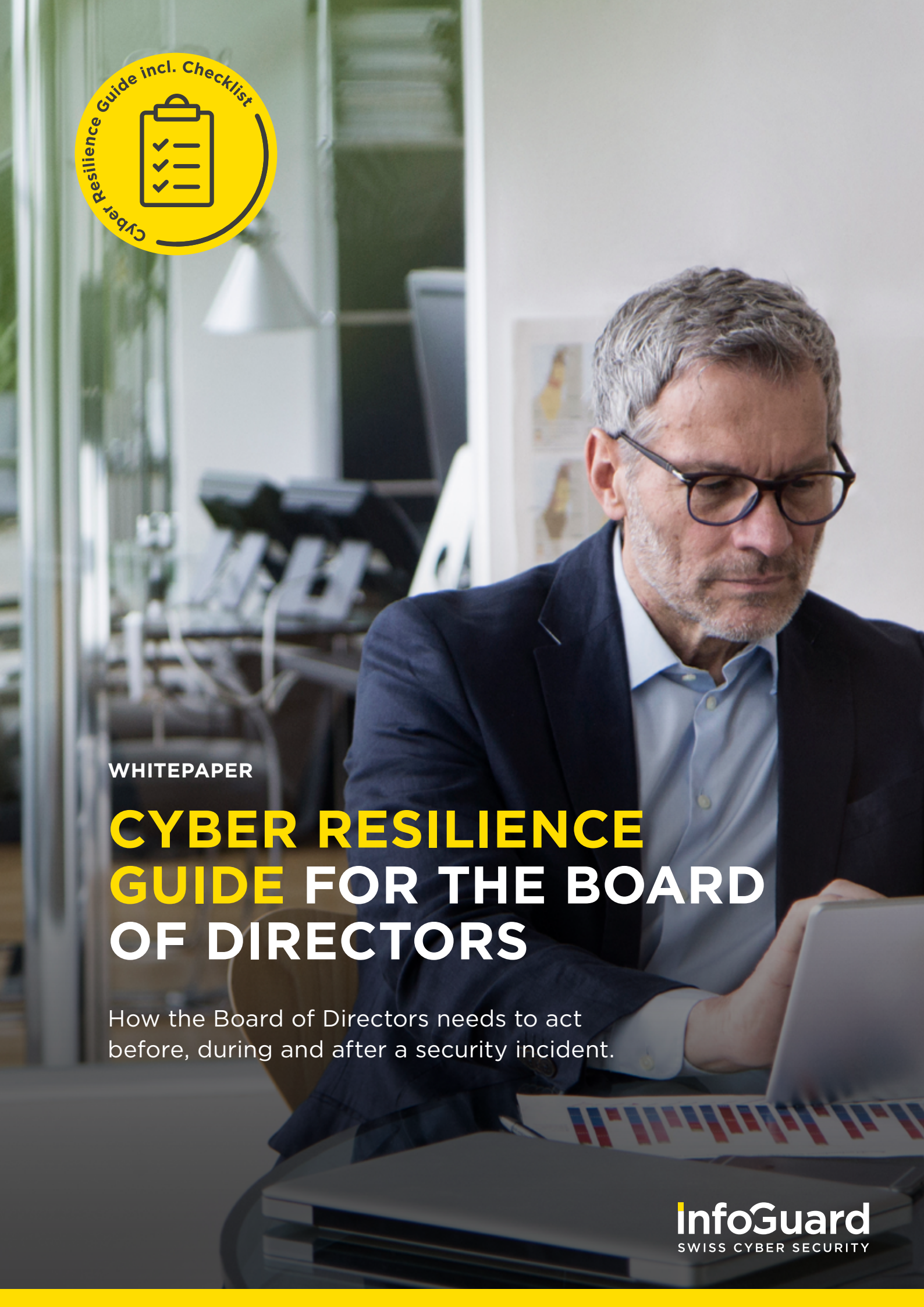


WHITEPAPER

CYBER RESILIENCE GUIDE FOR THE BOARD OF DIRECTORS

How the Board of Directors needs to act before, during and after a security incident.

