Information security issues and resources for small and entrepreneurial companies

A business companion to the
2002 OECD Guidelines for the security of networks and information systems: *Towards a culture of security*

Foreword

Every company, no matter how small or where it is based, has a role to play in creating a global culture of security. What is a 'culture of security'? It is when every participant in the information society, appropriately to their role, is aware of the relevant security risks and preventive measures, assumes responsibility and takes steps to improve the security of their information systems and networks. But how can small companies, or those in developing countries, know what their role is and how to play their part?

I asked the ICC Commission on E-Business, IT and Telecoms to consult its members around the world and come up with a way to explain the key points of information security to non-technical people whose first responsibility is running a business. Drawing on the principles of the *OECD Guidelines for the security of information systems and networks: Towards a culture of security*, ICC experts produced a practical guide on how to make good information security practice as familiar and intuitive as the steps we take to physically secure our businesses.

This guide shows that the questions we routinely ask ourselves before buying any new product - What do I really need it to do? How well will it work with what I already have? How do I learn enough about it to get the best performance? - are just as relevant to information security. It helps business-people ask the right questions to make sure their software and hardware, and their business processes and procedures, work together to keep the business secure.

Tackling information security can seem intimidating, especially if you're not a technical person. But this guide shows that the key is being able to ask the right questions and act promptly and decisively on the answers. I encourage people running entrepreneurial businesses all around the world to use this guide and the resources it points to, and take the first step towards making your business security-aware and security-assured.

Table of Contents

I Introduction

Networks and information systems have become essential to businesses both large and small. They hold the promise of expanded markets and overall economic growth. But these opportunities depend on the security of those networks and information systems . Even businesses that consider themselves less dependent on computers need to be active in ensuring their information security.

Any business that uses a computer needs to be a participant in the global drive toward a culture of security. Everyone has a role to play in securing the information on the systems and networks they control. The role played should be appropriate to the business's resources, and will change with the nature and sensitivity of the information involved.

In the past, information security was not often seen as essential or even relevant to smaller businesses in both developed and developing countries. Now, the interdependence of different communication infrastructures and business models mean that all businesses are potentially interconnected. So it is imperative that everyone play their role in the global culture of security.

II Dispelling the myths, possible solutions and a call to action

Myth*:*
'Security is important for large enterprises, but not for a small company like mine.'

Not true! Security is essential for large enterprises that provide access to systems and networks for hundreds or thousands of people. But it is also an important concern for a small or medium sized enterprise. If you answer 'yes' to any of the questions below, then security is an important issue for you.

- Is any of your important company or personal information (whether yours or that of employees, customers, contractors or partners) stored on a computer?
- Do you or your employees access any important information (including banking, credit card, supplier or delivery information) across an internal network?
- Do you have a company website?
- Do you or your employees use the Internet at work?
- Do you or your employees use e-mail at work?

If you answered 'yes' to one or more of these questions, then the security of networks and information systems is an essential part of your business. You need to take steps to review the security of your systems and networks and make sure that it is up to the task.

Possible Solutions*:*
'OK, so I need to consider security, but what can I do? We're not a technology company, I don't have an IT department, and I'm not a technical expert.'

Unfortunately, ignorance is no excuse for inaction. In these days of higher levels of network connectivity and 'intelligent' viruses, information on an unsecured system can be quickly compromised, or the system itself can be used as a launching point for attacks on other systems and networks. Even if you're not an expert, you still need to take steps to protect your company.

Even with limited resources and expertise, there is much you can do to help secure your system and network access. Consider the questions below. Are you taking these steps?

- Do you have a firewall on your computer if you have Internet access (especially broadband access)?
- Do you have software to prevent and detect viruses transmitted by email or in documents?
- Is security an important criterion when you choose software or service providers?
- Do you understand the security functions of the software and hardware you already have?

