International Chamber of Commerce

The world business organization

ICC Cyber Security Guide for Business

World Bank Seminar on Cyber Preparedness
Vienna. 18-19 May 2015

ICC NETHERLANDS
INTERNATIONAL
CHAMBER OF COMMERCE

@ICCNederland

www.icc.nl/cyber
www.iccwbo.org/cybersecurity

Gerard Hartsink

Chair ICC Task Force on Cyber Security (www.iccwbo.org Paris)
Chair Digital Economy Commission ICC Netherlands (www.icc.nl The Hague)
Senior Advisor ICC Netherlands (www.icc.nl The Hague)

Threats for Businesses

- **Without suitable precautions, the internet, enterprise information networks and devices are not secure.**

What is the background of ICC's Guide?

- ICC has a long history of providing companies tools and self-regulatory guidance to promote good business practice.
- ICC is dedicated to **facilitate trade and investment** including to foster e-commerce and confidence in the digital economy.
- An **open internet** will make the access to knowledge, information, goods and services possible for the **benefit of businesses and consumers**.
- Businesses are more and more confronted with challenges that the **internet**, **enterprise information systems and devices are not secure without suitable precautions**.
- ICC created the **Cyber Security Guide for Business** to make its about 6 million members of 90 National Committees aware of the risks and offer them a guide to mitigate their cyber risks
- ICC believes that **cooperation of businesses and the public sector** is essential to **mitigate cyber risk** in society

Target Groups of the Guide

- Guide to **raise awareness** of business role in ensuring security online
- **Conversation starter** between IT specialists and company management
- Relevant for **Corporates** (management and Board), **SMEs**, **merchants** and **webmerchants**
- Tool to demonstrate **business engagement** in addressing cyber security

NETHERLANDS INTERNATIONAL CHAMBER OF COMMERCE

@ICCNederland

www.icc.nl/cyber
www.iccwbo.org/cybersecurity

What should business do?

Businesses of all sizes need to develop and nurture key organizational capabilities to manage cyber security

- Undertake a **risk analyses**
- Take necessary actions to ensure **employment of best practices**
- Prepare to **detect and respond** (internally and externally) **to cyber events**

What should governments do?

- **Intensify international cooperation** in order to mitigate cyber crime risks (such as the Global Forum on Cyber Expertise: see www.gccs2015.com)
- **Stimulate public and private cooperation** in all jurisdictions to manage cyber security threats
- Support the **ISACs** (Information Sharing and Analysis Centers) in all jurisdictions
- Take **appropriate prosecution actions** in all jurisdictions in case of breaches

Key Security Principles

A: **Vision and mind-set**

Principle 1: Focus on information and not on technology
Principle 2: Make resilience a mind-set

B: **Organization and Processes**

Principle 3: Prepare to respond
Principle 4: Demonstrate a leadership commitment
Principle 5: Act on your vision

Six essential Security Actions

Action 1:	Back up business information and validate restore process
Action 2:	Update information technology systems
Action 3:	Invest in training
Action 4:	Monitor your information environment
Action 5:	Layer defenses to reduce risks
Action 6:	Prepare for when the breach occurs

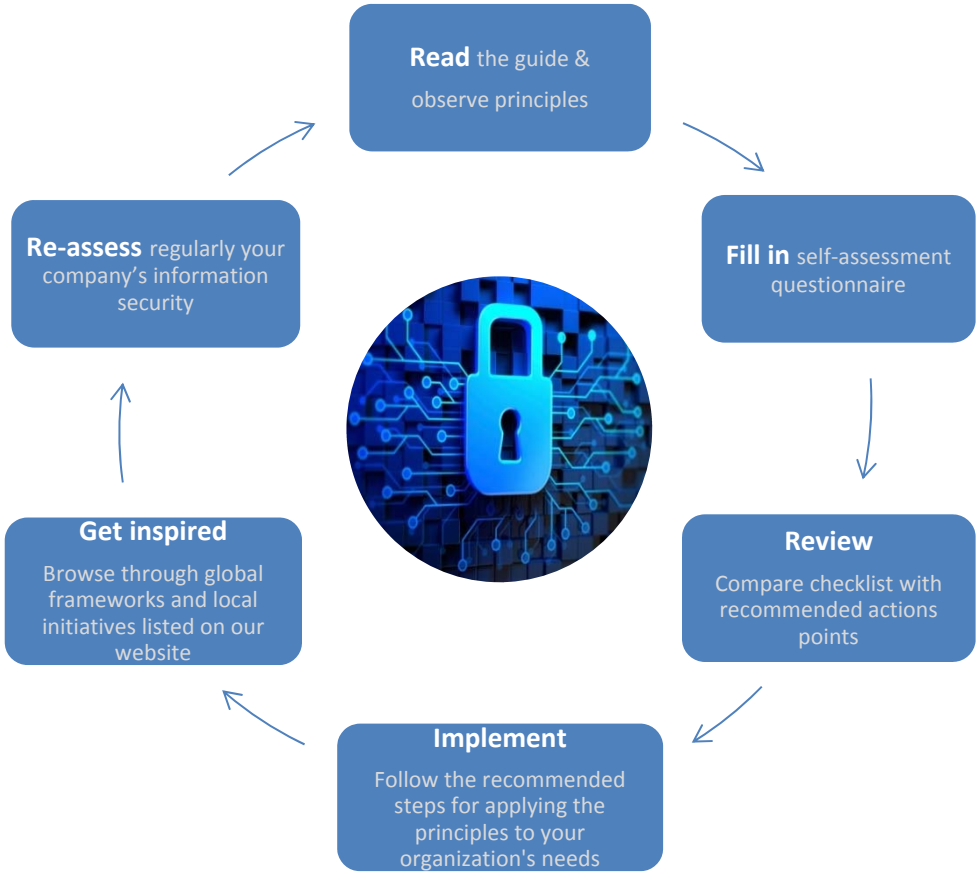
Security self-assessment (1)

