McKinsey&Company

Digital and Risk
A new posture for cyberrisk in a networked world

Leading in a disruptive world

March 2018

#3

A new posture for cyberrisk in a networked world

By Thomas Poppensieker, Wolf Richter, Rolf Riemenschnitter, Gundbert Scherf

WHY IT MATTERS

How secure is our organization? What is our value at risk? How do we compare to our peers? Are we investing enough in cybersecurity? How should we allocate our resources? How can we structure our organization to optimize protection? How should we track progress? These are the kinds of questions we hear from top managers when we talk to them about cyberrisk. Even after years of extensive press coverage and constant online buzz, there is still widespread uncertainty about what to do. So let's take a sober look at the current threat level, establish a line of defense, and examine the answers some of the world's leading companies have found to the questions above.

The threat is growing – as much in intensity as in numbers

The US government has identified cybersecurity as "one of the most serious economic and national security challenges we face as a nation."[1] Worldwide, the threat from cyber-attacks is growing both in numbers and intensity (Exhibit 1).

Traditionally, financial and military institutions were the primary targets of cyberattacks. Today, with connectivity permeating all major industries, all companies are affected. Recent examples include:

- Attacks on energy companies in the US, Canada, and Europe by the cyberespionage group Dragonfly, revealing significant potential for sabotage[2]

- WannaCry ransomware attacks on the public sector and on private companies in industries such as telecommunications and logistics[3]

1 www.mckinsey.com/business-functions/digital-mckinsey/our-insights/meeting-the-cybersecurity-challenge (retrieved September 2017)

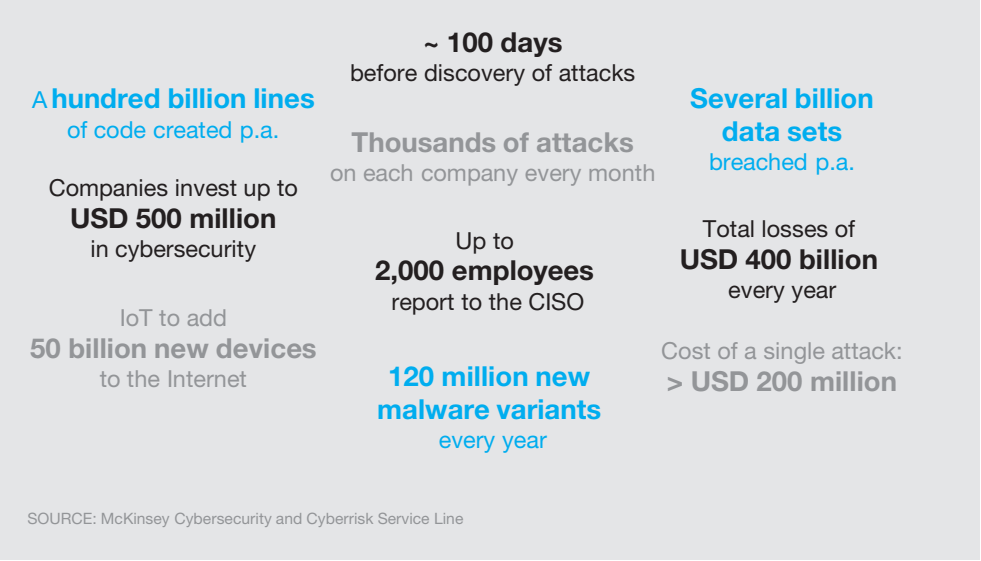
2 www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted- sophisticated-attack-group (retrieved September 2017)

3 www.natlawreview.com/article/wannacry-are-your-security-tools-to-date (retrieved September 2017)

- NotPetya ransomware attacks on major European companies from a wide variety of industries.[4]

These examples show that business continuity and crisis management are crucial aspects of cybersecurity, irrespective of the industry you are in. Paradoxically, most of the companies that fell prey to the likes of WannaCry and NotPetya would probably have said that they were well protected at the time of the attacks. Even if your company is not a primary target, there is an increasing risk of suffering collateral damage from untargeted malware and attacks on widely-used software and critical infrastructure. And despite extensive efforts to ramp up cybersecurity, companies still need about 100 days on average to detect a covert attack. Imagine the damage an undetected attacker could do to your business in 100 days. To make things worse, detection is becoming even more challenging as you read this.

Exhibit 1
The threat is growing



4 www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/ (retrieved October 2017)

Cyberattacks have become a global risk, affecting all industries and all aspects of our daily lives.

Growing complexity makes companies more vulnerable

While hackers are honing their skills, refining their techniques, and industrializing their craft, a number of business trends – although inherently unrelated to cybersecurity – make companies more vulnerable to cyberattacks:

- The digitization of the entire value chain means that assets from the design of new products and services to distribution networks and customer data are now at risk.

- At the same time, the complexity of corporate digital value chains is growing. Typically, these value chains span thousands of people, countless applications, and a myriad of servers, workstations, and other devices.

- Thanks to outsourcing and offshoring, the weakest link of a company's value chain may well be a supplier or other third party.

