

NOTICEBORED

Managing information security risks through awareness

Issue 62 Information security risk management July 2008

Editorial

Organizations of all types are very concerned by threats that could compromise their information security and managing this aspect has become a primary concern for their information technology (IT) departments.

ISO press release launching ISO/IEC 27005:2008

New international standard [ISO/IEC 27005 Information Security Risk Management](#) could hardly have been released at a better time, just a few days before this awareness module. The truth is, though, that it was simply a coincidence. Since we didn't know exactly when it would be published, we couldn't have planned to cover this topic at the same time. However this neatly illustrates one of the interesting features of risk: human beings often place extraordinary significance on sheer coincidence. While I'm sure I would have enjoyed exploring the human psychology behind risk, there were just too many other things to cover in July's awareness module. Maybe next time ...

Some graybeard professionals feel that the methods commonly used to assess, analyze and manage information security risks are little better than chicken entrails at predicting the future. By explaining the elements of the risk management process, we hope to demonstrate that rational analysis, prioritization, treatment and monitoring of information security risks does give us a bit of an edge over those entrails, and perhaps in our own small way we can help advance the profession a little through provoking thought. It's not all hocus pocus! ■

Gary Hinson, Editor

Background

Our topic this month is one that some people claim is virtually impossible in practice *i.e.* managing information security risks. They might accept that some risks can be predicted, to an extent, but actually managing them is a different matter. Judging by the number of security incidents in the news media every day, there may be merit in this point of view but this ignores the fact that many other security incidents have been avoided, prevented, minimized or contained. 'Security incident averted' makes for rather less dramatic headlines than, say, 'Thousands of personal identities exposed'. In this sense, managing information security risks is a thankless task.

Information security risks need to be considered in the wider context of all forms of risk. Business, and indeed life in general, subjects us to a huge range of risks. Success arises from making appropriate decisions more often than not, but this does not necessarily mean being risk averse. Risk management is *not* the same as risk reduction. It is not always in the organization or the person's best interests to avoid or minimize risks – in fact, there are situations where risk reduction runs counter to the organization's mission. The problem is to distinguish these situations from those where the risks are unacceptable.

Information security supports business objectives not only by reducing the number and severity of security incidents, but also by giving management the confidence to conduct business in situations that might otherwise be deemed too risky. Effective information security risk management is truly a business enabler.

Risk, a fundamental concept in information security

Try this thought experiment. Shut your eyes for a moment and try to imagine living in a strange

parallel universe where risk simply does not exist. What is different for you? How do you feel about the world? Go ahead and try it before you read on ... OK, now let's see if either or both of these scenarios seem to strike a chord:

1. There is absolutely nothing to fear in a world without risk. People confidently do things they would avoid or at least hesitate to do in the real world. There is no danger. All weapons and defenses are pointless. People only die of 'old age' at a certain predetermined point, never because of accidents or deliberate attacks.
2. There is no such thing as chance any more. Everything is based on certainty: there is no doubt that things either will or will not happen. Nothing is a gamble. Businesses know in advance whether their new products will sink or swim and of course only launch the latter. Failure in general is abolished. Stock markets have no real function. Interest and exchange rates mean nothing. And, as far-fetched as this may seem, even politicians *always* tell the truth.

The real point of this exercise is that risk is an integral and indeed beneficial part of the world as we know it. As we know from 9-11, fearless people with no regard to their own safety or that of others do crazy, antisocial things. With no chance of failure, even badly conceived and executed activities continue unabated, so the natural process of evolution no longer functions.

In relation to information security, the risks to our information assets of confidentiality, integrity or availability failures are what lead us to implement controls in our information processing systems and supporting processes. The risk of someone correctly guessing our password or encryption key is what makes us choose long complex words or keys. What we are doing is managing our risks.

