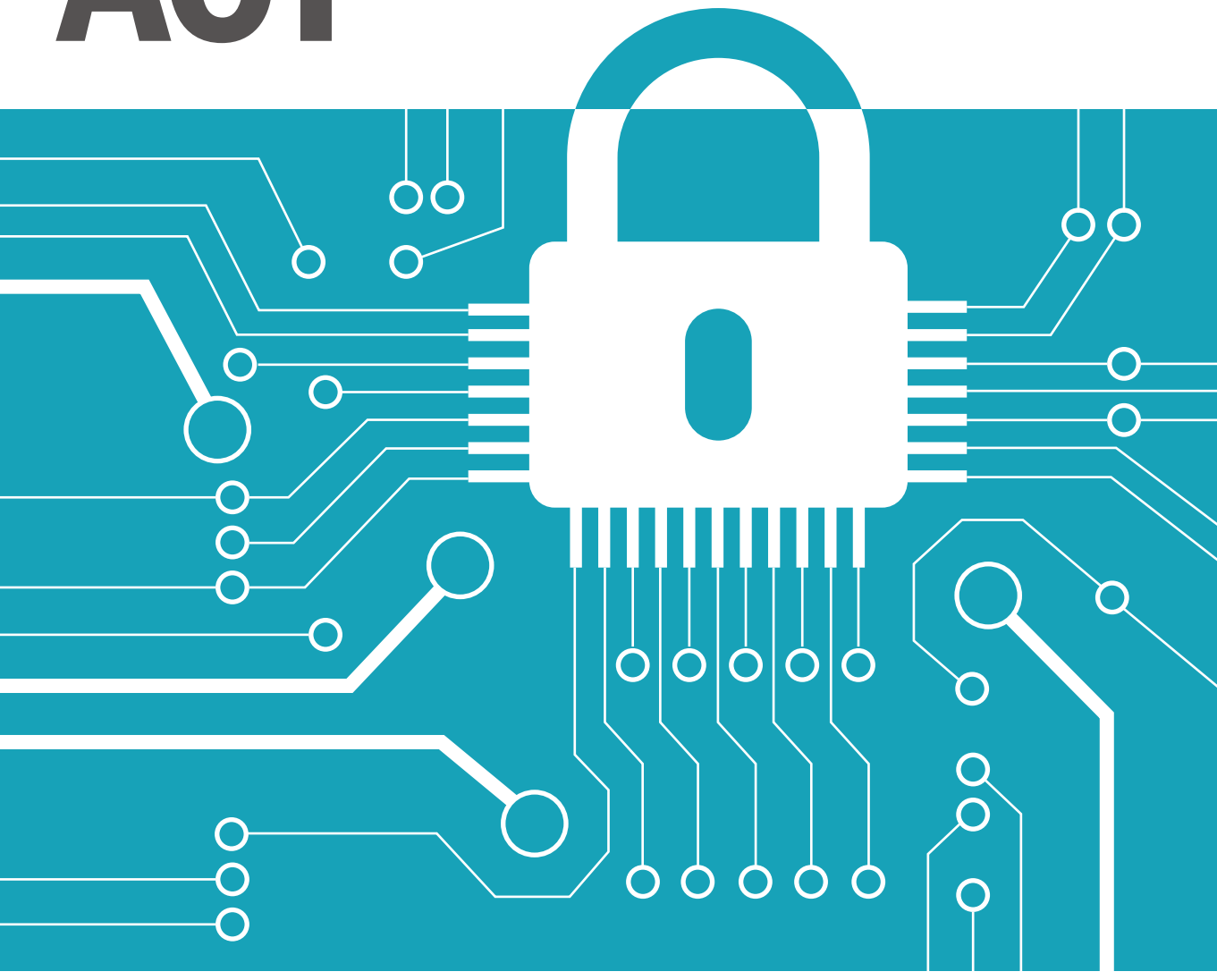
THINK ACT

BEYOND MAINSTREAM



CYBER-SECURITY

Managing threat scenarios in manufacturing companies

MARCH 2015

Roland Berger
Strategy Consultants

THE BIG 3

1 At·tack

The potential damage caused by cyber-crime is astronomical. At one British company, a single attack triggered losses of 950 million euros.
p. 4

2 In·dus·try 4.0

The radical digitization of production – and of products, too – leaves manufacturing companies even more vulnerable to cyber-assaults.
p. 6

3 De·fense

The Roland Berger Cyber-Security Approach places firms under a protective covering by sustainably reinforcing their organization, governance and processes.
p. 12

Summing up: the Roland Berger approach
p. 13

Reappraising cyber-security. Companies in the manufacturing sector are pressing ahead with the digital transformation. If they don't simultaneously realign their security systems and their security culture, they become more vulnerable to attacks.

Cyber-crime is making ever bigger and wider waves in the global economy. Attacks on companies are adding up, as advances in the digitization of production and work processes make their data easier prey. Hackers are training their sights primarily on firms whose business models depend on the availability of digital infrastructures and content.

De facto, all businesses in the manufacturing sector are potentially at risk. Why? Because every branch of the manufacturing industry is being swept along by the digital transformation. Think of the automotive industry, logistics, the various engineering disciplines, energy systems, the consumer goods industry, chemicals and aviation, to name but a few. Across the various sectors, the only real difference is the speed and dynamism with which the technological transition is taking place. Since the digitization of production and products is constantly deepening integration both inside and outside companies, the task of plugging potential gaps to protect data availability, integrity and confidentiality devours ever more of management's time and money.

It is based on these general observations that Roland Berger Strategy Consultants has drawn on its experience of information protection projects with both large corporate groups and medium-sized enterprises to formulate a successful concept in the fight against cyber-crime. The Roland Berger Cyber-Security Approach is a timely response to the constantly growing threat that such attacks pose to increasingly "digital" manufacturing companies. It is rooted in two fundamental strategic insights:

BE PROFOUND. Cyber-security means making sustainable changes to a company's structure to improve safety. First and foremost, that demands management skills, from which the required technical upgrades will necessarily follow. The deployment of hardware and software is only ever a means to an end.

BE PERSISTENT. Cyber-security means finding and establishing long-term solutions – and regularly adjusting them. Managers who believe it is enough to make the right changes once and leave it at that will experience only short-lived success in warding off threats.