Your critical systems may be protected by a state-of-the-art firewall and the latest malware detection software. But what about the hotshot design studio that has access to your intellectual property? They may have signed an NDA, but can you be sure their cybersecurity is up to your standards? The entry point for cyberattackers can be as trivial as a WiFi-enabled camera hooked up to a computer by an employee uploading pictures taken at the corporate retreat. For example, the recent cases of intellectual property theft from media companies all targeted third-party postproduction services with inferior cybersecurity.[5]

5 www.polygon.com/2017/8/8/16114308/hbo-hack-game-of-thrones (retrieved September 2017)

The Internet of Things multiplies the number of entry points for hackers

In the past, cyberrisk has primarily affected information technology (IT). But as the Internet of Things (IoT) grows, operating technology (OT) is coming under threat as well. Increasingly, companies hook their production systems and products up to the Internet. As a result, the number of vulnerable devices is increasing dramatically.

In the past, a large corporate network might have had somewhere between 50,000 and 500,000 end points; with IoT, we are talking about millions or tens of millions of end points. Unfortunately, many of these consist of legacy devices with inadequate security, or no security at all.[6] By 2020, IoT may comprise as many as 50 billion devices, many of which will at least partly be outside corporate control. Examples include smart cars, smart homes, and smart apparel. By 2020, 50 percent of all network connections will be machine-to-machine connections, and this number will keep growing.

In effect, the number of potential entry points for hackers and the value at risk will be multiplying across all industries.

Common pitfalls

The good news is that awareness of the magnitude of the threat is growing. According to a recent McKinsey survey, 75 percent of experts consider cybersecurity to be a top priority for their businesses. The bad news is that executives are overwhelmed by the challenge. Only 16 percent say their companies are well prepared to deal with cyber-risk.[7] Common pitfalls include:

Delegating the problem to IT. Many top executives treat cyberrisk as a technical issue and delegate it to the IT department. This is a natural reaction, given that cybersecurity

6 www.mckinsey.com/global-themes/internet-of-things/our-insights/six-ways-ceos- can-promote-cybersecurity-in-the-iot-age (retrieved September 2017)

7 www.mckinsey.com/global-themes/internet-of-things/our-insights/six-ways-ceos- can-promote-cybersecurity-in-the-iot-age (retrieved September 2017)

is a technical problem at its core. But defending a business is different from protecting servers. Defending a business requires a sense of the value at risk, based on an understanding of business priorities, a company's business model and value chain, the corporate risk culture, roles, responsibilities, and governance. IT alone cannot tackle cybersecurity.

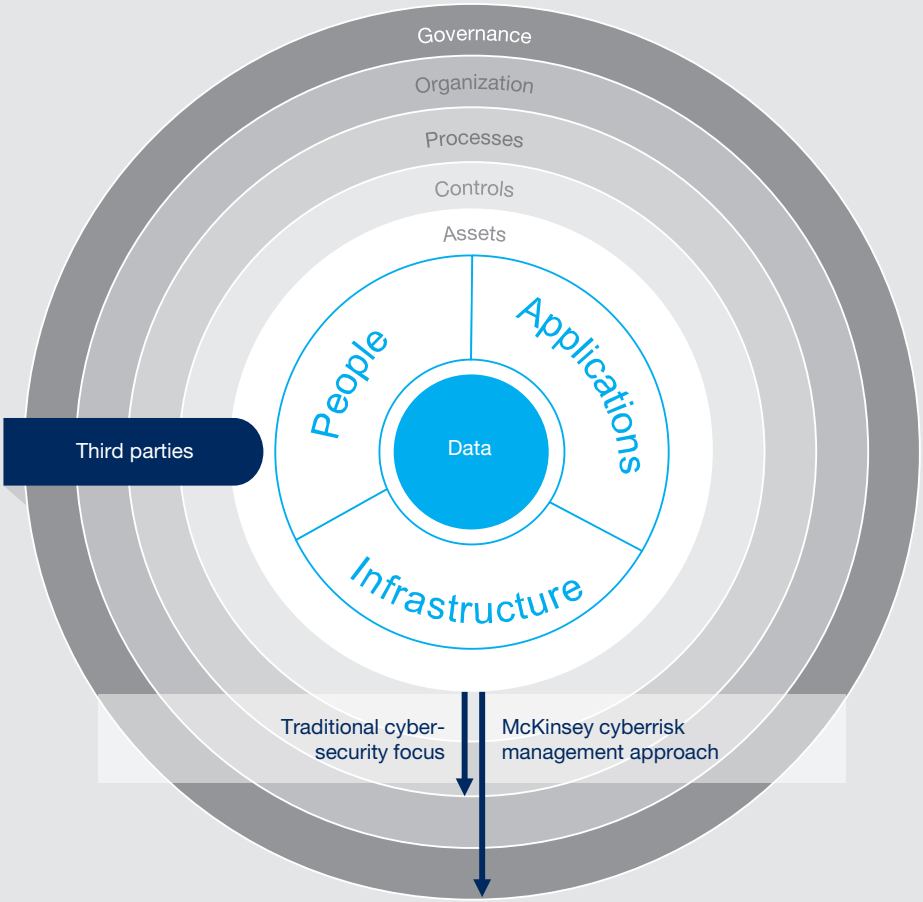
Throwing resources at the problem. Other companies try to solve the problem by throwing money and resources at it, assuming that the threat will go away if you persuade enough high-profile hackers to join the company's ranks. But even the finest hackers do not stand a chance at anticipating and fending off tens of thousands of attacks on millions of devices in a complex network.

