Organizational Security and the Insider Threat: Malicious, Negligent and Well-Meaning Insiders

David S. Wall, PhD. Durham University, UK
<d.s.wall@durham.ac.uk>
Organizational Security and the Insider Threat: Malicious, Negligent and Well-Meaning Insiders

Contents

Introduction .................................................................................................................. 1
Insiders and the Prevailing ‘Outsider’ Data Loss Threat Model ........................................ 1
The Nature of the Insider Threat ................................................................................... 2
The Non-Malicious Insider Threat to the Organization ..................................................... 6
The Implications of the New Insider Threat Model for Security Policy ................................ 8
Risk Groups .................................................................................................................. 9
Data Spillage and the Stuxnet Warning ............................................................................ 11
Reducing the Insider Threat ......................................................................................... 12
Reducing Data Loss Incidents ......................................................................................... 12
Recommendations for Preventing Data Spillage .............................................................. 13
How to Learn More about Data Loss Prevention .............................................................. 14
References ..................................................................................................................... 15
Introduction
There was a time when organizational security mainly focused upon keeping unwanted intruders out of the organization to prevent them from doing harm. As organizations turned to electronic rather than physical informational exchanges in order to improve their efficiencies and expand their scope, the organizational security mission broadened to encompass the new security challenges this shift presented. Today, the critical importance of electronic information exchanges in the operation of the organization means that the security lens now focuses also upon the custodians of exchanged data, those inside the organization in addition to those outside it.

This paper draws upon the finding of recent data loss surveys and other relevant information sources to develop an understanding of the nature of the insider threat to the organization. It will identify the salient discussion points and issues that assist organizations in formulating remediation strategies. Part one looks at the prevailing data loss threat model and introduces the problem of the insider threat. Part two deconstructs the insider threat in order to map out the respective risk profiles of the non-malicious and well-meaning insiders. Part three discusses the various options for security policy; options that should not simply demonize the well-meaning insider as another form of deviant or ‘criminal other’ but also address the problem from an organizational perspective.

Insiders and the Prevailing ‘Outsider’ Data Loss Threat Model
The debates over organizational information security have long been dominated by the need to keep dangerous outsiders such as hackers, fraudsters and those involved in industrial espionage from damaging its systems and itself. In more recent years the debates have broadened to include malicious insiders after they entered the threat landscape; to the point that participants in the debates appear to obsess on which of the two groups represents the greater threat to the organization. Both groups are in fact comprised of those who operate outside the organization’s norms and goal structure and whose actions seek to prey on the organization’s vulnerabilities in order to penetrate its computer systems, often as a means to defrauding it or stealing mission critical data. The ‘drama’ surrounding these enemies ‘without and within’ captures media and public attention, especially as their actions contribute to heightened public concerns about Internet safety. They are, however, not the focus of discussion here because there already exists a considerable amount of literature about malicious outsiders and insiders – see, for example, the reports by Symantec, 2008; 2009a; Verizon (2010) and other cyber-security companies, and also relevant chapters and references in books about cybercrime, for example, Wall (2007) and McQuade (2006), and many other books about cybercrime and criminals not listed here. They are not discussed here because while malicious outsiders and malicious insiders pose ‘the’ major threat to organizations, the attention paid to them in the security debates and security policy grossly underplays the threat constituted by the non-malicious insiders within the organization. They are the second major risk group working against the broader interests of the organization. Furthermore, the tendency to orient information security policies against the ‘bad guys’, the malicious insiders who abuse their access rights for personal gain, or the disgruntled insiders who wreak revenge by disrupting operations or humiliating the organization, ignores the complexity of the issue and can create adverse consequences. Not least that some well intentioned employees may feel that they are being treated like criminals, with a resulting loss of staff morale and the erosion of trust in organizational management and even the possible migration of some valuable employees to competitors and elsewhere.
**The Nature of the Insider Threat**

Data losses incurred by insiders are very costly to organizations as the following analysis of various reports of research into data losses, costs and incidents illustrates. The costs through losses have rapidly increased over the past decade along with the number of incidents. An analysis of the findings also indicates that different types of insiders have quite different threat profiles.

Ponemon’s calculations of the costs of breaches to organizations graphically illustrate the high stakes involved and why organizations should be concerned. The average organizational loss from reported data breaches in the U.S. rose from $6.65 million in 2008 to $6.75 million in 2009 with the cost of each compromised customer record rising from $202 to $204 respectively – almost 2% - less than in previous years (Ponemon, 2010a: 3). In the U.K. a slight decrease in the average organizational loss was found of just less than 3% from 2008 to 2009, although the average loss per breach rose by seven per cent from £60 to £64 (Ponemon, 2010b: 3), see Figure 1. Some cheer may be drawn from these relatively small changes when they are compared with the rises in previous years1, indicating the possible impact of improvements in security policies and associated training.

