



**An ISSA UK and Secoda Risk  
Management White Paper**

## **SECURITY AND THE GROWING INSIDER THREAT**

*Author: Adrian Wright  
Director of Projects ISSA-UK  
Managing Director  
Secoda Risk Management Ltd*

**15 February 2010**

## Contents

---

Introduction	2
About this paper	2
Confidentiality & attribution	2
Session objectives	3
Workshop dates & venues	3
Delegate feedback	3
Workshop topics	3
Event benefits	3
Workshop tasks	4
Session: Insider Threats	5
Key controls: non-malicious	6
Key controls: malicious acts	8
Speaker biographies	11
Company information	11
Reference materials	12
Acknowledgements	12

## Introduction

Two of the most important risk topics to emerge in the last year are the explosive emergence of cloud computing and the growing risks presented by insiders within organisations.

Both of these trends are fuelled by the need to cut staffing and technology costs, but organisations need to be vigilant in measuring and controlling risk in order to remain safe.

Member interest in these topics prompted the ISSA in conjunction with Secoda Risk Management to organise a series of three, half day workshop seminars for regional ISSA groups, which were kindly hosted by our sponsors KPMG. These highly interactive workshops brought together practitioners of information security, audit and risk from all sectors including finance, health, education and local government; each bringing their own unique perspectives and experiences on the risks and benefits of using cloud-based services and how they are assessing and addressing their respective insider threats.

## About this paper

This paper brings together and summarises the various risks, benefits and practical tips arising from all three workshop events for the benefit of attendees and the ISSA membership as a whole.

This white paper covers the **Insider Threat** stream from the above workshop sessions. A companion white paper is also available which deals with the **Cloud Computing** theme.

## Confidentiality & attribution

Workshop sessions were conducted under the Chatham House Rule<sup>1</sup> thereby allowing attendees to speak freely about their experiences, concerns and security measures without compromising their organisation's privacy.

Consequently, apart from the presenters, no attendee organisation or individual is associated with the various issues or controls noted in this paper, or any other material arising from these sessions but only noted by industry sector where appropriate.

---

<sup>1</sup> <http://www.chathamhouse.org.uk/about/chathamhouserule/>

## Session objectives

The presentations and workshop sessions were to enable attendees to identify the types of insider threats to which organisations are becoming exposed and via moderated workshop sessions discover the techniques your peers are using to balance risk and reward in today's challenging economy.

Handouts provided before and during these sessions, copies of the PowerPoint presentations used during the sessions and at a subsequent summary presentation given at the ISSA Chapter Meeting on 10<sup>th</sup> December along with the findings in this paper and its companion white paper on Cloud Computing, comprise the 'takeaway' deliverables being made available to workshop attendees and the ISSA membership overall.

## Workshop dates and venues

Three half day presentations + workshops

- Edinburgh      20<sup>th</sup> Nov 09
- Bristol          27<sup>th</sup> Nov 09
- Manchester      4<sup>th</sup> Dec 09

## Delegate feedback

Overall, attendees rated all workshops at 5/5 – 100% satisfaction. Below are selections of comments from the feedback forms:

*'Well focused'*

*'Workshops useful and interesting for exchanging ideas'*

*'Firstly many thanks for putting on a great event at Bristol on Friday. It was excellent to network with other IT professionals and the structure of the day (i.e. the workshop programme) allowed us to share ideas and concepts. It also continued to generate much conversation on the walk back to the train station!'*

*'Can I say what a very enjoyable time Friday was. I felt that the event was exceptionally productive and insightful. I look forward to seeing the results of the Whitepaper.'*

*'It was a most enjoyable session and really got me back into thinking the "correct" way'.*

*'I enjoyed the format and makes a change from the normal PowerPoint presentations'*

*'Refreshing to be able to interact with peers within a meeting'*

## Workshop topics

### 1: Develop a strategy for dealing with insider threats

Each workshop was preceded by a short presentation to introduce the topic, give examples and state the format and desired outcomes for the workshop itself. Delegates were divided into two teams of between 6-12 people per team working in different areas and then brought back to the main room to present their respective conclusions to the whole audience.

