

Cyber Security in Switzerland Finding the balance between hype and complacency



Key points

- While the term 'cyber security' means different things to different companies in Switzerland, sophisticated and targeted attacks pose a significant threat to most of them.
- Compared to Swiss companies operating internationally, companies that are primarily focused on the Swiss market tend to underestimate cyber threats.
- Businesses with immature cyber defences are often unable to quantify attacks and incidents. This can lead to a false sense of security and underinvestment in cyber security measures.
- Businesses need to assess the maturity of their cyber defences and take a strategic view of what measures are needed, rather than simply reacting to incidents or regulations.
- Cyber security is too systemic an issue to be the sole responsibility of the IT department. Businesses need an integrated cross-organisational strategy and operating model.

Contacts

Mark Carter
Partner

Deloitte AG
+41 (0)58 279 73 80
markjcarter@deloitte.ch

Dr. Klaus Julisch
Senior Manager

Deloitte AG
+41 (0)58 279 62 31
kjulisch@deloitte.ch

Contents

What is cyber security?	3
Threat awareness	5
Cyber maturity	8
Strategic importance	10
Recommendations	13
Endnotes	14

About the study

Deloitte interviewed 17 Chief Information Security Officers (CISOs) and Heads of Security Engineering or Operations from a cross-section of industries to understand how Swiss-based companies prepare for and respond to cyber threats. The interviews were conducted between October 2013 and January 2014. The key findings of our analysis are summarised in this report.

Acknowledgement

We would like to thank all the executives who were interviewed for participating in this report.

Additional contributors

Dr. Michael Grampp, Head of Research, Deloitte AG
Dennis Brandes, Research Manager, Deloitte AG

What is cyber security?

Since Operation Aurora was publicly disclosed in early 2010, reports on cyber security and Advanced Persistent Threats (APTs) have increasingly dominated the media. Recent revelations about government surveillance programmes have further fuelled concerns about security in a hyper-connected world.

Understanding the issue

Senior IT and business leaders across all industries have frequently voiced the view that they have no clear definition for the term 'cyber security'. Rather, the term is seen as "new words for old ideas". For decades, companies have been deploying firewalls, anti-virus scanners, intrusion detection systems and other security controls to keep hackers out. Therefore, some participants questioned the new sense of urgency regarding cyber security.

Among companies that embrace the term cyber security, definitions vary. A common definition is that cyber security provides defences against *targeted attacks* from *external actors* against a company's digital and online assets. Others take cyber security to mean attacks against the *embedded IT systems* in power plants, public transport systems or other critical infrastructure. Yet another definition is that cyber security is the defence against attacks using *incident detection and response* rather than preventative means such as firewalls or access controls.

Deloitte practitioners observe the same ambiguity among our clients world-wide. However, sophisticated and targeted attacks are a significant threat to companies' information assets, brands and financial accounts. Consider the following:

- More and more assets are going digital, including personal identities, money, intellectual property, books, movies, and health records. Most of these assets are vulnerable to cyber attacks and expose their owners and custodians to risks.
- Government agencies, organised cyber crime rings (e.g. the Elderwood hackers) and hackers-for-hire (e.g. Hidden Lynx), have all made the news because of their sophistication and technical prowess.
- Targeted attacks grew by an estimated 42% in 2012 following 6% growth in 2011.¹ Deloitte practitioner experience suggests that the majority of companies have experienced security breaches in the previous 12 months.
- Officials globally have taken notice and are introducing new cyber security laws and regulations.^{2,3} This increasingly forces companies to take action.

"The 2013 ENISA Threat Landscape clearly shows how serious cyber threats are. Past defences are no longer sufficient, today."⁴

CISO,
Swiss Insurance
Company



Are you prepared?