The percentage of losses specifically attributed to insider negligence was found to have declined slightly along with the overall number of insider caused breaches; decreases that could also be attributed to improvements in security awareness training (Ponemon, 2010a: 28). However, both the 2009 U.K. and U.S. samples still illustrated the large extent to which negligent insiders contribute to data breaches and also how costly to organizations that loss can be, even if the negligent costs are less than malicious ones. In the U.S., 40 per cent of data breaches (Ponemon, 2010a: 16) and 46 per cent in the UK (Ponemon, 2010b: 36) were estimated to be due to insider negligence. The losses are not only significant, but the analysis also shows that they result from the actions of a number of different types of insider. This point is brought out by the research data on incidents.

![Figure 1: Annual changes in overall costs of data breaches per unit.](image)

(Source: based upon statistics in Ponemon, 2010a: 3; Ponemon, 2009a: 3)

The Ponemon research makes the very important and useful distinction between malicious and non-malicious negligent insiders, but does not elaborate further upon the negligent insiders. The following CERT/USS studies help us further deconstruct the threat profile of the non-malicious insiders.

Randazzo et al., a research team comprised of members of the U.S. Secret Service National Threat Assessment Center and the CERT® Coordination Centre, studied known insider incidents relating to the banking and finance sector during the fiscal years of 2003 and 2004 (Randazzo et al., 2005). Banking and finance were one of thirteen critical infrastructure sectors prioritised by the President's Critical Infrastructure Protection Board in the 2003 The National Strategy to Secure Cyberspace (Whitehouse, 2003: 16). The study by Randazzo et al. came to a number of interesting and clear conclusions: most of the acts were committed whilst on the job with the incidents being detected by various methods and also by different people within the organization. Although financial gain was most offenders’ primary motivation and victim organizations suffered financial loss as a result of the incidents, the offenders were not found to share a common profile (Randazzo et al., 2005). A second U.S. Secret Service/ CERT® in 2005 (Keeney et al., 2005) analysed the role played by insiders in 49 specific attacks of sabotage upon the critical infrastructure between 1996 and 2002. The findings of this in-depth view of the insider threat largely reflected the many findings from the first study, but it also revealed some very interesting and important findings about the profile, psychology and motivations of malicious insiders. As might be expected, the findings confirmed that a negative work-related event triggered most actions. At the time of the incident, three fifths (59%) were former employees or contractors of the victims organizations, of whom a half (48%) had been dismissed, two thirds (38%) had resigned and a small portion (7%) had been laid off. The remaining two fifths (41%) were current employees or contractors. However, the findings also confirmed that the attacks were mostly carried out remotely, also that there was a high level of premeditation in the offending pattern.

Perhaps the most striking finding of the second CERT/ USS study was that the majority of the incidents were technically un-sophisticated (Keeney et al., 2005: 17). In over three fifths of the cases (61%), the insiders used relatively unsophisticated methods of attack, for example, user commands, information exchanges, and exploitation of physical security vulnerabilities. The remaining two fifths (39%) adopted relatively more sophisticated methods, such as employing scripts or programs, autonomous agents, toolkits, flooding techniques, probing, scanning and spoofing (Keeney et al., 2005: 17). The fact that the insiders perpetrating the attacks tended to have relatively low levels of IT skills and used relatively simple ‘trade craft’ to achieve their goals begins to dispel the prevailing myth that all attacks by malicious insiders are carried out by sophisticated operators.

The 2010 CERT® annual data on insider threats (a different series of data to the above) compares its most recent survey with previous years [2004-2009] and shows a slight drop in the percentage of organizations that fell victims to insider incidents from two thirds (66%) in 2007 to three fifths (60%) in the 2010 report. Whether or not the drop in insider incidents is significant or not is debatable. It may reflect improvements in security policies and training (as also found in Ponemon 2010b) as nearly one third of respondents (32%) monitored the online activities of disgruntled employees who had tendered their resignations or had been fired or laid off (CERT, 2010: 2). Or, it could simply be a reflection of sample bias since the sample was self-selected. Alternatively, it could be a combination of the two. More conclusive is that when an attack involved an insider, then victim organizations were more significantly affected and the consequences of the attack were more damaging and costly (than with losses incurred by outsiders) (CERT, 2010: 1). Verizon’s 2010 Data Breach Investigations Report, which also drew upon US Secret Service data, also found a decrease in data breach
incidents, but, in contrast to the CERT report, found an increase in insider attacks by those who maliciously abused their right to access corporate information (Version, 2010).

