How to protect yourself against cyber crime in 7 practical steps

Fox Harbour, NS

Presented by: Scott Crowley, Regional Managing Partner, MNP
Ken Taylor, President, ICSPA
Stephen Warden, Partner, MNP

Date: June 7, 2013

Presentation Agenda

- ✓ **Why you need a formal approach**
- ✓ **7 steps to build up your security**
- ✓ **Conclusion**

ICSPA Key Cyber Crime Study Findings

- 7 out of 10 companies have been attacked
- Almost 8 in 10 companies have NO internal Cyber risk assessment process (5866 cyber crime incidents)
- ONLY 3 in 10 companies have a plan in place to respond to a cyber attack
- ONLY 3 in 10 companies have personnel trained to respond to a cyber attack
- 94% of organizations surveyed were NOT accredited to national or international security standards
- Awareness of the Canadian cyber security strategy was 7%
- Almost 5 in 10 companies did NOT know who to contact if a cyber crime occurred

ICSPA International Cyber Security Protection Alliance

Why you need a formal approach

Various factors make it hard to be fully secure at all time:

- **Complexity of the technology:**
- **The constant evolution of the technology brings new risks:**
- **Various stakeholders/interests are involved:**

→ A formal approach helps you to address this complexity

7 steps to build up your security

The following 7 steps approach will help you to:

- **Clearly understand your security risks**
- **Effectively implement the protection you need, against the most critical risks**
- **Save cost by focusing on what's really necessary**
- **Build a sustainable security posture**

7 steps to build up your security

1. Understand the risks

- **Understand what technology is used and how:**
- **Formally qualify the security risks or potential incidents you are exposed to**
- **Perform a security assessment against industry best practice,**

7 steps to build up your security

2. Test your systems security and try to break in

- **Perform a vulnerability scanning of the network**
- **Perform a penetration testing against your key systems**

→ This will provide an immediate, realistic and clear understanding of the most critical security exposures and vulnerabilities

7 steps to build up your security

3. Develop a clear security roadmap

- **Document a security roadmap that list clear actions** to address high vulnerabilities / risks.

→ Prioritization is based on the risk assessment and testing in step 1 and step 2

7 steps to build up your security

4. Embrace compliance with laws and regulations

- **Make sure you comply with applicable legislative and regulatory security requirements, including:**
  - **IIROC rules**
  - PIPEDA and provincial regulations on **privacy**
  - **Other financial regulations** if applicable (National Instruments, MFDA, FINRA, NASD, SEC)

→ Non-compliance with applicable laws and regulations can result in hefty fines.

7 steps to build up your security

5. Consider advanced automated security tools

- **For larger organizations, specific security risks will need to be addressed with advanced tools, such as:**
  - **Management of professional and personal mobile devices**
  - **Protection against data leakage.**
  - **System log monitoring**

7 steps to build up your security

6. Make your employees you best partners in security

- **Develop security training and awareness for employees.**
  - Learn the safe behaviours
  - Security training is also key

7 steps to build up your security

7. Maintain your security posture by performing regular reviews

- **Because your business and technology environment is always evolving**
- **Schedule annual or semi-annual security reviews:**

Summary

- Security incidents occur more often than ever and affect all industries.
- Impacts of a security breach could be disastrous and may result in:
  a) a loss of clients and revenue,
  b) incur high costs to remediate,
  c) incur fines
  d) May impact operations
- It can be difficult to strike the right balance between security investments and a precise evaluation of the existing threats
- Having a team of specialists with you will allow you to clearly identify the security issues, and provide adequate, affordable recommendations to effective protect the organization

Questions?

Scott Crowley, CMC, MBA

Regional Managing Partner, Ontario Advisory

Enterprise Risk Services

416-596-1711

scott.crowley@mnp.ca

Ken Taylor

President

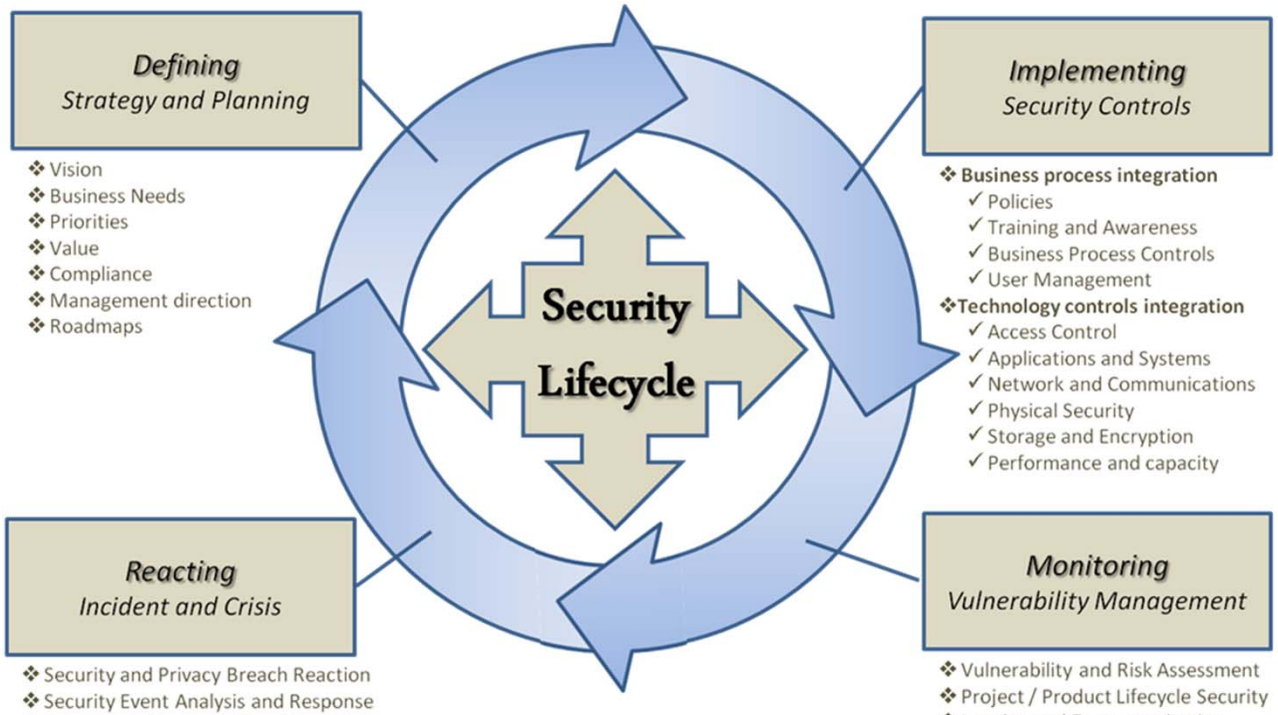
ICSPA

613-866-0423

ken.taylor@icspa.org

7 steps to build up your security

→ MNP “Security Lifecycle” proprietary framework represents the best practice security controls that should be in place for an optimal protection against cyber threats



ICSPA
International Cyber Security Protection Alliance

MNP LLP

MNP is one of the largest chartered accountancy and business advisory firms in Canada.

MNP offers a full suite of corporate governance and risk management services, including in-depth advice on corporate governance best practices; risk management; compliance; internal audit; security and privacy; forensics; technology and business resiliency.