## Event Benefits

- Sharing of knowledge, experience and solutions cross-sector
- Brainstorming to uncover unforeseen issues & controls
- Encourage information sharing on these topics
- Networking opportunities and connections
- Produce useful guidance & checklists
- Platform for further work in these areas

## **Workshop Tasks**

Each team was tasked with the following actions to discuss, prioritise and then present back to the main group. Moderators oversaw each session and collated the collective output of all workshops, the summarised results of which form the basis of this report.

- Consider the various types and sources of insider threats, and derive a common set of threats and actors that can be used to assess the merits of countermeasure proposals;
- Identify the types of risks involved, and whether these are new or changed risks or levels of risk;
- Define at a high level a list of technical, procedural, legal, framework (e.g. policies) and contractual controls to mitigate the risks;
- Produce a checklist of controls that could form the basis of a detailed audit plan;
- Nominate a spokesperson to present your list to the main audience, and;
- Be prepared to answer questions or justify particular items or omissions.

## **Workshop Session: Managing the Insider Threat**

The 2007 E-Crime Watch Survey found that in cases where respondents could identify the perpetrator of an electronic crime, 31% were committed by insiders. In addition, 49% of respondents experienced at least one malicious, deliberate insider incident in the previous year. The impact from insider attacks can be devastating. One employee working for a manufacturer stole blueprints containing trade secrets worth \$100 million, and sold them to a Taiwanese competitor.

### **Develop a strategy for dealing with insider threats**

In these days of downsizing and job reduction, incidents involving malicious or negligent loss and disruption to data have risen sharply to unprecedented levels. Fear of impending redundancies, increasing job competition, outsourcing and mergers are all factors that can motivate certain employees to act in ways that can jeopardise business.

This workshop session identified the types of malicious or accidental threats to data and systems that can occur, examined case studies of recent incidents and allowed participants to formulate strategies for managing risk and responding to incidents.

### **Workshop format**

The workshop sessions on Managing the Insider Threat were conducted in exactly the same format as the Cloud Computing workshops, with one significant difference: Due to the sheer scope of this topic, we decided to divide the Insider Threat workshop teams into two separate streams. Teams A&C were tasked at looking into the aspects of the insider threat that could be best addressed by **Technical controls**, while Teams B&D examined those aspects of managing the insider threat that would be served by **Non-Technical measures**, such as policies, awareness, legal, HR, whistleblowing<sup>2</sup> etc.

All teams came together again at the end of the sessions and presented their respective findings to the whole audience with subsequent questions and debate.

### **Malicious Vs Accidental threats**

All workshop teams quickly identified that insider threats could be split into two causal groups:

- Malicious Threats – where there was an element of premeditated intent to harm or steal;
- &
- Accidental Threats – often due to lack of training, naivety, carelessness or human error.

### **Current trends**

In these times of increasing unemployment and debt, the motivation to commit crime has also increased. Fears about impending redundancies, wage cuts or freezes and unpopular acquisitions or mergers have all served to increase workplace tensions and tempt many workers to carry out dishonest or malicious acts against their employer.

In particular there has been a recent sharp rise in acts of sabotage of computer records by former employees and theft of proprietary information such as customer lists and proprietary software source code. Recent examples from the press and other sources have served to emphasise and evidence this trend.

### **Accidental threats**

Reducing the risks arising from non-malicious acts by employees is significantly more difficult to address than protecting the organisation against malicious acts for two principal reasons:

---

<sup>2</sup> <http://en.wikipedia.org/wiki/Whistleblower>

Firstly, the number of *threat actors* (persons who could potentially cause a breach or loss to occur) equates to everyone in the organisation from the standpoint of non-malicious, e.g. accidental threats. In other words, virtually any employee or contractor has the potential to cause major loss to occur if they accidentally or negligently mess things up.

