KPMG

The five most common cyber security mistakes

Management's perspective
on cyber security

kpmg.ch

Contents

Preface

We know that cyber security is an important concern for every organisation. Daily occurrences demonstrate the risk posed by cyber attackers – from individual hackers to professional cyber criminals. The management of any organisation face the task of ensuring that their organisations understand the threat and set the right priorities. This is no easy task in light of the technical jargon involved and the pace of change. Non-specialists can find it difficult to know where to start, to focus on what is important.

At the same time, the media contributes to a culture of fear suggesting every organisation is an easy target. Reports often fail to distinguish between opportunistic fraudsters on eBay and organised criminal groups with strategies for systematically stealing intellectual property. Understanding the nature of the attacker is, however, very important in assessing the extent to which organisations are likely to become a target.

As outlined above, cyber security is a challenge for the leadership of many organisations. This, however, cannot be an excuse to divest responsibility to the 'experts'. It is essential that company management take leadership in the following areas: (1) allocation of resources to deal with cyber security, (2) governance and decision-making and (3) building an organisational culture in which everyone is aware of his or her responsibilities.

Company management need to be able to navigate through the complexity of cyber security by gaining the confidence to ask the right questions. But how do you do that? This whitepaper provides some advice on getting the basics right.

Matthias Bossardt
Partner, Cyber Security

+41 58 249 36 98
mbossardt@kpmg.com

Gerben Schreurs
Partner, Forensic

+41 58 249 48 29
gschreurs1@kpmg.com

What is cyber crime and who is carrying it out?

Cyber crime is a range of illegal digital activities targeted at organisations 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 organisation that is sponsoring or conducting the attacks, is essential for effective defence.

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 Organised 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. A publication by the Dutch Cyber Security Centrum (NCSC; National Cyber Security Centre) has provided further analysis of the cyber security landscape in the Netherlands, as well as a detailed description of various cyber actors.

01 Introduction

Cyber security: The things you probably already know

The amount of data continues to grow exponentially as does the rate at which organisations share data through online networks. The Internet of Things – in which billions of machines, from tablets and smartphones to ATM machines, security installations, oil fields, environmental control systems and thermostats, are linked together – has left the realm of science fiction and is becoming reality.

The consequence is that, in heavily networked societies, inter-dependencies increase. Organisations increasingly open their IT systems to a wide range of (mobile) machines and – by definition – lose direct control of data security. Furthermore, business continuity, both in society and within companies, becomes increasingly dependent on IT. Disruption to these core processes can have a major impact on service availability.

Criminals and/or criminal organisations are, of course, also aware of these vulnerabilities. Attacks on governments' and companies' networks have increased in volume and severity. The motives of cyber criminals are various, from pure financial gain, to espionage or terrorism.

Organisations need to protect themselves against cyber attacks and ensure that an appropriate response can be provided. The three areas of capability – prevention, detection and response – must be in effect to achieve this (see frame).

The things you may not know

You are probably already familiar with what has been outlined so far, as cyber security has received significant attention in recent years.

Despite the pervasive nature of cyber security, organisations should not allow themselves to be driven by fear. The media often sketch an alarmist picture of cyber security, one in which all organisations are an easy target for cyber criminals. This leads to disproportionate fear. A small or mid-sized company has a

More information is provided below:

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

Detection
Through monitoring of critical events and central safety incidents, an organisation 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 plan as soon as an attack occurs. During an attack the organisation should be able to directly deactivate all technology affected. When developing a response and recovery plan, an organisation should perceive (information) security as a continuous process and not as a one-off solution.

very different risk profile than a multinational, for example small to mid-sized companies are not generally subjected to many of the incidents mentioned in the media. The truth is more nuanced than the picture painted by the media. The risks can be controlled. Cyber criminals are not invincible geniuses, and governments and companies are capable of fighting cyber crime.

But we do have to realise that 100% security is an illusion, and that chasing that 100% target will lead not only to frustration but also to a false sense of security.

In fact, we have to treat cyber security as 'business as usual' – an area of risk that requires the same level of attention as fire or fraud. These are themes that are dealt with from a risk management perspective, rather than being based on an idea of building a system that is 100% watertight.

Leading from this, we believe that many organisations need to change their outlook on cyber security. They should do this by playing to their strengths rather than their fears of what might happen. Investment should be balanced between risks and potential impacts.