It is hard, if not impossible, to match the statistics and findings of the different breach reports because of their different methodologies and analytical frameworks. The CERT data, for example, is largely comprised of self-reported incidents and so is biased against those who do not report, where as the Verizon data is mainly composed of data from cases where the Verizon team was brought onsite to perform investigation by request of the victim and will be biased towards the more serious case and victims’ perceptions of what constitutes victimisation. The Ponemon data, in contrast, was solicited from a structured sample designed to eliminate bias, but inevitably contains a small bias towards the respondents who chose to participate. Having said that, the Ponemon data brings to the table a very detailed view of the individuals involved. The Open Security Foundation (OSF) data (see below) is obtained by its project curators and volunteers scouring news feeds, blogs, and other websites looking for data breaches, new and old. They search for incidents that need to be updated, or incidents that are not yet in the database. There is some bias here towards the larger and more public facing incidents. Finally, the LMRMC data drawn upon later canvassed responses from office workers over a two week period of time. As with some of the other studies there will be a bias here towards respondents who felt motivated enough to respond to the survey. Bring all these findings together, however, and it is nevertheless possible to identify some broad trends. Trends that can be expressed through an analysis of the OSF’s freely accessible database of reported data breaches. The OSF data also illustrates a gradual overall increase over the past five years in insider breaches against a decrease in breaches caused by outsiders from just under a quarter (23%) in 2005 to just under a half (47%) in 2010 (using data until November 2010).

**Table 1: Insider and Outsider Breaches**

<table>
<thead>
<tr>
<th></th>
<th>Insider</th>
<th>Outside</th>
<th>Unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-2005</td>
<td>34%</td>
<td>59%</td>
<td>7%</td>
</tr>
<tr>
<td>2005</td>
<td>23%</td>
<td>74%</td>
<td>4%</td>
</tr>
<tr>
<td>2006</td>
<td>32%</td>
<td>63%</td>
<td>4%</td>
</tr>
<tr>
<td>2007</td>
<td>22%</td>
<td>75%</td>
<td>2%</td>
</tr>
<tr>
<td>2008</td>
<td>31%</td>
<td>63%</td>
<td>6%</td>
</tr>
<tr>
<td>2009</td>
<td>40%</td>
<td>52%</td>
<td>8%</td>
</tr>
<tr>
<td>2010</td>
<td>47%</td>
<td>47%</td>
<td>6%</td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td><strong>33%</strong></td>
<td><strong>62%</strong></td>
<td><strong>6%</strong></td>
</tr>
</tbody>
</table>

3-See OSF site at: http://datalossdb.org/about.
What is certain from these reports and others, is that the number of insider related data loss incidents across the public and private sectors has increased during the past 5 years and is likely to be related to the number of individuals with direct access to financial, strategic or personal information and also its exchangeable value. Other contributory factors also include an increase in detection of insider breaches as the result of sensitization by corporate security departments and other interested parties to the problem – through reports produced at that time, such as CERT (2005) – with the implication that many insider breaches now detected may not have previously been detected. But, whilst there are broad similarities between the findings, there are also some differences in the conceptualisation of what constitutes an insider attack, and there also appears to be some disparity between those attacks that are malicious, and those which are damaging to the organization, but are not driven by malicious intent.

Further analysis of the insider cases summarised in Table 2 (which were shown as a total in Table 1), finds that although the overall percentage of insider driven breaches (and associated losses) has broadly increased over the years, as stated earlier, the percentage of non-malicious insider driven breaches increased inversely to the percentage of malicious breaches.

### Table 2: A breakdown of insider breaches

<table>
<thead>
<tr>
<th>Year</th>
<th>Insider-unknown</th>
<th>Inside-Accidental</th>
<th>Inside-Malicious</th>
<th>All Insiders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-2005</td>
<td>4%</td>
<td>19%</td>
<td>11%</td>
<td>34%</td>
</tr>
<tr>
<td>2005</td>
<td>1%</td>
<td>16%</td>
<td>6%</td>
<td>23%</td>
</tr>
<tr>
<td>2006</td>
<td>1%</td>
<td>25%</td>
<td>6%</td>
<td>32%</td>
</tr>
<tr>
<td>2007</td>
<td>3%</td>
<td>15%</td>
<td>5%</td>
<td>22%</td>
</tr>
<tr>
<td>2008</td>
<td>4%</td>
<td>18%</td>
<td>9%</td>
<td>31%</td>
</tr>
<tr>
<td>2009</td>
<td>1%</td>
<td>30%</td>
<td>9%</td>
<td>40%</td>
</tr>
<tr>
<td>2010</td>
<td>3%</td>
<td>31%</td>
<td>13%</td>
<td>47%</td>
</tr>
<tr>
<td>Totals</td>
<td>2%</td>
<td>22%</td>
<td>8%</td>
<td>33%</td>
</tr>
</tbody>
</table>
In light of the hitherto unsophisticated treatment of the ‘insider’ threat, the lack of detail in distinctions between malicious and non-malicious insiders may explain the apparent lack of effectiveness of some existing security policies, but also some of the differences between the various findings. An explanation for this lack of sophistication can be found in the way that conventional threat profiles tend to simply reflect the adversarial nature of criminal justice processes in most Western societies. It is an adversarial model that is historically based upon protecting the deserving members of society from the predations of the ‘dangerous classes’; the thugs, hooligans, footpads and pick-pockets etc., who robbed or humiliated innocent members of the public and made them fearful of walking the streets. Indeed, the police were formed in the early Nineteenth Century specifically to manage or prosecute these dangerous others (for they were not to be deemed part of mainstream society) in order to protect the public and maintain order. This practice has echoes today in cyber-security because this search for the ‘dangerous other’, immediately maps onto the hacker (or organized criminal in the case of financial crime, or the paedophile in cases involving images of child abuse).

