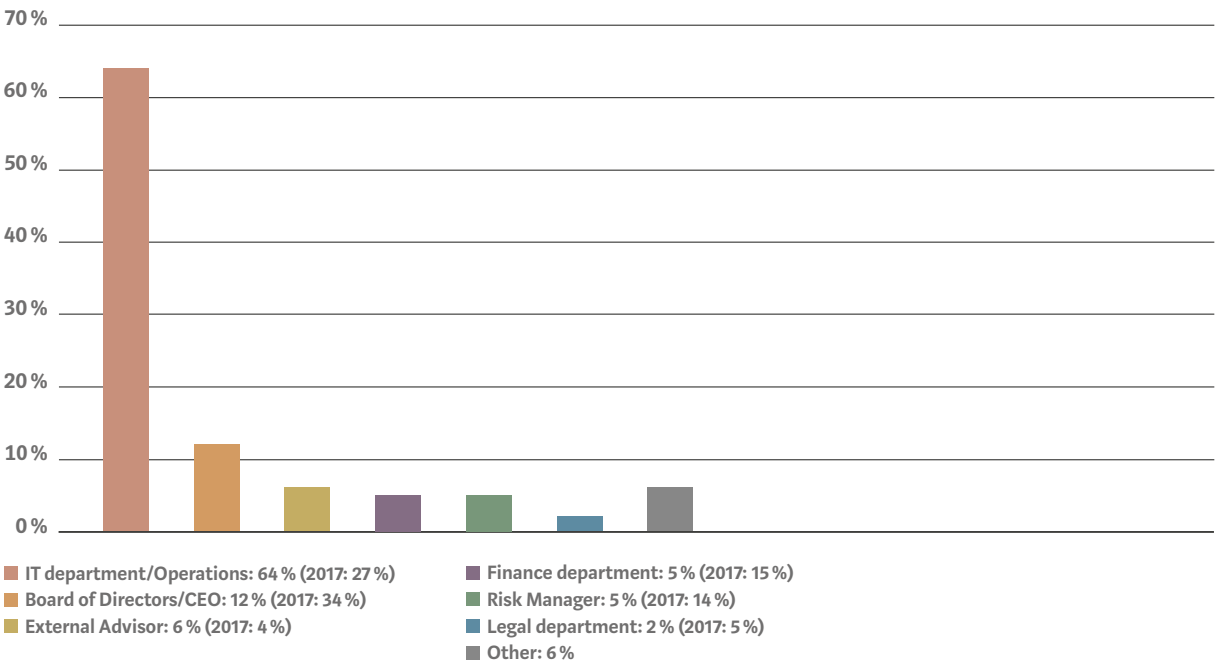


FIGURE 4

Where the board of directors/CEO is responsible for cyber risks, which of the following reports does it or he/she receive?

- Recommendations regarding cyber risk reductions: 67 %
- Awareness-raising measures: 48 %
- Report on problems or incidents that have occurred: 55 %
- Report on control activities (patches, training courses, phishing status): 36 %
- Information about the threat environment: 21 %
- Recommendations regarding cyber risk financing strategies: 12 %
- I don't know: 15 %

3

3.3 CYBER RISK MANAGEMENT: AN INDICATOR OF RISK AWARENESS

There is no right or wrong form of cyber risk management. Each company has its own focus for dealing with cyber risks, based on its core business and the strategic goals arising from this. The only incorrect approach is to do nothing. Awareness is one thing, taking the necessary action is another. The aim of cyber risk management is to plug this gap.

42 % of the survey participants have already quantified the financial impact of an operational cyber incident (compared with 58 % in 2017 and 41 % in 2016). Despite the unsettled trend, these results are pleasing and demonstrate, for example, that cyber risks are increasingly being perceived as serious company risks (Figure 5).

Of those companies that quantify cyber incidents, 34 % of those surveyed estimate the financial impact to be between CHF 1 million and CHF 10 million (Figure 6). 25 % of respondents estimate damage of more than CHF 10 million. We have noticed that of the companies that estimate cyber damage at less than CHF 1 million, 47 % are companies with a turnover of CHF 100 million or less.

