ICC CYBER SECURITY GUIDE FOR BUSINESS

INTERNATIONAL CHAMBER OF COMMERCE

The world business organization

ICC CYBER SECURITY GUIDE FOR BUSINESS

Acknowledgements

The ICC Cyber security guide for business was inspired by the Belgian Cyber security guide, an initiative of ICC Belgium and VBO-FEB, and the EY Belgium and Microsoft Belgium, with the B-CCENTRE and ISACA Belgium. Well-appreciated in Belgium, the Guide was offered to ICC's Digital Economy Commission as a model that could be adapted to serve as a global resource with the permission of the companies and organizations involved.

ICC kindly recognizes the contribution of those involved in the preparation and production of the Belgian guide as well as those members of the ICC Task Force on Cyber Security that developed the global guide.

ICC Publication No. 450/1081-5
ISBN: 978-92-842-0336-9

TABLE OF CONTENTS

FOREWORD

ICC Secretary General John Danilovich

The International Chamber of Commerce (ICC) has a proud, nearly hundred-year history of providing companies with tools and self-regulatory guidance to promote good business practice. As the world business organization, whose membership is composed of enterprises from all sectors and regions, ICC is especially pleased to provide business of all sizes this simple, clear guide to help business play their part in addressing the increasingly serious challenge of cyber security.

ICC is an organization dedicated to facilitating trade and investment, including to foster confidence in the digital economy and to increase the considerable opportunities that it brings to business, consumers, governments and society. Interconnectivity has transformed not just the marketplace but has changed the fabric of society. The benefits that flow from greater access to knowledge, information, goods and services are made possible by a global and open Internet. It needs to be trusted and secured. Therefore, any cyber security strategy should be appropriate, justified and proportionate, to preserve these benefits.

Because security – like perfection – is an elusive goal with multiple trade-offs, it can also be a daunting topic. Fear or lack of awareness can be a barrier to ensuring businesses evaluate risks and take suitable actions. This guide makes awareness a simple set of steps and takes down the intimidation barrier. ICC has produced the *Cyber security guide for business* to reach a broad audience with its over six million members in mind. It is intended to be accessible to business owners, staff or executives, not just limited to information technology teams, and it should be shared with business partners in the supply chain of goods and services and with the public sector to enhance resilience as broadly as possible.

The guide will be distributed through ICC's global network of national committees, member companies, business associations and chambers of commerce via the ICC World Chambers Federation, spanning over 130 countries. ICC believes that collective, global business action by its network and partners can make an essential contribution to reducing cyber risks for businesses and society at large.

CYBER SECURITY STARTS WITH YOU

Modern information and communications technologies are enabling businesses of all sizes to innovate, reach new markets and drive efficiencies that benefit customers and society. Yet, increasingly, business practices and policies are challenged by having to adapt to the direct and indirect impacts of pervasive communication environments and network information flows that are required in the delivery of goods and services. Many enterprises adopt modern information and communications technologies without fully realizing that new types of risks must be managed as a result. This guide addresses this gap and outlines how enterprises of all sizes can identify and manage cyber security risks.

Failures in cyber security are constantly in the press with reports of malicious actors breaching enterprises large and small – seemingly at will and with ease. Enterprises are now exposed to a growing source of risk[1] as criminal actors, hackers, state actors and competitors grow increasingly sophisticated in taking advantage of weaknesses in modern information and communications technologies. The combination of information systems with various external devices[2] increases the level of complexity and threats to enterprise information systems. Enterprises not only face external threats but must also manage the risks of internal threats to their information systems, with persons within the organization able to corrupt data or take advantage of enterprise resources from the comfort of their residence or the local coffee shop. From a business perspective, it is vital that a company – large or small – be able to identify their cyber security risk and effectively manage threats to their information systems. At the same time, all business managers including executives and directors must recognize that cyber risk management is an on-going process where no absolute security is, or will be, available.

Unlike many business challenges, cyber security risk management remains a problem with no easy fix available. It requires a consistent application of management attention with a tolerance for bad news and discipline for clear communication. Many excellent resources are available providing comprehensive explanations on top cyber threats, yet suitable material to assist business management in their approach to cyber security remains scarce. **This document will help business management** of small and large organizations **interact with their information technology managers** and **guide in the development of cyber security risk management practices**.

1 Examples of external cyber security threats which are increasing are malicious software (such as Intrusion software, code injection, exploit kits, worms, trojans, etc.) denial of services, data breaches and others. For a relevant update see e.g. ENISA Threat Landscape 2014, EL 2014 at https://www.enisa.europa.eu

2 Such as mobile phones, modems, payment terminals, automatic software updates, industrial control systems, vendor/customer interaction, as well as Internet of Things.

READ THIS FIRST

Improving an organization's cyber security is possible through a risk management process – with an emphasis on management. Because of a constantly shifting landscape of technology and threat vectors, enterprise information systems will never be complete, and they will never be completely secure. Operating effectively in such a changing environment requires a commitment to a long-term approach to risk management – without an end state. Business managers will remain frustrated with cyber security initiatives if they do not approach the work with suitable expectations for the task at hand. And without suitable constraints, enterprises can quickly consume all available resources in a quest to mitigate cyber risk. Approaching cyber security risk management through a process that enables an enterprise to understand and prioritize what is important for the organization (physical and information assets) is essential.