1. Do you evaluate how sensitive information is handled within you company?
2. Do you perform information security-related risk assessments?
3. At what level is information security governance implemented?
4. Do you have a dedicated information security function?
5. How does your company deal with security risks from your suppliers?
6. Does your company evaluate computer and network security on a regular basis?
7. When introducing new technologies, do you assess potential security risks?
8. Does information security training take place within your company?
9. How do you use passwords within the company?
10. Is there a policy in place for the appropriate use of the internet and social media?

Security self-assessment (2)

1. Do you measure, report and follow up on information security related matters?
2. How are systems kept up-to-date within your company?
3. Are user access rights to applications and systems reviewed on a regular basis?
4. Can your employees use their own personal devices to store company information?
5. Has your company taken measures to prevent loss of stored information?

ICC Cyber Security Guide for Business



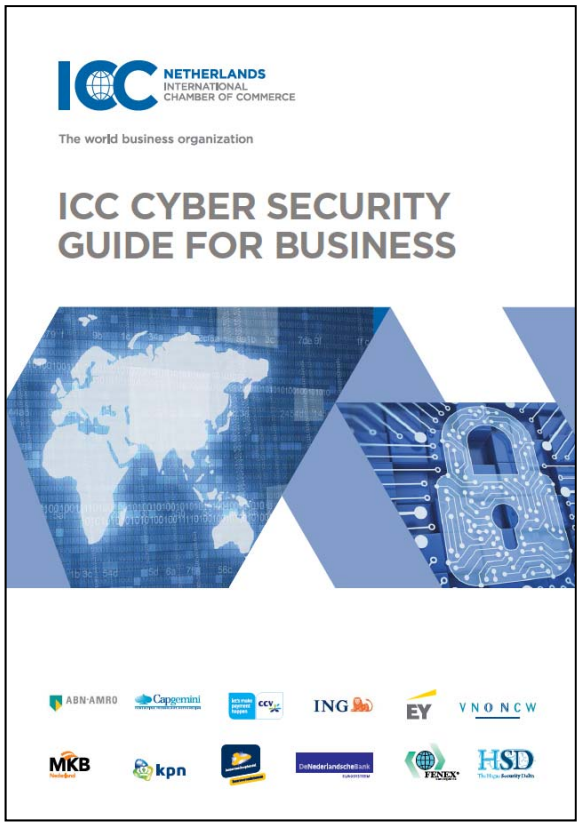
ICC NETHERLANDS
INTERNATIONAL CHAMBER OF COMMERCE

@ICCNederland

www.icc.nl/cyber
www.iccwbo.org/cybersecurity

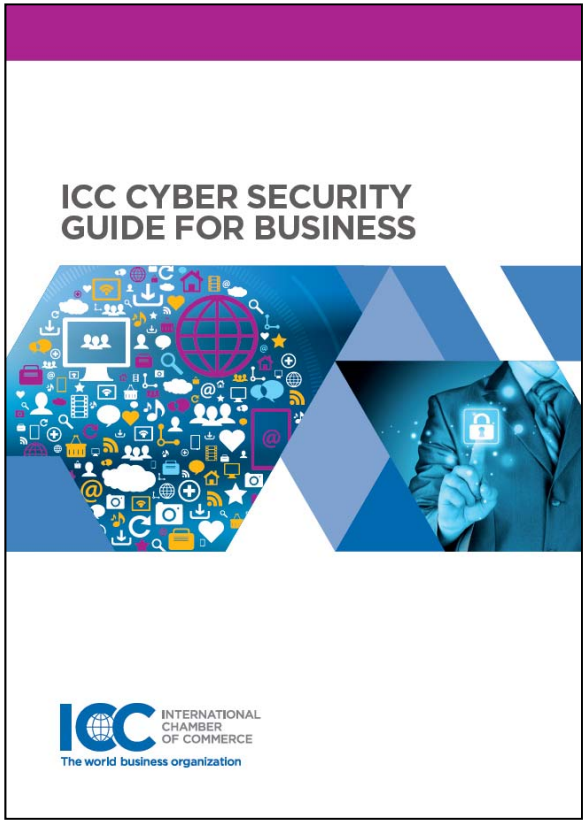
Edition ICC Netherlands

www.icc.nl/cyber



Global edition

www.iccwbo.org/cybersecurity



NETHERLANDS
INTERNATIONAL
CHAMBER OF COMMERCE

@ICCNederland

www.icc.nl/cyber
www.iccwbo.org/cybersecurity