Quantifying possible cyber damage events remains one of the greatest challenges within the process, as there is still a lack of reliable empirical data. Although initial loss figures would be available, insurers are extremely reluctant to publish even anonymized loss data.

The cyber attacks on the Marriott hotel group between 2014 and 2018, which were disclosed in autumn 2018, show just how crucial it can be to make a rough assessment of residual cyber risk. The pure notification costs associated with hacked sensitive personal data would be relatively simple to calculate, making it all the more surprising that the insurance cover allegedly in place was not even sufficient to cover the basic notification costs.

FIGURE 5

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

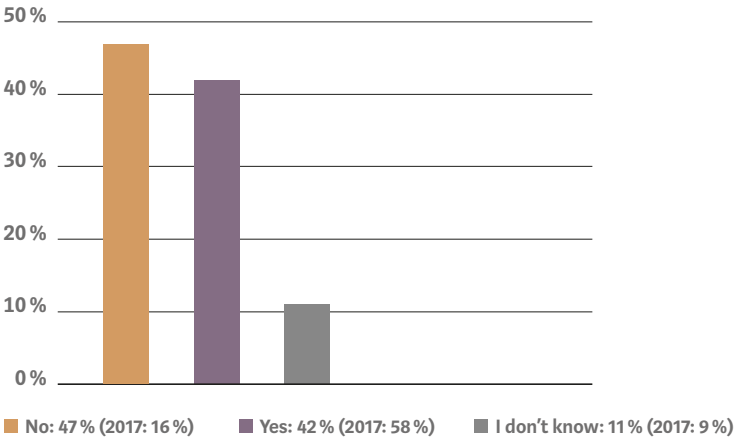
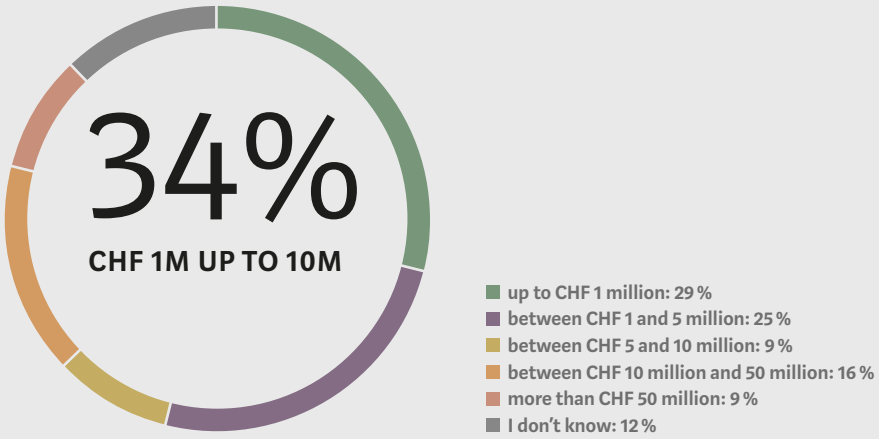


FIGURE 6

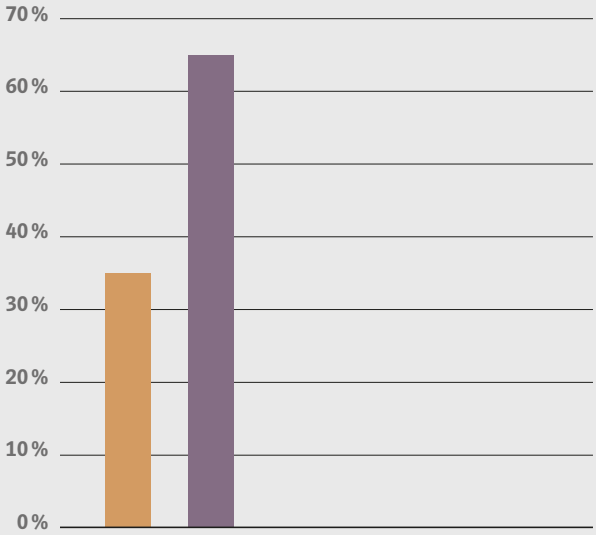
If your company has estimated the financial impacts of a cyber incident, what is the maximum potential loss value?