Threat profiles are therefore reduced to ‘good guy’/ ‘bad guy’ binaries that map onto contemporary criminal stereotypes, which subsequently defines the relationships between security personnel and the rest of the organisation.

The Non-Malicious Insider Threat to the Organization

The fly in the ointment here is that not all insider precipitated incidents are malicious, so they do not neatly fit into the good guy/bad guy binary; for example, some insiders may be negligent as illustrated earlier, or more competent others may simply skip security measures in order to increase their efficiency. Yet, the dogged pursuit of the stereotypes excites the media and shapes public opinion and leads to increased demands for security which cannot always be met. This is because the hunt for demons misses those outside the stereotype, which is why it is so important to distinguish between the different types of insiders who are clearly an important part of the security problem. The worst case security scenario here is that security policy becomes too draconian by demonizing insiders as well as outsiders, slowing down the enterprise without effectively protecting it. An equally worst case scenario is that the resulting security ends up simply being ‘presentational’, or what Schneier (2003) calls ‘security theater’ which is publicly visible security measures that are primarily designed to demonstrate to the public that security countermeasures to an identified problem have at least been considered, even though they have little actual influence upon security. In short, security policy could end up damaging the organization if it does not allow (and respond) to different types of insiders.

In order to develop our understanding of the non-malicious insider it is useful to draw upon the findings of recent research into information technology practices and perceptions of online risk in the workplace. An international research study of 3,250 office workers conducted by LMRMC over a two week period in September 2010 across six countries (1000, UK; 500, Canada; 500, Hungary; 250, Poland; 500, South Africa; 500, USA) reveals some interesting similarities of practice and also of attitude (LMRMC, 2010). Whilst a half (48%) of the workers used remote work systems (30% secure and 18% non-secure systems), almost three quarters (71%) emailed work documents to their private email address to work on them outside the employer’s premises. Half (49%) copied work to encrypted or protected USB sticks and two fifths (42%) to non-encrypted or non-protected USB sticks which they took home to work on. Much of this information, just over half (54%) was unauthorised even though most organizations (90%) had policies regarding information use and access.

Although there were some small fluctuations across countries, the figures confirm that large amounts of data circulate outside work-based systems in a number of different formats. Furthermore, the findings also reveal that these people are

---

4 Incidentally there is no suggestion being made here that hackers’, fraudsters or paedophile actions are not in any way be dangerous, what is at question here is the uncritical acceptance that outsiders are the only threat.
prepared to take risks, especially when they think it appropriate. They also use network technologies fairly intensively, especially social networking to extend their professional, as well as social, contacts. But, the reasons given by respondents for removing data from the organization were not due to malicious intent, rather they were quite pragmatic. A third (34%) wanted to use the information so that they could work from home, a further third (32%) wanted the information for an offsite meeting, and just over one fifth (22%) wanted to keep the information ‘in a safe place’. Just under a quarter (23%) did admit to taking information with them to a new job – though this practice is often deemed acceptable in the field of creative arts and designs where the creator has an intellectual property right in the information. A very small amount (6%) wanted to disclose it to a third party or make it publicly available (4%) – which might indicate some deviance. Similarly, a comparatively small percentages used social networking when they were not supposed to do so and less that one fifth (22%) worked in organizations that actively blocked social networking (LMRMC, 2010).

At this point the LMRMC findings can be used to argue that these workers present to the organization a considerable amount of risk. However, a more considered reading of the findings reveals that the respondents/workers were aware of not only the risks but also the capacities of the technology. Three fifths (60%) said that they were more cautious about their online behaviour at work than they were at home, with a further sixth (17%) saying that they were cautious at both home and at work. The ‘cautious’ group were equally concerned about infecting work computers, inadvertently accessing offensive content, or that they might face disciplinary action. Rather worryingly, the remaining quarter or so (23%) said that they were less cautious at work when online than they were at home. However, just because they said they were less cautious does not mean that they were being reckless. It is just that they felt that their work computer had better security than they did at home, or they had an IT department who would sort out any problems. In fact, more than three quarters (78%) think that their IT department solely holds the responsibility for information confidentiality.

To reaffirm the emerging theme of responsibility, the overall level of caution found earlier was also reflected in the very low percentages (2%) of respondents who admitted to losing information that they had taken home without permission. Only a small percentage (6%) had lost devices in the past year that contained information (1% laptop, 1% PDA, 3% Cellphone, 3% USB stick).

The findings of the LMRMC (2010) research appear to contradict the larger losses found in the CERT and Verizon studies. However, a simple explanation for this disparity might be that both studies had very different respondent groups. One could argue that the LMRMC data may be skewed sample because it comprises of people who chose to respond to the questionnaire and who were disproportionately committed to their occupation and to their organization – thus omitting an as yet unexplained group, the other types of non-malicious insiders - the type of individuals who would probably not be motivated enough to respond to an online survey. However, despite these ‘unknown unknowns’ the LMRMC data is important because it begins to explain some of the unknowns in the CERT data, namely the profile of the non-malicious insider.