The Roland Berger Cyber-Security Approach is a universal model that transcends the boundaries of individual industrial sectors. It can help companies reduce the risk of being spied on, robbed or sabotaged. The approach consists of three core principles and five

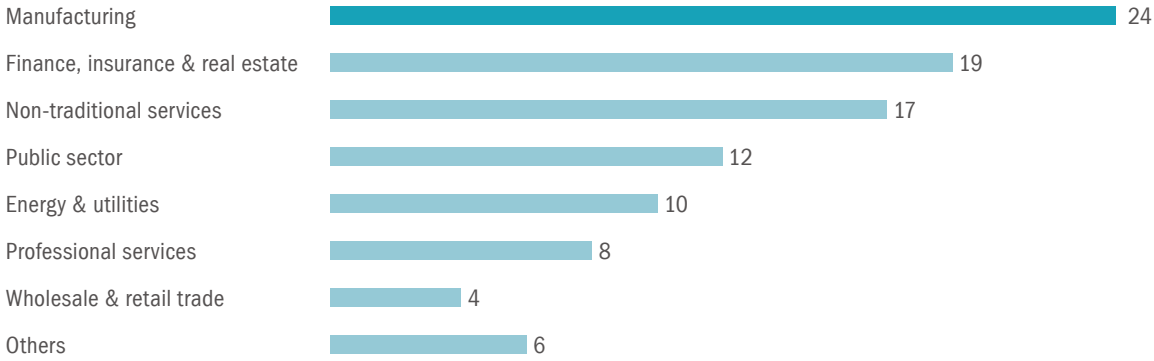
A

1 ASSAULT ON THE ECONOMY

DIMENSIONS OF CYBER-CRIME AT A GLANCE

CYBER-CRIME AFFECTS ALL INDUSTRIES

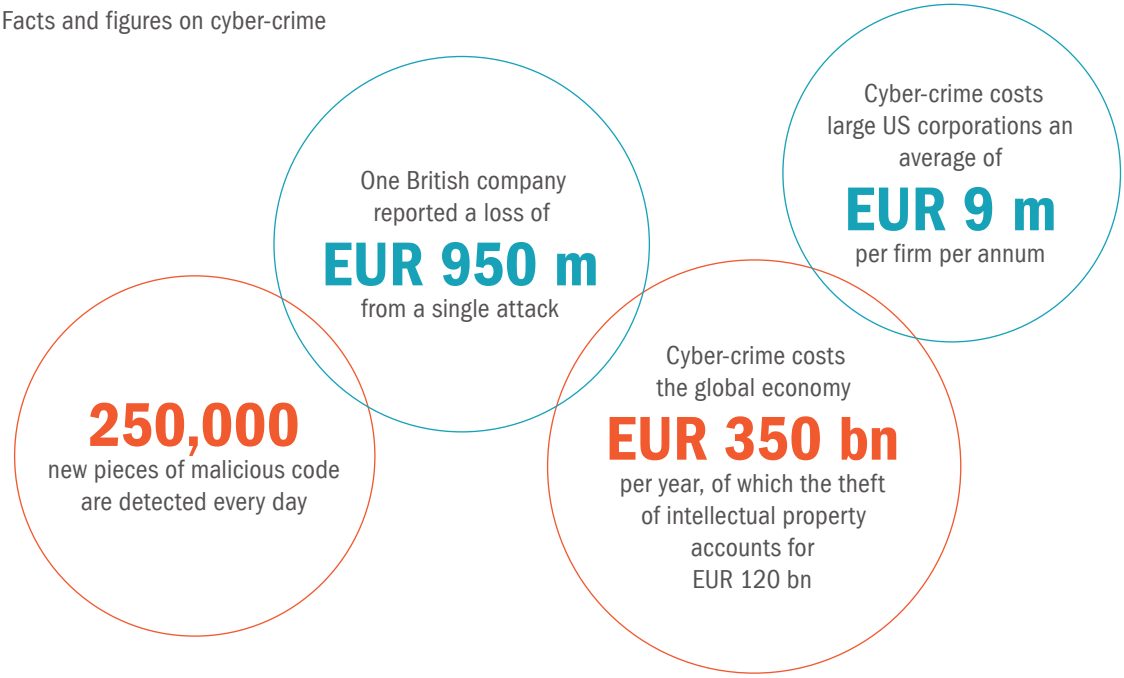
Distribution of cyber-attacks by industry, 2012 [in %]



Source: Symantec

CYBER-ATTACKS ARE NUMEROUS AND CAUSE SIGNIFICANT DAMAGE

Facts and figures on cyber-crime



Source: Center of Strategic and International Studies, Ponemon, McAfee

active success factors. Before we get to the heart of this security program, however, let us first take a closer look at the cyber-environment in which today's companies operate.

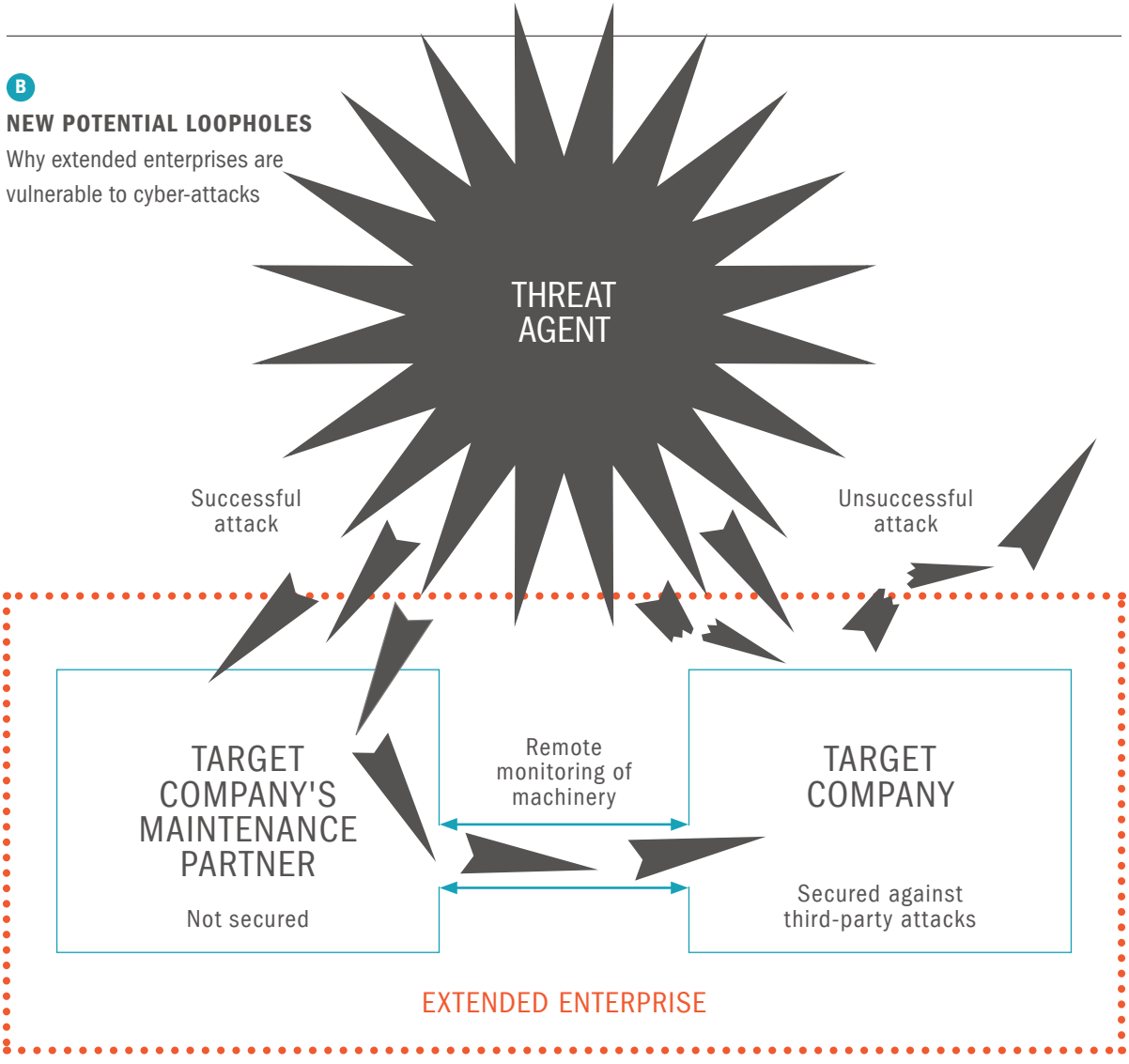
THE ENEMY FROM CYBER-SPACE. The general importance of cyber-security is widely acknowledged. Warnings of growing threats are ubiquitous. One highly regarded publication by US experts Peter Singer and Allan Friedman postulates the following assumption: "97 percent of Fortune 500 companies have been hacked [...] and likely the other 3 percent have too, they just don't know it." Recent analyses and studies reveal further worrying findings. A