3

FIGURE 7

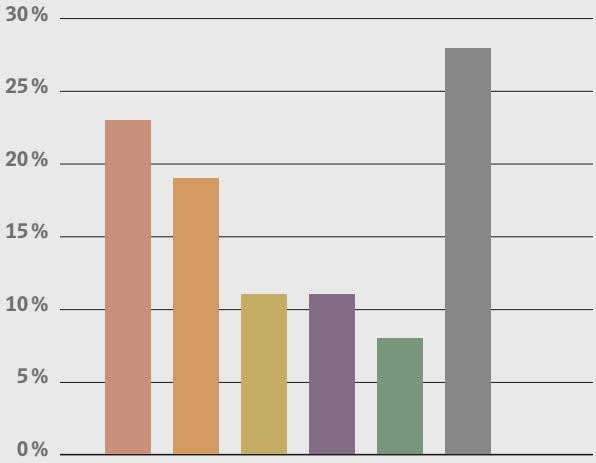
Has your company developed an emergency response plan over the last 12 t o 24 months to deal with cyber attacks?



- Yes: 35 % (2017: 29 %)
- No: 65 % (2017: 61 %)
- Ich weiss es nicht: 0 % (2017: 10 %)

FIGURE 8

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



- Cyber incidents are covered in other disaster plans, therefore do not require special treatment: 23 % (2017: 7 %)
- Cyber security/firewalls are sufficient for preventing cyber incidents: 19 % (2017: 18 %)
- The company lacks the required know-how: 11 % (2017: 9 %)
- The cyber risk is too low to justify the development of emergency plans: 11 % (2017: 4 %)
- We do not consider it a priority: 8 % (2017: 7 %)
- I don't know: 28 % (2017: 16 %)

The principle of hope rarely offers good counsel. Companies that count cyber risks as one of their top ten risks should put the creation of an emergency response plan at the top of their list of priorities. Plans must be put in place for dealing with cyber incidents that threaten a company, and staff must be suitably trained. Companies that consider the worst case scenario, which should consequently be all those that count cyber risks as one of their top company risks, are leaving things to chance if they do not have a suitable emergency response plan in place. Emergency planning for cyber worst case scenarios, like risk financing planning, are ultimately the responsibility of strategic company management. By contrast, the Computer Incident Response Team (CIRT) works at an operational and tactical level and ensures that a company's most important assets are as secure as possible.

THE BOAT WILL CAPSIZE WITHOUT TRAINING: THOSE WHO LEARN HOW TO SAIL IN A STORM HAVE SIGNIFICANTLY BETTER CHANCES OF SURVIVING SEVERE WEATHER ON THE OPEN SEA.

Only 35 % of survey respondents stated that they have developed an emergency response plan over the last 12 to 24 months (Figure 7). This is despite the fact that 59 % of the respondents who have estimated the cyber worst case scenario quantified the average amount of damage at over CHF 1 million (Figure 5). The justification given for the absence of a crisis plan is twofold: cyber incidents are already incorporated into other disaster plans, and – as last year – sufficient cyber security or firewalls are already in place (Figure 8).

With regard to the emergency action plan, the indirect contribution of the GDPR should not be underestimated. Since 25 May 2018, affected companies have been obliged to comply with their reporting obligations following a data security event, and fulfilling this obligation practically requires the creation of an emergency action plan (see also Figure 16).

3

As in the previous two years, most Swiss companies fear a business interruption as a result of a cyber incident. Reputational damage is the second biggest threat, followed by damage to data and software. Then come disruption/interruption of industrial systems or operational technology, compromising of customer data, extortion/ransomware, violations of the EU GDPR or other data protection laws, loss/theft of intellectual property and damage to persons and property (Figure 9).

Business interruption as a result of a cyber incident and scenarios involving personal data are rightly the most feared, as these damage events generally give rise to the biggest cost drivers. They are high cost drivers because the criminals responsible for the damage are sometimes highly adept at covering their tracks. Despite criminal charges being brought against persons unknown, companies are ultimately left with all the costs and a large dose of uncertainty.