In sum, the various research reports drawn from earlier all broadly suggest the presence of two main groups of non-malicious insiders: the negligent insider and ‘the well-meaning insider’ which are possible to distinguish between because of their different motives. The negligent insider primarily interest is the pursuit of their own goals, whereas the well-meaning insider pursues those of the organization. Since an organizational security chain is only as good as its weakest

---

5 This figure contrasts with the Ponemon (2008) study which found that 35 percent of companies said that the main single loss of data was through lost laptops. The difference may be methodological, e.g., the LMRMC (2010) study is of individual employees, whereas Ponemon’s respondents are companies.
link, and the risk potential of both groups is missing from discussions about organizational internet security, then we need to know more about them.

The negligent insider

The negligent insiders are those employees, associates or affiliates who have legitimate access to an IT system and, for want of a better description, are those individuals whose eyes are not always on the ball and who might cut corners to make life easy for themselves. During the course of their work they will accept the broader organizational goals, but only accept the policies designed to achieve them as far as they do not encumber them with much more additional work, or can be used to lighten their load. For the most part they will embrace organizational policy minimally and also in terms of their own interpretation of its spirit.

The well-meaning insider

Ever present, but rarely acknowledged in data breach research, the ‘well-meaning insider’ is the proverbial elephant in the room in the debates that have, and still are, taking place over organizational Internet security. The ‘well-meaning insider’ is often the valued employee who, unlike the other security threats (including the negligent insider), is dedicated to pursuing their organization’s primary goals. It is in the pursuit of those goals that they may place secondary importance on security policies which can sometimes, inadvertently, cause them to become a threat to their organization. Data split by well meaning insiders, for example, may swiftly become the target of hackers (the greater threat) who then use that data against the organization. Their ‘actions can act as a prequel event to subsequent attacks by more malicious parties’ and ‘they help proliferate the spread of confidential data, which makes it easier for malicious insiders to get a hold of it’ (Kevin Rowney quoted in Shiels, 2009). It is a problem that will only get worse as more and more individuals are laid off because of the 2010 public spending cuts and the well-meaning insiders will unintentionally assist more vengeful colleagues (Shiels, 2009).

The process of demarcating these risk categories is complicated by the presence of ‘outsider insiders’ or affiliates who are affiliated to the organization, say, where a function has been outsourced. Also, by the ‘insider outsiders’, those who work within the organizational boundaries, but who may, for example, be interns or be either seconded into the organization from elsewhere or seconded to elsewhere. These ‘hybrid’ insiders are acknowledged here as a group that require further study.

The ‘well-meaning’ and ‘negligent’ insiders blur the ‘the bad guys’/ ‘criminal outsiders and insiders’ stereotype and challenges conventional wisdoms relating to the data loss risk model, especially when the threat that they constitute may be directly linked to bad practice within the organization or even the organization’s own occupational culture. With these different risk groups on the organizational threat landscape in mind, this paper now explores the threat to data loss posed by the well-meaning and also negligent insiders.

The Implications of the New Insider Threat Model for Security Policy

The disproportionate attention and resource given to outsiders understates the current response to the insider threat, even though the financial implications may be considerable. Because of this we need to map out in much greater detail what we understand by the ‘insider threat’, especially as not all non-malicious insiders pose the same level of threat to the organization. We therefore have to discern between them and break this group down further.
The distinction between malicious and non-malicious insiders has two implications. Firstly, we need to know more about the insider profile in order to fashion a policy response. Secondly, rather than taking a 'wall-and-fortress' approach to the problem, a more risk-based approach is needed that, as DeZabala has recommended, focuses 'on what assets are at risk of leaving the organization through the IT environment as well as the threats entering the organization through the same means' (cited in CERT, 2010: 1).

We have already discerned between ‘negligent’ and the ‘well-meaning’ insiders in terms of motivation, but motivation cannot always be identified at the point of impact, so it is assumed that the two groups would act differently in each of the following categories, but likely with the same impact. The former group would negligently ignore or misapply rules, where as the latter could achieve the same effect by their eagerness to (as they see it) contribute to organizational goals. These distinctions should be useful in assisting the framing of questions in future surveys about insiders. Below is a general typology of different types of non-malicious insider in terms of the ways they can lose or spill data. The first typology is of four traits of employees within the organization who can cause data spillage, most of which can be either negligent or well-meaning in terms of motivation. The second typology outlines the various ways that data can spill.