- Has anyone in your company taken a computer course to become more familiar with these functions?
- If you have the resources and it's appropriate, have you consulted a local expert on the configuration and deployment of your IT system?
- Have you checked if there are resources from government, a local trade association or chamber of commerce that relate to computer security?
- Have you taken steps to physically secure your computers, especially laptops and portables?
- Do you regularly back-up data? And test your back-ups?
- Do you require your employees to use passwords?
- Do the passwords used contain both letters and numbers?
- Are passwords kept securely (not written down or shared, for example) and changed at least every three months?
- Do you try to train your employees on information security?
- Have you told your administrative support and reception staff what information they may and may not give to callers and visitors?

Call to Action:
'All these things apply to my business, but it sounds overwhelming!'

Like any challenge, security in its entirety can seem overwhelming. This guide provides you with a roadmap for how to start and what questions to ask. However, there is no one-size-fits-all security solution. And there is no free magic bullet. Information security costs both time and company resources. But security is an essential part of doing business today.

Information security may require some specialist knowledge, but the approach is not all that different from how you maintain the physical security of your business. For example, when you installed the doors and locks on your premises, you probably considered the following factors:

- Usability
- Functionality
- Security
- Reliability
- Cost
- Maintenance.

Your systems and network access are no different. Choosing and installing general software applications and specific information security measures requires the same calculation of factors and costs.

The steps you take to ensure the physical security of your business probably seem like second nature. But they are a learned response to known threats and vulnerabilities. Locked doors, secure filing cabinets, and a safe or cash register are all security steps that

we take for granted as just part of doing business. Securing our networks and information systems should be no different.

Just as with other purchases, good information security requires both initial effort and ongoing checks. You need to do your research before buying security software, hardware or services. While you should expect the technology to work well, you still need to carry out the right checks to ensure that it's working correctly. Appropriate features must be set and adapted to work with your existing computers, software and network connections.. . Many security vulnerabilities are created when people install a new application and simply leave all the default settings in place, making them much easier for unauthorized users to manipulate.

It may seem complicated or overwhelming at first, but over time your actions should become so familiar and automatic that they constitute a 'culture of security'. No one expects people running small businesses to review software code or understand the intricate workings of hardware. But you can and should read the relevant information, ask pertinent questions and get explanations of issues that don't seem clear. By taking the initiative and showing that security is important to your business, you can go a long way to making sure that your information systems develop in a secure way. In some cases, for example when making significant changes to your information systems, you may need expert assistance in the initial configuration and deployment of the system. But it's essential to keep asking the experts what they are doing and why, and to satisfy yourself that the choices made reflect your business needs and improve the information security of your business.

III The OECD Information Security Guidelines: the path forward.

The OECD Guidelines

On 25 July 2002, the OECD Council adopted the OECD Guidelines for the security of information systems and networks: Towards a culture of security ("the OECD Guidelines")[1].

The Guidelines address the interconnectivity and evolving risks of the networked economy. Until quite recently, information security was a specialist issue of little direct interest to most people. Today, countries' critical infrastructures (including energy, water, and communications) rely on information systems, making security a key concern for governments, business and citizens. This change is reflected in the new subtitle of the Guidelines, "***towards a culture of security***", and the fact that they are directed to ALL participants in the information society, as appropriate to their roles.

Background

The OECD Guidelines are basic and succinct, to make them understandable to everyone. Private businesses own and operate most of the world's information systems and infrastructure. They therefore have a clear responsibility tothe overall development and promotion of information security. This needs to be understood at the highest levels of companies. BIAC[2] and ICC developed *Information Security Assurance for Executive*[3] as a primer on security issues to help high-level executives put these issues in context and enable them to direct IT staff and specialists appropriately. *Information Assurance for Executives* elaborates on the OECD Guidelines to show their relevance to the business community.

The OECD Guidelines also apply to how smaller companies deal with security issues in a way that is appropriate to their role, size, resources and sector. While the principles in the OECD Guidelines and *Information Security Assurance for Executives* are applicable to all businesses, their content is not targeted at smaller companies, sole proprietorships and businesses with limited or no specialist IT resources. This guide, *Information security issues and resources for entrepreneurial companies*, elaborates on the OECD principles to make them relevant to smaller companies in developed as well as developing countries.