	Prevention	Detection	Response
Management and organisation	Appointing cyber crime responsibilities	Ensuring a 24/7 stand-by (crisis) organisation	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 is probably one of the reasons why it is not always approached appropriately. From our years of experience, we have identified the five most common cyber security mistakes. These are discussed below.

1

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

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

Almost every airline company claims that flight safety is their highest priority whilst recognising that there is an inherent risk in flying. The same applies to cyber security. Every large, well-known organisation will unfortunately experience information being either stolen privately or stolen and made public.

Developing the awareness that 100% 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 defence posture is based on understanding the threat (i.e. the criminal) relative to organisational vulnerability (prevention), establishing mechanisms to detect an imminent or actual breach (detection) and establishing a capability that immediately deals with incidents (response) to minimise 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', however, you also understand immediately that more emphasis must be placed on prevention and response. After a cyber crime incident, which may vary from theft of information to a disruptive attack on core systems, an organisation must be able to minimise 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, for example 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 defence capability. Although this is generally led by the IT department (who should be aware of the importance of cyber security), 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 organisations 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. As mentioned in the introduction, this is often about changing the culture such that employees are alert to the risks and are proactive in raising these 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 defence is, by definition, always one step behind. But is this true? And is it useful to keep pursuing attackers and investing in increasingly sophisticated tools to prevent attack?

Of course it is important to keep up to date and to obtain insights into the intention of attackers and their methods. It is also sensible to adopt a flexible, proactive approach. Managers need to understand the value of their information assets and the implication of any loss on the core business (including business continuity), for example damage to the brand, reduced income, intellectual property going public. The cyber security policy needs to prioritise investment into these areas rather than try and cover all risks. In short, managers should be aware of the latest techniques but should not let this distract them from protecting their most important assets. A business case for cyber security should form the basis for investment and resource allocation. Important questions for managers in this respect include: Do we know to whom we are attractive and why? Do we know what risks we are willing to take in this respect (risk appetite)? Do we have insight into which systems store our key assets (and our business' continuity)?

Regarding that last question, an organisation may perceive the value of its assets differently from a criminal. It is therefore important to look at the value of assets from the perspective of both the organisation and the criminal[1]. In that respect, we should also realise that business and technology have developed as chains, and therefore organisations are co-dependent 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**

Only an organisation that is capable of understanding external developments and incident trends and able to use this insight to inform policy and strategy will be successful in the long term. Practice shows that cyber security is very much driven by compliance. This is understandable, because many

[1] See also "A nuanced vision on cyber crime", KPMG 2012

organisations have to accommodate a range of laws and legislations. However, it is counterproductive to view compliance as the ultimate goal of the cyber security policy.

Effective cyber security policy and strategy should be based on continuous learning and improvement.

This means:

- Organisations 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 organisations to make sensible security investment choices, including investing to save. Unfortunately, in practice, many organisations do not take a strategic approach and do not collect and use the internal data available to them.
- Organisations 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 organisation to learn and put better security arrangements in place in the future.
- The same applies to monitoring attacks. In many cases, organisations have excellent monitoring capabilities, but the findings are not shared with the wider organisation. No lessons, or insufficient lessons, are learned from the information received. Furthermore, monitoring needs to be underpinned by an intelligence requirement. Only if you are very certain of what you want to monitor does monitoring becomes an effective tool to detect attacks.
- Organisations need to develop a corporate 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 organisation 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 five most common cyber security mistakes

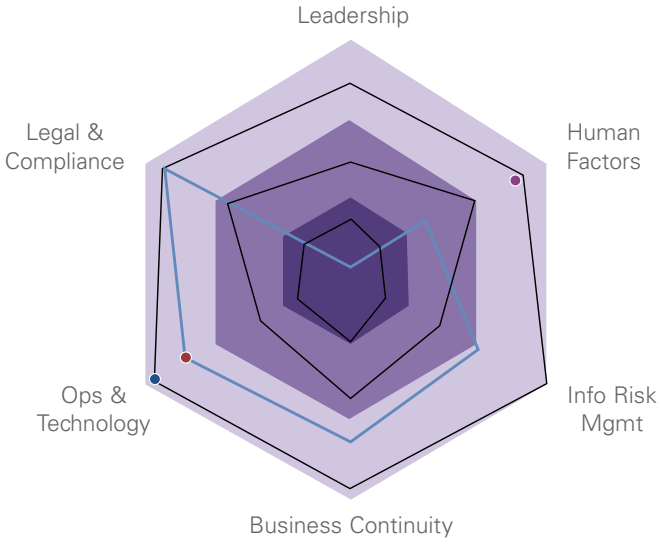
The risks faced by a local entrepreneur are very different from the risks faced by a globally-operating multinational. The latter is more visible to criminals, more dependent on IT, and the potential scale of the impact is greater. Both businesses, however, need to adopt a customised approach, based on the character of the organisation, the risk appetite and the knowledge available. At present this approach does not appear to be widespread.
As an example of a business that has a successful, realistic and, above all, customised approach to protecting its assets, we have compared the way in which a jeweller arrives at a proper level of security and the current common approach to cyber security of the business community.

