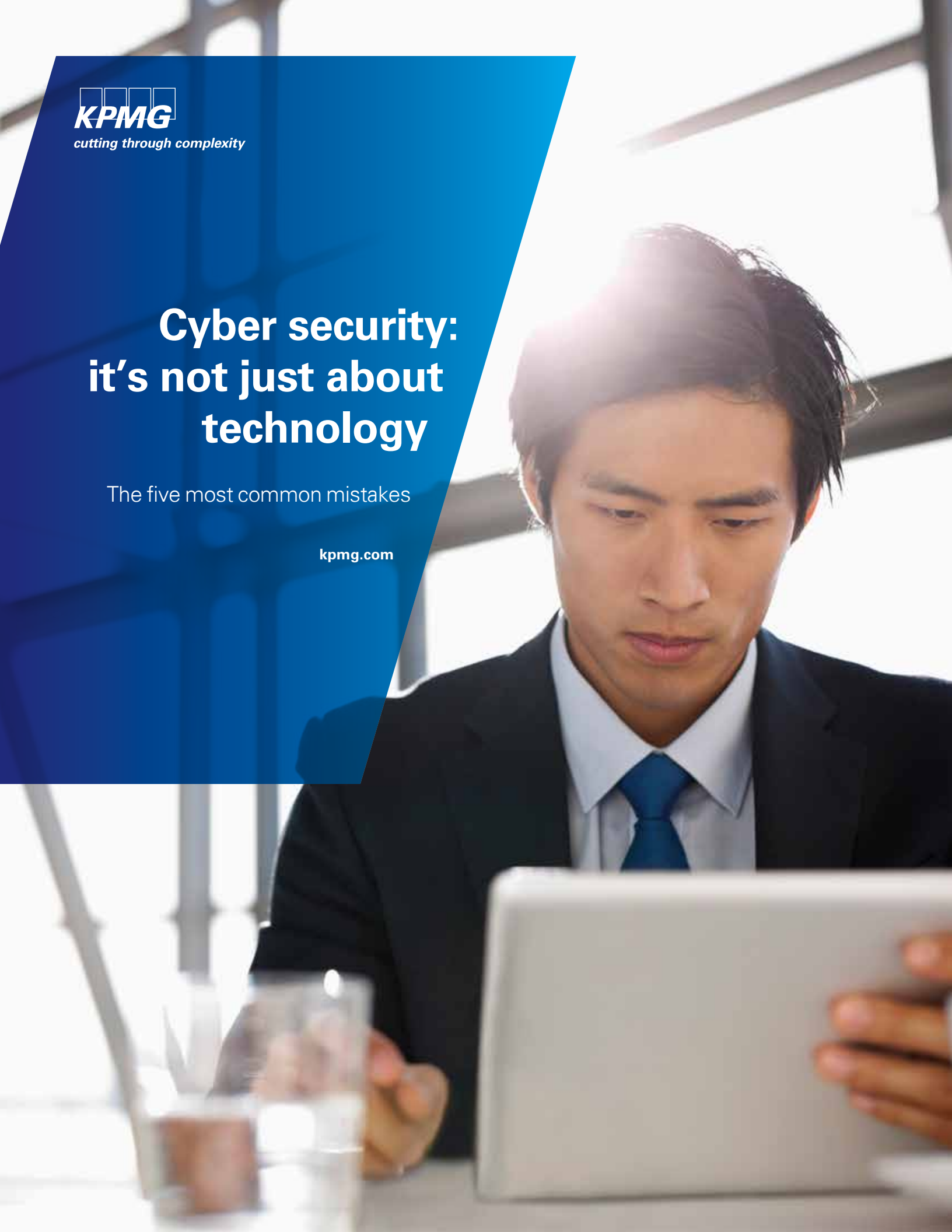