While the term might be controversial, the issue is not: cyber security is a real and growing threat. Security leaders must therefore ask:

*Does my company have the right cyber capabilities to prevent, detect, and respond to **targeted and sophisticated attacks** against our digital and online assets?*

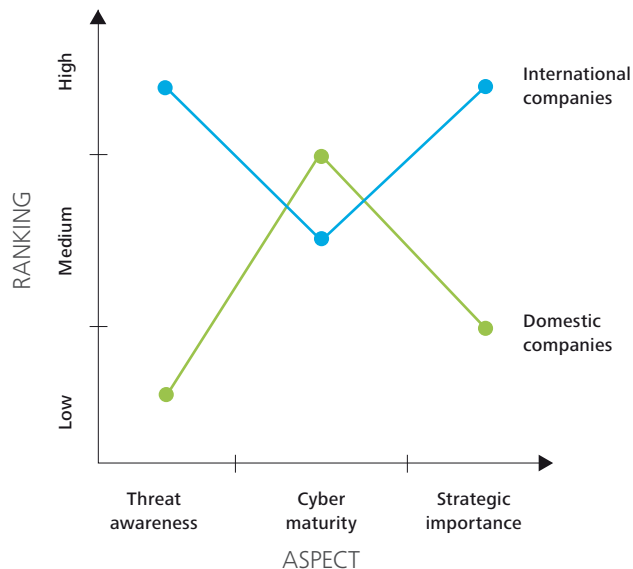
When discussing this question, interviewees had different views on three important aspects:

- **Threat awareness** – the assessment of the severity of cyber threats.
- **Cyber maturity** – the assessment of existing capabilities and defences.
- **Strategic importance** – the importance assigned to cyber security versus other priorities and how much risk to tolerate.

Businesses with mostly Swiss operations ranked these aspects differently from their internationally operating peers (see Chart 1). Domestically oriented companies rank cyber threats as low, their maturity as medium-to-high and the strategic importance as medium-to-low. International companies lean towards a high-medium-high ranking. While outliers exist, this model provides a concise view of the differences and raises interesting questions for companies regardless of their size or where they are located.

The following sections explore the three aspects of threat awareness, cyber maturity and strategic importance in more detail.

CHART 1. VIEWS ON CYBER SECURITY DIFFER BETWEEN DOMESTICALLY AND INTERNATIONALLY OPERATING COMPANIES



Threat awareness

While the majority of internationally oriented companies assess cyber threats as high, domestically oriented businesses generally rate these threats as medium-to-low (see Chart 1). Clearly, all companies operate in the same cyber space and the dichotomy can be traced back to differences in threat awareness. Interviewees with medium or low threat awareness frequently used arguments such as:

- “We have nothing of value that would motivate cyber criminals to attack us.”
- “Our audit reports show that we are ok.”
- “We have not experienced any severe cyber incidents in the recent past.”

Other interviewees’ experiences as well as our own project work with clients globally show that these arguments may not hold up to closer scrutiny. As such, they can create a dangerous and false sense of security.

Nothing of value versus the motives of hackers

Few, if any, businesses are so commoditised that they have no data, intellectual property, brand name, or financial resources that attackers might find attractive. However, even if there was nothing to be stolen, several CISOs pointed out that “organisations get hacked by opportunistic attackers, just because they are vulnerable.”

- Companies can get targeted, not because of their assets, but because they are a stepping stone to the ultimate target.
- Some companies are attacked because hackers want to control their computing resources, e.g. to turn the organisations’ networks into botnets.
- Hacktivists compromise companies to inflict reputational damage for political rather than economic motives.
- Foreign governmental agencies may seek control over other nations’ critical infrastructure for military advantage.
- Accidental failures and human errors can also result in cyber incidents. For example, web crawlers regularly find and retrieve sensitive data on misconfigured web servers. This type of error has been so common that an entire methodology, known as ‘search engine hacking’, was developed to take advantage of it.⁵ ‘Rogue clouds’ are another case in point.⁶

“The same weapons that are used against global and multi-national companies are also being used against small or regional companies.”

**Head of Security,
ICT Company**

It is important to factor in these aspects when assessing the cyber threats a company faces. Some interviewees could convincingly argue that their cyber controls were strong enough that the cost of overcoming them exceeded the value of what could be gained. This is a valid argument and the above objection merely addresses the notion that a company had ‘nothing of value to attackers’, which is hardly ever true.

“What we see depends mainly on what we look for.”