All manufacturing companies are potentially exposed to the risk of cyber-attacks, because the root cause of every threat is a new form of dependency. Entire industry value chains increasingly rely on complex and often interconnected digital assets, as well as the constant exchange of data, information and knowledge. Businesses store and share research findings in digital form, use computer-aided processes to develop products and manage their production and service networks online. Yet the associated data and communication streams can only be controlled to a certain extent. Their transparency, too, is limited.

B

NEW POTENTIAL LOOPHOLES

Why extended enterprises are vulnerable to cyber-attacks



2 INDUSTRY 4.0: OPPORTUNITIES AND RISKS. The concept of Industry 4.0 is driving the most rigorous advances in this kind of end-to-end connectedness at manufacturing companies. Industry 4.0 subsumes the industrial-scale use of digital technologies focused on manufacturing processes, the emergence of cyber-physical systems and the interconnection of productive units – which can be inside and/or outside the company – in production or monitoring. This constellation forges networks that speed up production, foster a high level of self-organization and thus facilitate the more efficient and flexible deployment of production resources. In effect, the core company swells to become an extended enterprise. There is no doubting the benefits this smart networking gives to firms up and down the value chain. The downside is that it leaves them more vulnerable to digital attacks as the number of touchpoints with the outside world increases. B

THE DIGITIZATION OF PRODUCTS. The threat to enterprises has long since also become a threat to their products, which themselves are increasingly smart and connected. The spectrum ranges from intelligent thermostats that control heating systems to automatic parking assist and cruise control systems in vehicles to entertainment electronics in long-haul aircraft. Cyber-security is even becoming a condition of purchase: Customers expect manufacturers to assume responsibility for the security of their products, and to do everything in their power to safeguard both functionality and personal data.

KNOWLEDGE AND CUSTOMER DATA AT RISK. Past attacks make one thing clear: While the threat is greatest for manufacturing firms with high-quality technological products and systems, the risk also extends to other firms with supposedly less sensitive goods and services. That is because they, too, use huge quantities of the most critical raw material in the digital era: data. In 2014, for example, an attack on an American e-commerce group caused a stir when confidential user information was hacked. An international film group likewise fell victim to a spectacular attack. C Only a fraction of all attacks appear in the media and come to public attention – fortunately for the companies affected, as this gives them time to plug security loopholes, and keep them plugged.

Cyber-attacks are by nature highly dynamic events that often catch companies unprepared. In an exclusive interview with Roland Berger, former Microsoft security expert Katie Moussouris points out that, despite the increase in digital raids, many companies still appear to be fairly unconcerned. D

In the fight against cyber-crime, responsible companies must tread new paths and dare to adopt new approaches. If they are not to fall behind potential hackers in the technological "arms race", it is crucial for firms to perform regular critical reviews of their own security solutions and to continually improve and develop them. Networks and partnerships – including those that transcend the boundaries of given industries – can help enterprises to quickly spot emerging threat scenarios and join forces to develop effective countermeasures.

Irrespective of how mature their cyber-security solutions are, companies must remain alert and ready to act if they are not to be caught off-guard by the pace of constantly changing threat scenarios.

A REALISTIC VIEW. On this vital issue for the corporate community, there is no shortage of prophets of doom. Yet heeding their warnings can can cause companies to skew their priorities and distort their perception of what is needed. Focusing on theoretically conceivable global disasters (how often do we hear people talking of "Cybergeddon", global cyber-shocks and digital catastrophes?) leads in the wrong direction. Companies may be tempted to do nothing at all, assuming that they cannot protect themselves anyway. Alternatively, they may do completely the opposite and overdo their security systems in response to the anticipation of maximum threat.

Somewhere in the middle, between these two extremes, lies a strategically well-planned yet pragmatic corporate security policy. It is important for managers to base their actions on the understanding that security serves the business, not vice versa. They also need to be aware that security risks can only arise in the first place if there are vulnerabilities in the company's security architecture. Hackers depend on precisely these

C

THE TIP OF THE ICEBERG

Well-publicized major cyber-attacks on companies

2010

MALWARE: Stuxnet

TARGET
Iran

AGGRESSOR
Unknown (secret services are suspected)

BACKGROUND

Stuxnet is a computer worm that infects industrial programmable logic controllers (PLCs).

Stuxnet infiltrated Iranian nuclear facilities via USB sticks.

The attack destroyed a sixth of Iran's capacity to enrich uranium.

2012

MALWARE: Flame

TARGET
Middle East, especially Iran

AGGRESSOR
Unknown (secret services are suspected)

BACKGROUND

Flame is a complex form of malware for audio recording, screen monitoring, the capture of keyboard input and network activities.

It spreads via USB sticks or the local network.

MALWARE: Shamoon

TARGET
Saudi Arabian oil company

AGGRESSOR
Hacker group "Swords of Justice"

BACKGROUND

The attack sought to interrupt oil production.

Although major production outages were averted, it took about a week to recover the 30,000 systems that were affected.

2013

MALWARE: Red October

TARGET
Unknown

AGGRESSOR
Unknown (Russian-language malware)

BACKGROUND

This malware propagated itself via e-mail attachments.

It aimed to steal data from computers, smartphones and network storage devices.

2014

MALWARE: Uroburos

TARGET
Unknown

AGGRESSOR
Unknown (secret services are suspected)

BACKGROUND

To this day, it has been impossible to ascertain how Uroburos infiltrates systems.

The malware has been in circulation since 2011 but was not detected until three years later.

MALWARE: Regin

TARGET
Private individuals and companies; mainly telecom companies in Russia and Saudi Arabia

AGGRESSOR
Unknown (secret services are suspected)

BACKGROUND

The Regin malware targeted both companies and government institutions (the EU Commission).

A modular malware concept allowed functionality to be added retroactively.

A virtual file system makes Regin hard to detect.

MALWARE: No name

TARGET
E-commerce group

AGGRESSOR
Hacker group "Syrian Electronic Army"

BACKGROUND

More than 200 million users' personal data was stolen.

The data stolen included user names, passwords, telephone numbers and addresses.

When the attack became known, the targeted company's stock price collapsed.

MALWARE: No name

TARGET
Film corporation

AGGRESSOR
Unknown (speculation points to an attack from North Korea or a company insider)

BACKGROUND

Hundreds of gigabytes of confidential e-mails and documents were stolen from company servers, including unpublished films and film scripts.

Parts of the company's computer networks were paralyzed.