FIGURE 9

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

	Switzerland	
Business interruption	65 %	(2017: 86 %)
Reputational damage	49 %	(2017: 57 %)
Data/software damage	39 %	(2017: 53 %)
Disruption/interruption of industrial systems or other operational technology	28 %	(2017: 33 %)
Compromising of customer information	25 %	(2017: 52 %)
Extortion/ransomware	25 %	(2017: 37 %)
Violation of GDPR or other data protection laws	22 %	(2017: n/a)
Loss/theft of intellectual property	16 %	(2017: 22 %)
Liability to third parties resulting from a system breach	15 %	(2017: 30 %)
Physical property damage and/or bodily injury	6 %	(2017: 11 %)
Other	2 %	(2017: 34 %)
I don't know	3 %	(2017: 2 %)

Integral customer or production data that is protected from unauthorized access and the fulfilment of contractually agreed delivery deadlines both have a major impact on an impeccable reputation.

In 2018, for example, the actions of Uber (discovery of the cover-up of a hacker attack with 57 million victims in 2016), Swisscom (delay of several months in announcing the loss of 800,000 people's data in 2017) and LinkedIn (discovery that LinkedIn Europe collected the e-mail addresses of 18 million non-users without their consent, processed the data in the USA and transferred it to Facebook for targeted advertising) showed that companies try to keep data breaches or the late detection of data misuse as secret as possible. The Marriott hotel group, by contrast, behaved in an exemplary manner following the hacker attack discovered in autumn 2018, informing its customers about the incident by e-mail.

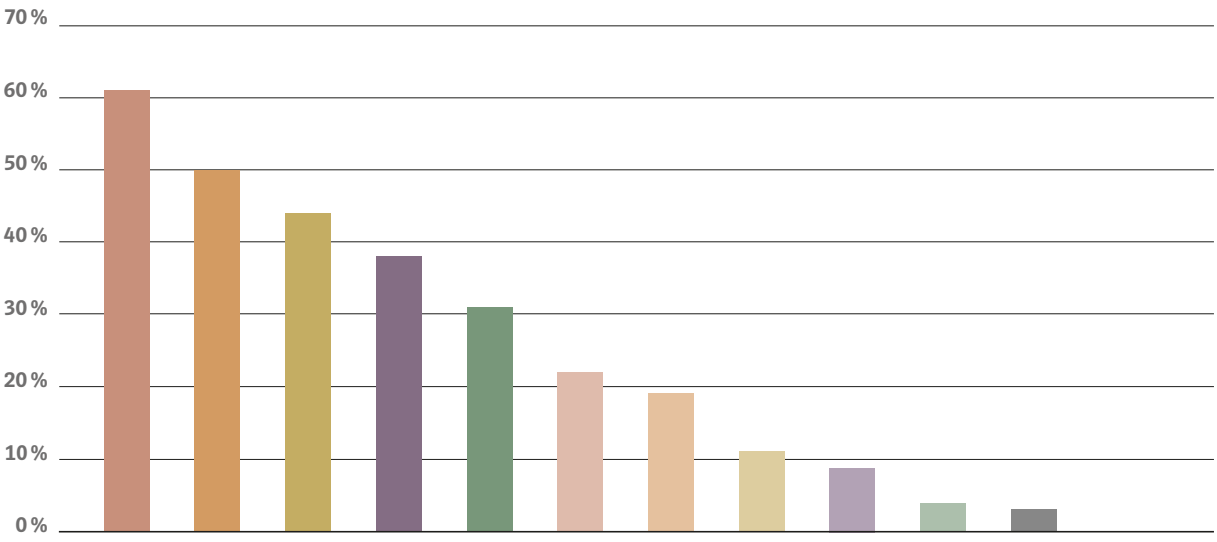
Transparent customer information in a crisis situation also has an impact on a company's reputation, usually a positive one.

Like last year, the cost/benefit decision «Are we able/willing to suffer a monetary fine or reputational damage?» will in any case require companies to develop new strategies in respect of transparency and costs.