Treating the problem as a compliance issue. Other companies introduce new cybersecurity protocols and checklists every other day. But these efforts often bring about an undue focus on formal compliance rather than real resilience. Even when all boxes on the chief security officer's (CSO's) checklist are ticked, the company may be no less vulnerable to cyberattacks than before.

In short, the traditional responses are inadequate. To counter the growing threat, accommodate the growing complexity of corporate networks, and keep up with the quickening pace of change, a new posture is called for.

Exhibit 2
Comprehensive cyberrisk management comprises multiple layers

Scope of our comprehensive approach



SOURCE: NIST; McKinsey Cybersecurity and Cyberrisk Service Line

A NEW POSTURE

To ready global companies for an age of all-encompassing connectivity, executives need to adopt a more adaptive, more omprehensive, and more collaborative approach to cyberrisk (Exhibit 2). We have derived the following principles from our work with some of the world's leading cybersecurity players:

Cyberrisk needs to be treated as a risk management issue. Cyberrisk needs to be dealt with like any other complex, critical, nonfinancial risk. Key elements include the prioritization of relevant threats, the determination of a company's risk appetite (i.e., willingness to accept risk), and the definition of initiatives to minimize risk. Additionally, companies need to put in place an organizational structure and governance approach that bring transparency and enable real-time risk management.

Cyberrisk needs to be addressed within a business context. Technical experts cannot solve the problem without understanding the underlying commercial and organizational requirements. Most current cybersecurity programs are inefficient. Companies tend to overinvest in technical gadgets and underinvest in complexity reduction and consistent coverage of their whole value chain, such as vendor risk management.

Cyberrisk needs to be dealt with on multiple levels. Different assets are exposed to different threat types and levels. Key asset categories include data, infrastructure, applications, and people. Creating a comprehensive register of all of these assets is tedious and time consuming. This is why companies should take advantage of automated tools to catalogue their assets, focusing on the areas that are most at risk.

Cyberrisk calls for adaptive defenses. Sooner or later, every organization will be affected by a cyberattack. A company's organization, processes, IT, OT, and products need to be reviewed and adjusted as cyberthreats evolve. In particular, business continuity and crisis management structures and processes must be adjusted to changes in the threat level.

Cyberrisk calls for holistic, collaborative governance. Traditionally, many companies distinguish between physical and informational security, between IT and OT, between business continuity management and data protection, and between in-house and external security. In the digital age, these splits are obsolete. Scattered responsibility can put the entire organization at risk. To reduce redundancies, speed up responses, and boost overall resilience, companies need to address all areas of the value chain that are affected by cyberthreats in a holistic cybersecurity governance approach. This holistic approach should also include suppliers and customers. To counter cyberrisk effectively, companies need to share information and work together across departments, as well as with outside service providers and across the industry.

Companies that adhere to these principles tend to be much more resilient to most attacks than their peers, and they typically make better use of cybersecurity resources and funds. Prioritizing investments on crucial assets alone can help save up to 20 percent of cybersecurity cost. In our experience, up to 50 percent of a company's systems are not critical from a cybersecurity perspective. And the cost of implementing a given security solution can vary by a factor of five between comparable companies.

But a holistic approach to cyberrisk not only helps keep cost at bay. It also enables companies to minimize the disruption of operations that current cybersecurity initiatives often bring about. By involving business owners from the beginning, companies can speed up the design and implementation of their cybersecurity architecture significantly. And while it may be hard – or even impossible – to protect a company against the most advanced attacks, systematic governance is the best insurance against the bulk of everyday attacks. Even when your in-house assets seem secure, attackers may still find a way in through subsidiaries or third parties. This is why comprehensive coverage of all critical assets along the entire value chain is crucial to achieving effective cybersecurity.

Specific benefits of systematic cyberrisk management include:

- Coverage of the entire value chain, including IT, OT, and products
- Clear prioritization of threats to inform investment decisions
- Focus on actual digital resilience rather than formal compliance
- Cyberrisk reduction without negative impact on agility and innovation
- Identification of cybersecurity opportunities, such as resilient products.