Generic definitions of risk

Rather like governance, risk is a term that is often used loosely or vaguely without being properly defined. Here are five generic definitions (taken from "*Seven myths of risk*" by Sven Ove Hansson in Risk Management: An International Journal, 2005, volume 7, issue 2) showing the different ways in which the word risk is used:

1. "Lung cancer is one of the major risks that affect smokers." Here, we use *risk* in the sense of an **unwanted event which may or may not occur**.
3. "Smoking is by far the most important health risk in industrialized countries." In this case *risk* is the **cause** of an unwanted event which may or may not occur.
4. "There is evidence that the risk of having one's life shortened by smoking is about 50%." Risk is the now **probability** of an unwanted event which may or may not occur.
5. "The total risk from smoking is higher than that from any other analyzed cause". Risk is the **statistical expectation value** of unwanted events which may or may not occur.
6. "The probabilities of various smoking-related diseases are so well-known that a decision whether or not to smoke is a decision under risk". Here, risk is the fact that a **decision is made under conditions of known probabilities**.

In addition to these five meanings, there are several narrower/technical meanings, especially in the world of finance and economics.

We mention all these definitions not to claim that any one is more or less correct than another since they are all valid and useful in particular circumstances. The real issue is just that. Risk reflects circumstances. A given situation may represent a "high" risk from some perspectives, yet be a "critical", "medium", "low" or even "negligible" risk from other points of view, all at the same time.

Context is everything

Perspectives on risk

People commonly consider risks from their own perspectives, thinking about how they might personally be affected. Risk analysis methods aim to bring more rationality to the process, considering alternative viewpoints.

Take a typical online Human Resources system for example, providing HR services to all employees through the corporate intranet. Individual employees may perhaps be concerned about risks such as their personal data leaking out (a confidentiality breach) or their pay rates being wrongly set (an integrity

breach). HR managers might also be worried about personal data exposures and data errors, but if the whole system was flawed or breached, the impacts could be much more serious than if only a single person was affected. Executives ought to worry about their personal liabilities through potential legal/regulatory compliance failures (governance and privacy acts, for example), and the consequences on staff morale and productivity that may arise from even small HR system issues. They are also going to be concerned about recovering the organization's investment in its HR system (financial risks). The CIO and IT managers care about keeping the HR system running, meaning an interest in all phases of the systems development lifecycle and the associated project and change management risks.

"People do not know how to analyze risk. They can't look at a vulnerability and make an intelligent decision about how bad it is. They can't look at an attack and make an intelligent decision about how likely it is. They can't look at a security situation and make an intelligent decision about what to do. The problem is not just one of not having enough information; people have trouble evaluating risks even with adequate information [although] not having enough information exacerbates the problem."

Bruce Schneier in Secrets & Lies

Now perhaps you can appreciate the complexities of trying to analyze all types of information security risks, or indeed all forms of risk affecting the organization. And we're talking about trying to project the risks over the next day, week, month, year, decade or whenever. ■

Information security risks

Specifically in relation to information security, the working definition of risk which we find most useful in practice is this: **information security risks arise from the coincidence of threats acting on vulnerabilities causing impacts on information assets.**

Five terms in our definition deserve further clarification:

Coincidence means the coming together of threats, vulnerabilities and impacts in discrete events, as well as implying a degree of chance or probability in the timing of such events. This

word indicates that our definition most closely resembles the first generic definition of risk above, namely an unwanted event which may or may not occur.

Threats are circumstances, events, situations or agents with the potential to cause harm to information assets. Threats are usually (but not always) external to the information assets being considered. The 'potential' again implies a probabilistic not deterministic situation.

Vulnerabilities are weaknesses, limitations or defects in information assets, or in the supporting infrastructure and processes. Vulnerabilities are usually (again, not always) internal/inherent to, or at least closely associated with, the information assets.

Impacts are events that affect the confidentiality, integrity and/or availability of information assets. This particular meaning clearly reflects the widely accepted definition of information security – impacts on other assets are not relevant, nor are other kinds of event affecting information assets. Notice that risk as strictly defined includes the potential upside (beneficial impacts) as well as the downside (harm), although in practice the beneficial value of taking a risk with information security is almost completely discounted. It is commonly dismissed as "being lucky", "taking a chance", "getting away with it" rather than implying a calculated outcome of deliberate decisions.