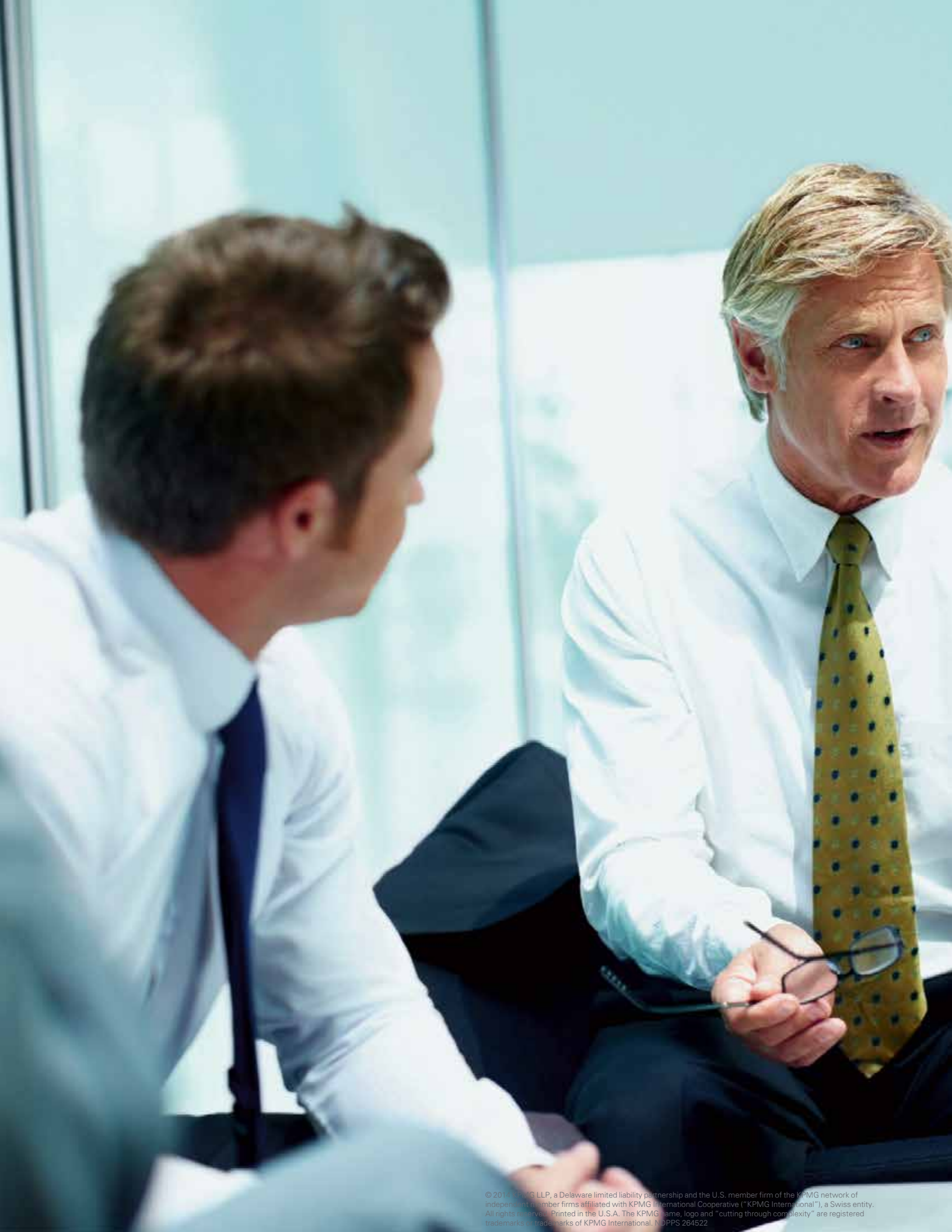
KPMG
cutting through complexity