InfoGuard
SWISS CYBER SECURITY

Executive Summary

Cyber risks are the greatest danger facing companies – what can be done?

Companies in Switzerland are increasingly becoming the focus of cyber criminals, as can be seen from the endless press reports on the subject. Companies often suffer severe damage from cyber attacks such as ransomware, phishing or DDoS. Entire networks and associated systems can be compromised, data stolen, as companies end up paralysed and exposed to blackmail. In many cases, such incidents can have existential consequences. **The number of cyber attacks is increasing dramatically and the losses can be huge**. What is more, this is a rising trend. That the size of the company is irrelevant is particularly shocking.

Cyber security is a hugely important topic for the commercial success of a company. Leading risk studies show that CEOs and top management consider cyber risks to be the greatest threat to companies. Reasons include advancing digitalisation and networking – just think home office, IoT/IIoT, remote access and cloud – along with the sharp rise in cyber crime ("cyber crime-as-a-service") and increasing compliance requirements.

And this is why cyber resilience – the fusion of cyber security, risk management, business continuity and resilience practices that promote an organisation's ability to withstand and recover from a cyber attack – must form a key part of your agenda. As the Board of Directors of a renowned company, you have a crucial role to play: under the Swiss Code of Obligations, every Board of Directors is obliged to design, implement and monitor an integral risk management system. Now for a question to you:

How effective is your company's cyber resilience strategy and what is your role as Board of Directors?

This guide and checklist, specially designed for Boards of Directors and executive teams, can help illustrate the status of your cyber resilience and how you can increase the resilience against cyber risks in your businesses. It also contains a seven-point plan for emergencies and clarifies what you need to do in the event of or after a security incident. **We wish you a successful implementation process and will be happy to provide you with any advice and support you may need.**

Thomas Meier
CEO & Board of Directors Delegate

Peter Letter
Board of Directors President

Content

01 | The Twelve Elementary Questions for the Board of Directors

The Board of Directors' understanding of the cyber threat and its involvement in identifying the response is critical both in terms of its role as a corporate strategist and its oversight function.

In our view, as a Board of Directors you therefore need to establish clarity on the following issues:

1. What are the new cyber threats and risks and how do they affect our business?
2. Is our cyber resilience programme equal to the ever-increasing challenges posed by today's and tomorrow's cyber threats?
3. Is our company sufficiently prepared to identify an attack and respond to it appropriately?
4. Have we implemented a process for data backup to ensure that backups are made regularly and that they are also stored offline? If so, are these also regularly tested for effectiveness (recoverability)?
5. Do we have a capable external partner who can support us immediately and comprehensively with expertise and resources (24/7) if necessary? And have we proactively discussed how the collaboration will work?
6. Do we understand our current vulnerabilities – including in relation to our suppliers and service providers – and what processes have we implemented to address the identified cyber risks?
7. Does our company comply with legal and regulatory obligations to protect data, for example in terms of data protection? Is sufficient documentation available?
8. What indicators of key risks and performance metrics do we need to monitor at Board of Directors level in order to successfully perform our oversight function?
9. Is cyber resilience (the company's ability to withstand cyber attacks) included in our strategic Board of Directors meetings? If so, when was the last time we addressed the cyber threat?
10. Which duties are we required to perform ourselves on the Board of Directors and which can be delegated?
11. How do we evolve our business from having a reactive to approach to the cyber threat to having an active, anticipatory one?
12. Do we have the edge over our main competitors? If so, how can we use this as a competitive advantage?