It is critical to be aware that **without suitable precautions, the Internet, enterprise information networks and devices are not secure**. Modern enterprise information systems are targets for a range of malicious actors. One useful concept to set expectations of those engaged in cyber security risk management is a simple refrain: "If something of value is online, it is at risk, and is likely compromised." Fortunately, what is valuable to one malicious actor does not always align with assets (such as money, business secrets and customer information) deemed valuable by your enterprise. While there are techniques and processes that can help to reduce the risk of compromise, a determined malicious actor benefits from the weakest link of interconnected systems. There are numerous potential vulnerabilities (organizational, human as well as technical) present across an enterprise. Despite the best work of technology vendors, service providers and employees within your organization, no absolute security is available. Therefore, cyber security risk management processes must assess the unique threats to and weaknesses of your enterprise and align these against the priority assets of the organization.

Despite the bleak outlook outlined above, enterprises of all sizes can develop and nurture key organizational capabilities to succeed at cyber security risk management.

- Firstly, business management must undertake a risk analysis for their organization and prioritize assets that require the most protection.
- Secondly, leadership is necessary to take necessary action and ensure information security best practices are employed by the enterprise.
- Thirdly, organizations must be prepared to detect and respond – internally and externally – to cyber events via institutionalized organizational processes.

Response activities will require enhanced communication among peers, relevant government actors, customers and even competitors. Preparation in advance of any cyber incident will ensure the initial problem is not compounded by preventable mistakes made during the response. Finally, mechanisms to learn from cyber incidents and modify practices are essential to drive institutional change necessary to promulgate cyber security risk management best practices throughout the enterprise.

USING THIS GUIDE

Over the last decade, governments, organizations and individuals developed numerous volumes on tackling the challenge of information security in cyberspace. So many documents and guidelines exist that it can be difficult to identify where to start reading and what kind of document is appropriate to your organization. The range of material available is considerable (in increasing specificity):

- **Guidelines** – High-level vision statements that scope concern for cyber security and provide a charter for organizations and individuals. Examples: OECD Security Guidelines, etc.
- **National strategies** – Often based on guidelines, these documents articulate an approach to cyber security tailored to a specific national or legal context. Examples: International Strategy to Secure Cyberspace[3], national strategies from Europe and other states[4], etc.
- **Frameworks** – Taking national strategies to a next step, frameworks gather a catalogue of prioritized or evaluated resources that help organizations to benchmark their maturity and progress in addressing cyber security risk. Examples: National Institute of Standards and Technology (NIST) Cybersecurity Framework[5], etc.
- **Standards of practice** – Documents that guide or govern organization processes to ensure robust and consistent operation of cyber security best practices. Examples: ISO 27001, 27002, 27032 process standards, PCI Security Standards, etc.
- **Technical standards** – Detailed specifications for implementation of interfaces to address specific types of interoperability requirements. Examples: HTTPS, AES, EMV, PCI payment standards, etc.

Firstly, this straightforward guide informed by global cyber security guidelines and national strategies offers businesses a framework to consider the question of security online – starting with a set of **five principles** for enterprises of all sizes as they approach cyber security risk. Secondly, this guide identifies **six key actions** that companies should be sure they are taking, drawing on materials from various sources and best practices. The guide then addresses **how to apply the initial five principles into policies** to guide development of an organization's cyber security risk management activities. An evolving digital appendix of resources to complement this guidance serves as a living resource to provide more specific advice as these materials are developed – from standards of practice to technical standards and more. While no absolute security is available, the cyber security risk management concepts outlined will help companies rise to the challenge of information security in this constantly changing environment. It is not just a guide of value for individual businesses but a guide to share with those in the chain of relationships with your organization to better secure all points of entry and exchange with your systems and activities.

3 http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

4 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

5 http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

USING THIS GUIDE

While approaches to information security may differ from company to company depending on a number of factors[6] there are a number of high-level principles that inform sound information security practice for all companies, independent of size or industry. This guide presents **five key principles** across two categories:

A. Vision and mind-set

B. Organization and processes

These principles are complemented by a set of six critical **security actions** and then **five starting elements to apply these principles** and bolster a company's information security policies.

Collectively, the suggested principles and actions in this guide will improve a company's resilience against cyber threats and limit disruption associated with a security breach.

A. VISION AND MIND-SET

Principle 1: Focus on the information, not on the technology.

You are the organization's first line of defence against cyber threats and will help to set the tone for your organization's approach to information security. As such, think of information security in its broadest sense, not just in terms of information technology.

Information security is a combination of people, processes and technology that is a business-wide issue, not just an Information Technology (IT) issue. Implementation of security measures should not be limited to the IT department but rather be reflected throughout the company in all its undertakings. The scope and vision of information security therefore includes people, products, plants, processes, policies, procedures, systems, technologies, devices, networks and information.

People are key. Identifying and managing information assets' vulnerabilities and threats can be an enormous task. However, based on experience[7], 35% of security incidents are a result of human error rather than deliberate attacks. More than half of the remaining security incidents were the result of a deliberate attack **that could have been avoided** if people had handled information in a more secure manner.

Focus security efforts specifically on the protection of your most valuable information and systems where loss of confidentiality, integrity or availability would seriously harm the company. This does not mean that other information assets can be ignored in terms of security. It implies that a risk-based approach with focus on the "crown jewels" of the organization is an efficient and effective approach to information security in practice. At the same time, it recognizes that 100% risk elimination is neither possible, nor required compared to the associated costs.

6 Including the nature of the business, risk level, environmental factors, interconnection level, regulatory requirements and size of the company, among many others.