---

[1] http://www.oecd.org/pdf/M00034000/M00034292.pdf

The 2002 Guidelines are an update of the OECD Security Guidelines first issued in 1992.

[2] The Business and Industry Advisory Council to the OECD (BIAC)

[3] Available at http://www.iccwbo.org/home/e_business/word_documents/SECURITY-final.pdf

What is the 'culture of security' and how is it relevant to me?
The concept of a 'culture of security' is described in the 'call to action' section of this guide (page 6 - 7). It simply means that we all have a role to play in improving global information security, and that each participant in the information society has a set of appropriate security responsibilities and behaviours, depending on their role and situation. Through learning and practice, security-enhancing behaviours should become so much like an intuitive response that we are all are part of a truly global 'culture of security.'

For example, in a culture of security, anti-virus software should always be deployed to screen incoming messages and files, and is kept up-to-date so that new viruses can be eliminated. In a culture of security, passwords and other authenticating procedures are kept secret so that they remain effective. A culture of security means that these and other behaviors become as automatic and common-sense as looking both ways before crossing the road.

Who is this guide for?
Information security issues and resources for entrepreneurial companies is addressed to people running smaller, entrepreneurial companies that do not have access to dedicated, full-time IT resources or expertise. These companies rely either on what information they can glean about networks and information systems from public sources, or on services provided by outside experts.

What does this guide do?
Building upon the previous OECD and ICC/BIAC work, *Information security issues and resources for entrepreneurial companies* follows the format of the OECD Guidelines. This guide;

- Shows the concept behind each of the Guideline principles
- Highlights examples of the principles being applied in practice
- Suggests pertinent factors that should be considered when deploying security solutions.

This will help smaller businesses to identify and respond to security issues. The guide cannot determine the best security solution for a particular company as this depends on factors including:

- Size and resources of the business
- Sensitivity of the information being secured
- Risks faced by the business in terms of external connectivity (potential exposure to threats) and hardware and software used (potential number of vulnerabilities).

This guide helps you to be better informed about the questions you need to ask, and should improve your understanding of the types of security solutions available to your company. It is supplemented by a set of online links to security resources around the world.

IV The Guidelines and their applicability

The nine Principles in the Guidelines can be considered in three main categories as follows:

Foundation Principles

- Awareness – what you should know.
- Responsibility - what you should be doing.
- Response – how you should react in a timely and cooperative way to security incidents.

Social Principles

- Ethics – what is appropriate in behaviour that affects others.
- Democracy – general respect for rights and freedoms.

Security Lifecycle Principles

- Risk assessment – understand threats and vulnerabilities to your systems, processes and employees.
- Security design and implementation – how you can select and deploy hardware and software.
- Security management – managing security over time and the business.
- Reassessment – security is a continuing process, not a one-time solution.

V Security checklist – path forward

Using the principles

While the OECD Guidelines follow a logical structure, their order does not provide a practical path to implementation. This section follows the OECD Guidelines, but re-arranges them to help the practical consideration, decision-making and implementation involved in good security practice. This guide focuses on two simple categories; what you should know, and what you need to do.

What you should know:

- What I need to know about information security in my company (Awareness).
- How can I understand threats to, vulnerabilities of, and effect on, my systems, processes and employees? (Risk Assessment).
- What is expected of me based on the size and nature of my business? (Responsibility).
- What social obligations must I be aware of? (Ethics and Democracy)

What you need to do

- Factors that I should consider in selecting and implementing solutions (Secure Design and Implementation).
- Developing and implementing practices and procedures (Security Management / Awareness).
- How to deal with incidents (Response).
- Review and improvement of processes and systems (Reassessment).

This guide is comprised mainly of checklists and possible solutions. As security is not a one-size-fits-all solution, you need to determine your requirements based on the business you are in, the type of information you handle and the nature of your technical infrastructure.