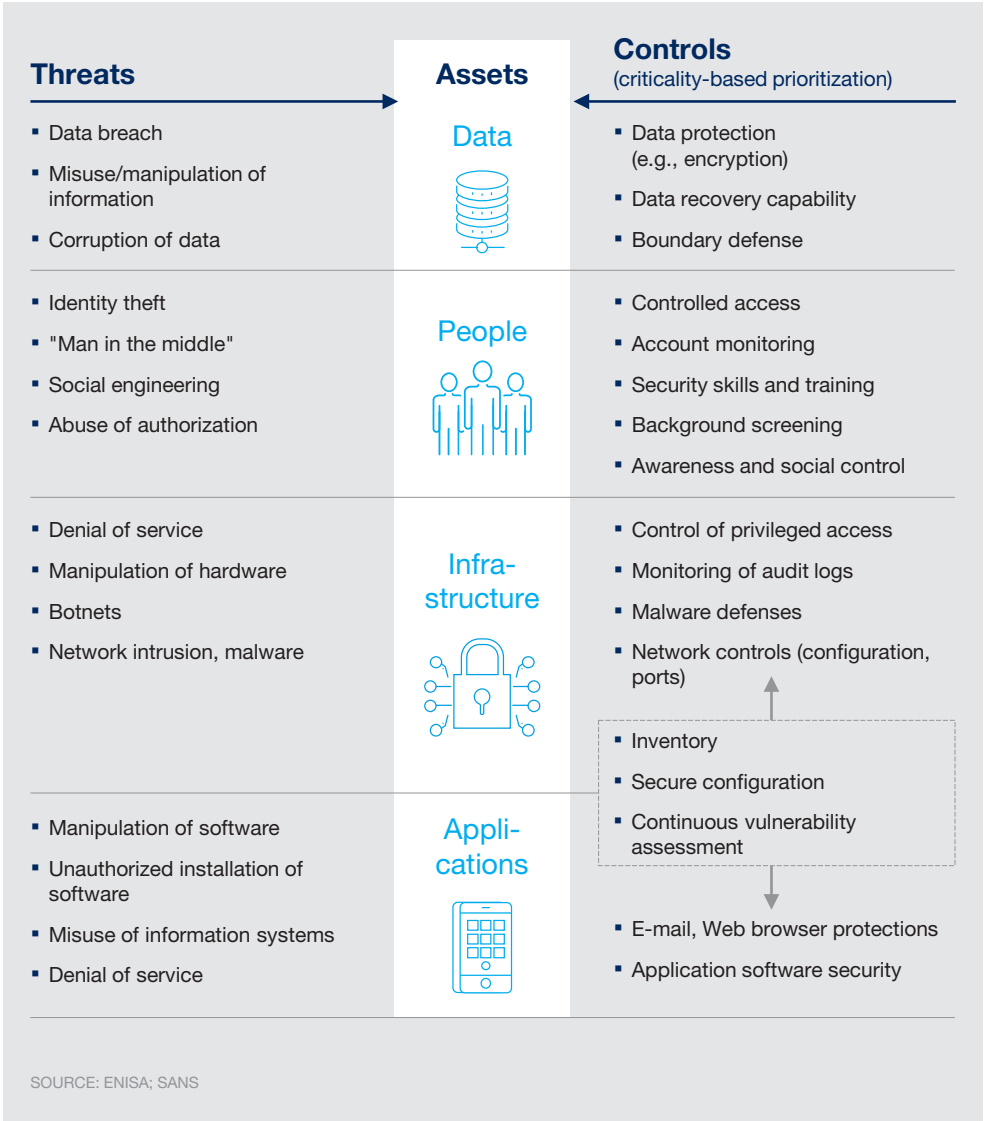
BUILDING UP RESILIENCE STEP BY STEP

Successful cyberstrategies are built one step at a time, drawing on a comprehensive understanding of relevant business processes and the mindset of prospective attackers. Leading players are moving from a compliance focus towards a focus on effective response and recovery. At the same time, leading companies are taking precautions to weave risk awareness into the DNA of their company. Given that a breach of cyberdefenses is only a matter of time, the right balance of prevention, professional crisis management, and business continuity management will bring the highest return on investment. Key steps include:

1. Prioritization of assets and risks by criticality

Assess your current digital resilience and aspiration level. Companies need to take stock of their cyberrisk capabilities along the entire value chain and compare their own performance to industry benchmarks. Based on these insights, executives in charge of cybersecurity should set realistic aspirations for their target resilience level. Generic visions to “become world class” are usually not productive. Rather, the aspiration level should be tailored to the industry and the current threat level as defined by objective, measurable key risk indicators (KRIs).

Exhibit 3
Prioritization of assets, threats, and controls



SOURCE: ENISA; SANS

Define relevant threats and attackers. Almost all companies are exposed to automated attacks and the risk of indirect impact from industry-wide attacks or impact on central eco-systems. Beyond these unspecified threats, the relevance of other attack categories differs significantly, depending on the industry and company-specific factors, such as the size and structure of the organization. Before investing in cyberdefenses, executives should strive to clarify which risks are most relevant for their business (Exhibit 3).