Hand on heart: were you able to answer most of the questions with a convincing "yes"? Or are individual aspects still something of a black box for your company? Either way, this guide actively supports your efforts in achieving a high level of cyber resilience in your organisation. At the same time, it provides concrete guidance on what you need to do before, during and after a security incident – not least thanks to the checklist. But, first things first:

02 | **Cyber Resilience as a Duty of the Board of Directors**

Cyber risks are making their way up the agenda of many board meetings, not least thanks to the numerous recent incidents and media reports. And we say: rightly so. The reason is self-explanatory. The consequences for affected companies are severe, often existential, or such attacks can culminate in insolvencies. In Switzerland, SMEs are increasingly being affected in addition to large companies. A cyber attack can quickly wreak a huge amount of damage. To name just a few (serious) possibilities:

- **Loss of customer trust and reputation**
- **Losses of revenue**
- **Follow-up costs for replacement and restoration**
- **Legal costs and fines**
- **Liability, damages, compensation for delays**
- **Loss of time, delayed market entry**
- **Insolvency**

Of course, it is not your job to be up to speed with the latest technologies or to stipulate or review operational measures. Instead, what matters is that you can address targeted questions to your IT and security managers to get at the information that enables you to assess your company's resilience and effectiveness against cyber threats – also with the help of this guide. Or indeed identifying where you may need to intervene and react.

Cyber resilience also means a strategic opportunity for your company. Use it as a USP to stand out from your competitors. Responsible management of cyber risks or a well-managed cyber incident can boost the confidence of a company's stakeholders – be they customers, investors, suppliers or regulators. Concentrate on defence alone is not enough. What matters is strengthening the overall resilience, recognising attacks quickly and reacting even more rapidly. To ensure that all this succeeds, it is advisable to evaluate and bring on board a suitable, professional and capable partner at an early stage. Proactively discuss how the collaboration will work..

The three success factors

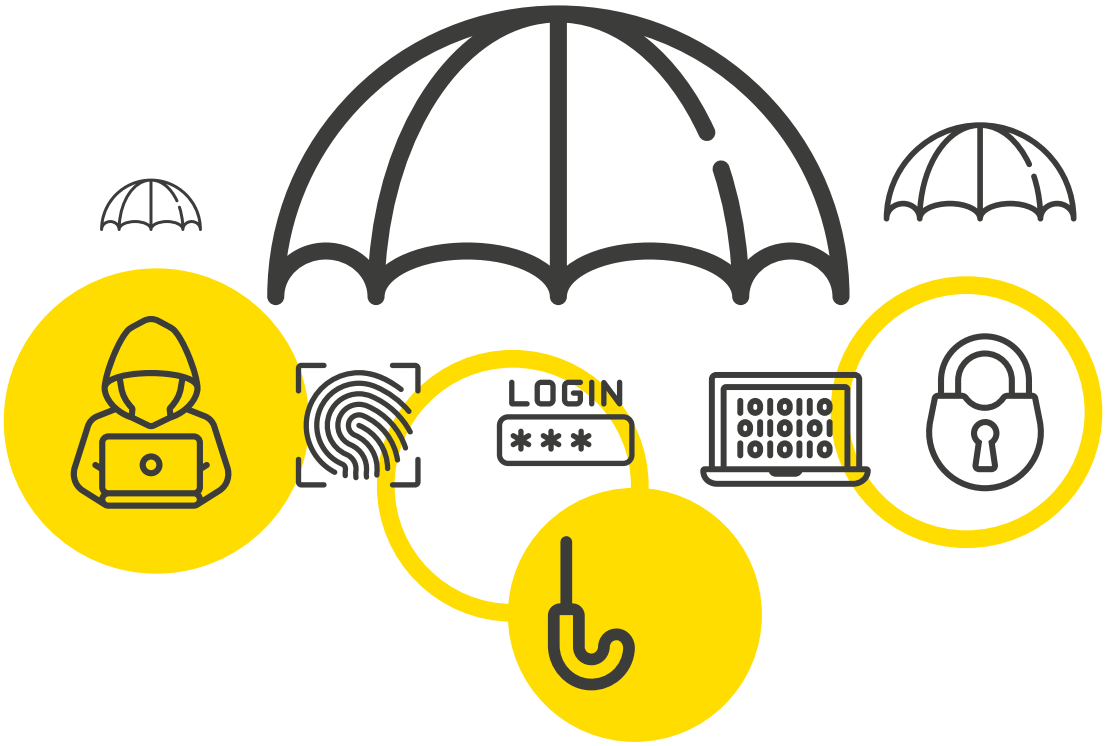
- ✓ Embrace cyber resilience at the highest corporate level.
- ✓ Include cyber resilience in the company-wide risk assessment.
- ✓ Establish appropriate cyber resilience measures and monitor implementation.