Information assets comprise all forms of information (both tangible and intangible such as printed matter, computer data and knowledge) plus the technology and supporting processes used to gather, process, store and communicate information. Information assets are a subset of all the organization's assets albeit with a significant overlap in terms of IT equipment (hardware – a physical asset) and knowledge or know-how (an important component of the value of our people).

"Risk management plays a critical role in protecting an organization's assets, and therefore its mission, from IT-related risk"

[NIST SP800-30 Risk management guide for IT](#)

The following lists show examples of commonplace information security threats, vulnerabilities and impacts that are worth managing in most organizations. Lists like these are sometimes used to ensure that risk

assessments consider a full range of possibilities:

Typical information security threats

- Malware such as worms and Trojans
- Hackers and crackers, whether Out There on the Internet or working on the corporate LAN
- Fires, floods, extreme weather and natural disasters
- Fraudsters and con-merchants
- Organized crime

Typical information security vulnerabilities

- Increasing reliance on increasingly complex IT systems and networks
- Human error and fallibility
- Bugs and design flaws such as buffer overflows and poorly designed or implemented technical security controls
- Lack of security awareness (no, surely not!)

Typical information security impacts

- Loss of confidentiality, resulting in the unauthorized and inappropriate disclosure of proprietary, personal or other private information
- Loss of integrity e.g. incomplete or inaccurate information used to make inappropriate decisions
- Loss of availability: the popularity of electronic/online business makes the commercial impacts of availability failure all too evident:

Industry	Application	Loss per hour of downtime
Financial	Brokerage operations	\$6,500,000
	Credit card sales	\$2,600,000
Media	Pay-per-view	\$150,000
	Home shopping (TV)	\$113,000
Retail	Catalog sales	\$90,000
Transportation	Airline reservations	\$89,500

Source: Gartner Group and Contingency Planning Research cited by Timothy Braithwaite in "Securing E-Business" (Wiley, 2002)

Business *versus* information security risks

Information security risks have some unique characteristics that make assessing and managing them that bit more difficult. The following analysis by Donn Parker compares risk in the context of information security with that in general business life.

1. Security risk: Involuntary risk of unknown value cannot be avoided.

Business risk: Voluntary discretionary investment decision can be made.

2. Security risk: Explicit sources of risk are not identifiable.

Business risk: Competitors are known.

3. Security risk: Adversaries' skills, knowledge, resources, authority, motives, and objectives are unknown.

Business risk: Competitors' skills, knowledge, resources, authority, motives, and objectives are known.

4. Security risk: Adversaries normally lie, cheat, deceive, and act irrationally.

Business risk: Predictable competitors normally follow ethical practices.

5. Security risk: Return on Investment is negative, unknown, and not provable.

Business risk: ROI is zero or positive and can be easily demonstrated.

6. Security risk: Positive benefit is absence of unknown possible loss.

Business risk: Positive benefit is measurable profit.

7. Security risk: Negative result is unlimited, unknown loss. Business risk: Loss is limited to investment.

8. Security risk: Risk assessment is not verifiable because results are obscure.

Business risk: Risk assessment is verifiable by obvious results.

9. Security risk: Amateurs perform risk assessment. Business risk:

Professional risk managers perform risk assessment.

10. Security risk: Limited resources are allocated for risk assessment.

Business risk: Generous resources are allocated for risk assessment.

Risks associated with the management of information security

As noted earlier, analyzing and characterizing information security risks is only part of what we need to do to bring them under control, so let's move on to look at the risks associated with *managing* information security.