Cyber security: it's not just about technology

The five most common mistakes

kpmg.com





Contents

Preface

Cyber security is an important concern for every organization. Daily occurrences demonstrate the risk posed by cyber attackers—from individual, opportunistic hackers, to professional and organized groups of cyber criminals with strategies for systematically stealing intellectual property and disrupting business.

The management of any organization faces the task of ensuring that its organization understands the risks and sets the right priorities. This is no easy task in light of the technical jargon involved and the pace of change.

Focusing on technology alone to address these issues is not enough. Effectively managing cyber risk means putting in place the right governance and the right supporting processes, along with the right enabling technology.

This complexity, however, cannot be an excuse for company management to divest responsibility to technical "experts." It is essential that leaders take control of allocating resources to deal with cyber security, actively manage governance and decision making over cyber security, and build an informed and knowledgeable organizational culture.

This white paper provides essential insights for management to get the basics right. We'll cover the world of cyber crime today, explore five common cyber security mistakes, explain the importance of customizing cyber security policies, outline the critical dimensions of a strong cyber security model, and look at key questions to help you navigate the "new normal" of cyber security.

Steve Barlock
Principal, Advisory
Information Protection and Business Resilience
T: 415-963-7025
E: sbarlock@kpmg.com

Tony Buffomante
Principal, Advisory
Information Protection and Business Resilience
T: 312-665-1748
E: abuffomante@kpmg.com

Fred Rica
Principal, Advisory
Information Protection and Business Resilience
T: 973-912-4524
E: frica@kpmg.com

What is cyber crime and who is carrying it out?

Cyber crime is a range of illegal digital activities targeted at organizations in order to cause harm. The term applies to a wide range of targets and attack methods.

Understanding the "actor," i.e. the person or organization that is sponsoring or conducting the attacks, is essential for effective defense.

Actors can be divided into four categories:

1. An individual hacker, generally acting alone and motivated by being able to show what he/she can do
2. The activist, focused on raising the profile of an ideology or political viewpoint, often by creating fear and disruption
3. Organized crime, focused solely on financial gain through a variety of mechanisms, from phishing to selling stolen company data
4. Governments, focused on improving their geopolitical position and/or commercial interests

Attacks by these different actors have a number of different characteristics, such as the type of target, the attack methods and scale of impact.

01

Understanding the cyber risk

The amount of data continues to grow exponentially, as does the rate at which organizations share data through online networks. Billions of machines – tablets, smartphones, ATM machines, security installations, oil fields, environmental control systems, thermostats and much more – are all linked together, increasing inter-dependencies exponentially. Organizations increasingly open their IT systems to a wide range of machines and lose direct control of data security. Furthermore, business continuity, both in society and within companies, is increasingly dependent on IT. Disruption to these core processes can have a major impact on service availability.

Cyber criminals are very aware of these vulnerabilities. Driven by a wide range of motivations – from pure financial gain, to raising the profile of an ideology, to espionage or terrorism – individual hackers, activists, organized criminals and governments are attacking government and company networks within increasing volume and severity.

But while the cyber threat is very real and its impact can be debilitating, the media often sketches an alarmist picture of cyber security, creating a culture of disproportionate fear. Not all organizations are necessarily easy targets for cyber criminals. For example, a small or midsized company has a very different risk profile than a multinational organization.

What is true for any government or organization is that cyber crime risks can be controlled. Cyber criminals are not invincible geniuses, and while they can cause real damage to your business, you can take steps to protect yourself against them. You may not be able to achieve 100 percent security, but by treating cyber security as "business as usual" and balancing investment between risks and potential impacts, your organization will be well prepared to combat cyber crime.

Organizations can reduce the risks to their business by building up capabilities in three critical areas – prevention, detection and response.

Prevention

Prevention begins with governance and organization. It is about installing fundamental measures, including placing responsibility for dealing with cyber crime within the organization and developing awareness training for key staff.

Detection

Through monitoring of critical events and incidents, an organization can strengthen its technological detection measures. Monitoring and data mining together form an excellent instrument to detect strange patterns in data traffic, to find the location on which the attacks focus and to observe system performance.

Response

Response refers to activating a well-rehearsed plan as soon as evidence of a possible attack occurs. During an attack, the organization should be able to directly deactivate all technology affected. When developing a response and recovery plan, an organization should perceive cyber security as a continuous process and not as a one-off solution.