Jeweller's perspective on theft security	Common 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% security.	I see cyber crime as something exotic and strive to achieve 100% 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 market place, 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 organisation 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

As a manager, how do you assess the cyber capability of your organisation?

As a manager, you want to know whether your organisation has an adequate approach to cyber security. At KPMG, we consider six key dimensions that together provide a comprehensive and in-depth view of an organisation'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 organisation and its delivery and supply partners?

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

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

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

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

- Minimising the risk of an attack on an organisation by an outside cyber criminal, as well as limiting the impact of successful attacks.
- Better information on cyber crime trends and incidents etc. to facilitate decision-making.
- Clear communication on the theme of cyber security. Everyone knows his or her responsibilities and knows what needs to be done when an incident has occurred or is suspected.
- Contributing to a better reputation. An organisation that is well prepared and has given careful consideration to its cyber security is better placed to reassure its stakeholders.
- Increased knowledge of and competence in relation to cyber security.
- Benchmarking the organisation in relation to peers in the field of cyber security.

Leadership and Governance
Board demonstrating due diligence, ownership and effective management of risk.

Business Continuity and Crisis Management
Preparations for a security event and ability to prevent or minimize the impact through succesful crisis and stakeholder management.

Human Factors
The level and integration of a security culture that empowers and ensures the right people, skills, culture and knowledge.

Operations and Technology
The level of control measures implemented to address identified risks and minimize the impact of compromise.

Information Risk Management
The approach to achieve comprehensive and effective risk management of information throughout the organization and its delivery and supply partners.

Legal and Compliance
Regulatory and international certification standards as relevant.

05 Conclusion... Time for action

Cyber security should be on your agenda. Your management, boards, shareholders and clients all expect you to pay sufficient attention to this problem. As such, your organisation needs to be able to answer the following questions.

1 How big is the risk for my organisation and the organisations I do business with?

This is where you should start when determining the risk profile of your organisation. How attractive is your organisation to potential cyber criminals? How dependent is your organisation on the services of other organisations? And finally, how much risk is your organisation willing to take, since there is no such thing as 100% security?

Key questions you can use to determine your risk profile and risk appetite:

- Do we know which processes and/or systems represent the greatest assets from a cyber security perspective?
- Have we considered how much risk we are willing to take in relation to these processes and/or systems (risk appetite)?
- How integrated/dependent is the organisation on services from partners and suppliers and how integrated are the corresponding IT processes?
- Do our partners have the same risk appetite and cyber security measures as us?
- Have we developed clear business cases for our cyber security investments?

2 Technology alone is not the answer: the answer also lies in a combination of governance, culture and behaviour. And you, as a manager,have an important role to play. Without your commitment, behavioural and cultural change in your organisation will not occur. How can such change be assured?

Key questions you can use to determine your current status:

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

3 As an organisation, how large should our cyber security budget be and how should we spend it?

This publication is a joint work prepared by:

Peter Kornelisse, Koos Wolters, Dennis van Ham, Ronald Heil, Harald Oymans, Stan Hegt, Tamara Kipp and John Hermans.

Depending on the risk profile of your organisation, the budget for cyber security should probably be in the range of 3%-5% 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:

- How much of our budget is spent on solving past problems and how much on structural investments in better security (security by design) of systems?

Ensuring your funds are spent appropriately on future system solutions is only part of the answer, however. Without good governance, proper cyber security processes and, of course, the appropriate culture and behaviours, these technological solutions will not prove their money's worth. The other question that needs to be answered is:

- How much of our cyber security budget is spent on systems and tools, and how much on awareness and culture change?

In short: it is time for action!

Contacts

KPMG AG
Badenerstrasse 172
PO Box
CH-8036 Zurich

kpmg.ch

Matthias Bossardt
Partner,
Cyber Security

+41 58 249 36 98
mbossardt@kpmg.com

The five most common cyber security mistakes June 2018