1. Threats

Legal and regulatory pressures are increasingly affecting the management of information security. Within the past two decades, we have seen firstly tortuous attempts to apply laws that pre-date the IT revolution to IT-related situations, then the emergence of data protection and software copyright regulations, and more recently the identification of information security obligations arising from governance, freedom of information, privacy, anti-terrorism, anti-money-laundering and various other issues. The combined effect of the raft of legislation is a substantial threat to any organization, or for that matter individual, who fails to manage information security properly. Jail terms, fines and career-limiting disciplinary actions are more than just possible. Even if one has been diligent, acted in good faith and simply fallen prey to adverse circumstances (a.k.a. "having a bad day"), it is tough to prove beyond reasonable doubt that all necessary steps have been taken to secure information assets under one's custodianship.

Public ridicule is a genuine possibility if information security is seriously mismanaged: just ask any member of the British Government about the recent incidents where secret intelligence information on Al Qaeda was left on trains. This is in addition to the potential impact on national and indeed global security.

Even within the organization, unrealistic expectations, especially from those managers who still view this whole area as "IT's problem", cause problems for risk management professionals who cannot realistically determine or address information security risks on behalf of the entire business. They simply do not have the wider business perspective. If managers are reluctant to invest their time to help assess the information security risks and requirements in their domains, is it any surprise if serious

information security risks remain unmitigated and incidents continue to occur?

Mismanagement can also increase risks, for example if executives insist on releasing or implementing software that is not sufficiently stable or secure. Software development project teams often experience extreme pressure from management to release immature IT systems by predetermined deadlines, even though the deadlines are seldom absolutely fixed ("Y2K" being a noteworthy exception).

2. Vulnerabilities

It has long been our conviction that information security is primarily a human behavioral and psychological issue, and so too of course is the management of information security. At the same time, however, a significant proportion of information security risks and controls are technology-related, requiring a high degree of technical competence to understand let alone resolve the issues. Effectively managing information security therefore requires that the managers possess that rare mix of social and technological skills – politically adept as well as technically competent.

This line of reasoning suggests a number of vulnerabilities or inherent concerns:

- Good information security managers are in short supply whilst the level of demand is increasing. On top of the routine pressures and stressful peaks endemic in their line of work, incompetent personnel management is likely to lead to recruitment and retention problems in stressful occupations for any organization;
- IT careers naturally tend to attract people with a bent for technology. There is a grain of truth in the stereotypical image of a teenage computer geek, hunched over the keyboard and totally absorbed with the computer to the exclusion of 'normal' social relations. That's not to say that IT people are totally unsociable, just that many seem to go through a phase of voluntary social exclusion (anyone for "Technologists Anonymous"?).

A further information security management vulnerability arises from the concepts of trust and integrity. Security is all about protecting valuable assets from harm, often requiring privileged access to those assets. The people responsible for protecting assets have ample

opportunity to abuse their privileged positions. The controls to guard against incompetent, untrustworthy, unreliable and fraudulent information security managers are relatively weak – trust is by far the most important control.

The trust/integrity issue is even more obvious in the case of outsourcing of services in general, and especially outsourcing information security management. Client organizations place a great deal of trust in the third parties managing their systems and networks, with security management being a particular concern.

3. Impacts

Inadequacies in the information security management function typically come to light in a crisis situation, perhaps as the result of information security incident. Proving a causative link between poor information security management and an incident is not always easy however. Failing to manage information security properly may not lead directly to security incidents and losses but it is surely a major contributory factor, in much the same way that negligent vehicle maintenance inevitably leads to an increase in vehicle accidents. This comes back to the point that information security is a risk management activity, a probabilistic rather than deterministic function. You may just be lucky!

In economically-challenged times, the security budget is an 'obvious' candidate for reduction (along with training and awareness, unfortunately!). The problem is that cutting back on information security expenditure usually has delayed rather than immediate effects. ■

ISO/IEC 27005, a new risk management standard

With perfect timing for this security awareness module, [ISO/IEC 27005:2008](#) was released at the end of June. The full title of ISO/IEC 27005 is "Information technology -- Security techniques -- Information security risk management".

At around 60 sides, ISO/IEC 27005 is a heavyweight standard although the main part is just 24 pages, the rest being mostly annexes with examples and further information for users. There is quite a lot of meat on the bones, reflecting the complexities in this area.