**Risk Groups**

a) **The underminers** are the insiders who routinely undermine computer security systems in order to improve their own access to them. They take the path of least resistance and ignore the spirit of security to make their working lives easier. These insiders use very simple passwords, or may use one password for all of the secure sites they access. Alternatively, these insiders might write down passwords on post-it notes attached to computer screens so as not to forget them, or they might circulate them to close colleagues to check emails whilst away on holiday. Passwords have even been known to have been circulated amongst friends via social networking sites. Like the data spills problem mentioned below, these personal practices fall under the provenance of IT management, but they may also result from too strong, rather than weak, IT management practices. They fall foul of the security paradox which describes a scenario where the more technically secure a system becomes, the weaker it becomes in practice because impatient humans who (tend to) have finite memory retention for passwords have to use it regularly.

b) **The over-ambitious** knowingly take risks to purposefully bypass bureaucratic security processes in order to be more effective in achieving what they think are organizational goals and often to advance their careers. They may be encouraged by the organization’s own culture and work ethos, skipping cumbersome security to become more efficient. Such examples might include eschewing encryption because it is time consuming and complicated – the fact is that it can take a worker’s mind off the job. Alternatively they may (mis)use their access privileges to drive business in a dangerous way, as has been the past experience of the banking sector.

c) **The socially engineered** are those employees, usually in low paid positions at the public facing end of the organization, who may be duped by malicious outsiders into sharing sensitive information or even giving access to systems. They are prone to fall victim to social engineering tactics employed (usually) by outsiders. These insiders can be deceived into giving out key information about an organization, or into giving out proprietary information or access codes that give outsiders access to its systems. Alternatively, they might give access codes or key information to others because they genuinely feel that they are being helpful and are acting in good faith. In such situations, the insiders may feel that they are being helpful in responding to a genuine request and may not employ routine due diligence as practice. They may also
feel as though they are acting in the organizations interests and/or according to company policy – the customer comes first! This may be a training issue also one of IT policy and levels of access.

d) **The data-leakers** are the growing cadre of ‘whistleblowers’ who, for various ethical or unethical reasons, leak to the public via social network technology, such as wiki-leaks, information they feel that the public should be informed about. Although they act against the organizational interests and often illegally (depending upon jurisdiction) they cannot simply be termed malicious in their actions if there is a public interest in the leak. As the wiki-leaks become more and more frequent and the technology that facilitates the leaks becomes more understood by the public, then it is likely that more and more secure information will be leaked, either for malicious or well-meaning reasons. The history of viral information flows across social networks would also suggest that the negative impacts of such leaks upon organizational reputations could be considerable.

e) **The data spilloers** are employees who have legitimate access to information or databases, but are prone to spill data because of (sometimes routine) organizational practices not checked by lax IT policies. Data spilloers may:

i) **Accidentally disclose** their key data and strategic information by losing unsecured computers or by losing memory sticks or other data storage devices whether encrypted or unencrypted. Such losses create a large amount of media coverage, public sensitivity and the emotional public responses to the losses by (especially public) organizations. See for example the public outcry and scandal following the 2007 loss of two CD-ROM data discs by staff at the UK HM Revenue and Customs which contained the details of 25 million Child Benefit claimants (BBC, 2007). The fact is, that relatively little direct financial loss appears to result from stolen laptops (according to the earlier findings), yet their loss is highly media sensitive enough to damage organizational reputations.\(^6\) See for example, the loss of laptops containing information about military recruits (Mail, 2008); pension data (BBC, 2008); personal bank information (Raywood, 2009); details of dairy farmers (Raywood, 2010). Also, while these were largely accidental and some prevention practices can be adopted, they are quite rare occurrences when they are placed against the backdrop of the billions of data exchanges that regularly take place within and between organizations. Unfortunately, it is only after data loss accidents occur that the full consequences, financial, reputational or otherwise, can be realized.

ii) **De-secured data for user convenience.** For the user’s convenience, data may be routinely copied from its secure location and then transferred to unsecured office or home computers (either portable or fixed) that are publicly shared and with no access control or other security.

iii) **Data left on the hard-drives of discarded machines.** Many computers are being discarded and then scrapped or sold on without their contents being secured and removed. In their 2009 research, for example, Kessler found that 40 percent of second hard drives bought through an auction site still contained data ranging from corporate spreadsheets to e-mails and personal photos (Mearian, 2009).

iv) **The inadequate management of data shared with third parties.** Weak third-party data governance policies can allow ‘outsider insiders’ or ‘insider outsiders’ (secondees and interns) mentioned earlier to lose data it or abuse it, typically, from the lack of use of encryption.

---

\(^6\) This is not to say that losses may not result in other increased vulnerabilities, either personally, organizationally or nationally.
v) **Sending unsecured data through public delivery systems.** Sending data via public delivery systems such as the postal service can lead to data being lost or falling to the wrong hands causing reputational, if not real damage, as happened in the major UK data spill events.

vi) **Not updating email and information distribution lists.** Automated data creation processes set up a long time ago and not updated will continue to send out key data, which becomes especially problematic if the data’s meaning and importance has changed in the years since a data collection process was initiated.

vii) **Not reviewing access rights.** Administrators can often fail to remove access rights to those who are no longer part of the organization, or not deleting leavers from email circulation lists. When either happens, data continues to flow to individuals who may have moved elsewhere in the organization or many have even left it. Most of these data spills result from routine practices that have been allowed to continue because of weak IT management practices and an under-prioritization of security.

