# No longer *if*, but *when*

by

Rudolf Sedmina,
Partner, Management Consulting, KPMG in Slovakia

**Cyber security is not just an IT challenge; it has become a core business challenge. CEOs need to act now to implement a strategic approach to cyber preparedness that will not only protect valuable data, but also enhance the company's agility and better position it for growth down the road.**

We're living in a world in which technological change is taking place at lightning speed, companies are transforming and everything is connected. Organizational leaders are fretting while hackers seem to be able to ghost their way effortlessly into their systems to steal emails and secrets. Over the last few years, we have seen confidence steadily decline as the number of serious cyber-attacks increases. On the positive side, executive boards have been very supportive to IT leaders struggling to keep their gateways secure. However, this heightened state of awareness is not translating into preparedness, which remains stubbornly low.

### Vulnerability is at an all-time high

According to the 2017 Harvey Nash/KPMG CIO Survey, the world's largest survey of IT leadership, cyber security vulnerability is at an all-time high, with a third of IT leaders reporting their organization had been subject to a major cyber-attack in the past 24 months. This represents a 45 percent increase from 2013. Larger companies seem to be more at risk. More than half of such companies have suffered recent attacks. Utilities and government organizations seem to receive the most attention from hackers, followed by the education, telecom and pharmaceutical sectors. Least affected are the charity and advertising sectors, but even here more than one in five reported a major incident in the past two years. Despite these facts, only one in five IT leaders (21 percent) commit to being "very well" positioned to identify and deal with a current or near future cyber attack.

The relative ease with which hackers seem to be able to ghost their way into apparently well-protected systems creates sleepless nights for any IT leader. Despite very visible headline-grabbing attacks such as the recent WannaCry ransomware attack, the biggest jump in threats comes from insider attacks, increasing from 40 percent to 47 percent over the last year.

### Traditional "defense-first" mind set is too limited

The introduction of disruptive technologies and the evolution of customers' expectations mean that the extent of connectivity and the volume of sensitive data accessible about a particular business and its customers are growing at an exponential rate. When you hear the term cyber security there's a very good chance that you immediately think of one thing: an IT infrastructure challenge. Of course, a strong IT security infrastructure is a critical part of any cyber security program. However, it is not the only part. In the reality of the 2017 world, this traditional "defense-first" mindset is too limited. If success today is defined by an organization's ability to absorb a cyber-attack and carry on with business as usual, you need a customized strategy that prioritizes business objectives while protecting critical information. A holistic approach to cyber security is more effective and more realistic than simply building digital walls.

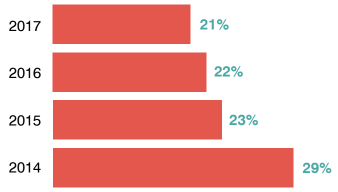
### Two sides of the cyber equation

Most companies have some perception of the risk side of the cyber equation. In other words, if we don't do this and we have a breach, we will lose customers, it will negatively impact our brand, etc. The full costs of a cyber attack are even higher. When you add to "slow-burn" costs (i.e. those associated with the long-term impacts of a cyber attack, such as the loss of competitive advantage and customer churn) also the immediate costs (i.e. legal and forensic investigation fees, and extortion pay outs) it can dramatically increase the final bill.

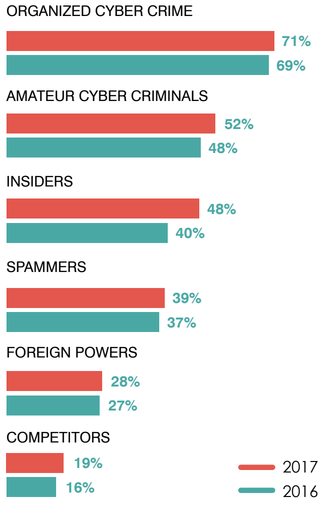
But there is also a positive aspect to this equation. Cyber preparedness can actually better position your company for new opportunities for revenue growth. That should be the message that more CEOs are listening to today. The question shouldn't be "How much of my IT budget are we spending on cyber?" It should be "How much of my business change or innovation budget are we spending on cyber security?"

Cyber security solutions are a core value proposition to customers to drive growth, and a necessity for management teams, board members, and investors to continue making investments in technology-enabled transformations. Without confidence in cyber security solutions from all of these stakeholders, organizations limit their ability to innovate business and operating models, leading to current customer defection and poor growth prospects. Leadership teams should always keep in mind that cyber security is not a one-time project, but rather an adaptive strategy aligned to business goals and focused on delivering long-term value for the business.

**Proportion of IT leaders "very well" prepared to respond to a cyber attack continues to fall**



**IT leaders are struggling the most with organized cyber crime**


ORGANIZED CYBER CRIME
AMATEUR CYBER CRIMINALS
INSIDERS
SPAMMERS
FOREIGN POWERS
COMPETITORS