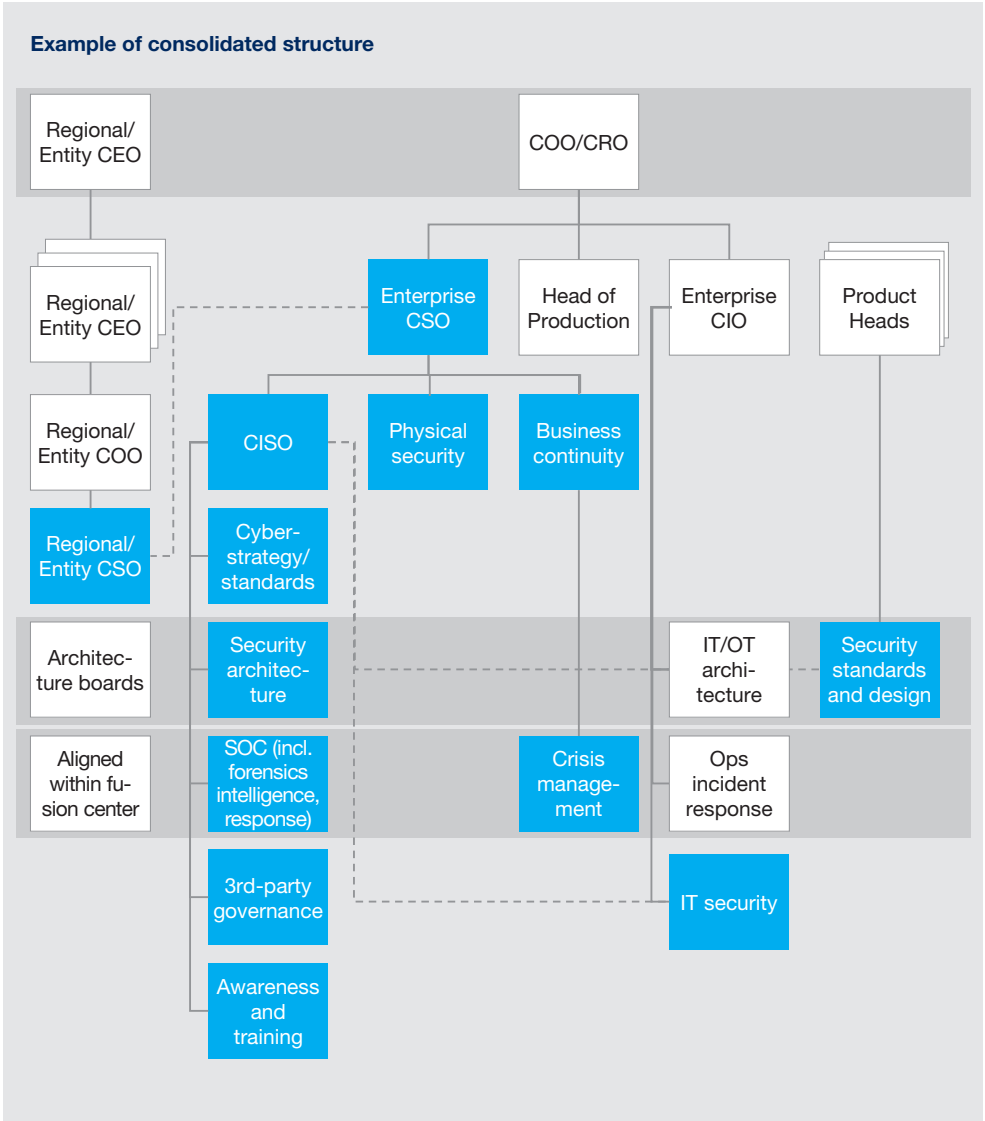
Know your critical assets. Effective cybersecurity starts with knowing what to secure. Automated tools can help executives keep track of all assets that are crucial for their business. The initial inventory should cover every asset that is connected to the corporate network (IT, OT, IoT), as well as all people that have access to the network, regardless of whether they are on the company payroll or work for a supplier, customer, or service provider. The asset inventory will help companies prioritize their security initiatives as well as their efforts and precautions to ensure effective recovery and crisis response during attacks.

2. Implementation of differentiated controls and effective processes

Differentiate your controls. Blunt implementation of controls across all assets is one of the key drivers of cybersecurity waste and productivity loss. Controls should be differentiated, based on a business-driven prioritization of assets and risks. The more critical a given asset is to your business, the stronger the control should be. Examples of strong controls include two-factor authentication and background checks of employees who have access to critical assets.

Establish effective cybersecurity processes. Traditional cybersecurity processes were focused on compliance, i.e., on adhering to protocols, ticking boxes on checklists, and filing documentation. This approach is no longer suited to respond to today's quickly evolving cyberthreat landscape. Companies need to embrace and adopt automation, big data solutions, and artificial intelligence to cope with the ever-increasing number of alerts and incidents. At the same time, it is crucial to build a solid ecosystem of partners, taking into account the fact that the war for talent is more intense in the cybersecurity space than

Exhibit 4
Leading organizations consolidate their cyberrisk structure



in any other area. Companies should keep reviewing their partner strategy, checking which processes can be outsourced and which should be handled in-house to protect intellectual property or fend off high risk.

3. Consolidation of cybersecurity organization and governance

Consolidate the cyberrisk organization. Most current security organizations are still driven by analog dangers, such as natural disasters. The resulting structures, decision rights, and processes are inadequate to deal with cyberrisk. A state-of-the-art cybersecurity function (Exhibit 4) should:

- Overcome the historic split of responsibility between physical security, information security, business continuity, and crisis management to minimize conflicts of interest and duplication of processes
- Ensure that the skills of all team members are up to the current threat level at all times
- Align cybersecurity functions with the standards defined by relevant institutions to streamline incident management and standardize stakeholder interfaces
- Define responsibilities and interfaces between all cybersecurity stakeholders at the corporate headquarters, regional teams, and/or subsidiaries
- Establish strong architecture functions (e.g., data, systems, security) to ensure “security by design” and build long-term digital resilience.

Introduce holistic cyberrisk governance. A strong, state-of-the-art cyberorganization needs to be embedded in an effective, company-wide governance structure, built on a strong cyberrisk culture. IT, OT, IoT, and product governance should be consolidated, and the entire value chain should be covered, including third parties (Exhibit 5). Effective empowerment of the cybersecurity function is comprised of ten elements:

Exhibit 5
Leading organizations consolidate their cyberrisk structure

- Led by a senior, experienced CSO with a direct, independent reporting line to the board
- Ownership of the overall cyberrisk budget
- Accountability for the implementation of a cyberrisk portfolio of initiatives
- Company-wide ownership of cybersecurity, supported by regular reports on the current status and progress of risk remediation to the board and other stakeholders
- Right to veto all cyberrisk-related decisions, such as outsourcing, vendor selection, and exceptions from security controls
- Effective committee structure from the board down, ensuring coverage of all cyberrisk-related aspects (e.g., outsourcing, vendor management, third-party management) across all businesses and legal entities
- Top-down awareness campaigns and training programs, adjusted at regular intervals to cover the latest threats
- Clear top-down communication and effective incentive structure to enforce adherence to cybersecurity controls
- Frequent realistic attack and crisis simulations within the organization, with partners, and with other players in the industry
- Efficient interfaces to law enforcement and regulators.