What you should know

Understanding the importance of information to your business:

- How does the information you use in your business relate to your primary business objectives?
- Have you identified the information that is critical for you to do business?
- What tasks do you perform that involve the creation, processing, storage, use and transmission of that business-critical information?
- What assets do you use to create, process, store and transmit that business-critical information (for example computers, card-indexes, mobile phones)?
- Do you know what would happen to your business if the confidentiality of those assets was broken (if, say, a competitor gained access to them)?
- Do you know what would happen to your business if the integrity of those assets was compromised, and you were unable to trust the information in them?
- Do you know what would happen to your business if those assets were unavailable to you for a period of an hour, a day, a week or a month?
- Using what you now know about the confidentiality, integrity and availability of your company's information assets, can you prioritize them?

Once you have prioritized information assets in order of their importance to your business, you will be able to ensure that they are given an appropriate degree of protection. Failing to do this could mean that you will be wasting time and resources on assets that are not critical to your business, or worse; that business-critical information is not adequately protected.

Understanding information security related assets

- Do you have a written inventory of your business-critical information assets: hardware, software and intellectual (such as patents and contracts)?
- Does that inventory tell you where the assets can be found?
- Do you regularly update the inventory and audit it to ensure that it remains comprehensive and valid?
- Are you aware of the security features in the hardware and software you use, and do you have appropriate manuals or training materials about these features?
- Has anyone in the office had previous experience with these products or taken classes on them?

Understanding how assets are used, by whom and for what reason

- Who in your company has access to business-critical assets?
- Do your employees use unique passwords to control access to the computer assets they use?
- Are those passwords kept securely and changed regularly?
- Do you ensure that access is given only for genuine work-related reasons?

- Do you keep lists of who has access to what, and do you regularly update those lists?
- Do you run a local- or wide-area network? If so, how do you control access to that network? If passwords are used, are these unique to each user, changed regularly and kept securely?
- Do you have Internet access? If so, do you have broadband access or dial-up?
- Which computers/devices in the company have network or Internet access, and do you know who uses these?
- Do employees have remote access to your network (either from home or on the road).
- How do employees gain access to your network when they are working remotely?

Understanding security management

- Read the following list of security technologies and ask yourself; which are you aware of, and which do you use?
  - firewalls and VPN (Virtual Private Networks)
  - access, authorisation and authentication controls
  - anti-virus
  - spam filters
  - Internet content control
  - network-security policy compliance tools
  - vulnerability and threat databases
  - cryptography tools such as SSL, public-key cryptography and hard-disk-encryption
  - intrusion detection systems.
- Do you regularly back up your business-critical data?
- Do you test the back-ups, restoring the data from them and making sure it's usable?
- Do employees using laptops or other computers for remote access have anti-virus software and firewalls on those computers?
- Do you allow employees to use the company's computers, systems or network access for non-business purposes? If so, do you make it clear to them that certain uses are unacceptable and may result in disciplinary action?
- Do you provide any security education or training for employees who use the company's computers or information systems?
- Do you have any policies, standards or procedures related to security?

Understanding your broader obligations:

- Are you familiar with legal requirements related to securing certain types of information (Financial services information, health information, personal data)?
  - This may involve privacy legislation as well as sectoral regulation.
  - In some cases, especially where personal, sensitive or confidential information is involved, you may be required to provide a minimum level

of protection for that information, irrespective of the size of your company.

- Are you familiar with the rights of employees in the workplace?
  - Some laws may limit your access to certain types of employee information and communications, or require notice or consent before you are able to access real or virtual information held in an employees' workspace.
- Are you aware of your role regarding the security of others?
  - The security of information systems is complex because businesses are connected to each other directly and through the Internet, creating interdependencies and spreading risk. Failing to properly secure your system may not just compromise and potentially harm your business; it can increase the risk of other systems to which you are connected. Greater risk could result from virus programmes using your contact lists to spread further, or from malicious programs using your unsecured networked computer to attack or send spam to other systems or computers.
  - Do your employees understand what is appropriate behaviour on the Internet? This goes beyond not downloading or posting illegal, inappropriate or offensive material, and includes general conduct that is in keeping with the values and ethical practices of your business.

