Companies around the world are at increasing risk of being subject to some form of cyber attack. In research undertaken by AIG, 86% of respondents (including risk managers, brokers and C-suite executives) said they were “very” or “somewhat” concerned about cyber risk. But are companies in Switzerland taking enough measures to protect their businesses?

Barely a week goes by without another high-profile cybercrime story in the media. A recent KPMG report, “Clarity on Cyber Security”, published in May 2015, stated that Swiss companies have suffered a loss of over CHF 200 million due to cybercrime only last year. “The threat of cyber attack continues to grow. Companies are becoming more aware that the costs can be steep for those that fail to understand, mitigate, and transfer cybersecurity risk,” said Tracie Grella, Global Head of Professional Liability, AIG, in April 2015.

No Room For Complacency

Swiss companies are not immune to such attacks, after all, there are no borders in cyberspace. In fact, Switzerland’s sophisticated infrastructure and high profile financial services sector add to its vulnerability. Further evidence of this, if it were needed, came in January, when one of the world’s biggest cyber heists to date was revealed. The gang responsible, dubbed ‘Carbanak’ and comprising of members from Russia, China and Ukraine, is believed to have stolen up to $1bn from around 100 banks and financial institutions in 30 countries, including Russia, France, Germany, the UK, Spain, Poland, Norway - and Switzerland. In the same month, the Banque Cantonale de Genève (BCGE) was targeted by an anonymous individual or group using the Twitter moniker ‘Rex Mundi’ that claimed it had hacked the bank’s servers and downloaded more than 30,000 emails by Swiss and foreign clients. The hacker then threatened to leak the confidential data if its demands for payment weren’t met.

While many Swiss companies have become more careful, there are many more that need to be more aware of the high risk of losses they face when it comes to cyber risk. The KPMG report mentioned above conducted interviews with cyber security professionals in Switzerland, which suggest that there is a widely held view that serious cybercrime “won’t happen”. This is despite the fact that 76% of respondents believe that cyber security is not just hype that will subside - but translating this awareness into robust action is proving to be difficult with 45% of KPMG’s respondents saying they have no incident response plan in place.

A Range of Risks

This is cause for concern. The attacks described above reflect only a small fraction of diverse threats that are covered by the phrase “cyber risk”. The historic focus in the cyber market has been around the consequences of data being lost or stolen. Depending on the regulation in the country where the company is based, a victim of a breach may be liable to pay out for notification costs, experts to control the damage, credit and ID monitoring, investigation costs, third party liabilities and regulatory investigations along with industry fines and penalties.

The cyber risk landscape continues to evolve at speed and, for most businesses, it is not a question of if but when they will come under attack. We expect to see an increase in cyber extortion claims as cyber criminals increasingly focus on ways to monetize their exploits, as in the BCGE case described above.

Businesses today rely more and more on external and internal communications networks to operate their businesses. If an attack disrupts such networks, or puts them out of commission entirely, then businesses may suffer financial loss and in some instances reputational damage.

The rise of the “internet of things” and the reliance on Cloud providers means that a host of devices connected to the internet is now exposed to new types of risk, which could increase the number of interruptions. Income loss can result from systems failure either from security malfunctions, attacks or viruses, or from something that could have come about internally - for example a patch that failed.

Stiff Penalties

Different countries have different approaches to both - legislation and how they may or may not penalize businesses. Some have focussed on cybercrime legislation (which deals with cyber attacks) and other on data protection legislation. For example, while Swiss legislation focuses on the protection of customer data, U.S. legislation focuses on regulatory notifications when there are data breaches. In Switzerland companies need to take appropriate measures to avoid data breaches in the first place (prerequisite to be compliant with regulatory requirements) but do not have any “self-incrimination” duty, i.e. the company does not have to notify the breach to the person whose data has been breached.

In the U.S., however, 48 States require companies to inform customers of every data breach, no matter how large or small.
In 2012, the Federal Council of Switzerland commissioned a national strategy for protection against cyber risks, with the following strategic goals:

- Early recognition of cyber threats and dangers
- Increase of the resilience of critical infrastructure
- Effective reduction of cyber risks, in particular of cyber crime, cyber espionage and cyber sabotage.