CYBERSECURITY TRANSFORMATIONS

In our experience, it takes global organizations two to three years to complete sustainable cybersecurity transformations (Exhibits 6.1 and 6.2), chiefly because of the cultural change in leadership and mindset that is required to succeed. Throwing money at the problem will not accelerate the process. Key success factors of successful transformations include:

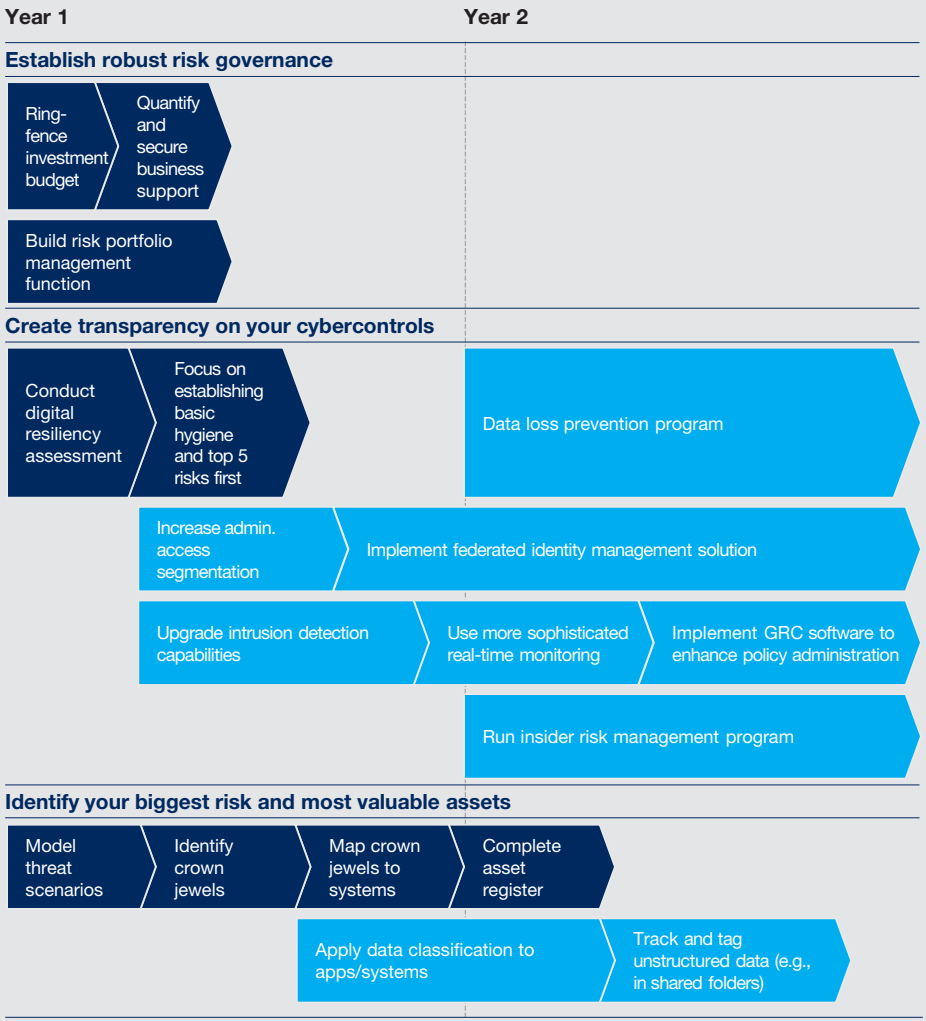
- Alignment of all stakeholders on the most important business risks and the priorities for risk mitigation actions
- Strong governance to provide the budget and resources required for each initiative
- Topmanagement sponsorship to get operational, risk, and IT departments to rally around the transformation during planning and implementation.

The most common bottlenecks are the commitment and the capacity of stakeholders outside the IT department. For cybersecurity transformations to succeed, it is crucial to make sure that key players from across the organization have the determination and the time to infuse cybersecurity with business acumen and operational experience. Business owners must engage in an assessment of threats from a commercial and operative perspective, agree on a prioritized mitigation strategy, and help draw up a transformation road map that reflects these priorities. Furthermore, business stakeholders must stay involved throughout the implementation – e.g., to build an asset inventory, introduce new processes, drive behavioral change, and participate in exercises and trainings. To get started, top management should empower the cybersecurity function, e.g., by moving it up to or near the board level in the org chart. Executives in charge of cybersecurity need to make sure that key players have the capabilities to deal with cyberrisk effectively, and that a new mindset takes hold among all personnel. Successful cybersecurity leaders encourage their teams and the whole organization to look at the company's assets the way an attacker would. Examples of enablers of this cultural change include

group-wide awareness campaigns, cyberattack simulations, and investments in fast detection, response, and recovery processes. Such measures will also help bridge the time needed to finalize the transformation towards full digital resilience.