Although the standard defines risk as "a combination of the consequences that would follow from the occurrence of an unwanted event and the likelihood of the occurrence of the event", the risk analysis process outlined in the standard indicates the need to identify information assets at risk, the potential threats or threat sources, the potential vulnerabilities and the potential consequences (impacts) if risks materialize. Examples of threats, vulnerabilities and impacts are tabulated in the annexes; although incomplete, these may prove useful for brainstorming risks relating to information assets under evaluation. It is clearly implied that automated system security vulnerability assessment tools are insufficient for risk analysis without taking into account other vulnerabilities plus the threats and impacts.

ISO/IEC 27005 includes a section and annex on defining the scope and boundaries of information security risk management which should match the scope of an organization's Information Security Management System.














The standard doesn't specify, recommend or even name any specific method (such as those listed in the [ISO27k FAQ](#)), although it does specify a structured, systematic and rigorous method of analyzing risks through to creating the risk treatment plan. It remains deliberately agnostic about quantitative and qualitative risk assessment methods, essentially recommending that users choose whatever methods suit them best, and noting that they are both methods of estimating, not defining, risks. Note the plural - 'methods' - the implication being that different methods might be used for, say, a high-level risk assessment followed by more in-depth risk analysis on the high risk areas. The pros and cons of quantitative *versus* qualitative methods do get a mention.

The steps in the process are (mostly) defined to the level of inputs → actions → outputs, with additional "implementation guidance" in similar style to [ISO/IEC 27002](#).



The standard incorporates some iterative elements e.g. if the results of an assessment are unsatisfactory, you loop-back to the inputs and have another run through. For those of us who think in pictures, there are useful figures giving an overview of the whole process and more detail on the *risk assessment* → *risk treatment* → *residual risk* bits. ■


Contents of the NoticeBored awareness module for July


Awareness materials for all employees

1. **Awareness seminar: infosec risk mgmt**  15 slides outline information security and risk management issues that everyone should know.
2. **Awareness posters: infosec risk mgmt**  x20 Six new poster images to remind everyone about risk & security management, plus 14 more that were released previously.
3. **Screensavers: infosec risk management**  x4 Reinforce key awareness messages daily.
4. **Staff guideline: infosec risk mgmt**  2 pages A double sided overview of the subject.
5. **Staff guideline: data backups**  1 page Advice on taking and retrieving backups.
6. **Case studies: infosec mgmt**  4 x 2 pages ea. Four information security risk management scenarios to consider, discuss and learn from.
7. **Top tips: infosec management**  1 page
8. **Take home messages: infosec mgmt**  1 p.
9. **Crossword puzzle: infosec management** 
10. **Security awareness survey form**  1 page
11. **Security awareness test: infosec mgmt**  1 p. Check comprehension and recall.
12. **Glossary: infosec risk mgmt terms**  5 p. A glossary with hyperlinked explanations.
13. **Links: infosec risk management resources**  Annotated hyperlinks to [information security risk management resources](#) on the Internet.

Awareness materials for managers

14. **Mind-maps: infosec risk mgmt**  x3 Pictorial representations of the topic.
15. **Board agenda: managing sec risks**  1 page Getting senior executives to discuss security risk management helps garner their support for it.

16. **Model policy: infosec risk mgmt**  4 pages
4 axioms supported by 6 policy statements.

17. **Mgmt seminar: infosec mgmt**  11 slides
Discusses things from management's viewpoint.

18. **Exec briefing: infosec risk mgmt**  1 page

19. **Exec briefing: infosec mgmt**  1 page

Two short exec briefings focusing on the information security risk management process and governance aspects, respectively.

20. **Mgmt briefing: infosec mgmt**  2 pages

Supplemental notes for the seminar (item #17).

21. **Mgmt brief: outsourcing infosec mgmt**  2 p.

While outsourcing such a trusted function itself carries some risk, there are also potential advantages in having information security managed by dedicated, trained and experienced professionals.