Whereas we assume (hope) that only a tiny proportion of insiders would be motivated and tempted to deliberately perform a malicious or criminal act; as most people are essentially honest. Consequently the prospect of having to safeguard *anything* that could go wrong and result in a material loss, from *everyone* who could potentially cause those things to go wrong through human error or negligence, is a massive undertaking. Nonetheless, we do need to strive to reduce risks arising from non-malicious as well as malicious actors, because some of the world's biggest losses have been down to non-malicious actions by individuals.

#### **Example: Excel error leaves Barclays with unwanted Lehman assets**

*In 2008 investment bank Lehman Brothers collapsed into bankruptcy. Three days later, lawyers for Barclays Capital were finishing up an agreement to purchase some of Lehman's assets in time to meet a bankruptcy court deadline. Those assets were listed in a spreadsheet with a column indicating whether those assets should be acquired or not: "Y" for yes and "N" for no. Four hours before the deadline the spreadsheet had to be converted from Excel to a PDF to be submitted to the court. A clerk was instructed to cut out certain columns and turn it into a PDF. No one noticed that the new version was 179 rows longer than the original. In fact, 20% of the items in the spreadsheet -- the ones with an "N" reappeared and the whole list was presented to the court without anyone noticing the mistake.*

*Now Barclays is hoping the court will let it off the hook for millions of dollars in assets it never intended to buy.*

### **Key Controls to Reduce Risks from Non-Malicious Acts**

It was generally agreed that the most important controls to reducing risks arising from non-malicious human actions are around **Training** and **Awareness**. If people are shown the correct way of doing things and warned about the consequences of doing things incorrectly, then most will naturally comply; provided the reasons are well understood and the process of complying is not onerous.

A clearly written and presented **Policy** acts as a vital reference for the training and awareness piece. To be effective the Policy must also use mandatory terms, e.g. 'must' and 'will' rather than 'should' or 'can', and must also carry the authority and backing of top management in order to be effective. In addition to security, policies must also inform and mandate staff to comply with things like acceptable use of systems and the internet, staff handbook (HR), personal data, and health & safety.

Creating a corporate culture founded on Awareness and Compliance is the most effective strategy for reducing overall risk and meeting all legal and regulatory obligations. As part of this it is vital to mandate **Ownership** and **Accountability** for specific assets and adherence to laid-down procedures.

**Segregation of duties** and **restricting access privileges** to all systems and physical areas help to reduce the likelihood and impact of any accidental error, by restricting the range of assets that could be affected. By applying the 'principle of least privilege' in allowing each employee only the minimum level of privilege and access needed to perform their work, drastically reduces the overall 'attack surface' (or perhaps more appropriately – 'misoperation surface') open to potential abuse or error. Similarly, access to all sensitive and critical information should be limited on the basis of a 'need-to-know' policy.

**Change management** controls help ensure that any changes to software applications, systems, hardware and documents are fully tested and approved prior to being put into operation or proliferated further. Software testing and QA help to reduce accidental failures and helps spot any maliciously-introduced ones also.

## **Coaching**

Staff who are overworked or under pressure from internal or personal issues tend to perform badly and are more likely to make mistakes than workers who are focused on their job. Programmes that help identify and deal with employee stress and fatigue can help reduce the risk of errors being made and can help improve productivity overall.

## **Data De-duplication**

Most organisations have at least 5 copies of every piece of information, email and document distributed across various different systems, databases etc. Many have 10-15 copies of each item. This not only has implications for Data Protection, Freedom of Information and Legal Discovery – by making subject access requests costly and disruptive – but increases the risk of data leakage by unnecessarily increasing the amount of information that needs protecting.

## **Environmental**

Information and business can be lost due to external factors, such as flood, hurricane, earthquake or pandemic; or by external non-malicious human acts such as workers drilling through power cables, cooling pipes or communications cables. These threats are typically outside of your control to avoid, but the risks and impacts are offset by having tried and tested Business Continuity Plans and Disaster Recovery mechanisms and procedures in place.