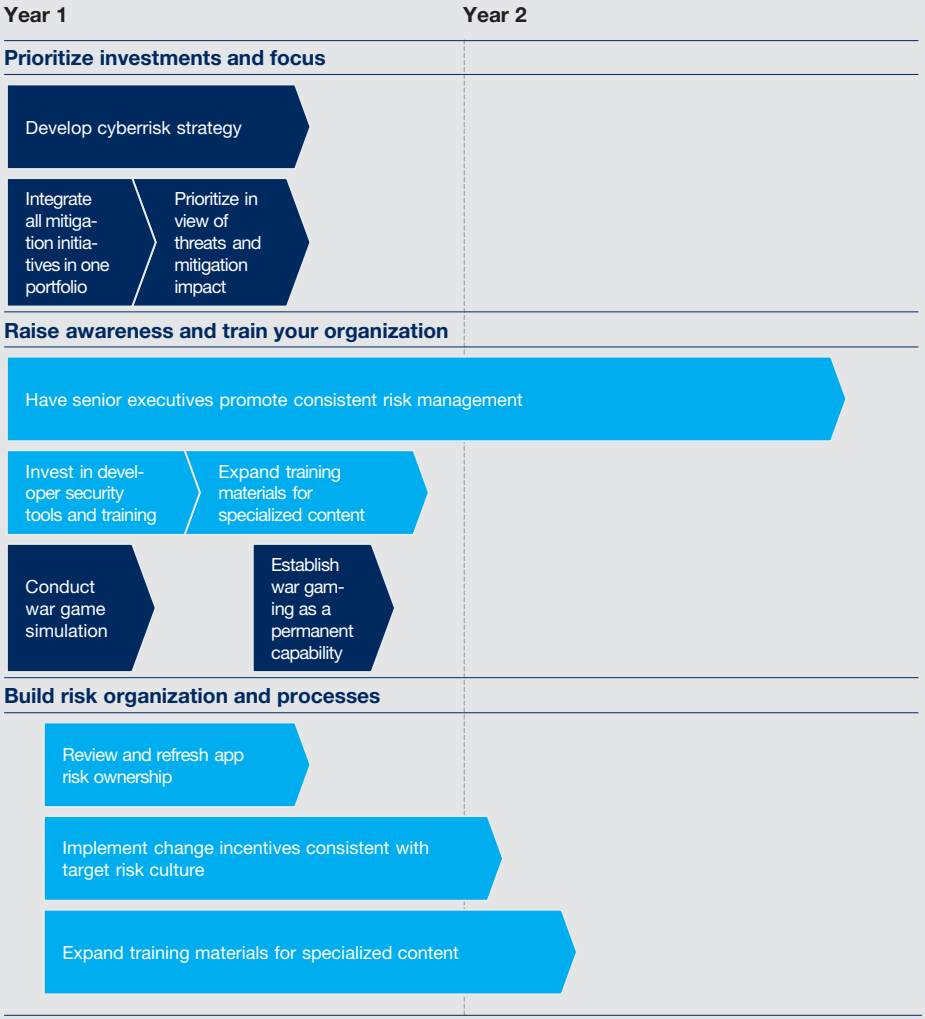
Ultimately, winning the war against cyberrisk is tantamount to winning the war for cyber-talent. Cybersecurity has rightfully become a CEO topic, and the caliber of cyberteams needs to reflect this increase in importance. Cybersecurity functions need to attract, retain, and develop people who – unlike many IT experts today – are nimble, innovative, and open-minded. No matter how refined your technology, it is the human factor that will win the war.

Exhibit 6.1
Building up next-generation cybersecurity capabilities is a multiyear journey



SOURCE: McKinsey Cybersecurity and Cyberrisk Service Line

Exhibit 6.2 Building up next-generation cybersecurity capabilities is a multiyear journey



SOURCE: McKinsey Cybersecurity and Cyberrisk Service Line

APPLICATION EXAMPLES

We work with international financial institutions, large companies, global corporations, and not-for-profit providers of critical infrastructure. Recent examples of cybersecurity efforts supported by our experts include:

Resilience ramp-up triggered by global malware attack

A global industrial company suffered substantial damages from a cyberattack. The extent of the impact took executives by surprise because the company had put mature IT security processes and a highly standardized software architecture in place prior to the attack. Precautions they had taken at their central IT organization included patching solutions and automated backups. The issue was that part of their IT was still managed regionally. This prolonged the time the company needed to recover from the global attack. It also turned out that there had been gaps in business continuity management, vendor risk management, and stakeholder communication along the value chain. Based on the lessons learned from the specific incident and a holistic analysis of cyberresilience gaps, the company started a number of initiatives to increase resilience. Examples include:

- An empowered CSO function to increase cyberrisk awareness and establish a cybersecurity culture at all levels of the organization
- The implementation of state-of-the-art global business continuity management processes across the organization
- Building redundancy of critical systems to reduce risk concentration
- Improved vendor risk management processes.

This case demonstrates the importance of a omprehensive, top-down approach to cybersecurity. If the company had tested the resilience of their entire global organization

to major threats, if the concentration of risks had been monitored and reduced systematically, and if gaps in cybersecurity governance had been detected before the attack, the impact would have been far less dramatic.