02.1 | **Embrace cyber resilience at the highest corporate level**

You will doubtless be aware that the Board of Directors is responsible for identifying, assessing, managing and monitoring cyber risks and
the corresponding resilience. You can take responsibility for action yourself or delegate it to an existing body (e.g. audit or risk committee) or to a specific cyber resilience expert team. Leadership responsibility, on the other hand, cannot be delegated. Based on experience, we recommend that you set out in writing the scope and responsibilities and the manner in which these responsibilities should be exercised – including the structure and processes for reviewing cyber resilience.

02.2 | **Include cyber resilience in the company-wide risk assessment**

As the Board of Directors, it is your responsibility to ensure that management has integrated cyber resilience and cyber risk assessment into overall business strategy and enterprise-wide risk management, budgeting and resource allocation. It is similarly essential that you are regularly informed about current threats and trends and that this is also documented. If necessary, consult independent external experts with a proven track record.
You can count on us. We at InfoGuard are happy to support you!!



02.3 | **Establish appropriate cyber resilience measures and monitor their implementation**

Identify

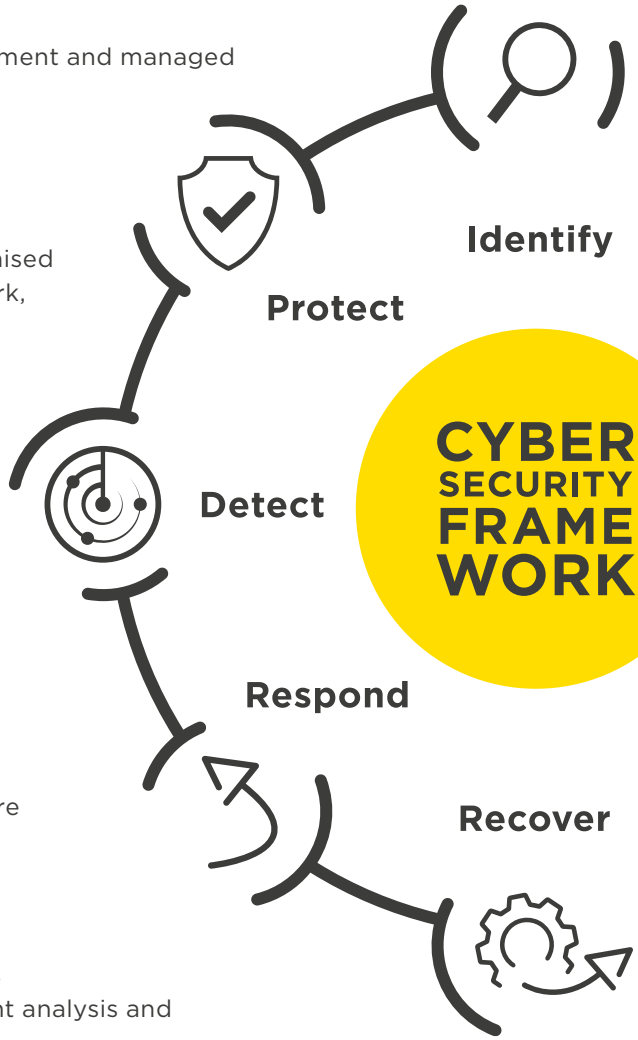
- Operate appropriate risk management processes and identify security risks
- Assign tasks, competences and responsibilities
- Know which data and business processes are business critical
- Create an inventory of IT systems and software (also Internet of Things, IoT) with the corresponding dependencies to your business services
- Vendor management: supply chain monitoring & management and managed services & outsourcing