3

FIGURE 10

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



- Financially-motivated threat such as organized crime and/or groups of hactivists: 61 % (2017: 43 %)
- Human error by employees or contractual partners: 50 % (2017: 21 %)
- A malicious employee or third party with authorized access to our company's IT resources: 44 % (2017: 27 %)
- Technical error/operational error: 38 % (2017: 8 %)
- Fire/natural disasters: 31 % (2017: n/a)
- Internet outage: 22 % (2017: n/a)
- Power outage: 19 % (2017: n/a)
- Physical attack on hardware: 11 % (2017: n/a)
- Politically-motivated threat: 9 % (2017: 2 %)
- Other: 4 %
- I don't know: 3 %

The waves of cyber attacks in June 2017, led by the crypto Trojan horses WannaCry, Petya and NotPetya, provided a striking demonstration of the IT monoculture endemic in Europe, the unpredictability of the situation and the fact that humans are the key factor in cyber risks. The human factor is particularly important in cases where the installation of malware on a company network is facilitated by an inadvertent «click».

One important step would be to objectively incorporate the residual risk associated with potentially criminal or easy-to-manipulate employees into the cyber risk analysis. We estimate the residual cyber risk arising from human nature to be at least 95 %, and assume that 50–80 % of cases involve a perpetrator with internal know-how, regardless of whether this know-how was acquired in their current or former employment. With this in mind, preventive measures must be targeted specifically at those areas where the damage could be greatest. Key IT staff with comprehensive administrator rights and other key personnel should be checked as a priority in accordance with the need-to-know principle. It is illogical and disproportionate that a bank transfer of CHF 1,000 or more requires two signatures, whereas IT staff with comprehensive administrator rights can cripple a company with just a few clicks of the mouse.

3

3.4 SUPPLIER CYBER RISK MANAGEMENT

The cyber risks associated with IT providers are all too often forgotten. The reality is that companies are increasingly attacked via their IT providers. The more reliant a company is on external outsourcing partners, the more important it is for the failure of these partners to be integrated into the company's operational cyber risk management. The focus should ideally be on the entire value chain. Companies can no longer be considered in isolation.

Initial responsibility for damage caused by IT providers lies with companies themselves. They generally have to pre-finance any potential liability risks, which requires adequate liquidity. Other disadvantages include the possible loss of control over data, inadequate isolation of the various data processing steps from other cloud users, compliance risks, lock-in effects and access to company data by foreign authorities.

ISO CERTIFICATIONS OF IT PROVIDERS DO NOT GUARANTEE BETTER CYBER SECURITY.

48 % of companies now assess the vulnerability of their suppliers to cyber risks, compared with just 33 % in 2017. This pleasing result reflects the growing awareness of this important topic.

Figure 11 clearly illustrates that compiling an inventory of supplier relationships is still a rarely taken precautionary measure. Besides compiling an inventory, the following should also be documented: access rights to company data and systems, evaluation of suppliers with regard to

their own cyber security, the requirement of guarantees for monitoring or other protective measures,

contractual agreements regarding liability limits for cyber-related losses, analysis of suppliers' financial strength and suppliers' obligation to take out their own cyber insurance.

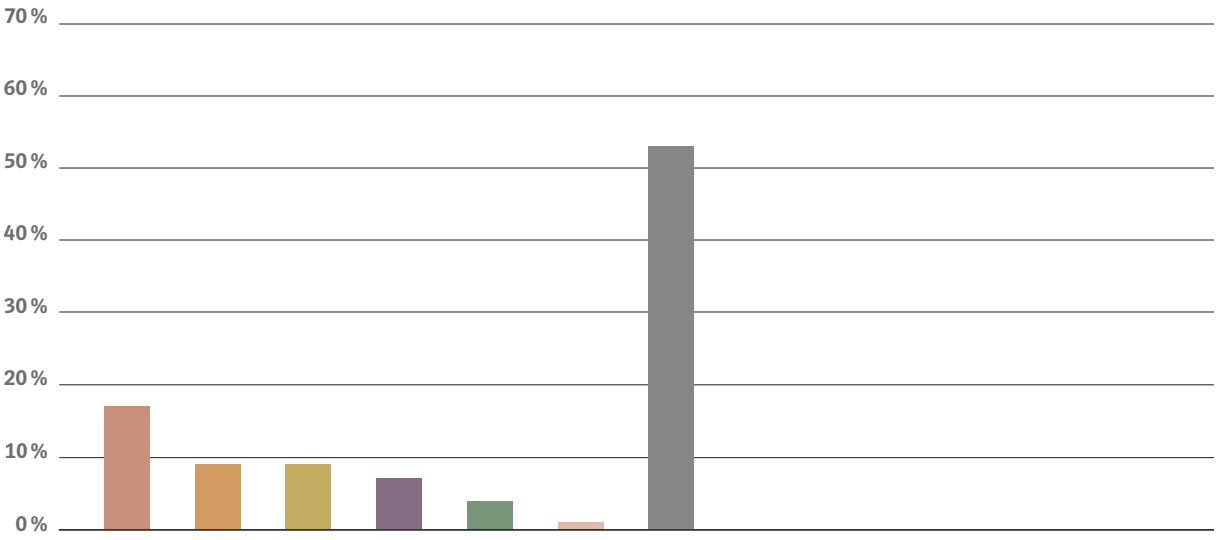
47 % ASSESS THE VULNERABILITY OF THEIR SUPPLIERS TO CYBER RISKS.

