A dangerous waiting game: Many companies only increase their security expenditure after an incident of loss or damage

- For 63 percent of companies, a cyber-attack that does not cause any damage would be no reason to increase investment in security
- 54 percent of companies have reported a cyber-attack
- IT and security managers say there is a need for large increases in the budget to protect against cyber-attacks
- 30 percent complain that the company lacks the necessary knowledge

ZURICH, 30 OCTOBER 2018 – The economy is becoming increasingly networked, making customer data, trade secrets and internal communication vulnerable to hacker attacks. Thus, the majority of companies (54 percent) have recently registered a cyber-attack. However, often something serious has to happen before security is improved: For 63 percent of companies, a cyber-attack that did not result in any damage would probably not lead to increased spending on security. 76 percent of those surveyed would consider it likely that spending on cybersecurity would only be increased if real damage has occurred. These are the results of the current study “Global Information Security Survey 2018-2019” by the auditing and consulting organisation EY. More than 1,400 IT and security managers from companies around the world took part in the survey, which has now been conducted for the 21st time.

Still, the majority of companies are starting to spend more on defending themselves against attacks over the Internet: two thirds of the respondents anticipate budget increases in the next twelve months. 15 percent even expect an increase of more than a quarter. Despite improved financial resources, the budget may not be sufficient in the battle against cyber-attacks: 40 percent of IT and security managers believe that budget increases of a quarter or even significantly more are necessary.
“Cyber-attacks against companies are no longer isolated incidents. On the contrary – they are a daily occurrence,” says Tom Schmidt, Cybersecurity Leader at EY FSO in Switzerland. “Even companies that have not registered an attack may be affected without noticing it. Companies that react only when the damage has been done are acting negligently. An incident of loss or damage can quickly result in devastating consequences: customer data falls into the wrong hands, servers are paralysed, costly production downtime, stolen trade secrets and a lasting loss of trust.”

**Cybersecurity is hampered by a lack of expertise and funds**

Money is certainly a decisive factor in the battle against cyber-attacks – but not necessarily the most important one. 25 percent of respondents say that their budget constraints limit the functionality of cybersecurity. 30 percent even say that the company does not have the necessary know-how. This extends right up to top management: in six out of ten companies, the person responsible for cybersecurity is not a member of the executive board or board of directors. Perhaps this is one reason why only 39 percent of IT and security managers respond with a definite "yes" to the question of whether the danger posed by cyber-attacks is fully understood at management level and whether appropriate measures are being taken. In addition, only 16% of the financial companies surveyed (banks, insurance companies, asset managers) say that their information security reporting within the company meets the needs. The other sectors, however, perform even worse in this area.

"Many companies are currently developing or implementing a digital strategy. At the same time, this is a good opportunity to include cybersecurity right from the start and to make it an integral part of business processes and their resilience. Companies are well advised to see cybersecurity as a basis of trust and a decisive factor for business success and to make it a matter for the top management," adds Roman Haltinner, who is responsible for cybersecurity for industrial companies at EY.

**Larger companies are more likely to detect attacks than smaller ones**

Smaller and medium enterprises (SME) in particular often do not have the means or structures to immediately detect attacks. Thus, 64 percent of IT and security managers in large companies (with annual sales of CHF 1 billion or more) consider it likely that they would detect a sophisticated cyber-attack. Of the smaller companies, only 56 percent share this optimism. It also depends on the structures in place: thus, we find that 16 percent of registered attacks were detected by a “security operations centre” which coordinates the cybersecurity of the company. But only 40 percent of smaller companies have set up such a centre, compared to 72 percent of large corporations. “Especially SME’s which do not have the money or the know-
how for internal solutions should evaluate outsourcing their security solutions. Only in this way can they protect themselves reasonably against attacks,” says Roman Haltinner.

**Customer and financial details are particularly sensitive data**

The respondents believe that the greatest security risks are those directly related to operational business: customer details, financial information and strategic plans are the most sensitive data that criminals might gain access to, from the standpoint of IT and security managers. From the respondents’ point of view, the number one security vulnerability lies in their own employees: a third of respondents cite inattentive or careless employees as a gateway for cyber criminals, while one quarter blame outdated security programmes.

“Employees must be trained continuously and be informed about data security,” cybersecurity specialist Tom Schmidt emphasises. “Humans are still the weakest link in the security chain. They fall for phishing attacks or surf on unsafe websites. Companies can minimise this risk by providing training programmes.”

---

**About the global EY organization**

The global EY organization is a leader in assurance, tax, transaction, legal and advisory services. We leverage our experience, knowledge and services to help build trust and confidence in the financial markets and in economies all over the world. We are ideally equipped for this task – with well-trained employees, strong teams, excellent services and outstanding client relations. Our global mission is to drive progress and make a difference by building a better working world – for our people, for our clients and for our communities.

The global EY organization refers to all member firms of Ernst & Young Global Limited (EYG). Each EYG member firm is a separate legal entity and has no liability for another such entity’s acts or omissions. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information, please visit www.ey.com.

EY’s organization is represented in Switzerland by Ernst & Young Ltd, Basel, with ten offices across Switzerland, and in Liechtenstein by Ernst & Young AG, Vaduz. In this publication, “EY” and “we” refer to Ernst & Young Ltd, Basel, a member firm of Ernst & Young Global Limited.