The launch of a comedy film about North Korea was initially canceled as the hackers threatened terror attacks.

D

"TAKING ABNORMAL ATTACKS INTO ACCOUNT"

Katie Moussouris, former security expert at Microsoft, comments on uncritical companies, the Internet as a gateway and the responsibility of CEOs

Everyone will remember the hack on a film corporation which took cyber-threats into a new dimension in 2014. Cyber-attacks can evidently endanger a company's very existence. How can this be? Are companies still too naive?

KATIE MOUSSOURIS: The hack you just mentioned is one famous example, but this could happen to anyone. No software or company is ever 100% secure, no matter how mature their security model. It is wise for an organization to be proactive and to have good processes in place in case something happens, because the likelihood that threats will become actual attacks is increasing. It is necessary that we are aware and prepared to respond in these situations.

More and more companies are increasingly digitizing their value chains and products, which leaves them less resistant to attacks. How high and sophisticated is the general level of security awareness in these companies?

A considerable lack of concern still prevails. Threats affect every industry and every company, yet every user can also potentially be a high-value target for very different reasons. Therefore, it is important to know your particular assets, e.g. intellectual property, customer data, company secrets, employee data, competitive advantages, etc., to be able to protect these assets specifically. Furthermore, access controls need to be in place. Every individual and every organizational entity needs to understand that so-called abnormal behavior occurs in digitized processes. And when it occurs they need to detect it quickly and respond actively to it. This is what we call effective risk management: Know what is valuable and manage your risks properly.

What is the attackers' business model?

No uniform business model exists. Specific companies do attract specific attackers, and understanding what motivates these attackers is important. For example, criminals typically want money, while hacktivists often have political goals. As some have speculated in the case of the international film corporation, it could also be an unhappy insider. The hack on a popular gaming device over Christmas, however, was a group of kids who simply wanted to have fun. Sometimes attackers are powerful but irrational enemies we have to face.

What are the most obvious vulnerabilities at companies that are in the process of digitizing their businesses?

The largest gateway is, without a doubt, the Internet. It was not built with security in mind. It has been developed for more and more users over time and we added components that have lots of bugs and vulnerabilities, like building a castle in the sand. With the growing complexity of and dependence on the Internet, we built a global economy around it. We need to improve technology to become resistant to attacks. We cannot expect the technology to be perfect; that will never happen. So what we need to do is to get better at dealing with the technology.

How can companies become more alert and safer?

Companies often look at the functionality of systems, but not at implementing good security standards in these products. Therefore, my first piece of advice is to set up a secure development lifecycle and to integrate it into the governance that affects suppliers as well as your own organizational entities. Especially the IT procurement office needs to regard this as a standard for all IT-related purchases, so the pressure on all market participants is increased. Once there is a standard, there is a request for compliance, which is always the bare minimum. Awareness, risk assessment and detection are the steps to follow thereafter.

What further steps do you recommend?

Secondly, I advise companies to adopt the new ISO standards that regulate vulnerability disclosures (ISO 29147) and vulnerability handling in processes (ISO 30111). It is surprising that most organizations do not even have an easy way to report vulnerabilities discovered by a hacker – let alone organizational processes to deal with issues once they are reported.

Thirdly, CEOs need to consider that digitization needs attention to mitigate all kinds of risks. These risks could impact the whole organization and they need to be aware of them in the first place before they can protect themselves. It is wise to designate someone who is equipped with sufficient authority and resources to deal with the security issues of digital business. This can be a Chief Security Officer, Chief Technology Officer, Chief Information Officer or a Chief Risk Officer. This too would be an enormous step towards digital maturity.

***Katie Moussouris** is the Chief Policy Officer for HackerOne, a platform provider for coordinated vulnerability response and structured bounty programs. Previously, she worked as a leading senior security strategist at Microsoft. The interview was conducted at the Hamburg Cyber Security Conference BSidesHH & 31C3 at the end of December 2014.*

vulnerabilities for their attacks to succeed. The Roland Berger Cyber-Security Approach helps managers to identify and close these gaps. The figure below E outlines some of the players involved in and the forms taken by cyber-attacks in practice.

Clearly, cyber-security is a complex, multidimensional topic for today's businesses. The list of potential enemies is a long one: Assaults can be launched by industrial spies, secret service agents, criminals, political activists and even internal employees. The spying methods, too, are growing ever more sophisticated. Any and all sensitive company assets, i.e. data, information and intellectual property in the widest sense, are considered fair game for attacks.

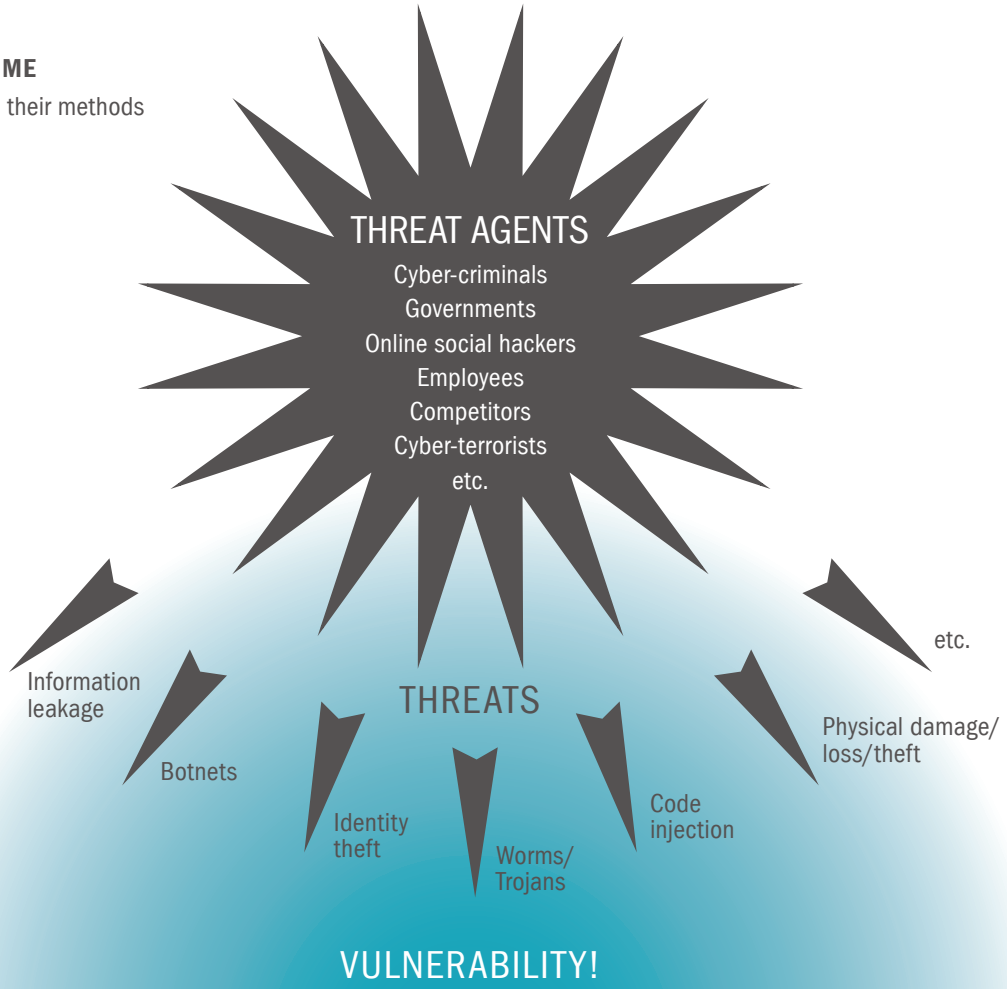
The digitization of value chains, touchpoints with customers and interfaces to suppliers means that companies' protective measures must extend far beyond their own premises. For manufacturing firms of all shapes and sizes, working in extended enterprise constellations has become common practice. Increasingly, it is also the digital products and services they sell that expose companies' innovations and knowledge to vulnerable environments. Product security – protecting the value that products represent to the company, but also protecting customers from attacks while they use these products – is a further aspect of cyber-security that often commands too little attention.