7 EY – 2012 Global Information Security Survey – Fighting to close the gap

Principle 2: Make resilience a mind-set

The objective should be the resilience of the company to risk of information loss or damage. Companies are subject to many laws and regulations, many of which require the implementation of appropriate security controls. Compliance with these laws, regulations and standards can lead to improved information security; however, it can also lead to complacency once compliance objectives are achieved. Security threats change much faster than laws and regulation, creating a moving target for risk management activities. As a result, existing business policies and procedures may be obsolete or simply ineffective in practice.

Periodic assessment of a company's resilience against cyber threats and vulnerabilities is essential to measure progress towards risk management goals and adequacy of cyber security activities. Assessment activities can be accomplished through internal and/or independent assessments and audits including measures such as penetration testing and intrusion detection.

Responsibility for cyber security must go beyond the IT department, the decision-making stakeholders should be involved in identifying the problem, but also in the long term in implementing a healthy ecosystem in the organization. Yet, the true value of periodic business review materializes when the process is used to improve company culture and employee mind-set towards cyber security risk management practices.

A mind-set for resilient information systems is most critical during times when new solutions and devices are adopted by the business. During this time, appropriate security measures must be considered as early as possible in the adoption period, ideally during the identification of business requirements. Such "security by design" can empower employees, who make innovations happen in a company, to focus on information security risk management.

B. ORGANISATION AND PROCESSES

Principle 3: Prepare to respond

Even the best protected enterprise will at some point experience an information security breach. We live in an environment where this is a question of **when**, not **if**. Therefore, how a business **responds** to a breach is where **you** will be evaluated.

In order to minimize business impact of cyber security incidents, enterprises must develop organizational response plans in addition to technical response measures. A response plan should establish guideposts to help business managers understand when to engage specialized third parties to help contain and remedy a security incident, and when it is appropriate to contact other external parties (including law enforcement or government oversight agencies). Keep in mind that reporting to appropriate authorities is a way to improve the overall security landscape and in some cases can be mandatory in order to avoid regulatory violations and fines. Successful incident response management includes a communication strategy (internal and external), which can make the difference between ending up as an embarrassing headline on page one of the newspaper, or a successful business case study in a university curriculum.

While internal risk management activities are essential, remember to also take time now to engage with peers and partners across your company's industry, the wider business community and with law enforcement to help to maintain an understanding of current and emerging threats, and also to build relationships that can be relied upon during an incident.

Principle 4: Demonstrate a leadership commitment

In order to manage information security effectively and efficiently, business leadership must understand and support risk management activities as an essential element for success of your organization**. You** and your management team should visibly engage in the management and oversight of your company's cyber security risk management policies. They should ensure that adequate resources – both human and financial – are allocated to protection of company assets. But resources alone are not sufficient; an information security function

for enterprises, both large and small, should be empowered to enable a company-wide response to cyber threats and vulnerabilities.

The effectiveness and adequacy of the company's information security measures should be formally reported to the highest business manager of your company, and at least once a year to the management team, the auditors, and the board of directors. On a regular basis, these reports – based on various security indicators and metrics – should help to inform decision-making for information security policy and investments, and provide insight into how well your company is protecting its assets.

Although often referred to as the *weakest link* when it comes to information security – educate your people into being the *greatest asset to good security* by creating information security awareness that leads to effective skills.

Principle 5: Act on your vision.

Just reading this guide is not enough – you must translate your unique company vision for cyber security risk management into practice by creating (or revising) various information security policies. Corporate information security policies provide a standard baseline to guide security activities across the company for all business units and staff while also increasing security awareness throughout the business.

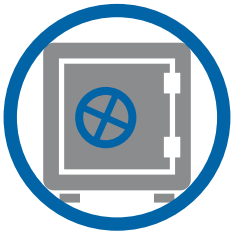
Typically, a security policy document and its supporting guidelines and standards are assembled into an information security policy framework that is subsequently translated into normal operational procedures. However, with increasing adoption and integration of third-party service providers into business value chains, organizations must understand how their information assets flow among, and are interdependent on, various external parties. If a third party is not adequately protecting your information (or their information systems on which you rely), **their** security incident may become a serious liability to **your** business operations, reputation and brand value. Encourage suppliers to adopt at least the information and information security principles applied within your company where appropriate conduct audits or request service providers detail their information security practices to gain additional assurance in their business practices.

Third parties are not just sources of risk – some may help to reduce risk and enable you to meet critical cyber security risk management objectives. Information technology service providers can help to improve your cyber security risk management infrastructure, including through security assessments and audits and through the use of information security devices and solutions or services, whether on-site, managed externally or cloud-based[8].

8 Cloud services are solutions whereby you use an outside service provider to store, process or manage data over a network like the Internet with a very high degree of flexibility and real-time monitoring.

This action list is a set of practical steps that enterprises of all sizes can take to reduce risk associated with cyber security incidents. While not comprehensive or exhaustive, ensuring your business is engaged in these activities will set a proper course towards information security excellence.

You should remember that cyber security risk management is an on-going process. Once you are satisfied that these initial activities are underway, look to the web portal associated with this guide and identify standards and resources that will help you to take further steps to increase the resilience of your information security programme.



Action 1: Back up business information; validate restore process

Ensure your business information is protected by making a back-up – before your business is subject to a security breach where information is stolen, altered, erased or lost. Just making a back-up is insufficient[9]. A proper management of back-up processes includes validating the content of the business data and information contained in the back-up files as well as testing restored processes. If third parties are used for the storage of information (e.g. cloud-services), ensure back-up provisions are also made for that information.