We are hugely concerned by the dearth of inventories and thus the substantial lack of transparency regarding existing quantitative and qualitative IT supplier relationships. This lack of transparency effectively equates to ignorance, and ignorance is dangerous.

There is an obvious preventive measure, however: a corresponding list of suppliers can create transparency and greater understanding with regard to dependencies should a cyber damage event occur. It is therefore understandable that cyber insurance companies demand transparency throughout the entire IT value chain of the companies they insure.

FIGURE 11

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



- Inventory of supplier relationships and data access rights: 17 % (2017: 31 %)
- Assessment of suppliers with regard to cyber security and the demand for guarantees in terms of cyber security measures: 9 % (2017: 12 %)
- Contractual regulations with regard to liability limits for cyber losses: 9 % (2017: 10 %)
- Regular monitoring of suppliers in terms of their cyber security measure: 7 % (2017: 8 %)
- Analysis of suppliers' financial capacity: 4 % (2017: 5 %)
- Obligation of suppliers to take out cyber insurance: 1 % (2017: 1 %)
- We do not assess our suppliers, or I don't know: 53 %

3

3.5 CONTINUED INCREASE IN NUMBER OF CYBER INSURANCE POLICIES

The cyber insurance landscape continues to develop in Europe and Switzerland. The insurance offerings are still difficult to understand for non-experts, making professional advice and a review of individual coverage requirements essential. The increase in cumulative risks means that companies' assurances regarding their own IT security and compliance standards will become more important in the future. Insurers will justifiably be increasingly reluctant to insure a pig in a poke.

Cyber insurance should compensate for any material losses resulting from a cyber incident. The transfer of risk must therefore be assessed not on the grounds of hype but based on cost/benefit considerations.

We believe it is realistic that 16 % of the companies surveyed have already taken out cyber insurance: 70 % of the respondents are SMEs with a turnover of up to CHF 250 million. SMEs are currently taking out the most policies due to the favorable insurance conditions, not just via brokers but also directly with insurers.

387 companies (customers and non-customers of Kessler) participated anonymously in this year's survey. 16 % of the respondents stated that they have already taken out cyber insurance, while 23 % are planning to take out corresponding insurance over the next 12 months or increase the current level of coverage. 12 % stated that they do not have cyber insurance but that certain cyber risks are already covered by their conventional insurance policies. Finally, 31 % currently have no plans to take out a cyber insurance policy (Figure 12).

CYBER RISKS CONTINUE TO RISE. INDIVIDUAL CYBER RISKS MUST BE EVALUATED AND OPTIMALLY INSURED. PROFESSIONAL ADVICE IS ESSENTIAL.