**Data Spillage and the Stuxnet Warning**

Many enterprises do not have data loss prevention systems or tools that identify data spillage (Symantec, 2009b), but the recent Stuxnet worm brought with it a serious warning about the importance of preventing spillage from and also into computers. Analysis of the worm’s structure and its pathways through computer systems shows that organizational insiders are likely to have been enablers in its creation, installation and propagation through various types of spillage. A more detailed analysis of Stuxnet can be found in Falliere et al. (2010), but in short, it is a form of malicious software that can be used to sabotage SCADA (Supervisory Control and Data Acquisition) based industrial control systems ranging from water utilities to gas pipelines to power stations, including some nuclear power plants. Stuxnet represents a ‘paradigm shift’ in malware threats because of the way that it enters sometimes closed operating systems through USB sticks; it propagates itself by establishing a rootkit as well as backdoor connections that can allow external control; and also attacks only specific types of SCADA systems produced by specific manufacturers. Although a range of antecedents exist, the most recent iteration of Stuxnet, discovered in mid-2010, was found to have infected approximately 100,000 systems worldwide, although the evidence so far suggests that it has not yet found its specific target.

Where Stuxnet contrasts with the design and function of preceding malware is that it is a ‘large, complex piece of malware with many different components and functionalities’ and constitutes a particularly complex threat (Falliere et al., 2010). Falliere et al. (2010) estimate that Stuxnet took many months to create and was the work of a fairly large and highly skilled team. Important is the fact that the malware needed to be directly introduced into the target environment by an insider because the most sensitive SCADA systems are usually kept unconnected to the Internet. Falliere et al. (2010) argue that removable drives, typically USB sticks were the most likely means by which the malware was introduced into the system: it ‘... may have occurred by infecting a willing or unknowing third party, such as a contractor who perhaps had access to the facility, or an insider’ (2010). More significant is the observation that the designers of Stuxnet will have needed to possess very detailed knowledge about the design of the SCADA particular systems to be attacked. This information could only be obtained with the assistance of an insider, very likely the result of careless practice by a well-meaning insider which led to a data spill that was capitalized by a hacker.
Reducing the Insider Threat

Although Stuxnet is not unique in requiring insider complicity, see, for example, the Hydraq Trojan (Symantec, 2010), it has raised the risk stakes and has highlighted the insider threat issue. The example also suggests that being forewarned about the nature of the different types of insider threats is to be forearmed and that some of the events that lead to insiders spilling data could be reduced. Greater security, for example, around the schematic plans of all systems, also tighter security policy about the use of removable drives could make life much harder for data spillers/propagators (the insiders with USB sticks). Finally, the Stuxnet example also illustrates the necessity to ensure that security measures are both effective and understood by all employees whilst being internalized into organizational structures. Measures that might, for example, combine technologically based security such as content aware systems to control identity and access with staff education about the issues and the law and even, perhaps, some financial incentive or disincentive related to compliance or non-compliance. Content aware control systems supplemented by some form of social or economic value system would be preferable to say, pure network analysis based systems such as computer traffic monitoring algorithms, which may be able to differentiate between the different Internet traffic patterns of malicious outsiders and all insiders, but not necessarily between malicious and non-malicious insiders.

This problem is succinctly described by Caputo, et al., (2009: 2). “One of the real challenges in developing technology to help us tackle this cyber challenge is that malicious insiders usually do not need to engage in rule breaking behavior. They can use their legitimate access to gather and steal sensitive information. Their actions remain largely unseen using traditional cyber-detection methods such as log auditing and intrusion detection, which largely focus on detecting attempted or actual rule-breaking behavior”. Caputo, et al., (2009) actually argue that they have developed technology based methods to discern between malicious and non-malicious activity, but this remains at an early stage of development and does not as yet show signs that it could discern between the different types of non-malicious and well-meaning insider. Until the social science (e.g. conceptualizations of non-malicious insiders) matches the science (developing competent algorithms to interpret the conceptualizations) then the problem of false-positives will undermine the micro-politics of security.

Reducing Data Loss Incidents

The different categories of non-malicious insiders outlined earlier show that any strategies to reduce incidents of data loss (whether by well-meaning or negligent insiders) will have to be multi-faceted and combine a number of tactics. This is because the two most common characteristics found in each category of the above typology of non-malicious insider threats are, firstly, a combination of the failure of the individual insider to protect key data, but also the failure of organizational management to install and maintain workable procedures to ensure that insiders protect data. Secondly, even where there are competent data security policies in place, there is a often a failure to account for changes over time, such as changes in the importance of data or not removing those no longer part of the organization from email circulation lists. Such considerations are important because the main threat of the well-meaning insider is the release of data that can be misused by others, usually as a prequel event to a subsequent attack. So data loss and security strategies will, on the one hand, have to be designed to prevent poor employee work practices and attitudes which result in the six ways that data can be lost. But, on the other hand, they will also have to incorporate actions that will reduce the impact of any bad employer practices that may enable the poor employee work practices and attitudes that lead to data spillage. In reality
there tends to be a fusion of risks which forms a toxic combination of the two, so remedies may be need to be reflexive, complex and situationally different, if not bespoke.