	Prevention	Detection	Response
Management and organization	Appointing cyber crime responsibilities	Ensuring a 24/7 stand-by (crisis) organization	Using forensic analysis skills
Processes	Cyber crime response tests (simulations) Periodic scans and penetration tests	Procedures for follow-up of incidents	Cyber crime response plan
Technology	Ensuring adequate desktop security Ensuring network segmentation	Implementing logging of critical processes Implementing central monitoring of security incidents	Deactivating or discontinuing IT services under attack

02

The five most common cyber security mistakes

To many, cyber security is a bit of a mystery. This lack of understanding has created many misconceptions among management about how to approach cyber security. From our years of experience, we have seen the following five cyber security mistakes repeated over and over – often with drastic results.

1

Mistake: **"We have to achieve 100 percent security"**

Reality: **100 percent security is neither feasible nor the appropriate goal**

Almost every airline company claims that flight safety is its highest priority while recognizing that there is an inherent risk in flying. The same applies to cyber security. Whether it remains private or is made public, almost every large, well-known organization will unfortunately experience information theft.

Developing the awareness that 100 percent protection against cyber crime is neither a feasible nor an appropriate goal is already an important step towards a more effective policy, because it allows you to make choices about your defensive posture. A good defensive posture is based on understanding the threat (i.e., the criminal) relative to organizational vulnerability (prevention), establishing mechanisms to detect an imminent or actual breach (detection) and establishing a capability that immediately deals with incidents (response) to minimize loss.

In practice, the emphasis is often skewed towards prevention – the equivalent to building impenetrable walls to keep the intruders out. Once you understand that perfect security is an illusion and that cyber security is "business as usual," you also understand that more emphasis must be placed on detection and response. After a cyber crime incident, which may vary from theft of information to a disruptive attack on core systems, an organization must be able to minimize losses and resolve vulnerabilities.

2

Mistake: **"When we invest in best-of-class technical tools, we are safe"**

Reality: **Effective cyber security is less dependent on technology than you think**

The world of cyber security is dominated by specialist suppliers that sell technical products, such as products that enable rapid detection of intruders. These tools are essential for basic security, and must be integrated into the technology architecture, but they are not the basis of a holistic and robust cyber security policy and strategy. The investment in technical tools should be the output, not the driver, of cyber security strategy. Good security starts with developing a robust cyber defense capability. Although this is generally led by the IT department, the knowledge and awareness of the end user is critical. The human factor is and remains, for both IT professionals and the end user, the weakest link in relation to security. Investment in the best tools will only deliver the return when people understand their responsibilities to keep their networks safe. Social engineering, in which hackers manipulate employees to gain access to systems, is still one of the main risks that organizations face.

Technology cannot help in this regard and it is essential that managers take ownership of dealing with this challenge. They have to show genuine interest and be willing to study how best to engage with the workforce to educate staff and build awareness of the threat from cyber attack. This is often about changing the culture such that employees are alert to the risks and are proactive in raising concerns with supervisors.

3

Mistake: **"Our weapons have to be better than those of the hackers"**

Reality: **The security policy should primarily be determined by your goals, not those of your attackers**
The fight against cyber crime is an example of an unwinnable race. The attackers keep developing new methods and technology and the defense is always one step behind. So is it useful to keep investing in increasingly sophisticated tools to prevent attack?

While it is important to keep up to date and to obtain insights into the intention of attackers and their methods, it is critical for managers to adopt a flexible, proactive and strategic approach to cyber security. Given the immeasurable value of a company's information assets, and the severe implication of any loss on the core business, cyber security policies need to prioritize investment into critical asset protection, rather the latest technology or system to detect every niche threat.

First and foremost, managers need to understand what kinds of attackers their business attracts and why. An organization may perceive the value of its assets differently than a criminal. How willing are you to accept risks to certain assets over others? Which systems and people store your key assets, keeping in mind that business and technology have developed as chains and are therefore codependent on each other's security?