Summary

The first five steps to knowing about good information security are:

1. Assess your business objectives, information-related tasks and critical information assets – and thus your risk.
2. Identify and make an inventory of your business-critical information assets.
3. Know who accesses those information assets, how and why.
4. Find out how to improve the secure management of those information assets.
5. Get to know your broader obligations in the use of your information assets and in relation to society as a whole.

Having taken these steps, you will be in a good position to implement some of the security basics outlined in the next section.

What you need to do - security basics

Security Policy, Standards and Procedures

Every business should have a set of information security policies, standards and procedures so that all employees know exactly what is expected of them. The policy constitutes the 'Why' of information security; Security standards represent the 'What'; and procedures are the 'How'.

Below, policy and standards are explained. Since procedures are detailed instructions that flow from standards, they must be tailored to each individual business; and are therefore beyond the scope of this guide.

Security Policy

A simple and clear information security policy is essential. It should be as short as possible – no more than a few pages - and should be given to all employees.

The policy should include the following:

- Information is vital to our business.
- We protect the confidentiality, integrity and availability of our business-critical information.
- We have standards that help us to do this – including:
    - physical security
    - personnel security
    - access controls
    - security technology
    - security response and recovery, and
    - security audits.
- We have procedures that help us to meet our standards.
- Employees should be familiar with the procedures relevant to their roles and responsibilities.
- We take disciplinary measures against employees who persistently or deliberately flout these information security policies, standards and procedures.

The policy should say where details of the standards and procedures can be found.

Security Standards

The standards listed in the security policy section above are examined in more detail below.

- **Physical security**
    - Fit appropriate locks or other physical controls to the doors and windows of rooms where you keep your computers.
    - Physically secure lap tops when they are unattended (for example, by locking them in a drawer overnight).

- Ensure that you control and secure all removable media, such as removable hard-drives, CDs, floppy disks and USB drives, attached to your business-critical assets.
- Make sure that you destroy or remove all business-critical information from media such as CDs and floppy disks before disposing of them.
- Make sure that all business-critical information is removed from the hard drives of any used computers before you dispose of them.
- Store back-ups of your business-critical information either off-site or in a fire- and water-proof container.

- **Access controls**
  - Use unique passwords, that are not obvious (not birth dates or easily found or guessed information) and change them regularly, preferably every three months.
  - Use passwords that contain letters in both upper and lower case, numbers and special keys, and are six or more characters in length. It helps if you consider your password as a memorable sentence, rather than a single word. For example the sentence: "at forty-two I'm a star!" could be translated into an eight-character password that looks like this: @42Ima*!
  - Don't write your password down, and never share it with anyone. If you do have to share it, make sure you change it as soon as possible – no matter how well you trust the person you shared it with!

- **Security technology**
  - All computers used in your business should have anti-virus software installed, and the virus definitions must be updated at least once a week (many providers have a one-click update). All incoming and outgoing traffic should be scanned for viruses, as should any disk or CD that is used, even if it is from a 'trusted' source. At least once a month, computers should be scanned for viruses.
  - If your computers are connected to the Internet, and especially if you use a broadband connection, you must deploy a software firewall. This will help to prevent malicious code from entering your computer and potentially compromising the confidentiality, integrity and availability of your network. It will also help to stop your system being used to attack other systems without your knowledge. Software firewalls for use by non-professionals are readily available at a reasonable cost. Your operating system, virus control software or ISP may also offer a firewall. Consumer and popular trade magazines compare firewall functions and features of well known products, and so are a good source of information. Free shareware firewalls are available, but these usually require expert knowledge for correct use.
  - If your business has a small network that is connected to the Internet, you should consider deploying an 'all-in-one' hardware box that contains a firewall, anti-virus program and an intrusion detection system. This will

greatly simplify your use and maintenance of essential Internet security technology.