Keep in mind that physical media, such as a disc, tape or drive used to store data back-ups, are vulnerable to risks as well. Back-up material must enjoy the same level of protection as the source data, especially with regard to physical safety as those items are easily moved.

Action 2: Update information technology systems

Systems and software of all kinds, including network equipment and devices, should be updated as patches and firmware upgrades become available. These upgrades and security patches fix system vulnerabilities that attackers could abuse. Many successful breaches result from system vulnerabilities where updates are available, often even more than a year prior to the incident.

9 A back-up procedure is a technical process that must be managed properly. For example, just using several simultaneously connected storage repositories at the same site is insufficient as a back-up procedure. An effective back-up policy needs to consider multiple types of risk including data loss as well as operating location loss, among other concerns, typically requiring that back-up copies are physically located off-site.

When possible, use automated updating services; especially for security systems such as anti-malware applications, web filtering tools and intrusion detection systems. Automating update processes can help to ensure that users apply valid security software updates directly from the original vendor.

Action 3: Invest in training

Establishing baseline awareness about important cyber threats and security topics is essential for your personnel throughout your company and should recur continually. Training[10] ensures that all personnel, who have access to information and information systems, understand their daily responsibilities to handle, protect and support the company's information security activities. Without suitable training, employees can quickly become sources of risk within the enterprise, creating security incidents or vulnerabilities that adversaries can use to breach your information security measures.

You **can** establish a culture of information security risk management in your business. Investment in training will reinforce business information security messages to staff over time, and will develop desired security skills and attributes in personnel.

Action 4: Monitor your information environment

Enterprises must deploy systems and processes to ensure that they are alerted if an information security incident is happening within their organization. All too often businesses are unaware of a security breach; some businesses experience breaches or infections for months or years before someone detects the intrusion.[11] Various technology solutions exist to assist with this task including intrusion detection and prevention systems and security incident management; however, simply installing these solutions is insufficient. Continuous monitoring and analysis of the outputs from these systems is necessary to benefit from the technology.

Many enterprises may not have internal expertise or resources required to monitor vital systems and processes. On-site and managed

10 General cyber security information and awareness for end users can be found on www.staysafeonline.org. http://www.enisa.europa.eu/media/multimedia/material, an initiative of ENISA. You are authorised to use all this information, videos, and infographics for education purposes within your company

11 http://www.verizonenterprise.com/DBIR/

security services are available from various providers under different business models including cloud-based technology and services. Find the right fit for your organization and seek assistance from experienced parties for advice, and support to include appropriate terms in contracts.

If your company is experiencing a cyber-incident, consider reporting the activity to appropriate government agencies[12] and industry associations – communication with others can help to determine if your business is experiencing an isolated event, or is part of a larger cyber incident.[13] Often, outreach can result in information and advice that can help a business take effective countermeasures.

Action 5: Layer defences to reduce risk

Network perimeter security and traditional access control are no longer sufficient, especially when the enterprise information system connects to the Internet, Internet service providers, outsourcing and cloud services, vendors and partners, as well portable devices, which are outside the company´s reach and control. Effective protection against viruses, malicious software or devices and hackers requires layers of defensive measures to reduce the risk of an information security incident. Combining multiple techniques[14] to address cyber security risk can significantly reduce the chance a small breach will turn into a full-blown incident.

Layered information security defences work to limit the degrees of freedom available to adversaries and increase opportunities for detection by enterprise monitoring systems.

Cyber risk insurance can be a way for companies to mitigate the financial consequences of an incident, but also to proactively manage exposures, and strengthen a company's internal risk management.

12 Victims of (cyber) crime should also file a complaint with appropriate law enforcement officials. The local police is often the best point of contact for traditional crime, however more specialized law enforcement authorities may specialize in cybercrime (hacking, sabotage, espionage).

13 An attack can be horizontal (companies from the same sector are targeted) or vertical (subcontractors are targeted) or can be a security threat specific to a particular item of software or hardware.

14 Including web filtering, antivirus protection, proactive malware protection, firewalls, strong security policies and user training, to name just a few.

Action 6: Prepare for when the breach occurs

Risk management is not only about diminishing probability, but also about minimizing the potential damage of an event occurring. This means preparing to quickly investigate an incident – ensuring that adequate resources will be at hand and systems and processes are tuned to capture critical information. If the breach is the penetration of a malicious programme, it needs to be eliminated. Preparation also means having an organizational plan to make good decisions quickly and coordinate the necessary actions to take control of an incident. Who will respond and how? Your team can shape the outcome through well-designed actions and effective communication.

Finally, advance preparation can minimize some of the most damaging elements of a breach – loss of operability, lack of access to data, inability to resume business in a timely manner. Business continuity and recovery planning minimizes this loss by focusing on priorities and preparing in advance.

APPLYING PRINCIPLES TO AN INFORMATION SECURITY POLICY

A frequent task for business management is translating principles provided by documents like this into policies and practices that make sense for their organization. Making that task easier to complete is the objective of this section. Organized by the five key security principles outlined in this Guide, the following elements offer starting points for development of your organization's cyber security risk management policy and practices.

Focus on the information, not the technology

- Create a function and nominate a person leading and facilitating information security initiatives, while the accountability of security remains shared across the company.
- When planning how to achieve its information security objectives, an organization should determine the following:
  - What will be done;
  - What resources will be required;
  - Who will be responsible;
  - When it will be completed;
  - How the results will be evaluated.[15]
- In the event where a business does not have sufficient internal security experience, seek out additional information and cyber security experts to help to embed information security into the design of business process and information systems.