4

Mistake: **"Cyber security compliance is all about effective monitoring"**

Reality: **The ability to learn is just as important as the ability to monitor**
Reality shows that cyber security is very much driven by compliance. This is understandable, because many organizations have to accommodate a range of laws and legislation. However, it is counterproductive to view compliance as the ultimate goal of cyber security policy.

Only an organization that is capable of understanding external developments and incident trends and using this insight to inform policy and strategy will be successful in combating cyber crime in the long term. Therefore, effective cyber security policy and strategy should be based on continuous learning and improvement.

- Organizations need to understand how threats evolve and how to anticipate them. This approach is ultimately more cost-effective in the long term than developing ever-higher security "walls." This goes beyond the monitoring of infrastructure: it is about smart analysis of external and internal patterns in order to understand the reality of the threat and the short-, medium- and long-term risk implications. This insight should enable organizations to make sensible security investment choices, including investing to save. Unfortunately, in practice, many organizations do not take a strategic approach and do not collect and use the internal data available to them.
- Organizations need to ensure that incidents are evaluated in such a way that lessons can be learned. In practice, however, actions are driven by real-time incidents and often are not recorded or evaluated. This destroys the ability of the organization to learn and put better security arrangements in place in the future.

- The same applies to monitoring attacks. In many cases, organizations have certain monitoring capabilities, but the findings are not shared with the wider organization. No lessons, or insufficient lessons, are learned from the information received. Furthermore, monitoring needs to be underpinned by an intelligence requirement. Only if you understand what you want to monitor does monitoring become an effective tool to detect attacks.
- Organizations need to develop an enterprise-wide method for assessing and reporting cyber security risks. This requires protocols to determine risk levels and escalations, and methods for equipping the board with insight into strategic cyber risks and the impacts to core business.

5

Mistake: **"We need to recruit the best professionals to defend ourselves from cyber crime"**

Reality: **Cyber security is not a department, but an attitude**

Cyber security is often seen as the responsibility of a department of specialist professionals. This mindset may result in a false sense of security and lead to the wider organization not taking responsibility.

The real challenge is to make cyber security a mainstream approach. This means, for example, that cyber security should become part of HR policy, even in some cases linked to remuneration. It also means that cyber security should have a central place when developing new IT systems, and not, as is often the case, be given attention only at the end of such projects.

03

The key is customization

The risks of cyber crime for a local entrepreneur compared to a globally operating multinational are vast. The former may not have the resources or expertise to adequately detect or prevent cyber crime. But the latter is a more attractive target to criminals: it is more visible, more dependent on IT, and has far more valuable assets.

It is clear that both businesses need to adopt a customized approach to cyber security, based on the character of the organization, its risk appetite and the knowledge available. Consider how a jeweler arrives at the proper level of security through a strategic, realistic and customized approach to protecting its assets. Then compare it to the current common corporate approach to cyber security.

Jeweler's perspective on theft security	Corporate perspective on cyber security
I know which assets to protect and have set up the appropriate measures.	I take measures without a having a clear idea of the assets it is essential to protect.
I perceive theft as a risk in the business and know that realistically I can't be in business if I want 100 percent security.	I see cyber crime as something exotic and strive to achieve 100 percent security.
I focus on measures that prevent a person from leaving with valuable goods.	I focus on measures that prevent a person from entering and forget to take measures that prevent a person from taking away information.
I do not let security suppliers spook me and I make my own purchasing decisions.	My security policy depends on the tools available in the marketplace, without knowing exactly what I need.
When it goes wrong or almost goes wrong, I learn a lesson.	When it goes wrong or almost goes wrong, I panic.
I train employees in how to reduce the risk of theft and talk to them when they make mistakes.	I view cyber security as mainly a matter for specialist professionals and don't want to burden the rest of the organization with it.
I invest in tools because they assist the continuity of my business.	I invest in tools because it is mandatory and because the media reports on incidents every day.

04

The six dimensions of cyber maturity

As management, you want to know whether your organization has an adequate approach to cyber security. At KPMG LLP (KPMG), we consider six key dimensions that together provide a comprehensive and in-depth view of an organization's cyber maturity.