Seeing the big picture and covering the entire lifecycle from the earliest phases of product development through its sale and operation and, where appropriate, to its scrapping, is thus an integral part of the challenge.

E

CYBER-CRIME

Hackers and their methods



Rethinking cyber-security. Complexity is growing as security risks spill over into new areas. Management must redefine processes and spheres of responsibility. The three core principles of the Roland Berger approach.

PRINCIPLE
1

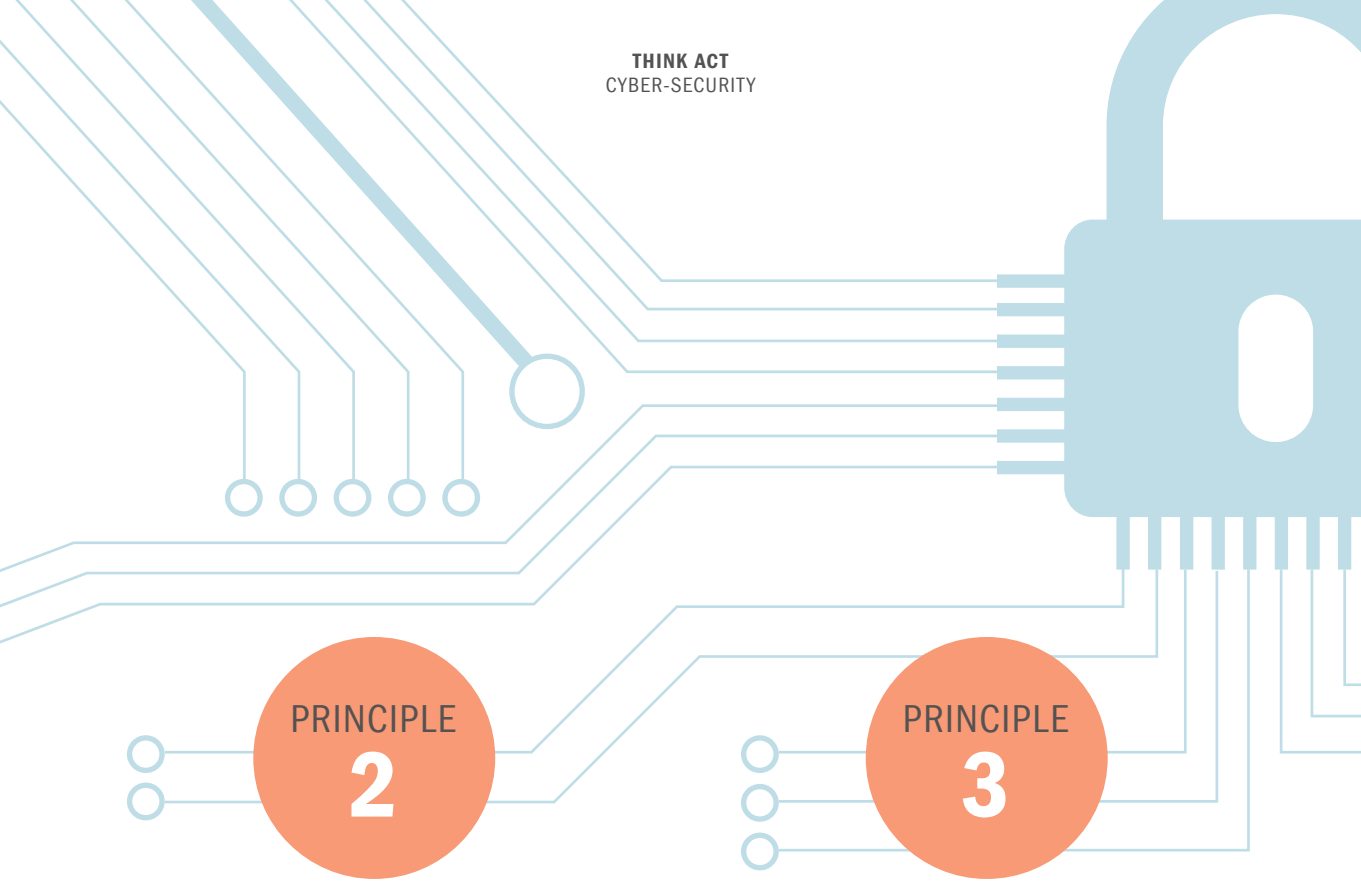
Management defines spheres of responsibility

The challenges associated with hack attacks and data theft go beyond the job description of traditional IT departments. Threat scenarios are complex because attacks can be launched against any conceivable link in the value chain, thereby affecting widely differing parts and levels of the company. It is time for managers to face up to this complexity and sharpen their focus on cyber-security. Three principles are pivotal to their response:

As digitization penetrates more and more products, companies and value chains, the need to protect digital assets has risen dramatically in many areas. Connectedness is spreading and now embraces every area of the company, from procurement and logistics to production, sales and service.

This has far-reaching implications for the architecture of the security organization. In many companies, IT – or a special IT security department – is still responsible for cyber-security. Yet focusing on conventional IT systems is not enough to deal with the demands of an ever more connected corporate environment. Vulnerabilities can often be found in product development, production and service units, for example, all of which are beyond the reach of traditional IT security.

It follows that one of top management's central responsibilities must be to organize end-to-end responsibility for cyber-security. Adopting a transversal approach across all areas of the company is the only way to ensure that products and the whole enterprise receive optimal protection.



PRINCIPLE
2

New security systems build on existing capabilities

For every firm, the battle against cyber-crime is a long-term undertaking. It means (constantly) evolving existing approaches and solutions. It cannot be about developing revolutionary new approaches for the company from a standing start. What sets the pioneers in corporate cyber-security apart is that they take existing fields of responsibility, structures, processes and systems as their point of departure, develop and improve them, and piece them together to form new end-to-end solutions.

Evolutionary development requires vigilance and agility. When threat scenarios change, firms must adapt their security systems accordingly. In a complex, high-risk environment, no one can afford to stand still. At the same time, it is equally dangerous to overdo the security management. Yes, companies must prepare themselves for new threats and make existing processes safer. In doing so, however, they must not lose sight of or even contradict their business model. Achieving greater security must always remain a means to an end.

PRINCIPLE
3

Cyber-security becomes an integral part of the corporate culture

Cyber-security affects the entire enterprise. It is a common theme across all divisions and functions. It is not enough for management and security units alone to tackle the subject. Every employee in the whole company must play a part in implementing a new security architecture.