Protect

- Raise awareness among employees
- Establish a security framework in compliance with recognised standards, e.g. ISO-27001, NIST Cyber Security Framework, ICT minimum standard
- Identity and access management, including monitoring
- Implement appropriate security and defence measures, professional operation and cyber security architecture (also in cooperation with third parties)
- Regular patch & vulnerability management of all IT systems

Detect

- Security surveillance/monitoring for the detection of attack traces, lateral movement and typical procedures based on the cyber kill chain
- Segment and monitor the networks
- Periodic/continuous technical safety tests, also in software and product development



Respond

- Develop and test/exercise the incident contingency plans for successful response planning, communication, incident analysis and mitigation.
- Implement a continuous improvement process to optimise cyber resilience

Recover

- Develop and test/exercise cyber disaster recovery planning incl. communication, follow-up for continuous improvement of own cyber resilience
- Regular offline backups of systems are performed, managed and tested (including restorability of backups)

The executive team thus steers the implementation of measures (definition, implementation, testing and continuous improvement of measures and processes) to improve cyber resilience and ensures that these are aligned throughout the company.

02.4 | **Checklist to assess your cyber resilience**

We have compiled a checklist which should enable you as a Board of Directors to make a realistic self-assessment regarding cyber resilience in your company.

As the Board of Directors, you should be able to answer the following questions in the affirmative for your company with a clear conscience.

- ✓ Do you get regular updates about cyber resilience topics and can you assess the impact on your own company?
- ✓ Is there a documented data protection and cybersecurity programme consisting of adequate and appropriate policies and procedures? Does the entire workforce understand and follow this policy?
- ✓ Have you defined the responsibility for action and who it is assigned to?
- ✓ Have your key information assets been identified and their vulnerability to cyber attacks thoroughly assessed?
- ✓ Are regular independent assessments/audits of your cyber resilience carried out and are the relevant results – i.e. those with high priority – communicated to you?
- ✓ Have you conducted a cyber security risk assessment?
- ✓ Do you know your current risk situation, vulnerabilities and the impact on your cyber resilience?
- ✓ Is your cyber resilience strategy periodically reviewed, including whether key cyber security risks have been assessed, prioritised and minimised?
- ✓ Has sufficient account been taken of the impact of cyber risk on the business, such as business interruptions, impact on the quality of products/services, reputation etc.?
- ✓ Do you evaluate the cyber risk impact in advance of new business ventures (e.g. mergers, acquisitions and joint ventures) or even new products or technologies?
- ✓ Do you have basic cyber resilience policies in place, including business continuity and disaster recovery, incident response, as well as for continuous improvement and communication?
- ✓ Do you use proven security mechanisms for defence and monitoring systems for early detection of cyber attacks?
- ✓ Do you have a contingency plan in case of a cyber incident? Is the contingency plan practised regularly? And are backups and offline backups of the relevant assets available in a timely manner?
- ✓ Do you have experts in optimising cyber resilience (identifying, protecting, detecting, responding, recovering from cyber attacks)? Do you have procedures in place so you can call on external experts when needed?
- ✓ Are KPIs used and reported for the continuous improvement of cyber resilience (e.g. response times to security events, response times to vulnerabilities)?

03 | **First Response in the Event of a Security Incident**

Given the prevailing situation, it would be remiss to assume that out of all possible companies, your company is of no interest in terms of hacker attacks. **The guiding principle today is that it is not a question of if, but when your company will be the target of a successful cyber attack.** You are doubtless aware of this, which is precisely why it is of existential importance for you to take appropriate precautionary measures to safeguard your cyber security.

Of central importance is the detection, analysis and response to cyber attacks – around the clock. A CSIRT (Computer Security Incident Response Team) from a professional Cyber Defence Centre (CDC) helps you minimise how long a security incident lasts and the damage it causes, while also drastically reducing the business impact.