Federal experts in Switzerland have strengthened their crisis management plans and are asking for stakeholders to review their procedures with a focus on cyber security and protection of vulnerable high-tech infrastructures and commercial assets. In addition, they have called for the creation of an in-depth Public Private Partnership to help find efficient, feasible and tailor-made solutions to cyber threats. Also in Switzerland, directors can be held liable if their failure to prepare for cyber events constitutes a breach of their duty to the company - by, for example, failing to ensure compliance by a regulated company.

As in Switzerland and Europe - the National Institute of Standards and Technology (NIST) in the U.S., the Center for the Protection of National Infrastructure in the UK as well as MELANI (Reporting and Analysis Centre for Information Assurance) in Switzerland - are pushing private sector organizations to boost security. The NIST’s recently finalized voluntary Cybersecurity Framework makes clear that company boards are expected to be aware of cyber risks and opens the door for securities class actions for shareholder losses if directors and officers don’t live up to its standards.

In the U.S., President Obama has been calling for improvements to cyber defenses and in April 2015 issued an executive order that gives the government new powers to target significant cyber threats that affect critical infrastructure, disrupt the availability of websites or networks or steal trade. As a result, cyber criminals could face new potential punishments including having any U.S. bank accounts or other assets frozen and banning U.S. entities or people from doing business with them. Beyond data protection, the European Commission is prioritizing its digital agenda aimed at encouraging easier and safer transfer of information across the EU. In Switzerland, the Swiss Cyber-Strategy is on the agenda of the National Assembly for 2015. The result is a continually shifting regulatory landscape and an uncertain impact on businesses.

Preventative Measures

Cyber security is one area where prevention is really better than cure. The responsibility for this rests with the leadership of the company; it cannot simply be delegated to the Chief Technology Officer (CTO) and IT department. The board and senior management need to create a robust cyber security framework that focuses on the allocation of resources, governance and decision-making, and the building of an organizational culture - supported by awareness training and development - which ensures that every employee is aware of his or her responsibilities with respect to cyber security. The framework should also include a disaster recovery plan, which sets out the specific steps to be taken in the event that the worst should happen. Currently, just 45% of companies have an incident response plan in place and a mere 14% test that plan regularly, according to KPMG.

While leadership must retain overall responsibility for cyber security, there are clear advantages in taking guidance from third-party experts. For example, insurance companies may be in partnership with information assurance experts and key law firms who together can offer IT audit and recommendations on how a company’s data security can be improved.

And through these partnerships, insurers like AIG, for example, can offer their clients access to pre-breach threat intelligence, governance tools, and the latest best practices to help gain a holistic understanding of their cybersecurity exposure, including the responsiveness of their insurance program to a cyber attack.

Ongoing Challenge

The reality is that the stakes are very high for the Swiss where it comes to cybercrime – the country contains attractive targets, both in financial services but also in Swiss industry, with its intellectual property and high standards in terms of innovation. For all Swiss businesses, it is critical to understand that creating a cyber security framework is only the first step. This is not something that can simply be produced, signed off and filed away to be forgotten as “another box ticked”. By its very nature, cyber security is something that demands relentless vigilance. Risks are constantly evolving and companies need measures in place that allow them to keep abreast of developments. It is also important to track current and impending legislative and regulatory developments.

However, even organizations that recognize the scale of the cyber threats they face and the importance of taking proactive security measures can find themselves exposed to a breach. As soon as an attack occurs, the disaster recovery plan needs to be put into action. Beyond this, the company needs to know that it has adequate protection in place. This means an insurance policy that can cover a range of exposures including business interruption, loss of income and brand damage.

Ideally, that policy coverage will provide the additional peace of mind of knowing that it brings access to information security specialists who can take control of a crisis and help to minimize network downtime and mitigate the scale of potential losses. Indeed, the larger insurers such as AIG will routinely include as part of their offering direct access to their network of legal advisors, forensic investigators and crisis management firms, each of whom has specialist experience in responding to cyber attacks.

At the end of the day, total security is unachievable. Whether it’s due to activists, nation states, criminals, suppliers or insiders, organizations of any scale, anywhere in the world must assume that a breach at some point is inevitable. What is achievable though is an awareness of the threats that are out there as well as a level of preparedness that allows businesses to recover from a cyber breach as quickly and painlessly as possible.

About the author:

Alexander Nagler is Managing Director DACH Region at AIG Europe Limited, London in Glattbrugg. He is a member of the Chapter Board Doing Business in Switzerland of the Swiss-American Chamber of Commerce.