John Lubbock
Banker, politician and
scientist from the
19th century

Using audit reports as a yardstick

Some interviewees relied on their financial or regulatory audits as assurance that cyber threats were under control. We caution companies to examine their audit reports carefully before drawing such conclusions. Financial and regulatory audits are risk-based and cover certain applications and IT infrastructure controls in the areas of access security, IT change management and IT operations. In particular external audits generally exclude large parts of IT as well as many pertinent security controls such as intrusion detection systems and vulnerability management. As a result, external audit reports are generally not the right yardstick for measuring cyber security.

Seeing is believing

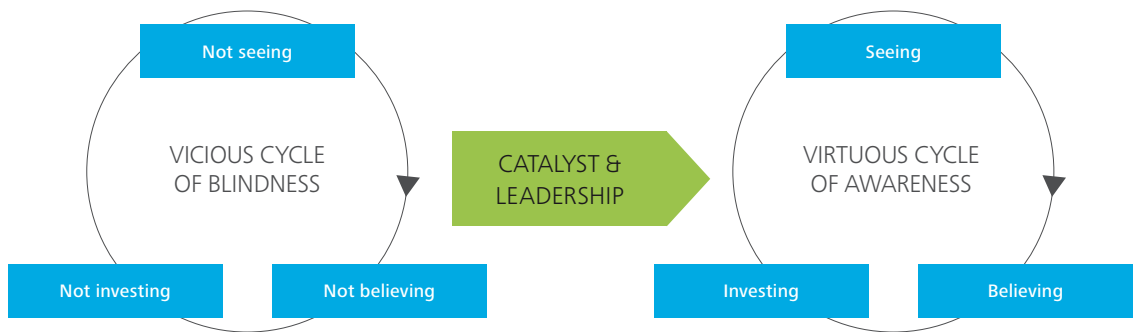
Companies that have experienced few security incidents should be careful not to draw the wrong conclusions. Companies are notoriously bad at detecting security incidents as demonstrated by the fact that approximately 70% of incidents are detected by external parties – rather than the companies themselves – and the majority of incidents take months to discover.⁷ Moreover, a self-reinforcing ‘cycle of blindness’ can set in when a state of ‘not seeing’ any incidents leads to ‘not looking’ (a classic case of confirmation bias).

Chart 2 shows what occurs in many companies. Those that are not aware of a cyber incident may tend to belittle such threats. Lacking a business case, they do not invest in the kind of capabilities that would make them more aware of their true exposures. This creates a self-reinforcing cycle, which continues until it is broken. Experience shows that this only happens through a ‘catalyst’ such as a major cyber incident, regulatory pressure or a devastating security assessment that attracts the attention of senior management.



A catalyst by itself, however, is seldom enough to break the cycle. It also takes a strong executive leader who can mobilise the company, secure funding, deliver results and articulate the value of these results to maintain momentum. Maintaining momentum is crucial because major cyber security transformations can take two to three years. Once companies start investing, they are better able to see threats and their true state of security improves. However, this can reveal disturbing facts. For example, one interviewee noted that security incidents detected have been increasing by 40 per cent per year over the last several years – mostly, as a result of investments in security monitoring capabilities. This experience is not uncommon and helps establish a virtuous cycle of continuous learning and improvement.

CHART 2. MOVING FROM BLINDNESS TO AWARENESS



Action Points

- Revisit your threat assessment and make sure to factor in all adversaries (opportunists, cyber criminals, corporate spies, hackers, nation states) as well as non-malicious accidents.
- Avoid getting stuck in the 'cycle of blindness'. As a security professional you cannot defend your company unless you are aware of the threats, attacks and incidents the company faces.
- Ask yourself: If our IT systems were compromised, how would we know? How can we be certain that intellectual property is not being sent to competitors? How would we learn about fraudsters that steal our brand to establish a fake Internet presence? What don't we know that could hurt us?