## **Audits and Control Self-assessments**

Regular audits and self-assessments on the presence and effectiveness of controls are useful in identifying weak areas before they cause a breach, and ensuring that remediation plans and responsibilities are assigned.

Control self-assessments make individual managers and data / asset owners responsible for performing their own mini-audits of information, assets and processes that they use or manage. The results of these assessments can feed into an overall register of assets and risks, which is an effective way of measuring and tracking risk ownership and management.

## **Data Leakage Prevention**

Clearly data loss can occur as a result of deliberate theft or sabotage, but the vast majority of data loss still occurs as a result of human error or negligence; such as unencrypted laptops, CDs or memory sticks being left on trains, non-shredded customer printouts being dumped, or unprotected media being lost in postal transit. A combination of training and awareness, together with enforcing technologies such as encryption, device authorisation and inspecting / controlling outbound email / FTP / web transfers etc are vital tools in preventing both malicious and non-malicious data leakage.

## **End User Computing**

'End user computing' (EUC) is a term used to describe how non-technical staff are able, using today's ordinary desktop environment, to create software applications and databases that can unwittingly expose organisations to significant risk. Users are able to create spreadsheet tools with embedded macros and calculations that store and process thousands of customer records, or create local databases that may be copied and proliferated in many ways.

Unfortunately, these desktop-developed applications go 'under-the-radar' insofar as normal development, testing and change management processes are concerned and usually lack a proper data owner or custodian responsible for maintaining the security of the application and its associated data. Unauthorised and untested changes may be made, and there are few security controls to prevent data leakage occurring through loss or proliferation of the tool and its contents. (*See above example re Barclays Capital / Lehman Bros*)

Many organisations, particularly in regulated business sectors, have undertaken programmes to identify high-risk EUCs and take action to reduce the risks that they pose. Where EUCs present a very high risk, such as having the capability of causing serious regulatory breaches;

there should be a plan in place to migrate the EUC function to core system applications where the applications and data can be properly owned, secured, monitored and change-managed.

In the case of medium or low risk EUCs, the approach is often to centrally register and monitor use of these applications subsequently, ensure data owners are assigned and made responsible, and/or apply an additional layer of technical control to restrict access and prevent unauthorised changes to the application or its data.

## **Key Controls to Reduce Risks from Malicious Acts**

In the case of deliberate insider acts like theft, sabotage and improper use, we expect there to be a very small number of threat actors (bad people) but they are afforded a high level of opportunity and access to carry out misdeeds. Unfortunately all organisations have relatively 'soft' internal security compared to the controls in place to protect against external attacks. Also the internal 'attack surface' is extremely high; as potentially all internal systems, networks and information can be accessed by people working inside the organisation.

It was generally agreed that **HR policies and procedures** play an important role in preventing miscreants getting into the organisation in the first place. **Employee vetting** and other background checks should verify identity, right to work in the country specified, and where possible unearth previous criminal convictions, undeclared insolvency etc. Also in times of employment uncertainty (like now), your organisation needs to better anticipate and manage negative workplace issues, e.g. layoffs and compensation.

## **Monitoring**

Monitoring of employee activity needs to be conducted lawfully, and ideally with the informed consent of employees. Detecting patterns of misuse, such as access to prohibited internet sites, downloading of improper or illegal material, and attempts to access systems, areas and resources to which an individual has no legitimate need; are all detective measures that can help identify problem behaviour before an incident occurs. Audit logs and reports from monitoring systems also provide an evidential trail that can assist in subsequent dismissal or prosecution.

It is essential that any monitoring logs and alerts are acted on and followed up, and that any evidence from an incident or discovery is preserved in accordance with proper forensic practices.