In this context, the creation of an incident response plan is one of the most important tasks in establishing effective incident management processes. An incident response plan documents who should take what action and how if a security incident occurs. It also defines the necessary procedures, guidelines, roles, responsibilities and not least the communication and escalation channels.

As the Board of Directors, you must ensure that such a process is established, documented and also practised accordingly. **The lessons learned from this must of course also be fed back in to enable continuous optimisation.**

When dealing with such a situation, your company also needs immediate access to specialists. After all, you not only face technical hurdles, but customers, business partners and not least employees – and possibly also the public – need to be informed.

You gain valuable time if you can rely on your tried-and-tested partner – and do not need to evaluate a suitable support partner and thrash out contractual details in the midst of a cyber attack. The time a security incident lasts and the damage it causes can be minimised with the help of a CSIRT (Computer Security Incident Response Team) – such as provided by InfoGuard. At InfoGuard, we place great value on the rapid reconstruction and restoration of the production or business capability of the affected companies.

03.1 | **Seven-point plan for emergencies**

A security incident can occur at any time in any company, regardless of size or industry. Most of the time, it hits those with operational responsibility quite unexpectedly and they are often overwhelmed with the situation – something our CSIRT experiences almost daily.

For this reason, we have developed a seven-point plan for board members like you:

1. **Set up a crisis team.**
Involve relevant internal bodies at an early stage, for example in the form of a crisis team.

2. **Plan regular meetings.**
Plan regular consultation phases of the crisis team that alternate with work phases. Recommended agenda items include situation analysis and collection of facts, immediate measures, risk-opportunity analysis, options for action, decision-making, timing, responsibilities as well as the review of the achievement of objectives.

3. **Communicate regularly.**
Internal and external communication is one of the most important tools for managing the incident visibly to the outside world and at the same time one of the biggest challenges. Our recommendation to you:

- Leave the communication to the specialists!
- Identify the stakeholders and agree on the language!
- Follow the principle of internal before external communication!
- Centralise the flow of information and use FAQs!
- Bear in mind: there is no room for “blame, name, shame” and “bashing” in the crisis!
- Tell the truth publicly and to your employees at all times!

4. **Think about reporting obligations.**
The obligation to notify the supervisory authority must be observed in the event of data protection violations. As a rule, a report must be submitted within 72 hours. Also, inform your cyber insurance company at an early stage, and consult specialised lawyers.

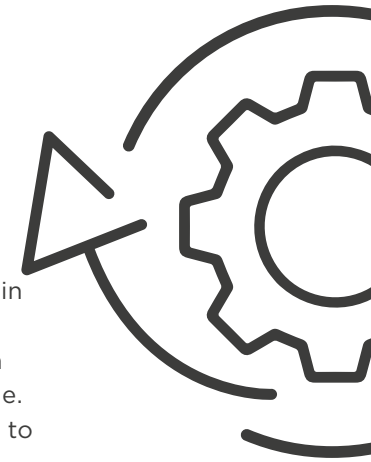
5. **Get external support at an early stage.**
Affected companies often do not have enough internal expertise or resources to successfully manage such security incidents. External specialists also support you in legal matters and in negotiating with the attackers.
In many cases, the amount of the ransom can be massively reduced (should this be necessary).

6. **Restore your ability to act.**
It is essential that you make regular backups and store them offline. This can ensure the continued existence of the company in the event of a ransomware attack. In the short term, data important for emergency operation may also be located at remote offices or on systems of employees who are away on leave that are not (yet) affected.

7. **Do not forget the follow-up tasks.**
Remember to perform a professional debrief for evaluation and optimisation. Define any long-term security measures and plan an audit of your IT by external experts as soon as these measures have been implemented. Last but not least: thank your contractors and customers for their understanding,
patience and support. When the dust has settled, plan some kind of a “thank you” for all staff involved.