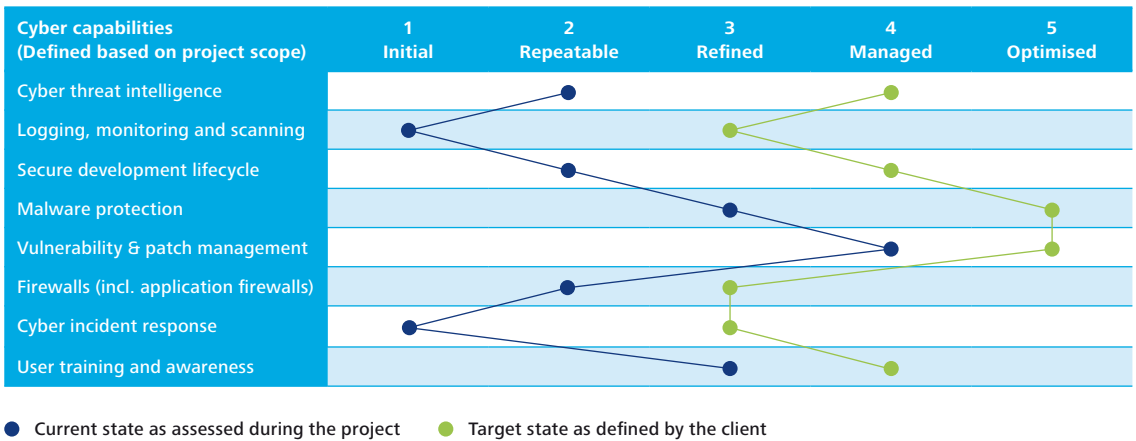
Cyber maturity

When asked whether companies are doing enough to protect their assets against cyber attacks more than 80 per cent of interviewees answered “not yet”. The list of gaps included everything from relatively basic capabilities (e.g. configuring firewalls, basic network monitoring, detection of unauthorised devices, patching software) to more advanced cyber capabilities such as cyber intelligence, zero-day protection⁸ or cyber incident response. The following sections summarise the four key points that stood out from the conversations.

Difficulty measuring cyber maturity

Many companies find it difficult to assess how good their cyber security is and find it even more difficult to decide how good their cyber security should be. Consequently, they do not have a strategic view of where they stand and where they want to go. In such companies, security priorities are generally based on audit issues, compliance requirements, past security incidents or an effort to salvage sunk costs. Based on our project work, we would recommend a more strategic approach, which is also embraced by some of the companies interviewed for this study. In this approach, a scoping step is used to identify the key capabilities the company wants to focus on. Subsequently, each capability is ranked on a 1-to-5 maturity scale and a target state is defined to document the aspired maturity (see Charts 3 and 4).




CHART 3. MEASURING CYBER MATURITY – EXAMPLE FROM A DELOITTE PROJECT



Tools are not capabilities

Many companies have a tendency to deploy new tools faster than they are able to integrate them into their processes and organisational structures. This leads to situations where, for example, intrusion detection systems are deployed without having provided the processes to configure, maintain and monitor them. While companies realise that tools are not capabilities, they struggle to drive the necessary organisational transformations. Moreover, to build mature cyber capabilities, companies must take a holistic approach that advances the maturity of people, processes and technology (see Chart 4).

CHART 4. CYBER MATURITY SCALE

	1 Initial	2 Repeatable	3 Refined	4 Managed	5 Optimised
People 	Basic knowledge, undefined roles and responsibilities, reactive.	Fragmented expertise, roles and responsibilities defined in silos.	Trained security staff, enterprise-wide roles and responsibilities exist.	Broad and deep expertise, use of threat intelligence to act proactively.	Highly skilled staff, holistic and systematic work approach using KPIs.
Processes 	Ad hoc and mostly manual, inconsistent execution, little documentation.	Processes exist in silos, but inconsistent design and execution.	Defined processes, some automation, documentation.	Strong focus on automation, KPIs used to improve effectiveness.	Continuous improvement and integration with enterprise risk management.
Technology 	Basic security technologies managed in a piecemeal manner.	Foundational security technology managed in silos.	Centralised technologies in line with enterprise policies.	Best of breed technology aligned with policies.	Extensive automation using technologies.