The smallest contribution can be keeping an eye on processes in the company with a keener understanding of the need to protect internal data and a sharper awareness of security risks. Technical solutions alone can never guarantee no-gaps protection. The level of security at any given company is also determined by the level of vigilance among its people.

Specific training and campaigns that tie up comparatively few resources can drive an immediate and lasting effect, as more conscious action during everyday routines prevents vulnerabilities from arising in the first place.

3 **Reimplementing cyber-security.** Companies must establish a system that lets them control their security level continuously, flexibly and proactively. The five areas of action in the Roland Berger approach.

Five specific areas of action can be distilled from the three fundamental principles described above. Together, they add up to the Roland Berger Cyber-Security Approach. F These five steps help companies to very quickly identify and assess risks and then define appropriate solution paths. Development of an auxiliary cyber-security management system – part of the fifth and final step – ensures that defined solutions firmly take root in the company's DNA.

STEP 1
Establish the scope and define the priorities

BACKGROUND. Given the multiplicity and diversity of threat situations, the strategic importance of information and data and the potential damage that can be done, cyber-security is a job for the company's strategists and top managers. Simply put, there is no such thing as watertight security. This being the case, clearly defined priorities are essential, and they can only be prescribed by top management. To do so, management must first find out precisely what – data, knowledge, process and design expertise, and so on – needs protecting for which (operational) reasons.

PROCEDURE. The first test of how much protection certain data and goods require involves measuring three elementary dimensions: strategic relevance, business relevance and ability to influence. The digital assets that achieve priority status based on this preliminary test must then be screened a second time, with management this time seeking to identify and evaluate the company's "crown jewels": information and assets that it is vital to protect.

ACTIONS. Assets that are worth protecting often have to be evaluated from the top down on the basis of simple but clear and intuitive criteria. Depending on the precise procedure, business lines, product lines and even (cross-divisional) processes are screened to determine how relevant they are to the company's cyber-security. During this analysis, it is equally important to clearly identify areas for action so that the ground is thoroughly prepared for future operational measures.

STEP 2
Understand your threat exposure

BACKGROUND. A risk only exists when a threat scenario (the combination of a threat agent and a threat) coincides with an unprotected vulnerability. Without a

F

THE ROLAND BERGER CYBER-SECURITY APPROACH

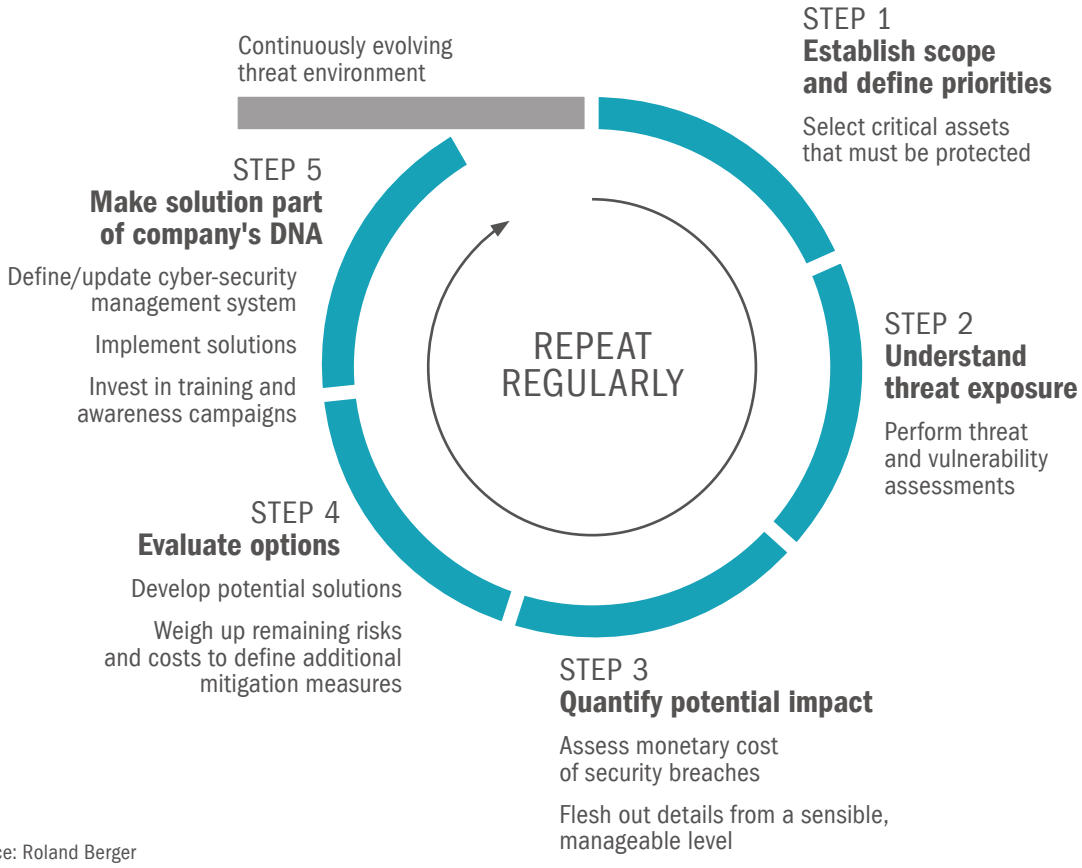
THREE BASIC PRINCIPLES

1 **Management defines spheres of responsibility**

2 **New security systems build on existing capa-bilities**

3 **Cyber-security becomes an integral part of the corporate culture**

FIVE CONCRETE STEPS



Source: Roland Berger

threat scenario, there can be no risk. Without vulnerability, the same applies. It is only a combination of the two that makes an issue important and creates the need to do something to protect the company. G Having said that, assessing the threat situation is a complex challenge, mainly because each company must be assessed individually. Off-the-peg statistics give you an idea of where to look, but actual analysis must always be tailored to the specific company.

PROCEDURE. A threat and vulnerability assessment must be performed for the identified areas of action. In other words, threat scenarios and the current level of protection must be determined for high-priority digital assets (which can be products, processes or valuable information, for example). Threat vectors – combinations of threats and vulnerabilities – never stand still. Since they are subject to rapid change, any thorough analysis will also include a time-specific component.

ACTIONS. Analyzing threats and vulnerabilities demands a carefully harmonized toolset, because an efficient and, ultimately, comparable procedure must be guaranteed at all times. Cyber-security specialists should be involved from start to finish. Internal experts are naturally needed for the various areas of action. However, experience also shows the value of calling in external specialists. Their imaginative capabilities (in identifying potential threat agents) and technical knowledge (using penetration tests to detect vulnerabilities, for instance) can complement and enrich the firm's own capabilities.

STEP 3
Quantify the potential impact

BACKGROUND. Decision-makers need to see the big picture if they are to know how to deal with an identified threat scenario. This is because any well-reasoned decision to establish protective measures can only be made once the company can put a number on the potential damage. That is often difficult to do for cyber-attacks, especially where human life and/or the company's reputation is at risk. This is the hurdle at which many activities fall: Because cyber-risks can almost never be condensed into a single (potential) loss figure, many managers make the mistake of not bothering with the subject at all.