Establish a resilience mind-set

- Information security activities should be aligned – and where possible integrated – with compliance and other risk mitigation efforts to reduce overlapping initiatives and responsibilities.
- Risk aversion should not block the introduction of new technologies. Information security approaches can position a company for introduction of new and innovative technologies in addition to reaching cyber security risk management objectives.
- Make sure security is taken into account in each and every project your enterprise is carrying out, especially new projects. When included from the outset, with the right business involvement, security does not significantly increase projects cost and duration. But when security is added later, or – worst case – after a breach has occurred, then cost overruns, delays and other impacts are several orders of magnitude higher.

15 ISO/IEC 27001:2013

- Determine what devices – with a focus on mobile devices, such as those of your staff or business partners – may access the company network and/or information[16], and consider how to manage software and security settings on company equipment.
- Evaluate access to data to ensure controls are in effect to preserve the confidentiality, integrity and availability of information.
- Managers should receive, review and validate users (internal and external) who have access to applications and data in their department – access is a responsibility and a risk so suitable control over employees' access to data and information systems is advisable.
- Develop reporting procedures for lost or stolen equipment and, where possible, remote wiping functionalities to delete all company information from lost or stolen devices.

Prepare to respond

- Everyone makes mistakes and companies that turn such information security mishaps into an opportunity for an open review about security incidents can create a culture where employees are not afraid to report security incidents when they happen.
- Empower selected personnel to share appropriate information with peers and other stakeholders within the industry, both to help build leading practice and warn of potential upcoming attacks.
- Designate a responsible party to ensure a proper safeguarding of evidence from the start when dealing with a security incident and in particular a case of cybercrime.[17]
- Determine how and when to report information security incidents to cyber emergency response teams (also known as CERTs), government agencies or law enforcement officials.

16 Require users to configure the appropriate mobile device security settings to prevent criminals from stealing information via the device.

17 Guidelines for data acquisition in security incidents for investigation purposes by ICT staff or in case of malware infection, are available online at: http://cert.europa.eu/cert/plainedition/en/cert_about.html

Leadership matters

- Personnel should be accountable for information and its protection and should have the right authority, access to the top management, tools and training to prepare them for their responsibilities as well as the threats they might encounter.[18]
- Small companies should have someone within or outside their company who regularly checks the adequacy of the information security and formally takes the responsibility for information security. Although this might not be a full-time role, it is an important one that can prove vital for the survival of the company.
- In large companies, the allocation of functions, roles and responsibilities should be a deliberate mix of individuals and (virtual) working groups and committees. Each team member should clearly know his/her responsibility and accountability. Proper documentation and communication is essential in this case.

Act on your vision

- Control access to (and from) your internal network, prioritizing access to services and resources essential to business and employee needs.[19]
- Enforce the use of strong passwords and consider implementing strong authentication methods[20] that require additional information beyond a password to gain entry.
- Use encryption where appropriate to secure data at rest and in transit,[21] with a particular focus on public network connexions and on portable devices such as laptops, USB keys and smartphones that are easy to lose or are targets for theft.

18 An important threat employees should be trained on, is social engineering. Social engineering is the technique of manipulating people into performing actions to divulge sensitive or confidential information.

19 Consider filtering services and websites that increase security risks for company resources, for example peer-to-peer file sharing and pornographic websites. Filtering rules should be transparent to all users in the organisation and include a process to unblock business websites which may be inadvertently denied.

20 Multi-factor authentication uses a combination of elements, such as things I know (e.g. password or PIN), things I have (e.g. a smartcard or SMS) and thing I am (e.g. fingerprint or iris scan).

21 For example as email sent over the Internet is often in clear text companies should consider methods to encrypt email when sensitive information is transmitted.

APPLYING PRINCIPLES TO AN INFORMATION SECURITY POLICY

- Create a detailed backup and archive policy aligned with legal and regulatory requirements for retention of information detailing:
  - What data is backed up and how;
  - How often data is backed up;
  - Who is responsible for creating back-ups and validating the content;
  - Where and how the back-ups are stored;
  - Who has access to those backups;
  - How restore processes work (and are tested).

- Develop training programmes on information security awareness, including topics such as:
  - Communicating safely and responsibly;
  - Using social media wisely;
  - Transferring digital files in a safe way;
  - Proper password usage;
  - Avoiding losing important information;
  - Ensuring only the right people can access your information;
  - Staying safe from viruses and other malware;
  - Who to alert when you notice a potential security incident;
  - How not to be tricked into giving information away.

SECURITY SELF-ASSESSMENT

The following section presents a simple checklist as a tool for management to help guide their internal review of their company's cyber resilience capabilities, and to enable them to ask the right questions to the teams involved in these initiatives. The questions asked in the tool can help them to identify specific strengths and weaknesses – and paths to improvement within their respective company.

At the same time, this self-assessment questionnaire can be used as a checklist by companies that are just beginning in their information security initiatives, and want to use the information as a basis for planning their cyber resilience capabilities.

For each of the questions below, companies should identify from the provided options the one that is the most accurate reflection of the current practices of the company. Each of the options has been given a bullet colour, where:

- This is the least desirable response; Improvement should clearly be considered.
- Additional improvement is possible to better protect the company.
- This answer is the best reflection of resilience against cyber threats.