03.2 | **Reverting from emergency to standard operation**

It is crucial for every company to implement a process for backup and recovery. This is an essential part of a company's disaster recovery strategy because your data is too valuable and business critical. This is more than a matter of processes, technologies and procedures for making regular copies of data and applications to a separate, secondary device. It also extends to the recovery of these in case of data loss/damage along with the IT environment necessary for data handling of the business processes based upon it and on which you depend. In today's diversified and multi-layered IT environment, this is a major challenge. Broadly speaking, there are three things you need to do or arrange:



1. **Plan: create a plan as a basis: WHAT,** WHEN (recovery point objectives (RPO), recovery time objectives (RTO) and service level agreements (SLAs)), WHO.
2. **(Rapid) recovery of systems and data.**
3. **Testing of the plan and continuous improvement.**

Experience shows that the reversion to normal operation after an incident takes a considerable amount of time. Advance planning of the allocation of resources and activities based on the available time allows the fastest possible, targeted recovery in line with defined priorities, sequences and quantity structures. Particular emphasis should be placed on closely monitoring and recording activities during this phase in order to prevent improvised and uncoordinated participant actions as far as possible. The knowledge and information gained from such planning and testing enables you to optimise the recovery phase in terms of effectiveness and efficiency.

It is especially advisable to rely on the support of an external partner during this phase. This expertise helps you to revert from emergency to standard operation efficiently, safely and successfully without having to completely reinvent checklists, action plans etc. Do not forget to communicate with your internal and external stakeholders. Ensure that communication is regular and transparent to dispel any doubts, rumours and decision-making uncertainties from the outset and ensure that there is no confusion around decision-making and escalation authority.

"**Successfully managing a security incident requires rapid and professional support from experts** who can actively assist you with resources and expertise. Thanks to InfoGuard's support, we were quickly up and running again. I can highly recommend the Swiss cyber security company."

DR. STEPHAN WARTMANN,
CEO of BRUGG GROUP AG

04 | Cyber Security Is Our Passion

InfoGuard is the Swiss expert for comprehensive cyber security. Our more than 230 security specialists in Zug, Bern, Munich and Vienna take care of information security for over 400 customers in Switzerland, Germany and Austria each and every day. We offer you a holistic range of solutions for implementing and strengthening your cyber resilience.

Cyber security is a challenge – and also our passion. Every day, we strive to make the world digitally a more secure place. With our 360° expertise, as well as innovative services and solutions, we set the benchmark. Over 230 security experts across four locations ensure comprehensive protection around the clock for our clients in Switzerland, Germany and Austria. Years of experience, a broad portfolio of solutions, recognised certifications and attestations as well as qualified employees are the cornerstones of our business, offering the highest level of security, professionalism and reliability. As an independent company, we are able to react quickly and flexibly to changes in clients' needs.

Our vision of making the world digitally more secure day by day is at the heart of all our actions and motivates us to go above and beyond to ensure our clients' security. In doing so, we embody the values of passion, trust, client satisfaction, expertise and innovation, which shape our work and spur us on to deliver the best performance at all times.

2001
Over 20 Years of Experience and Expertise

100%
Independent

230+
Security Experts

4
Locations in Switzerland, Germany and Austria

24/7
Real-Time Monitoring and Emergency Response

ISO 27001
ISO 14001
ISAE 3000 Type 2

Swiss CDC Cyber Defence Center

CSIRT Computer Security Incident Response Team
FIRST Member and BSI-Qualified APT Response Service Provider

05 | Cyber Security Made in Switzerland

Cyber security is an essential aspect of today's digital world. At InfoGuard, we're synonymous with reliable, innovative services and solutions that protect your security and trust. Our 360° expertise ranges from Cyber Defence Services and Incident Response Services to Managed Security & Network Solutions, Penetration Testing & Red Teaming and up to Security Consulting Services. Offering cloud, hybrid and on-premise services, we provide the degree of flexibility that meets your individual requirements. A holistic approach, highly specialised employees, efficient processes and state-of-the-art technologies ensure your security in a complex digital world – today and in the future.

Cyber Defence

In the dynamic, ever-changing world of cyber threats, cyber defence is critical for the rapid detection and combatting of potential threats – 24/7. All services are provided from the ISO 27001-certified Cyber Defence Center (CDC) in Switzerland.