FIGURE 12

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

- My organization does not have cyber insurance and does not intend to take out a cyber insurance policy: 31 % (2017: 16 %)
- My organization is planning to take out a cyber insurance policy over the next 12 months or increase its level of coverage: 23 % (2017: 29 %)
- My organization has taken out a cyber insurance policy: 16 % (40 %)
- My organization does not have cyber insurance, however we do have a certain level of cyberinsurance cover through other insurance policies: 12 % (2017: n/a)
- I don't know: 18 % (2017: 15 %)

3

FIGURE 13

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

- Cyber risk management plans: 51 % (2017: 44 %)
- Order of the Board of Directors: 14 % (2017: 26 %)
- Have experienced a cyber attack themselves: 10 % (2017: 10 %)
- Regulatory requirements such as those of EU GDPR: 7 % (2017: 16 %)
- Prompted by a cyber attack on another company: 4 % (2017: 30 %)
- Obligation to provide proof of insurance: 4 % (2017: 3 %)
- Other: 7 % (2017: n/a)
- I don't know: 3 % (2017: 13 %)

FIGURE 14

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

- Lack of internal agreement regarding the requirement: 23 % (2017: 14 %)
- Our cyber security is strong enough, therefore we do not need cyber insurance: 21 % (2017: 17 %)
- Cyber insurance does not provide adequate coverage of the costs: 19 % (2017: 62 %)
- We do not understand the available coverage: 10 % (2017: 21 %)
- Cyber coverage is included in another policy: 10 % (2017: 14 %)
- Insufficient budget or resources: 8 % (2017: 7 %)
- Our cyber risks are borne by our captive insurer: 1 % (2017: 3 %)
- Other reasons: 26 % (2017: n/a)
- I don't know: 9 % (2017: 3 %)

More than half of the companies surveyed that have already taken out cyber insurance or are planning to take out cyber insurance or increase their level of coverage cited their current cyber risk management plan as a driver (Figure 13). This is understandable, as anyone who opens Pandora's box recognizes the potential damage relatively quickly.

According to the survey, cyber risk management (cited by 51 % of respondents) is far and away the most important driver for taking out cyber insurance or increasing the level of coverage. Damage events at other companies do not seem to make a huge impression on respondents, with only 10 % viewing these as a driver for taking out cyber insurance or increasing coverage. A top-down cyber risk financing strategy is also still considered a minor driver at 14 %: going forward we see boards of directors as a key driver for starting the cyber risk discussion. Their legal obligation to consciously adopt a cyber risk financing strategy should be reason alone for companies to start recognizing cyber risk as a top priority (see also Figure 1)

43 % of Swiss companies have no cyber insurance, do not intend to take out cyber insurance, do not have an appropriate plan in place or state that they do not have cyber insurance because certain cyber coverage components are already covered by other insurance policies (Figure 12). This year, the main reasons cited for the above situation are the lack of internal agreement on cyber insurance requirements and the strength of existing operational cyber security. Inadequate coverage of costs is still cited as a reason, but unlike last year it is no longer the main one (Figure 14).

4
EU GDPR STRENGTHENS CYBER RISK MANAGEMENT

4.1 COSTS ARISING FROM DATA PROTECTION LAW VIOLATIONS

The costs that arise in connection with data protection law violations can be calculated and to a large extent insured. The conscious decision to implement the EU GDPR to a suitable degree is therefore on the company management agenda. The EU GDPR strengthens cyber risk management.

It can be assumed that claims arising from cyber damage events in Europe will in future be asserted increasingly 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.

The latest developments in data protection law are boosting awareness of cyber risk management and cyber resilience within companies: the EU GDPR virtually compels company management to address cyber risk management and data protection due to the threat of high costs. In addition, the forthcoming revision of the Civil Procedure Code (CPC) will put the right to bring group actions (permitted under the EU GDPR and already in force in Germany) squarely on the agenda of board of directors meetings in Switzerland. The proposed option of a group action will considerably raise awareness of cyber risks and data protection.

In the event of a data leak, those familiar with the relevant data protection laws can perform the necessary duties and implement targeted operational measures to avoid official data protection proceedings, fines and other consequential costs. One aspect of cyber insurance that may be of interest to certain sectors is that costs associated with data breaches are largely covered.

Of the companies surveyed, 66 % are subject to the GDPR, 20 % are not, and 14 % do not know whether they are or not (Figure 15).