22. **Mgmt briefing: infosec mgmt metrics**  4 p.

Measures to improve your information security and risk management activities.

Awareness materials for IT pro's

23. **Newsletter: infosec risk mgmt**  8 pages

Introduces the topic and explores the risks.

24. **Awareness activities for July**  5 pages

Ideas to keep your awareness program rolling.

25. **Tech seminar: infosec risk mgmt**  9 slides

Describes the processes used to identify and bring information security risks under control.

26. **Tech briefing: infosec risk mgmt**  3 pages

Summary notes on the topic. Seminar handout?

27. **White paper: infosec risk mgmt**  13 pages

A more detailed explanation of how information security risks are identified, prioritized, mitigated and monitored. Includes sample risk-control matrices as an appendix.

28. **Checklist: infosec risk mgmt controls**  9 p.

Assess your organization's information security and risk management activities against these good practice criteria. ■

NoticeBored topic diary

Awareness materials on the topics listed below are currently on the NoticeBored production line. To contribute to these modules, please email info@NoticeBored.com. We are always researching and looking for suggestions for new modules and different types or formats of awareness material. Email us your bright ideas and we'll see what we can do.

August – information security governance

Following directly on from this month's topic, we'll be looking into governance in the context of IT and information security, specifically. What does 'governance' mean, in practical terms? How does it affect NoticeBored's three target audiences? What are the essential elements that everyone needs to know about? Explore the questions and hopefully find some answers with NoticeBored next month.

September – email security (core topic)

Phishing (covered last month) is but one example of the information security threats that are communicated by electronic mail. Find out about many others such as 419 scams, malware, social engineering and unauthorized disclosure of confidential information, and learn how to deal with them, in September's NoticeBored module.

October – ethics

We're currently researching a completely new security awareness module for October covering ethics and morality. Self restraint is an important control in many spheres, including information security, but people sometimes need a little guidance on what they should and should not do, 'where to draw the line'. ■

NoticeBored & IsecT news

IsecT is on the move yet again, this time hopefully for good. We're moving to Hawke's Bay on the central East coast of North Island, New Zealand, not far from the Art Deco town of Napier, oh and some of the world's finest viticulture. Please forgive us if we are a little slow to respond to queries and inquiries during the next two weeks. If we hear the office phone ringing, it may take a while to figure which box it's in! Normal service will be resumed ASAP.

Information security resources

Apart from writing our own [blog](#) and contributing to the recently launched [\(ISC\)²](#) blog, we routinely follow about 40 others, finding them an interesting source of news and commentary on information security, risk management and related issues. To see what we're reading lately, check out the slow-loading blogroll to the right of the items posted at blog.noticebored.com and do let us know if *you* run a blog in this area.

As soon as we find time, we'll be publishing several more information security book reviews on the NoticeBored site, including one on Gary McGraw's "Software Security: Building Security In", a new book on achieving compliance with PCI-DSS, and "The Official Guide to the CISSP CBK" by Tipton and Henry. Some useful information sources there: find out which ones are really worth reading on our website. ■



Newsletter published by:

[IsecT Ltd.](#)
1262 Taihape Road
Hawkes Bay
New Zealand

Tel: +64 6874 3344

Copyright and disclaimer

All NoticeBored materials including this newsletter are protected by international copyright law. For more information, please contact the copyright holder, IsecT Limited (visit www.isect.com or see above for our contact details).

You are encouraged to circulate the Adobe Acrobat PDF version of this newsletter to anyone *provided* that it remains unchanged and intact (including this copyright notice), is not embedded in any other product or service and is provided free of charge. The MS Word RTF version is provided to customers purely for internal use as per the NoticeBored license.

The information in this newsletter is provided free, for information only and 'as is'. Whilst believed correct, it is in no way comprehensive. It is provided for interest only and is not intended to be relied upon as formal advice. It is not legal advice. Seek your own legal advice from a qualified legal practitioner, not us. No liability is accepted for any errors or for any losses that may be incurred if any such information is relied upon.