The answers to the questionnaire are the unique response of each evaluator, the presence of a *more specific checklist under each question* is intended to help identify and document the status of a set of basic information security controls for your company. The information gathered in this question process will help highlight gaps or vulnerabilities so companies using this guide know where they need to take action next.

1

Do you evaluate how sensitive information is handled within your company?

✖ No, but we have a firewall to protect us from theft of information.

! Yes, we understand the importance of our information and implement general security measures.

✔ Yes, and we have an information classification model and know where our sensitive information is stored and processed. We implement security measures based on the sensitivity of the information.

The questions below are offered as a basic information security checklist for your company to help assess where you are in the process.	YES	NO
Is your sensitive data identified and classified?		
Are you aware of your responsibility regarding the identified sensitive data?		
Is the most sensitive data highly protected or encrypted?		
Is the management of personal private information covered by procedures?		
Are all employees able to identify and correctly protect sensitive and non-sensitive data?		

2

Do you perform information security-related risk assessments?

- ✖ We do not perform risk assessments.
- ! We perform risk assessments but not on any specific information security-related topics.
- ✔ We perform risk assessments on specific information security topics.

The questions below are offered as a basic information security checklist for your company to help assess where you are in the process.	YES	NO
Do you address vulnerability results in order of high risk to low risk?		
Are events that could cause interruptions to business processes identified and is the impact of the potential related interruptions assessed?		
Do you have a current business continuity plan that is tested and updated on a regular basis?		
Do you regularly perform a risk assessment to update the level of protection the data and information need?		
Are areas of risk identified throughout your business processes to prevent information processing corruption or deliberate misuse?		

3

At what level is information security governance implemented?

- ✖ There is no information security governance in place.
- ! Information security governance is installed within the IT department since that is where the information needs to be secured.
- ✔ Information security governance is installed at the corporate level to ensure an impact on the entire company.

The questions below are offered as a basic information security checklist for your company to help assess where you are in the process.	YES	NO
Do board members and the CEO allocate an information security budget?		
Is information security part the existing risk management of the directors?		
Does management approve the information security policy of the company and communicate it by an appropriate way to the employees?		
Are board members and management informed on a regular basis of the latest developments in information security policies, standards, procedures and guidelines?		
Is there at least one officer part of the management structure in charge of the protection of data and the privacy of personal information?		

4

Do you have an information security team or a dedicated information security function within your company?

- ✖ We do not have an information security team or specific roles and responsibilities concerning information security.
- ! We do not have an information security team but we have defined specific information security roles and responsibilities within the company.
- ✔ We have an information security team or a dedicated information security function.

The questions below are offered as a basic information security checklist for your company to help assess where you are in the process.	YES	NO
Does an identified information security specialist or team coordinate in-house knowledge and provide help to the management in decision-making?		
Is the identified information security specialist or team responsible for reviewing and systematically updating the information security policy based on significant changes or incidents?		
Has the identified information security specialist or team enough visibility and support to intervene in any information-related initiative in the company?		
Are there different managers responsible for separate types of data?		
Are the information security policy's feasibility and effectiveness as well as the information security team's efficacy regularly reviewed by an independent body or auditor?		

5

How does your company deal with information security risks from suppliers who can access your sensitive information?

✖ We have a relationship based on mutual trust with our suppliers.

! For some contracts we include information security-related clauses.

✔ We have processes in place to validate access for suppliers and specific security guidelines are communicated and signed by our suppliers.

The questions below are offered as a basic information security checklist for your company to help assess where you are in the process.	YES	NO
Are contractors and suppliers identified by an ID badge with a recent picture?		
Do you have policies addressing background checks for contractors and suppliers?		
Is access to facilities and information systems automatically cut off when a contractor or supplier ends his mission?		
Do suppliers know how and to whom to immediately report in your company any loss or theft of information?		
Does your company ensure suppliers keep their software and applications updated with security patches?		
Are clear security requirements defined inside contractual agreements with contractors/suppliers?		

6

Does your company evaluate computer and network security on a regular basis?

- ✖ We do not perform audits or penetration tests to evaluate our computer and network security.
- ! We do not have a systematic approach for performing security audits and/or penetration tests but execute some on an ad hoc basis.
- ✔ Regular security audits and/or penetration tests are systematically part of our approach to evaluate our computer and network security.

The questions below are offered as a basic information security checklist for your company to help assess where you are in the process.	YES	NO
Do you test on a regular basis and keep records of identified threats?		
Do you have procedures to evaluate human threats to your information systems, including dishonesty, social engineering and abuse of trust?		
Does your company request security audit reports from its information service providers?		
Is the utility of each type of stored data also assessed during the security audits?		
Do you audit your information processes and procedures for compliance with the other established policies and standards within the company?		

7

When introducing new technologies, does your company assess potential information security risks?

- ✖ Information security is not part of the process for implementing new technologies.
- ! Information security is only implemented in the process for new technologies on an ad-hoc basis.
- ✔ Information security is included in the process for implementing new technologies.

The questions below are offered as a basic information security checklist for your company to help assess where you are in the process.	YES	NO
When considering implementing new technologies, do you assess their potential impact on the established information security policy?		
Are there protective measures to reduce risk when implementing new technologies?		
Are the processes to implement new technologies documented?		
When implementing new technologies, could your company rely on partnerships, to enable collaborative efforts and critical security information sharing?		
Is your company's information security policy often considered as a barrier to technological opportunities?		
Does the company manage the new technology using a security system development methodology within systems' life cycle?		