Cloud Security

Comprehensive security and expertise in the cloud – from strategy, architecture and transition to professional implementation and secure operation, to continuous optimisation, and smooth off-boarding.

Incident Response (IR)

Successful cyber attacks can never be completely ruled out. In the event of an emergency, our Computer Security Incident Response Team (CSIRT) is on hand immediately to stop the attackers and minimise the damage. We support companies at every stage and ensure that they can resume operations as quickly as possible.

Security Consulting

Professional security consulting is indispensable for meeting the diverse requirements and achieving the individual goals – be it in the area of strategy, governance, risk and compliance, architecture and design, security assessments or in promoting a security-conscious corporate culture.

Managed Security & Network

Cyber security can only succeed with a stable, reliable foundation. To this end, we develop IT security architectures based on state-of-the-art network and security solutions. Through comprehensive Professional Services and 24/7 Managed Services, we also ensure the continuous protection of digital infrastructures and the highest availability.

Penetration Testing & Red Teaming

Effective cyber security requires a profound understanding of cyber criminals' methods and tactics. Drawing upon our expertise in Penetration Testing & Red Teaming, we not only identify vulnerabilities, but also develop tools and procedures to detect them before they can be exploited by potential attackers.

06 | **Conclusion**

Cyber risks are among the most significant operational risks a company faces. It is the responsibility of the Board of Directors and the executive team to implement an effective risk management concept. It is imperative that the cyber strategy is geared towards resilience.

The last few months have shown clearly that the quantity and especially the quality of attacks have increased markedly. The dangers are also becoming more complex and varied. For example, we are currently seeing many cases of cloud compromise: cyber incidents in the Azure environment, primarily in the area of “business email compromise” – better known as “CEO fraud”.
Research shows that many IT administrators cannot handle the complexity of MS Cloud solutions and are overwhelmed. The danger is also greater than ever in the area of “mergers & acquisitions”, which covers mergers, company purchases, takeovers and acquisitions. It is not uncommon for the newly acquired companies to have already been unwittingly hacked, thus posing a grave security risk.

As you can see, the cyber risk landscape is very complex and challenging. Cyber security is a key business issue and is strategically relevant for many reasons. Not least because IT security risks can take on business-critical proportions, cyber resilience belongs on the agenda of the Board of Directors and executive team – no ifs or buts. This cyber resilience guide – including checklist – is intended to serve as an impetus and concrete support for you on the Board of Directors. We also firmly believe that companies like yours need a capable and reliable partner at their side – experts who actively support you with resources and expertise.

At InfoGuard we are there for you – 24/7, with a comprehensive 360-degree cyber security portfolio and full of enthusiasm!

Invitation to exchange experiences

Let’s set up a no-obligation round table discussion to establish where and what your biggest challenges and threats in the security ecosystem are. We look forward to having a personal discussion with you. From Board of Directors to Board of Directors. From executive team to executive team. Or from CIO to CIO. Get in touch!

Arrange a no-obligation meeting

infoguard.ch/en/cyber-resilience-strategy/board-of-directors

CYBER DEFENCE AT THE HIGHEST LEVEL.

How secure is your company?

InfoGuard
SWISS CYBER SECURITY

Securing Your Digital World – Today and Beyond

Baar (Head Office)
InfoGuard AG
Lindenstrasse 10
6340 Baar
Switzerland
+41 41 749 19 00
info@infoguard.ch
infoguard.ch

Bern
InfoGuard AG
Stauffacherstrasse 141
3014 Bern
Switzerland
+41 31 556 19 00
info@infoguard.ch
infoguard.ch

Munich
InfoGuard Deutschland GmbH
Landsberger Straße 302
80687 Munich
Germany
+49 899 040 5064
info@infoguard.de
infoguard.de

Wien
InfoGuard GmbH
Graben 19
1010 Vienna
Austria
+43 123 060 6538
info@infoguard.at
infoguard.at