- **Personnel**
  - Perform integrity checks on all new employees to make sure that they haven't lied about their background, experience or qualifications.
  - Give all new employees a simple introduction to information security, and make sure that they read and understand your information security policy. Make sure they know where to find details of the information security standards and procedures relevant to their role and responsibilities.
  - Ensure that employees have access only to the information assets they need to do their jobs. If they change jobs, make sure that they do not retain their access to the assets they needed for their old job. When dismissing employees, ensure that they do not take with them any business-critical information.
  - Make sure that no ex-employees have access rights to your systems.
  - Make sure your employees know about the common methods that can be used to compromise your system. These include e-mail messages that contain viruses and 'social engineering' ploys used by hackers to exploit employees' helpfulness to gain information that will give them access to your system. Examples of 'social engineering' include a hacker using the telephone to pose as a systems maintenance engineer or pretending to be a new employee.

- **Security Incident/Response**
  - A security incident is any event that can damage or compromise the confidentiality, integrity or availability of your business-critical information or systems.
  - It is important to make your staff aware of telltale signs of security incidents. These could include:
    - strange phone requests, especially for information
    - unusual visitors
    - strange patterns of computer activity
    - unusual appearance of computer screens
    - computers taking longer than usual to perform routine tasks.
  - Your staff should understand that it is always better to notify the right person if they observe anything that might be a telltale sign of a security incident.
  - If a security incident happens, employees should know who to contact and how.
  - You should have in place a plan to assure business continuity in the event of a serious security incident. The plan should specify:
    - Designated people involved in the response

        - External contacts, including law enforcement, fire and possibly technical experts.
        - Contingency plans for foreseeable incidents such as:
            - Power loss
            - Natural disasters and serious accidents
            - Data compromise
            - No access to premises
            - Loss of essential employees
            - Equipment failure.
    - Your plan should be issued to all employees and should be tested at least once a year, even if you haven't had a security incident.
    - After every incident when the plan is used, and after every test, the plan should be re-examined and updated as necessary using the lessons learned.

- **Audit Controls/ Due Diligence**

Good information security includes knowing who has access to your system and being able to log that access. You also need to have in place a system to make sure that your security procedures are actually followed. The ability to audit and evaluate information security compliance is essential – you can't manage what you don't measure!

- You should audit important aspects of your security, for example, who has access to your systems and who has used what information.
- You should have a record for each one of your security procedures. For example, if your procedure says that you test your back-up generator once a week, someone should sign a record to show that this has been done. Keeping good records is essential to audit control.
- Some audit controls may be necessary for legal or regulatory purposes. Good record keeping will clearly demonstrate that you are complying with your obligations.
- An audit should ensure that the procedures you have in place are effective and relevant. It is a trigger to re-assess and re-evaluate the effectiveness of your information security standards and procedures.
- Audits are only effective if you follow through on their findings and identify and implement the steps that need to be taken.

A good audit trail is not just a paper exercise. If something goes wrong, the trail should let you to see what happened and why. This will help you to keep improving the security of your business.

The path forward

There is no 'one size fits all' approach to information security, and there are no magic bullets. *Information security issues and resources for small and entrepreneurial companies* helps managers to identify and respond to the security issues that are relevant to their companies. Everyone who uses this guide needs to tailor their information security policy, standards and procedures to their own company. Each company is unique, with its own set of needs, resources and circumstances. But what every company, no matter its size or location, shares is the need to play its role in creating a global culture of security.

If your company uses a computer, and if that computer is connected to a network, information security must be a part of the way you do business. Information security isn't just about technology, and it's not just for experts. You can radically improve the security of your business – and those you do business with – by taking a few small steps. Using proper passwords, a firewall, virus detection and making regular back-ups will make a significant improvement in your security and the security of those you deal with. These steps require research and effort to begin with, but will soon become second nature to you and your employees.

But remember, security is a continuous process, not an end-state. The extensive resources on the ICC website give more information on a range of security topics, and from experts around the world. *Information security issues and resources for small and entrepreneurial companies* is simply a starting point for securing the way you do business.

For more information and resources on information security, please visit the ICC website at http://www.iccwbo.org/home/menu_electronic_business.asp.