Of the companies that are subject to the EU GDPR, 49 % stated in autumn 2018 that they had a response plan in the event of a data protection violation (Figure 16). This is a pleasing development, up from just 23 % in the previous year. It is striking that 35 % of companies still do not have an appropriate response plan in place, even though the EU GDPR has been directly applicable to EU countries since 25 May 2018 and EEA countries since 30 July 2018. Although the EU GDPR does not oblige companies to implement a response plan for cyber incidents, it does for example require that they inform the supervisory authorities within 72 hours of a data security incident being detected. It goes without saying that meeting this deadline is easier with a response plan than without one.

FIGURE 15

Is your company subject to EU GDPR?

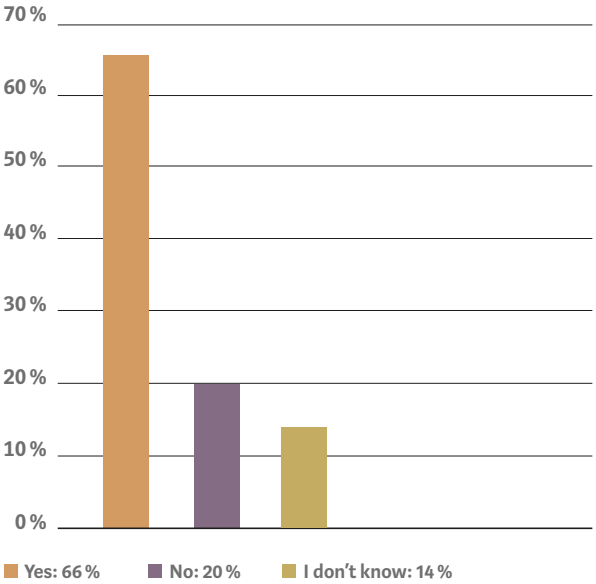
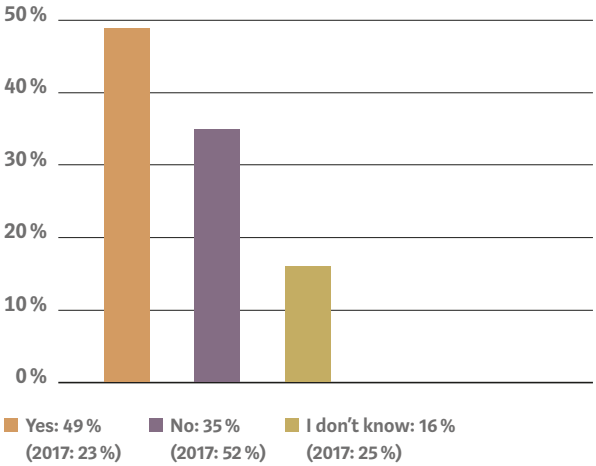


FIGURE 16

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

Cyber risk is a hot topic right now. Awareness has been created, but awareness alone is not enough to achieve company goals. It has to lead to concrete measures and a change in approach, as ensuring the confidentiality, integrity and availability of data is an essential part of daily business operations in today's digital age.

Cyber risks are unpredictable and harbor various unforeseeable costs, due not least to the lack of transparency in the IT supply chain and the weakest link in the entire IT security chain: human beings with their typically human characteristics such as willingness to help, good faith, vengefulness, greed, pride, egotism and fear. All of these factors can influence human behavior and turn a motivated employee into a criminal. Targeted attacks combined with internal know-how have the greatest damage potential.

Pure pessimism is destructive, but a pinch of pessimism is necessary to protect a company against cyber risks and implement the relevant preventive measures. The best security gaps in a system and an organization will probably be found by adopting the mindset of a criminal.

NEED FOR ADVICE

Managing residual cyber risks is still a complex and challenging task. We have identified an ongoing need for advice with regard to the assignment of responsibility for and quantification of cyber risks within a company, and increasingly with regard to the implementation of appropriate and diversified preventive measures. The main argument in favor of transferring cyber risks is the unpredictable human factor, which is the main cause of current cyber risks. Cyber risks are company risks and should undergo an annual cost/benefit analysis to determine whether they need to be insured.

Do you have any questions?
Arrange a personal consultation:

Pascal Schweingruber
Member oft he Executive Committee
pascal.schweingruber@kessler.ch
T +41 44 387 87 65

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, our innovative strength as well as 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 as well as the public sector). 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 its headquarters in Zurich as well as at further sites in Aarau, Basel, Bern, 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 are 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 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