

Practical Paranoia

“Security is an exercise in applied paranoia” (unknown)

Introduction

Today’s connected world is a dangerous place. You already know about hackers, viruses, Trojan horses, worms, malware, adware and phishing. And those are just the impersonal risks. Home computers used to connect to the office may contain confidential information that can later be found in computer junkyards. Or at the repair shop at BestBuy being combed over by the Geek Squad. And did we tell you about the USB pen drives?

How can you be sure to get the best out of your connectivity without risking your business?

Remind me why I want to be connected to the internet in the first place?

- Ability to escape the chains of the desk – e.g. Saturday mornings “at the office” or burning the midnight oil
- Working on trial preparation remotely in client offices, or in hotel rooms
- Deal rooms with the client – doing “due diligence” with all the documents before a merger or an acquisition using a shared workspace accessible by client and legal team.
- Litigation document review using an outside provider to host all the documents. Again, review by both client specialists and lawyers, working together as a team
- Business resumption – in the event of a disaster where your offices are no longer physically accessible
- Improved client responsiveness through lawyer use of webmail and Blackberries
- Teleworking

So, what’s the downside?

Let’s start with the premise that your only safe course of action is to disconnect from the internet entirely and remove all disk drives, USB ports and CD/DVD burners from your workstations. However, in today’s connected world where access to the internet for research and communications is an accepted normal practice, disconnecting simply wouldn’t be practical. So what can go wrong?

Loss of confidential information

Confidential information includes not only that belonging to the firm, such as trade secrets like annotated precedents and financial information, but also that belonging to the client. Early drafts of agreements for mergers and acquisitions, solicitor’s advice, evidence in a suit, could all be lost or leaked in a security breach.

Loss of information integrity

Definition of “integrity” from Best Practice Guide – Information Risk Management: “The assurance that information has been created, amended or deleted only by the intended authorized means.”¹

Information can become inaccurate or corrupted after unauthorized access. Could involve use of an email account or an unauthorized financial transaction or website spoofing.

Lost productivity

2003 was the worst year for viruses and worms. There was the Slammer attack in January, followed by MSBlaster and Sobig in August. Email systems were completely shut down for days on end, and connections to the internet were suspended until the appropriate patches on the Exchange servers were applied. For those of us in Ontario and the U.S. Northeast, Blaster was accompanied by a huge power outage which, though unrelated, exacerbated the loss of productivity.

Viruses can be more than a nuisance – they can delete files, modify settings on the computer and corrupt documents. Not only is the end-user idle until repair, there is the actual cost of the restoration by the IT team.

Loss of reputation

Consider the damage that would result from a leak to the street of a proposed sale or merger? Or the embarrassment that could result from a lost pen drive containing the document collection for a suit.

Managing the risk

Risk (risque) - (i) chance of vulnerabilities being exploited; (ii) uncertainty.²

Risk assessment (évaluation des risques) - an evaluation, based on the effectiveness of existing or proposed security safeguards, of the chance of vulnerabilities being exploited.

Vulnerability (vulnérabilité) - (i) an inadequacy related to security that could permit a threat to cause harm; (ii) an inherent weakness in information technology that makes it.

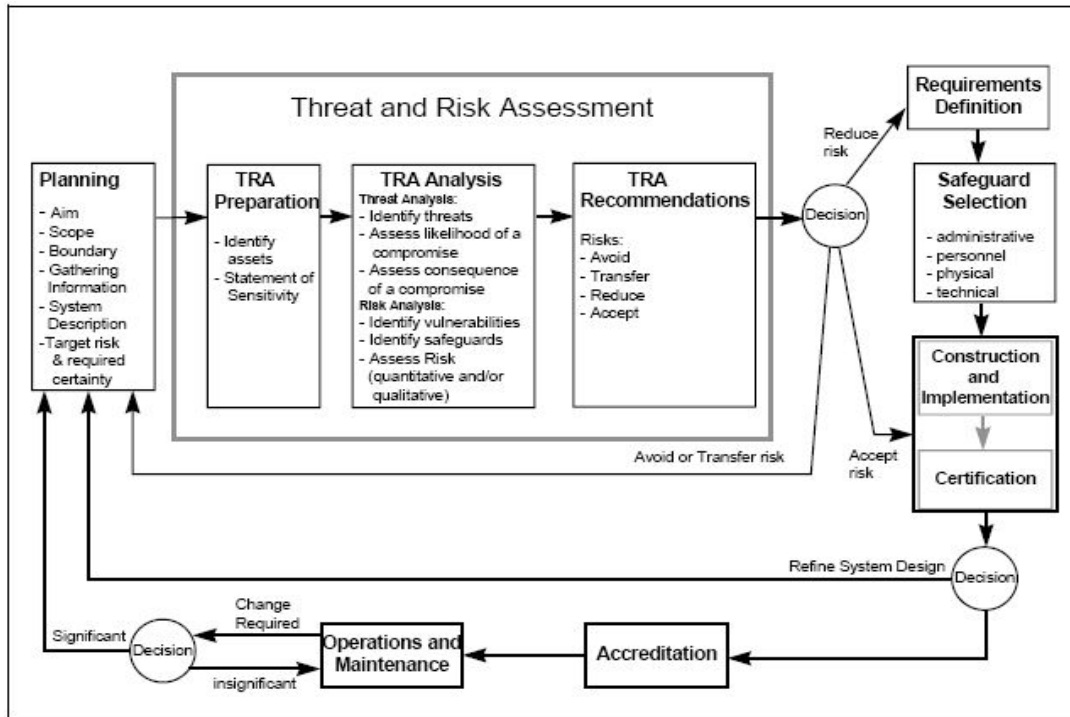
Threat (menace) - any potential event or act that could cause one or more of the following to occur: unauthorized disclosure, destruction, removal, modification or interruption of sensitive information, assets or services, or injury to people. A threat may be deliberate or accidental.