PROCEDURE. Although quantification is complex, is based on scenarios and assumptions and can never lay claim to absolute mathematical accuracy, it is nevertheless indispensable. One key aspect of good management is the ability to make decisions under uncertain circumstances. Risk assessment is not built on the semblance of stochastic precision provided by calculating to so many decimal places. Rather, it is rooted in the well-founded estimates of proven experts, and in thorough consideration and analysis of the various threat vectors and their possible consequences for the company.

ACTIONS. It is absolutely critical to involve and elicit the support of top management in the transparent assessment of quantitative risks. Only then can business cases be put together for alternative courses of action. This process can often receive valuable technical support from the enterprise risk management unit. If it is to prove successful, however, it also requires management's willingness to act and make decisions ("to deal with the unknown or the unknown unknowns").

STEP 4
Evaluate your options

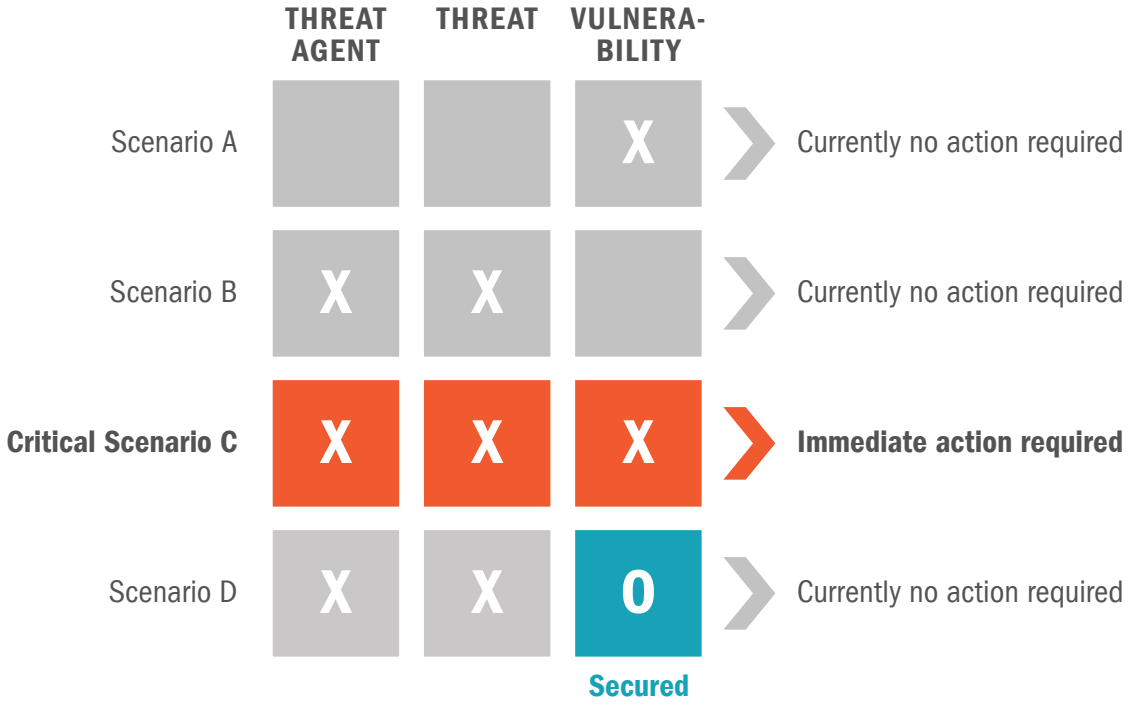
BACKGROUND. Assessing what constitutes an "acceptable" risk is an important task that management must understand and give its backing to. This means determining the maximum notional risk – the combination of the probability of an event and its possible impact – that a company can cope with. Also, to ensure that scenarios that are very unlikely but carry very considerable loss potential do not get overlooked, it is important to complement the maximum global risk by defining a ceiling for (actual) single loss events.

PROCEDURE. In line with the basic principle that there is no such thing as 100% security, acceptable risk tolerance levels must be defined. The possible courses of action needed to achieve these levels must likewise be mapped out. Tolerance ranges can be de-

G

THREAT SITUATIONS AND RESPONSES

When companies have to take action



fined for concrete threat scenarios, although a clear economic focus must be ensured – in accordance with previous quantification exercises – to guarantee reasonable objectivity.

ACTIONS. Selection is based on a routine cost/benefit analysis. As with all quantified risks, those courses of action whose benefits outweigh the costs should be pursued. The actions themselves range from focused security concepts for clearly delimited vulnerabilities to enterprise-wide technical solutions for network, operational, data, application and physical security. Alongside the implementation of measures and action packages, it is also necessary to align both the formal aspects (spheres of responsibility, structures, processes, systems) and the informal ones (codes of conduct, cultural changes) within the company. This fifth and, ultimately, mission-critical factor is described below.

STEP 5
Make solutions part of the company's DNA

BACKGROUND. Once the first four steps of the Roland Berger Cyber-Security Approach have been completed and the resultant actions implemented, management has a full and clear picture of the current threat situation, the associated financial risks and possible courses of action to reduce risks. The fifth and final step is crucial to ensure that protection against threats remains equally strong in the long run. It involves firmly establishing all cyber-security activities as an ongoing part of the organization. Company assets and threat scenarios are subject to constant change. Assets that are deemed essential today may see their importance wane in the future. Similarly, new threat scenarios may emerge, while existing ones may

change or even disappear. The only way for a company to sustainably improve its level of protection against digital threats is for cyber-security to become an integral part of its processes and part of the company's DNA.

PROCEDURE. These advances can in turn only be realized if cyber-security itself is anchored in the management system. That takes time. Establishing the four critical steps described above as regular activities is a protracted but vital process. Examples of successful integration include grafting cyber-security requirements into development and procurement processes, as well as the regular revision of maintenance routines for industrial plant. Some changes also affect the very core of the organization, because they concern attitudes and the way people think – the corporate culture, essentially. Broadly speaking, the rebuilding and revectoring of cyber-security management can begin on the following levels:

Organization – In keeping with Roland Berger's principles for successful cyber-security strategies, every part of the company for which cyber-security is a relevant issue must be involved in defining who is responsible for what – starting with development, production and IT in all cases. Creating a clearly defined cross-divisional field of responsibility is imperative if all potential vulnerabilities are to be fully covered. It is also advisable to set up an enterprise-wide cyber-security network. Working together with full-time cyber-security experts, permanent contact persons or "focal points" in the departments usually devote part of their time to the same task to ensure that risks are spotted quickly and defined measures are implemented promptly. Establishing this kind of network across focal points and experts encourages relevant dialog and helps keep cyber-security on people's radar throughout the organization.

Processes – Organizational routines shape the DNA of every company. That's why it is essential to screen all processes and measure their importance to the fight against digital threats. Logically, therefore, the same goes for the methods and tools that are linked to these processes. Generally speaking, there are two ways to integrate cyber-security in processes, methods and tools: One is to incorporate the appropriate cyber-security requirements in existing process descriptions, for example by introducing a security-by-design concept in the product development phase. Alternatively, these requirements can be compiled in several central reference documents. To emphasize the importance of the topic, it is also wise to draw up a fundamental cyber-security policy that is ratified by the company's top management. Formal process integration must then be flanked by communication and training activities.