8

Does information security training take place within your company?

- ✖ We put trust in our employees and do not consider information security guidance as added value.
- ! Only our IT personnel receive specific training for securing our IT-environment.
- ✔ Regular information security awareness sessions are organised for all employees.

The questions below are offered as a basic information security checklist for your company to help assess where you are in the process.	YES	NO
Are some information security awareness sessions adapted to the activity field of the employees?		
Are employees taught to be alert to information security breaches?		
Does your company have a guideline for users to report security weakness in, or threats to, systems or services?		
Do employees know how to properly manage credit card data and private personal information?		
Do third-party users (where relevant) also receive appropriate information security training and regular updates in organizational policies and procedures?		

9

How do you use passwords within the company?

✖ We share passwords with other colleagues and/or no policy exists for the safe usage of passwords or for the regular change of passwords.

! All employees, including the management, have unique passwords but complexity rules are not enforced. Changing passwords is optional, but not mandatory.

✔ All employees, including the management, have a personal password that must meet defined password requirements and must be changed regularly.

The questions below are offered as a basic information security checklist for your company to help assess where you are in the process.	YES	NO
Has your company established and enforced a globally-accepted password policy for all company assets?		
Can you assure the following about all passwords in your company? They are not stored into easily accessible files; They are not weak or blank or left as the default setting; They are not left unchanged or only rarely changed, particularly for mobile devices.		
Do you feel well protected against unauthorized physical access to systems?		
Are users and contractors aware of their responsibility to protect unattended equipment as well (i.e. to logoff)?		
Have employees been taught how to recognise social engineering tricks that deceive people into divulging security details and do they know how react to this threat?		

10

Is there a company policy in place for the appropriate use of the Internet and social media?

✖ No, there is no policy in place for the appropriate use of the Internet.

! Yes, a policy is available on a centralised location accessible to all employees but has not been signed by the employees.

✔ Yes, a policy for the appropriate use of the Internet is part of the contract / all employees have signed the policy.

The questions below are offered as a basic information security checklist for your company to help assess where you are in the process.	YES	NO
Are there general communication guidelines and processes for employees in the company, including relation to the press and social media?		
Is there a disciplinary process for employees violating the company's communication guidelines?		
Does an identified communications manager or team screen the Internet in order to assess e-reputation risks and status?		
Has your company assessed its liability for acts of employees or other internal users or attackers abusing the system to perpetrate unlawful acts?		
Has your company taken measures to prevent an employee or other internal user to attack other sites?		

11

Does your company measure, report and follow-up on information security related matters?

- ✖ We do not monitor, report or follow-up on the efficiency and adequacy of our implemented security measures.
- ! Our company has implemented tools and methods to monitor, report and follow up the efficiency and adequacy of a selection of our implemented security measures.
- ✔ Our company has implemented the necessary tools and methods to monitor, report and follow up on the efficiency and adequacy of all our implemented security measures.

The questions below are offered as a basic information security checklist for your company to help assess where you are in the process.	YES	NO
Are audit trails and logs relating to the incidents maintained and proactive action taken in a way that the incident doesn't reoccur?		
Does your company verify compliance with regulatory and legal requirements (for example data privacy)?		
Has your company developed some own tools to assist the management in assessing the security posture and enabling the company to accelerate its ability to mitigate potential risks?		
Does an information security roadmap including goals, progress evaluation and potential collaborative opportunities exist in your company?		
Are monitoring reports and incidents reported to authorities and other interest groups such as a sector association?		

12

How are systems kept up-to-date within your company?

- ✖ We rely on automatic patch management, provided by the vendor, for most of our solutions.
- ! Security patches are systematically applied on a monthly basis.
- ✔ We have a vulnerability management process in place and continuously seek information concerning possible vulnerabilities (e.g. through a subscription of a service that automatically sends out warnings for new vulnerabilities) and apply patches based on the risks they mitigate.

The questions below are offered as a basic information security checklist for your company to help assess where you are in the process.	YES	NO
Is vulnerability scanning a regular scheduled maintenance task in the company?		
Is the application system reviewed and tested after any change in the operating system?		
Can users check for themselves on the existence of unpatched applications?		
Are users aware that they also have to keep the operating system and applications up-to-date including security software of their mobile devices?		
Are users trained to recognize a legitimate warning message such as permission request to update (distinguished from fake antivirus requests), and to properly notify the security team if something bad or questionable has happened?		

13

Are user access rights to applications and systems reviewed and managed on a regular basis?

✖ Access rights to applications and systems are not consistently removed nor reviewed.

! Access rights to applications and systems are only removed when an employee is leaving the company.

✔ An access control policy is established with regular reviews of assigned user access rights for all relevant business applications and supporting systems.

The questions below are offered as a basic information security checklist for your company to help assess where you are in the process.	YES	NO
Is access to electronic information systems and facilities limited by policies and procedures?		
Does your company rely on a privacy policy stating the information it collects (for example about your customers: physical addresses, email addresses, browsing history, etc.), and what is done with it?		
Do the policies and procedures specify methods used to control physical access to secure areas such as door locks, access control systems or video monitoring?		
Is access to facilities and information systems automatically cut off when members of personnel end employment?		
Is sensitive data classified (highly confidential, sensitive, internal use only.) and are its users, which are granted access, inventoried?		
Are processes developed to regulate remote access to company electronic information systems?		

14

In your company, can the employees use their own personal devices, such as mobile phones and tablets, to store or transfer company information?