## **Policies**

Mandatory policies and procedures which employees are required to read and acknowledge are an important cornerstone of internal prevention, provided they are rigorously enforced. Policies should make it clear not only what is required of staff, but also what the consequences are if the policy is deliberately circumvented or breached. Appropriate Use Policies are essential to controlling risks.

Policies and procedures also help educate and raise awareness of others in the organisation that have a duty to report any suspicious or improper behaviour by colleagues.

## **Access Controls**

Implementing good access control and authorisation ensures that a malicious insider is not able to access systems, information and physical area that they are not entitled to. In particular ensuring that unattended PCs are automatically logged off, building access controls are in place to prevent access to sensitive or mission-critical areas, and strong authentication is used to prevent password abuse.

One vital area to address is that of termination procedures. Many breaches have occurred due to failure to deactivate computer access following termination. Procedures must include removal of all system accounts and reclaiming information assets such as company-owned mobile devices, access tokens, building access and remote VPN facilities, which should all be inventoried and deactivated immediately upon departure.

## Encryption and DLP

Encryption of sensitive information combined with Data Loss Prevention measures make it harder for a malicious insider to get hold of, and transfer-out large quantities of unauthorised data. Some systems do not actually prevent the copying of internal data onto removable media, but can nonetheless raise alerts that can be investigated if transfers appear suspicious. Alternatively DLP controls can be enforced rigorously, ensuring that sensitive information is entirely contained within corporate systems and networks.

System lockdown is additionally necessary to ensure that any technical controls like DLP – can be circumvented by a user gaining access to underlying operating systems, applications or the network level. Removal of unwanted media interfaces and devices like CD/DVD writers, open wireless connections and flash card readers are all measures that may be needed to ensure that other DLP controls are not circumvented.

## Protection against Programmed Threats

Recently there has been a rise in publicised breaches involving internal programmed threats such as planting logic bombs or malicious deletion of company data.

*Last year, a former IT contractor at the giant US mortgage bank Fannie Mae was indicted for having planted – on the day he was fired - a logic bomb<sup>3</sup> that would have trashed all 4,000 of its production servers had it not been found.*

*A former sysadmin at UBS Paine Webber was last year sentenced to 8 years jail without parole for unleashing a logic bomb on the company's network and causing \$3m damage. Roger Duronio, 64, who was found guilty of computer fraud, was also ordered to pay \$3.1 million in restitution to UBS.*

Disgruntled software programmers and technical staff present a major risk, as they have the necessary access and knowledge to embed programmed threats in software applications, or as scripted scheduled processes on company systems. This type of malicious code or script is very difficult to detect, but has the potential to cause the most loss or damage to information and service availability.

Programmers have also been known to leave 'back doors' in software, to allow them to re-enter systems and applications even after they or the system have moved elsewhere.

The best ways of reducing this type of threat are:

1. Peer review of developed or changed code. Get another developer to review and check the code line-by-line before release;
2. Thoroughly test new software before release. Testing can uncover hidden bugs and anomalies, and should be conducted in a test environment segregated from all production systems and data;
3. Secure code storage and MD5 checksums. Use of a secure code store like SourceForge Enterprise, Microsoft SourceSafe, or SourceGear Vault to manage under-development software and change control. Changes to code can be logged and tracked before checking-in the current version; allowing collaboration and peer review processes to happen – thereby improving oversight and supervision. The use of hash checksums helps prevent undetected malicious alterations or unauthorised modifications from being added later;
4. Removal / banning of all development tools, compilers, decompilers and debuggers like Visual Studio etc from non-development systems. These powerful tools give

---

<sup>3</sup> [http://wapedia.mobi/en/Logic\\_bomb](http://wapedia.mobi/en/Logic_bomb)

opportunities to hackers and can be used by non-developers to make unauthorised changes to applications.

### Firewalls and filters

Internal network segregation can help ensure the integrity of production systems, when segregated away from general user networks. Filtering outbound traffic as well as inbound can help block or identify malicious behaviour and the unauthorised export of internal information via email, web or file transfers.