Cyber intelligence is a focus area

The majority of interviewees are investing to improve their companies’ cyber intelligence. In general, these efforts focus on implementing classic security logging and monitoring capabilities including Security Information and Event Management (SIEM). These are important steps towards breaking the cycle of blindness previously discussed. Only a small number of interviewees are investing in more advanced cyber intelligence such as malware forensics, commercial intelligence feeds, big data analytics or low-interaction honeypots.⁹

Cyber incident response is in its infancy

Most companies have historically underinvested in incident response. Even today, few have started to invest in this area to build teams that are capable of responding to attacks in a coordinated manner that integrates all affected parties and captures forensic evidence to support law enforcement and continuous improvement efforts. This makes cyber response the ‘orphan child’ among cyber capabilities – and an important area of improvement because it literally is the last line of defence when all other controls have failed. Moreover, professional incident response capabilities are indispensable when cleaning up incidents caused by Advanced Persistent Threats.¹⁰

Action Points

- Form a strategic view of your cyber capabilities’ current and target states.
- Take people, processes and technology into account when assessing the maturity of cyber capabilities. If available, factor empirical evidence into the assessment.
- Specifically assess if you need to invest in specialised incident response capabilities or if you should contract with an external provider who can provide these skills on demand in the event of incidents.

Strategic importance

Lack of strategic support and funding

Only a third of interviewees responded that in their companies, cyber security is considered a “must have” of strategic importance that cannot be traded off against other priorities. The remaining respondents did not single out cyber security as a category of its own, but rather managed it as part of their general information security budgets. These companies reported varying degrees of difficulty in obtaining executive support and funding to strengthen cyber security. The root cause for this difficulty was partially attributed to the vicious cycle of blindness described previously: When empirical evidence is lacking, it is difficult to create a compelling business case and gain executive sponsorship for cyber security investments.

However, the situation is exacerbated by a widespread bias among C-level executives who tend to view security as a second-tier priority. Three main factors are seen as contributing to this bias:

- Security in general, and cyber security in particular, are seen as highly technical IT problems that are preferably delegated to IT specialists.
- Cyber incidents are rarely made public, which creates a shortage of recent, vivid and memorable examples. Psychological studies have shown that without such examples, risks are perceived as more benign.¹¹
- C-level executives are highly focused on managing financials and leading change and innovation. These predispositions can be at odds with the values of security, stability, and operational continuity. Thus, what could be described as a ‘bias for action’ puts the priority of security projects under pressure.



Changing priorities

In the words of one CISO, “the lynchpin is getting executives to understand that cyber security is *their* responsibility”. This is because rather than being an IT problem, cyber security is a systemic problem that has its roots in IT and affects all parts of a company. Consider the following examples:

- In general, IT departments do not monitor blogs and online communities to detect when a company’s brand is belittled on the Internet. Nor do IT departments prepare press releases when such Internet chatter is picked up by mainstream media.
- Attacks that abuse corporate brands such as cyber squatting or brandjacking¹² are generally not addressed by IT departments.
- While security breaches at third parties are a significant security threat to many companies, most IT departments do not own the topic of third party security.¹³
- Businesses must maintain relationships with industry peers, customers, suppliers, regulators and governmental agencies to exchange threat intelligence and respond to incidents in an effective manner.

The bottom line is that C-suite leadership is essential to manage all facets of cyber security holistically and across organisational silos. The majority of interviewees confirmed this point, but less than half of all companies have established the necessary executive support.

Action Points

- Continue to brief senior management on cyber security to win strong and broad sponsorship among C-level executives.
- Take an enterprise-wide view of cyber security: Identify all internal and external parties that have a stake in cyber security. Define their roles and responsibilities, and establish end-to-end processes for incident detection, incident response, and other cyber capabilities.
- Appoint a single C-level executive or a management board who is accountable for all aspects of cyber security across the company.

“Security is the last remaining
IT Risk.”