"Crown jewels" cybersecurity program in the financial industry

A global insurance company had planned to invest USD 70 million in a comprehensive cybersecurity risk mitigation program. One year into the program, only a fraction of the measures the company had initially devised had actually been implemented. Our team found that the business units had put pressure on the IT department to prioritize the implementation of business-driven changes, such as a sales campaign or the creation of new types of reports, at the expense of security measures, such as e-mail encryption or multifactor authentication. The business units also took issue with the restrictions that came with cybersecurity measures, such as the extra efforts that went into data loss prevention, or limitations on the use of third-party vendors in critical areas. To balance cybersecurity requirements with smooth business operations, we worked with the company to set up a comprehensive "crown jewels" program that helped identify the biggest business risks and the IT assets that business continuity depends upon. Subsequently, the cybersecurity investment portfolio was streamlined, focusing on the crown jewels. As a consequence, the acceptance of the required initiatives among business owners grew dramatically. Not only did the crown jewels program help increase buy-in and speed up implementation, it also led to a substantial cost reduction relative to the original plan.

Cybersecurity transformation at a military institution

A military institution set out to ramp up cyberresilience across its entire organization. Scenario simulation exercises helped increase cyberrisk awareness and instill a sense of urgency in key stakeholders. Specifically, we encouraged the client to explore and understand the mindset of potential attackers, focusing on the concept of the weakest link in the chain of defense. Through an extensive training program, this kind of thinking was

rolled out to the entire institution, making sure skills were passed on from expert to expert. Throughout the project, the military intelligence unit acted as the stronghold of cybersecurity expertise and the catalyst of change. In parallel, IT architecture was reviewed and adjusted to increase resilience against destructive attacks, such as data corruption.

Cyberstrategy to protect critical infrastructure

Although the probability of direct and indirect attacks on our critical infrastructure is increasing, the cyberrisk awareness of key players in affected institutions is still limited. At the same time, many cybersecurity experts have only a limited understanding of the inner workings of industries such as energy and other utilities. In a given case, a major energy provider was worried about the increasing number of attacks in the sector. Based on an industry-specific assessment of critical assets and relevant capabilities, we defined a cyberstrategy to increase the company's long-term resilience to cyberrisk. To maximize the return on the required investments, our team went beyond risk prevention and helped the company identify opportunities to use cyberresilience as a differentiating factor when developing and deploying new products and services (think "hacker-proof power supply"). Such initiatives help transform cybersecurity from a cost driver into a growth opportunity.

Across industries, we have helped numerous clients deal with ransomware attacks, including NotPetya and WannaCry. As part of this kind of support, we work with our clients to implement state-of-the-art crisis management and recovery processes. We also oversee entire cybersecurity transformation journeys, from the initial resilience assessment to the training of future leaders. In one particular case, our cybersecurity team leader even stepped in as a client's interim chief information security officer (CISO). As part of our cybersecurity Build-Operate-Transfer model, we designed the new cybersecurity architecture, defined the org chart, closed the biggest gaps right away, helped recruit new cybertalent, trained new hires, and handed over cybersecurity leadership to the client step by step.

While traditional approaches to cyberrisk focus on technology, our approach also comprises organization and governance. Supporting tools, such as McKinsey's cyberrisk cockpit (Exhibit 7), help senior executives stay on top of different types of cyberrisk and prioritize their investments in cybersecurity accordingly. This kind of transparency helps executives deploy funds and cybersecurity resources to those areas in which they will create, or help protect, the biggest value.

Exhibit 7
Systematic cyberrisk management

Information is systematically gathered for continuous decision making …

… and aggregated in dashboards for continuous monitoring and managing of cyberrisks

- Understanding of critical assets
- Threat levels in relation to assets
- Prioritization of investment needs
- Effectiveness of controls and enhancements
- Organizational responsibilities

McKinsey's cyberrisk cockpit

Risk situation
- External threat level
- Critical external threats
- Cybersecurity incidents
- Cyberrisk status

Subrisks
- Status
- Forecast of initiative impact

Asset risk exposure
- Asset criticality
- Control status

SOURCE: McKinsey Cybersecurity and Cyberrisk Service Line

KEY RECOMMENDATIONS

1. Treat cyberrisk as a strategic risk, rather than as a technical issue. Make sure this is reflected in your organizational structure and your governance approach.

2. Make business leaders accountable for their aspects of cybersecurity. A omprehensive cybersecurity posture needs to be driven and managed by business owners.

3. Create transparency about relevant threats, critical assets, and effective controls to focus your investments. Systematic information gathering is crucial to maximize ROI.

4. Ramp up the skills of your cyberrisk teams and the seniority of your cyberrisk leaders to ensure they are well-equipped for taking on the growing threat.

5. Get ready for the Internet of Things and Industry 4.0 by extending your cyberrisk efforts beyond IT applications and infrastructure. Your industrial systems or products may be more vulnerable than your IT systems.

6. Make it easy for employees to do the right thing by providing efficient cybersecurity solutions that do not restrict agility and innovation. Conversely, make it difficult to expose critical assets.

7. Invest in response and recovery as much as you invest in resilience. You cannot fend off all attacks. This is why you need to be able to get back into business quickly after an attack.

8. Pay special attention to subsidiaries, contractors, and service providers. Third parties are typically one of the most vulnerable parts of your value chain.

March 2018

Visual Media Europe
www.mckinsey.com