### Risk Assessment & Countermeasure Selection

As with all Risk Management disciplines, it is important that each organisation carries out a proper risk assessment, analysing threats and vulnerabilities, identify key assets, and implement appropriate controls to reduce risk to an acceptable level for the business.

One group devised a matrix for mapping identified threats to the classes of controls needed to mitigate. Broadly, these control objectives range from the most favourable outcome on the left i.e. prevent it happening, to the least favourable outcome i.e. prosecute the guilty, on the right.

#### Example matrix of threats and control objectives:

	Prevent	Deter	Mitigate	Stop	Evidence	Discipline
Theft						
Service Interruption						
Modification of Service						
Accidental/unintentional						
Ignorance of IS landscape						
Augmentation of IS landscape						
Education and re-education						

1. Prevention of the threat becoming an impact is obviously the most favourable option, but in practice it is never possible to achieve all the time, and some breaches will still occur;
2. If we can't totally prevent an attack happening, we can reduce its likelihood by deterring an attacker from trying in the first place. Making ourselves appear secure, putting up clear warnings, and stating the penalties that exist for transgression – are all examples of this strategy;
3. If an attack occurs anyway, we should do what we can to mitigate the impact. Limiting the quantity and value of information held, and having an incident response plan in place, are examples of this class of control objective;
4. Stop or arrest is where, despite our best efforts, a breach has occurred and we need to quickly detect it, identify the source or point of breach, and then immediately close the breach to prevent further loss occurring;
5. Having done this, it is important to ensure that any evidence that could identify the source and culprit is preserved in a way that allows it to be used in any subsequent disciplinary, enforcement or legal action;
6. Finally, and particularly in regard to insider breaches of security or policy; there must be a clear disciplinary policy and procedure in place to deal with offenders. Where used, it is also important to ensure that all staff understand that there are both rules in place – and that there is a penalty for flouting them; "Pour l'encouragement d'les autres!"

## Speaker Biographies

### Your Presenters and Moderators

**Adrian Wright** is one of the UK's most experienced technology risk practitioners. With 25 years in IT, 8 years as global head of information security at Reuters and more recently founder and lead consultant at Secoda Risk Management, he lectures and consults globally on all aspects of information security, governance risk and compliance. His key clients include FTSE 100 listed companies and other blue chip names in all sectors plus SMEs and professional bodies. Adrian is a Certified Information Systems Auditor and Director of Projects for ISSA-UK.

Contact details: [adrian.wright@secoda.com](mailto:adrian.wright@secoda.com) tel: +44 (0)8456 4 27001 / +44 (0)780 363 9704

Website: [www.secoda.com](http://www.secoda.com)

**Nick Thomas** is a knowledgeable security professional with over a decade of experience supporting organisations and their information security needs. Nick is an active board member of the ISSA UK Chapter and product specialist at Qualys where his role helps businesses address their security and compliance requirements. Nick is an advocate of cloud computing and passionately offers solutions involving the 'as a service' model.

Contact details: [nthomas@qualys.com](mailto:nthomas@qualys.com) tel: +44 (0)1753 872094 / + 44 (0)7701 036 696

Website: [www.qualys.com](http://www.qualys.com)

### About Secoda and the ISSA

**Secoda Risk Management:** Was formed in 2002 by former heads of Information Security and Technology Risk Management from some of the world's best-known organisations. Secoda develops, sells and maintains the RuleSafe suite of GRC software applications, as well as providing the support and consulting services on which many thousands of corporate users depend for their employee GRC programmes.

Our mission is one of continual evolution and development of high quality products and services that uniquely serve our customer's GRC needs, through our software, professional solutions, services and consulting operations. [www.secoda.com](http://www.secoda.com)

**ISSA:** The Information Systems Security Association (ISSA) is a not-for-profit, international organisation of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

Members include practitioners at all levels of the security field in a broad range of industries, such as communications, education, healthcare, manufacturing, financial and government.

