Commission on the

DIGITAL ECONOMY

ICC CYBER SECURITY GUIDE FOR BUSINESS

INTERNATIONAL CHAMBER OF COMMERCE

The world business organization

Commission on the

DIGITAL ECONOMY

THE GUIDE

INTERNATIONAL CHAMBER OF COMMERCE

The world business organization

Commission on the DIGITAL ECONOMY

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.

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.

ICC INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

Commission on the

DIGITAL ECONOMY

VISION AND MIND-SET

ORGANISATION AND PROCESSES

USING THIS GUIDE

INTERNATIONAL CHAMBER OF COMMERCE

The world business organization

Commission on the

DIGITAL ECONOMY

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.

ICC INTERNATIONAL CHAMBER OF COMMERCE

The world business organization

Commission on the

DIGITAL ECONOMY

THE WEBSITE

ICC INTERNATIONAL CHAMBER OF COMMERCE

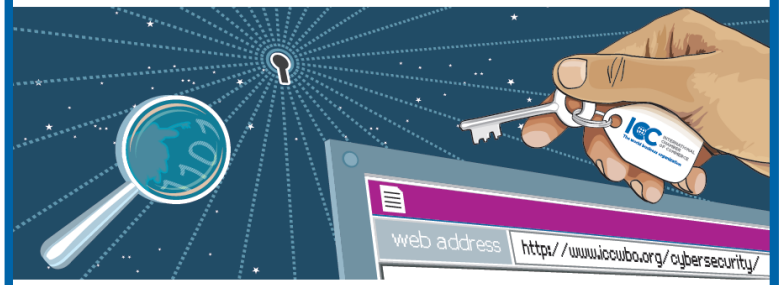
The world business organization

Commission on the DIGITAL ECONOMY

ICC INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

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.