Leadership and Governance
Is the board demonstrating due diligence, ownership and effective management of risk?

Human Factors
What is the level and integration of a security culture that empowers and ensures the right people, skills, culture and knowledge?

Information Risk Management
How robust is the approach to achieve comprehensive and effective risk management of information throughout the organization and its delivery and supply partners?

Business Continuity
Have we made preparations for a security event and the ability to prevent or minimize the impact through successful crisis and stakeholder management?

Operations and Technology
What is the level of control measures implemented to address identified risks and minimize the impact of compromise?

Legal and Compliance
Are we complying with relevant regulatory and international certification standards?

Addressing all six of these key dimensions can lead to a holistic cyber security model, providing the following advantages to any organization:

- Minimizing the risk of an attack on an organization by an outside cyber criminal, as well as limiting the impact of successful attacks
- Better information on cyber crime trends and incidents to facilitate decision making
- Clearer communication on the theme of cyber security, enabling everyone to know his or her responsibilities and what needs to be done when an incident has occurred or is suspected
- Improved reputation, as an organization that is well prepared and has given careful consideration to its cyber security is better placed to reassure its stakeholders
- Increased knowledge of competence in relation to cyber security
- Benchmarking the organization in relation to peers in the field of cyber security
-

05

Are you ready for action?

Cyber security must be on your agenda. Your management, boards, shareholders and clients all expect you to pay sufficient attention to this problem.

But just because you recognize the problem doesn't mean you are ready for action.

Developing a strategic, customized and comprehensive cyber security program, driven from the top, will help you avoid five common cyber security mistakes:

1. "We have to achieve 100 percent security"
2. "When we invest in best-of-class technical tools, we are safe"
3. "Our weapons have to be better than those of the hackers"
4. "Cyber security compliance is all about effective monitoring"
5. "We need to recruit the best professionals to defend ourselves from cyber crime"

If you have taken a holistic view of cyber security and can answer the following questions about your approach, **you are ready for action!**

1. How big is the risk for your organization and the organizations you do business with?

- How attractive is your organization to potential cyber criminals?
- How dependent is your organization on the services of partners, suppliers and other organizations, and how integrated are the corresponding IT processes?
- Do you know which processes and/or systems represent the greatest assets from a cyber security perspective?
- Have you considered how much risk you are willing to take in relation to these processes and/or systems, since there is no such thing as 100 percent security?
- Do your partners have the same risk appetite and cyber security measures as you do?
- Have you developed clear business cases for your cyber security investments?

2. Do governance processes and the organizational culture enable effective risk management?

- Do you know how the culture of your organization contributes to (or hampers) good cyber security?
- When was the last time your board communicated something about the importance of cyber security?
- Are you prepared to act in the event of a crisis or incident? Do you know how you should communicate and who should do it?
- Can you provide assurance to stakeholders on your cyber security policy?

3. How large should your cyber security budget be and how should you spend it?

Depending on the risk profile of your organization, the budget for cyber security should probably be in the range of three percent to five percent of your total IT budget. Currently, a significant part of such budgets is often spent on implementing technological solutions and solving problems from the past. The key question you need to answer is:

- Is at least three to five percent of the total IT budget dedicated to cyber security?
- How much of your cyber security budget is spent on solving past problems?
- How much is spent on structural investments in better security systems?
- How much is spent on systems and tools?
- How much is spent on awareness and culture change?

For more information on the cyber maturity assessment, incident response or KPMG's cyber security services, please visit us at www.kpmg.com/US/informationprotection or contact one of our Information Protection and Business Resilience team leaders:

Steve Barlock
Principal, Advisory
Information Protection and Business Resilience
T: 415-963-7025
E: sbarlock@kpmg.com

Tony Buffomante
Principal, Advisory
Information Protection and Business Resilience
T: 312-665-1748
E: abuffomante@kpmg.com

Fred Rica
Principal, Advisory
Information Protection and Business Resilience
T: 973-912-4524
E: frica@kpmg.com

kpmg.com