ISSA was formed over 25 years ago and now has over 10,000 members in over 140 chapters worldwide, of which ISSA-UK is the second largest ISSA chapter in the world with a membership base of over 1500 and growing at a rate of 12%.

With active participation from individuals and chapters all over the world, the ISSA is the largest international, not-for-profit association specifically for information security professionals. [www.issa-uk.org](http://www.issa-uk.org)

## Reference Materials

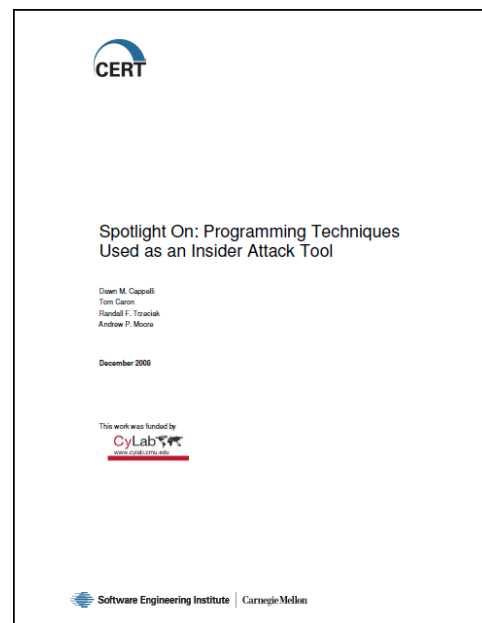
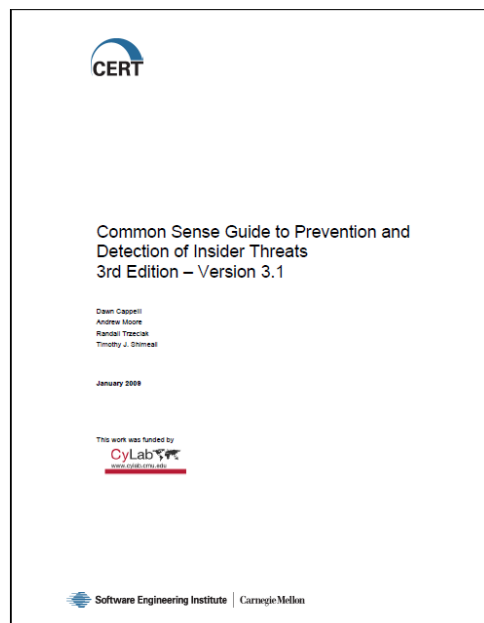
Several good reference sources on preventing insider breaches were put forward. Both of these publications are from CERT (Computer Emergency Response Team at Carnegie Mellon):

- *Common Sense Guide to Prevention and Detection of Insider Threats 3rd Edition – V3.1 Jan 2009*
- *Programming Techniques Used as an Insider Attack Tool - Dec 2008*

Both of these publications are available free of charge and may be downloaded from CERT at:

<http://www.cert.org/archive/pdf/CSG-V3.pdf>

[http://www.cert.org/archive/pdf/insiderthreat\\_programmers\\_1208.pdf](http://www.cert.org/archive/pdf/insiderthreat_programmers_1208.pdf)



## Acknowledgements

We wish to acknowledge and express thanks to the following individuals and sponsor organisations for kindly agreeing to contribute their time and resources to help host and deliver these workshops:

- KPMG – sponsors and workshop venue hosts
- Nick Thomas – VP Internet Services ISSA-UK; speaker and workshop co-moderator
- Geoff Harris – President of ISSA-UK; workshop organisation and management
- Roger Ellis – Treasurer of ISSA-UK; workshop co-moderator
- Sophie Wingrove – Administrator ISSA-UK; workshop organisation and facilitation
- Louis Gamon – Director of Administration and Alliances ISSA-UK; workshop co-moderator

end. Doc version 1.3 Release date 15 Feb 2010