✖ Yes, we can store or transfer company information on personal devices without the implementation of extra security measures.

! A policy exists that prohibits the use of personal devices to store or transfer company information but technically it is possible to do so without implementing extra security measures.

✔ Personal devices can only store or transfer company information after the implementation of security measures on the personal device and/or a professional solution has been provided.

The questions below are offered as a basic information security checklist for your company to help assess where you are in the process.	YES	NO
Does your company rely on a well-accepted 'bring your own device' policy?		
Are mobile devices protected from unauthorized users?		
Are all devices and connections permanently identified on the network?		
Is encryption installed on each mobile device to protect the confidentiality and integrity of data?		
Is the corporate level aware that while the individual employee may be liable for a device, the company is still liable for the data?		

15

Has your company taken measures to prevent loss of stored information?

- ✖ We have no back-up/availability process in place.
- ! We have a back-up/availability process but no restore tests have been performed.
- ✔ We have a back-up/availability process in place that includes restore/resilience tests. We have copies of our back-up stored in another secured location or are using other high-availability solutions.

The questions below are offered as a basic information security checklist for your company to help assess where you are in the process.	YES	NO
Are there enough members of the staff able to create retrievable back-up and archival copies?		
Is the equipment protected from power failures by using permanence of power supplies such as multiple feeds, uninterruptible power supply (ups), back-up generator etc.?		
Is the back-up media regularly tested to ensure that it could be restored within the time frame allotted in the recovery procedure?		
Does your company apply reporting procedures for lost or stolen mobile equipment?		
Are employees trained on what to do if information is accidentally deleted and how to retrieve information in times of disaster?		
Have measures been implemented to protect both confidentiality and integrity of backup copies at the storage location?		

16

Is your company prepared to handle an information security incident?

✖ We will not have any incidents. In case we do, our employees are competent enough to cope with them.

! We have incident management procedures, however not adapted to handle information security incidents.

✔ We have a dedicated process to handle information security incidents, with the necessary escalation and communication mechanisms. We strive to handle incidents as efficiently as possible so we learn how to better protect ourselves in the future.

The questions below are offered as a basic information security checklist for your company to help assess where you are in the process.	YES	NO
Does your process address different types of incidents ranging from denial of service to breach of confidentiality etc., and ways to handle them?		
Does your company have an incident management communication plan?		
Do you know which authorities to notify and how in case of an incident?		
Does your company have contact information sorted and identified for each type of incident?		
Do you rely on an internal communication manager for contacts with employees and their families?		
Is a lessons-learned process in place in order to make improvements to incident management after an information security incident?		

RESOURCES AND REFERENCES

A companion digital appendix of further material from standards of practice to technical standards is offered with the guide. Catalogued on the www.iccwbo.org/cybersecurity website, the site includes a listing of relevant global frameworks, resources and contacts and over time local frameworks where provided through ICC national committees and members. It is a snapshot of resources provided by the time of the publication but will be a resource that will be updated and expanded over time.

www.iccwbo.org/cybersecurity

The ICC Cyber security guide is also online with a one-stop resource portal offering globally relevant and localized standards, practices and advice on matters relating to technical as well as functional aspects of information security.

The portal features:

- Downloads of the ICC Cyber security guide for business
- Translated and/or locally adapted versions of the guide
- Links to globally recognized good practices, standards and frameworks
- List of public bodies and organizations with a global reach that are active in the domain of cyber and information security
- Links to country-specific resources developed by companies, government agencies and other entities.

THE INTERNATIONAL CHAMBER OF COMMERCE (ICC)

ICC is the world business organization, a representative body that speaks with authority on behalf of enterprises from all sectors in every part of the world.

The mission of ICC is to promote open international trade and investment and help business meet the challenges and opportunities of globalization. Its conviction that trade is a powerful force for peace and prosperity dates from the organization's origins early in the 20th century. The small group of far-sighted business leaders who founded ICC called themselves "the merchants of peace".

ICC has three main activities: rule setting, dispute resolution, and policy advocacy. Because its member companies and associations are themselves engaged in international business, ICC has unrivalled authority in making rules that govern the conduct of business across borders. Although these rules are voluntary, they are observed in countless thousands of transactions every day and have become part of the fabric of international trade.

ICC also provides essential services, foremost among them the ICC International Court of Arbitration, the world's leading arbitral institution. Another service is the World Chambers Federation, ICC's worldwide network of chambers of commerce, fostering interaction and exchange of chamber best practice. ICC also offers specialized training and seminars and is an industry-leading publisher of practical and educational reference tools for international business, banking and arbitration.

Business leaders and experts drawn from the ICC membership establish the business stance on broad issues of trade and investment policy as well as on relevant technical subjects. These include anti-corruption, banking, the digital economy, marketing ethics, environment and energy, competition policy and intellectual property, among others.

ICC works closely with the United Nations, the World Trade Organization and intergovernmental forums including the G20.

ICC was founded in 1919. Today its global network comprises over 6 million companies, chambers of commerce and business associations in more than 130 countries. National committees work with ICC members in their countries to address their concerns and convey to their governments the business views formulated by ICC.

INTERNATIONAL CHAMBER OF COMMERCE

The world business organization

33-43 avenue du Président Wilson, 75116 Paris, France
T +33 (0)1 49 53 28 28 **F** +33 (0)1 49 53 28 59
E icc@iccwbo.org www.iccwbo.org

Publication number: 450/1081-5
ISBN: 978-92-842-0336-9