*The following considerations become the building blocks of policy.*

Firstly, there is the need to be pragmatic about the well-meaning (and negligent) insider by ensuring that security policy addresses the problem from an organizational perspective and does not simply demonize the well-meaning insider as a deviant or criminal ‘other’.

Secondly, there is the need to avoid a blame culture and not immediately interpret the actions of non-malicious insiders as criminal. After all, the information given by a well-meaning insider who has inadvertently compromised a system may have been given in good faith. Indeed, these insiders are not (usually) criminals. Far from it. They are often the product of the organization and, in the case of the well-meaning (rather than negligent) insider, are often trying to please the organization – they just see the goals in a slightly different way. It has to be accepted that this is a different kind of threat to malicious outsiders and insiders and security policies have to be framed accordingly. Each of the different outsider and insider groups need to be recognized and responded to by different strategies or sub-strategies. Well-meaning insiders usually have the organizations interests at heart and require further training, not discipline. Negligent insiders do not always understand the organizations interests and require training and incentivization, not discipline in the first instance.

Thirdly, the underlying source of the potential data loss problem is not necessarily the individual workers themselves, but the way they react to, or interpret the organizational goals as they are expressed in company policy and organizational cultures. So, when addressing this problem – which is the organization’s problem - a greater understanding is required of how their employees view them, their mission and also the goals. They also need to be acutely aware of their own organizational culture - which is the unwritten part of organizational life that is comprised of the professional and personal experiences that employees communicate to one another through their work based interactions and which shapes the way that employees interpret organizational goals and management directives. Categorizing these well-meaning insiders as deviants in the first instance will not resolve the problem and lessen the risk, and it will certainly not buy their compliance in clearing up the aftermath. Simply put, the work ethic that firms value most – 100+ percent commitment - can become a weak point. By encouraging hard work ethics and personal commitment to the job by providing laptops etc., plus off-site access to systems so that they can work at home, etc., employers improve their productivity. But this practice can also create weaknesses as well as benefits at the risk of data loss increases. Not least, the weakness of the human condition when workers are working too hard or are off their guards etc. This is not a question of ceasing such activities, else most organizations would collapse. But what it does say is that both employers and employees have to be aware of the potential weaknesses. It also impresses upon those drafting security policy the need to achieve an acceptable balance in the work-life relationship.

**Recommendations for Preventing Data Spillage**

Security policies have to ensure that there is clarity about who should and should not have access to different types of data. The same policies also need to ensure that the nature of relationships between staff with regard to access to data is both explicit and clear; including the relationships with ‘outsider insiders’ (outsourced staff) and ‘insider outsiders’ (e.g. interns or those seconded in, or those seconded out). Whilst appropriate access can be enforced via technology driven content-aware systems for controlling identity and access, the policies behind the design of those systems need to be
sensitive enough to allow for appropriate individual staff innovation and also not to restrict productive working relationships between staff within the organization.

All current staff should be made aware of the risks arising from data loss, especially the following:

- the need to protect data that belongs to the organization or its clients in the organization's interests
- the implications to the organization and themselves for not doing so
- the need to be vigilant against the intentions of malicious outsiders and insiders, especially those who might try to socially engineer them into giving them access to systems

Managers and administrators need to ensure that the relationship with former staff is immediately decided once their employment ceases. Also to make sure that both parties are clear about the following:

- what information leavers can and cannot take
- when their access rights will be removed or what they will be authorized to access if some rights remain after departure from the organization
- what email lists leavers will be removed from
- that other staff are aware of the arrangements that have been decided upon with the leaver
- that current staff have the means to check on the status of former employees, and also affiliates

Security policies need to outline remediation procedures once a data spill has been detected in order to clean it up without disrupting the business process - preferably automatically. Content-aware technologies, for example, could assist in quickly identifying the true owner of the file as well as the individual(s) using it. They could also assist in informing, even educating, the information owner and user about the loss so as to prevent a re-occurrence. Finally, content-aware technologies could even be used to forcibly remove the spill if repeat notifications were being ignored.

Install a discrete security hotline for staff to report suspicions or request advice from senior staff.

How to Learn More about Data Loss Prevention

To learn more about how your organization can take advantage of data loss prevention technology, visit the Symantec website at http://www.symantec.com/business/products/family.jsp?familyid=data-loss-prevention or contact the Symantec representative in your area.

To speak with a Product Specialist in the U.S.
Call (415) 829-5013

To speak with a Product Specialist outside the U.S.
For specific country offices and contact numbers, please visit our website at www.symantec.com
References


Organizational Security and the Insider Threat: Malicious, Negligent and Well-Meaning Insiders

Ponemon (2009b) *Data Loss Risks During Downsizing: As Employees Exit, so does Corporate Data*, Ponemon Institute, https://www4.symantec.com/Vrt/offer?a_id=78695


About Symantec
Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our website at www.symantec.com

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2011 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
1/2011 21164352