Threat assessment (évaluation de la menace) - an evaluation of the nature, likelihood and consequence of acts or events that could place sensitive information and assets at risk.

¹ [Best Practice Guide – Information Risk Management](#), published by the Queensland Government (Australia)

² [Information Technology Security – Audit Guide](#), published by Treasury Board Secretariat, Government of Canada

What is a Threat and Risk Assessment?



From: *Threat and Risk Assessment Working Guide*³

A “threat and risk assessment” provides a framework for the process of identifying threats and the consequences, examining vulnerabilities and devising safeguards and assessing the remaining risk.

Taking the example of a law office, where the “assets” include work product prepared by lawyers, client information, financial information and the productivity of the staff in general, what might be the threats associated with remote computing?

Threat	Hackers unauthorized access to servers
Likelihood	Low
Consequence of compromise:	Loss and/or disclosure of confidential information; corruption or deletion of information; reputation (high severity)
Vulnerabilities	“Back doors” in operating systems; default names and passwords left on “admin” accounts; privileged and powerful software like “ftp” available for exploitation. Disgruntled employee in IT or outsourcer.
Safeguards ⁴	Employee screening. Ensure IT staff have adequate training and experience in configuring servers; establish a standard configuration with documented exceptions where required. Reduce number of staff with privileged access to servers and firewalls. Security consultant review server practices to recommend ways to reduce exposure.

³ [Threat and Risk Assessment Working Guide](#), published by the Government of Canada, Communications Security Establishment

Threat	(1) Loss of USB pen drive (2) Information removed using pen drive
Likelihood	High
Consequence of compromise:	Limited loss and/or disclosure of confidential information, client contact information; reputation (low severity)
Vulnerabilities	They're small! And easy to misplace – like reading glasses. Can be easily hidden if departing employee wishes to copy client contact lists or precedents.
Safeguards	Limit number of people provided with pen drives. Require users with personal pen drives to disclose if they are using them for firm work. Employee screening during hiring. Policies about acceptable use. Use a “thin client” at the workstation end with no USB ports or drives.

Threat	Loss or theft of laptop computer
Likelihood	Low to medium
Consequence of compromise:	Moderate loss and/or disclosure of confidential information, client contact information; reputation (low severity)
Vulnerabilities	Human nature – left in unlocked car. Misplaced during travel. Attractive asset.
Safeguards	Encryption of information on laptops. Complex passwords. Policies requiring employee to pay for lost laptops.

Threat	Viruses, worms, malware, etc.
Likelihood	High
Consequence of compromise:	Productivity loss; information integrity and confidentiality problems; (high severity because affects numerous machines)
Vulnerabilities	Use of home computers to access firm computers. Home computers may not have all security patches on the operating system and browser, and virus and adware signatures may not be up to date. Security settings on computer may not require scanning of downloaded files or scheduled checks. Home computers often used by other family members.
Safeguards	Use a quarantine approach when allowing outside computers to connect – check status of OS patches and virus signatures. If not current, refuse connection.

⁴ Safeguards shown are for purposes of illustration and are not necessarily recommended

Threat	Disk drives on laptops and home personal computers are discarded during upgrade, or older laptops and computers are offered to employees for home use.
Likelihood	High
Consequence of compromise:	Limited loss and/or disclosure of confidential information, client contact information; reputation (low severity)
Vulnerabilities	Companies often donate obsolete or lower-powered computers to charities or schools, or offer them to their employees. The software is left on, raising licence issues, and the documents are not wiped from the disks. Uncontrolled access to firm information on the disks.
Safeguards	Awareness programs. Disk wiping software. Inventory management procedures.

The above set of threat scenarios are by no means exhaustive and work as examples only.

Prepared for the worst

The “threat and risk assessment” doesn’t look at the benefits of connectivity – it is an entirely pessimistic exercise. However, connectivity can be used to mitigate other kinds of risks – natural disasters like Hurricane Katrina that make the office uninhabitable. With proper disaster/recovery systems in place, a firm can quickly re-establish business “virtually” even if the desks and chairs, and an office to put them in, are still several months away.

Links:

<http://www.sans.org/rr/whitepapers/auditing/76.php>

<http://www.ncisse.org/conferences/cisse2003/courseware/nsacourses/lesson1/lesson1.PPT>

<http://www.kpmg.ca/en/industries/fs/insurance/documents/ii200208.pdf>

<http://www.mcafee.com/us/security/resources/home.htm>

<http://en.wikipedia.org/wiki/Malware>

http://www.rcmp-grc.gc.ca/tsb/pubs/phys_sec/r1-001a_e.pdf

http://www.windowsecurity.com/articles/Risk_Assessment_and_Threat_Identification.html

<http://www.itc.virginia.edu/security/riskmanagement/appendixH.html>

<http://www.acmqueue.com/modules.php?name=Content&pa=showpage&pid=142&page=4>

<http://antivirus.about.com/od/securitytips/a/removespyware.htm>

© Peg Duncan 2006