Governance – Introducing an end-to-end communication and reporting system and a transparent system of key performance indicators (KPIs) ensures that the different levels of management are regularly informed about cyber-security topics and – if necessary – able to take action. In the process of integration, existing management structures and bodies can be used to keep the extra burden on the decision-makers involved to a minimum.

ACTIONS. Depending on the size of the company, the complexity of the threat situation and the level of risk, it makes sense either to set up a dedicated cyber-security management system with its own committees, processes and organizations, or to integrate this system in existing structures. Either alternative has advantages and drawbacks. The ability to focus attention on one topic and the neutrality of the people involved are two of the main arguments for a dedicated cyber-security management system. On the downside, this approach drives up costs and runs the risk of undermining acceptance among managers and throughout the company. The benefits and disadvantages are exactly the opposite with the integrated approach. Irrespective of the system adopted, however, we advise clients to have the degree of implementation regularly reviewed by internal and external auditors.

At the end of the day, if companies want to substantially improve the quality of their cyber-security, they need to take a critical look at their structures, their processes and their culture. A checklist is a good way to start identifying where change is needed and to what extent. H

Reprioritizing cyber-security. Major stakeholders will no longer tolerate failure to guard against digital threats. Step by step, customers, governments, rating agencies and insurers are all raising the bar.

Many companies still hesitate to track down and close the security loopholes in their own organization and their own products. Some assume they will not be targeted by attackers simply because it has never happened before. Others hope they will quickly be able to deal with any intruders and plug any gaps that arise.

Neither approach is sensible, because neither constitutes a lasting answer to existing threat situations. Firms run the risk of misreading reality on three counts: First, their assessment of the losses that are theoretically possible in their domain is incorrect. Cyber-criminals are becoming more professional all the time. Second, management is often unaware that it is directly accountable for cyber-security. Management's general responsible to safeguard the interests of its employees, business partners and consumers unreservedly includes optimizing the protection it provides against digital threats. Third, companies close their eyes to the fact that important stakeholders are significantly stepping up their demand for security. Increasingly, they are calling on firms to take carefully planned preventive action. Here are just some of the new demands being asserted by today's stakeholders:

CUSTOMERS. For some years, customers have been becoming noticeably more sensitive to cyber-security issues across all branches of industry and all product groups. For commercial and private customers alike, data and information protection are becoming increasingly important as a purchase criterion. In many cases, we are seeing that cyber-security is regarded not as an optional add-on, but as a minimum requirement. Market players who fail to meet this requirement do not even make it onto the short list for purchase decisions. A few providers have recognized this requirement and are starting to step up their cyber-security capabilities – and to specifically advertise this fact.

GOVERNMENTS. A growing number of governments are taking up the fight against cyber-crime, even though most of them are "going it alone" and there is as yet no harmonized international strategy. Most of the laws and initiatives that are ratified and launched effectively place companies in various industries under obligation to protect their systems and data. Some oblige them to comply with new, stricter security standards. At the same time, more and more countries are forcing firms to disclose information about IT attacks.

RATING AGENCIES. IT outages, for example, constitute an operating risk for a company. This being the case, assessments of creditworthiness increasingly also require proof of an effective security architecture. This is especially true for companies that depend on the smooth, seamless operation of a complex interna-

H

THE CYBER-SECURITY CHECK

Five key questions to help a company identify what needs to be done

1. Does your company have cyber-security guidelines that cover production/product risks and the extended enterprise in addition to traditional IT security?
2. Have you cataloged your assets (products and production plant), and do you know the gateways for potential cyber-attacks on these assets?
3. Do you know which of your assets are the "crown jewels" – those assets that are critical in the event of an attack on your company?
4. Are the measures currently in place sufficient to guard the company against potential losses (i.e. is the business case positive)?
5. Has your company defined cascading spheres of responsibility for cyber-security, and are employees on all levels aware of the risks?

tional supply chain. In such constellations, even comparatively brief system outages or minor data losses can cause serious damage. Accordingly, companies whose "security grades" deteriorate may well find it more difficult to source funding on the global financial markets – and, in extreme cases, see their very survival at risk.

INSURANCE COMPANIES. More and more insurance companies are selling policies that cover cyber-risks. As a result, insurers are accumulating greater expertise in the analysis and assessment of companies' information protection systems. This will have a knock-on effect on other commercial insurance policies that already cover selected data theft and online crime risks. All in all, more is being expected of corporate cyber-protection systems.

In part, the cyber-security approach developed by Roland Berger also responds to the growing demands of these stakeholders in the corporate environment. It seeks to provide companies with fresh stimulus and ideas for a strategic approach to the protection of their data, information and communication technology. We want firms to be armed and ready for the pitched battle against cyber-crime. And we want them to win it! ◆

ABOUT US

Roland Berger Strategy Consultants

Roland Berger Strategy Consultants, founded in 1967, is the only leading global consultancy of German heritage and European origin. With 2,400 employees working from 36 countries, we have successful operations in all major international markets. Our 50 offices are located in the key global business hubs. The consultancy is an independent partnership owned exclusively by 220 Partners. **WWW.ROLANDBERGER.COM**

Further reading

COO INSIGHTS
All about digitization of manufacturing

Our research across Europe shows that digital production has already begun to revolutionize value chains at many companies. Based on talks with management and associations, we compiled this COO Insights issue on Industry 4.0 and its many facets. Speaking in an exclusive interview, Harald Krüger, the BMW Group's Chief Production Officer and future CEO, is clearly optimistic about what human-machine interaction will bring to automobile production.

INDUSTRY 4.0
How Europe will succeed

The declining competitiveness of manufacturing companies in Europe, especially in the face of new market players from Asia, is jeopardizing the European model. The digitization of the industry now offers the opportunity to regain lost ground.

THE EUROPEAN A&D INDUSTRY

The Aerospace & Defense Industry in Europe is undoubtedly a success story, leaning against the de-industrialization trend we have been experiencing for years. However, despite its strong growth, the industry is not immune to challenges faced by industry in general: a decline in profitability, rise of new competitors and an insufficient level of investments. Building on its success, it must address the evolution of its industrial model and investment input, while European governments have a bigger role to play in bolstering A&D integration.

Tablet version

DOWNLOAD OUR KIOSK APP

To read our latest editions on your tablet, search for "Roland Berger" in the iTunes App Store or at Google Play. Download the Kiosk App for free.

Links & likes

ORDER AND DOWNLOAD
www.think-act.com

STAY TUNED
www.twitter.com/RolandBerger

LIKE AND SHARE
www.facebook.com/RolandBergerStrategyConsultants

Publisher

ROLAND BERGER
STRATEGY CONSULTANTS GMBH
Sederanger 1
80538 Munich
Germany
+49 89 9230-0
www.rolandberger.com

Editor

DIRK HORSTKÖTTER

Contributors

HENNING BRAUSER
FREDERIK HAMMERMEISTER
GERRIT SCHMIDT
CAROLINE KROHN

The authors welcome your questions, comments and suggestions

MANFRED HADER
Senior Partner
+49 40 37631-4327
manfred.hader@rolandberger.com

CARSTEN ROSSBACH
Senior Partner
+49 69 29924-6318
carsten.rossbach@rolandberger.com

TA_14_025_TAB_01