Former CIO
Global Fortune 10 Company

Recommendations

The threat from sophisticated and targeted attacks against digital and online assets is real and growing. To respond to this situation, security leaders should consider the following steps:

- 1. Reassess cyber threats.** Make sure to consider all threat actors (opportunists, cyber criminals, corporate spies, hacktivists, nation states, etc.) and their motivations (financial gain, publicity, inflicting damage, access to computer resources, theft of knowledge). Given these motivations, what threat do your digital and online assets face from potential attackers?
- 2. Gain visibility.** Companies often underestimate threats because they do not observe them. Companies that lack the technical capabilities to monitor attacks and detect incidents should prioritise investments in these areas.
- 3. Take a strategic view.** Take a strategic view of the cyber capabilities your company needs, their current maturity and the target maturity that is required. Then invest in achieving those capabilities' target maturities. Doing so will ensure that scarce resources are allocated wisely, rather than being lost in tactical battles.
- 4. Build company-wide governance.** Cyber security is a systemic issue that requires a coordinated approach involving IT, legal & compliance, public relations, fraud investigations, external regulators, customers, partners and the broader public. Companies should therefore build a holistic cyber governance approach that manages these stakeholders end-to-end.
- 5. Maintain communication with senior management.** C-level executives are biased to focus on change initiatives and financial performance while delegating cyber security to IT departments. Security leaders must counter this bias by maintaining continuous communication with senior management to gain their support and sponsorship.



Endnotes

- 1 2012 and 2013 Internet Security Threat Report, Symantec 2012 and 2013, see also: http://www.symantec.com/de/de/security_response/publications/threatreport.jsp
- 2 Digital Agenda for Europe – Cybersecurity; European Commission, see also: <http://ec.europa.eu/digital-agenda/en/cybersecurity>
- 3 National Cyber Security Strategies in the World; ENISA, see also: <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world>

In particular, regulators take a keen interest in the cyber resilience of the banking system, as evidenced by the 2013 cyber simulations “Waking Shark II” in the United Kingdom and “Quantum Dawn II” in the United States.
- 4 2013 ENISA Threat Landscape; ENISA, 2013, see also: <http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats>
- 5 Understanding the Web: A Guide to Internet Research, National Security Agency, 2007. See also: http://www.nsa.gov/public_info/_files/Untangling_the_Web.pdf
- 6 Navigating Social Media Legal Risks: Safeguarding Your Business, Robert McHale, Que Publishing, 2012.
- 7 The 2013 Data Breach Investigations Report, Verizon, 2013, see also: <http://www.verizonenterprise.com/DBIR/2013/>
- 8 Zero-day attacks are attacks that exploit previously unknown software vulnerabilities.
- 9 Virtual Honeypots: From Botnet Tracking to Intrusion Detection, Niels Provos and Thorsten Holz, Addison-Wesley Professional, 2007.
- 10 Security Incident Response in the Age of APT, Anton Chuvakin, Gartner, September 25, 2013.
- 11 The Psychology of Security, Bruce Schneier, Africacrypt 2008, LNCS 5023, Springer-Verlag, 2008, pp. 50-79.
- 12 Navigating Social Media Legal Risks: Safeguarding Your Business, Robert McHale, Que Publishing, 2012.
- 13 Blurring the lines, 2013 TMT Global Security Study, Deloitte; 2013, see also: https://www.deloitte.com/view/en_GU/gu/industries/tech-media-telecommunications/5772cd015031f310VgnVCM3000003456f70aRCRD.htm

About Deloitte in Switzerland

Deloitte is a leading accounting and consulting company in Switzerland and provides industry-specific services in the areas of audit, tax, consulting and corporate finance. With approximately 1,100 employees at six locations in Basel, Berne, Geneva, Lausanne, Lugano and Zurich (headquarters), Deloitte serves companies and institutions of all legal forms and sizes in all industry sectors. Deloitte AG is a subsidiary of Deloitte LLP, the UK member firm of Deloitte Touche Tohmatsu Limited (DTTL). DTTL member firms comprise of approximately 200,000 employees in more than 150 countries around the world.



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/ch/about for a detailed description of the legal structure of DTTL and its member firms.

Deloitte AG is a subsidiary of Deloitte LLP, the United Kingdom member firm of DTTL.

Deloitte AG is recognised as auditor by the Federal Audit Oversight Authority and the Swiss Financial Market Supervisory Authority.

This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication. Deloitte AG would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. Deloitte AG accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

© 2014 Deloitte AG. All rights reserved.

Designed and produced by The Creative Studio at Deloitte, Zurich. 33830A