WORKING PAPER: *preprint* of article, please cite as Wall, D.S. (2013) 'Enemies Within: Redefining the insider threat in organizational security policy', *Security Journal* Security Journal, 26(2) 107-124.

ENEMIES WITHIN: Redefining the insider threat in organizational security policy[1]

David S. Wall, Criminology, SASS, Durham University, 32 Old Elvet, Durham, DH1 3HN, UK. d.s.wall@durham.ac.uk

Abstract
The critical importance of electronic information exchanges in the daily operation of most large modern organizations is causing them to broaden their security provision to include the custodians of exchanged data – the insiders. The prevailing data loss threat model mainly focuses upon the criminal outsider and mainly regards the insider threat as 'outsiders by proxy', thus shaping the relationship between the worker and workplace in information security policy. Policy, that increasingly takes the form of social policy for the information age as it acquires the power to include and exclude sections of society and potentially to re-stratify it? This article draws upon empirical sources to critically explore the insider threat in organizations. It looks at the prevailing threat model before deconstructing 'the insider' into various risk profiles, including the well-meaning insider, before drawing conclusions about what the building blocks of information security policy around the insider might be.

Keywords: Information Security, Security Policy, Cybercrime, Organizations, Insider Threat

Introduction

As nearly all types of private and public sector organizations have turned to electronic rather than physical informational exchanges in order to improve their efficiencies and service delivery, their security mission has broadened from keeping unwanted intruders out of the organization to also responding to the problem of the insider threat. Today, the critical importance of electronic information exchanges in the operation of almost any organization now means that the security lens has to focus equally upon the custodians of exchanged data, those inside the organization as it does upon those outside it. To illustrate this point, forty three percent of the 607 respondents to the 2011 Cyber Security Watch Survey (CSWS) (CERT, 2011)[2] reported that they had experienced an insider incident in the previous year. Most of the CSWS respondents found 'insider incidents' to be more damaging than outsider attacks (CERT, 2011).

[1] This research originated as a white paper prepared for Symantec on the well-meaning insider (Wall, 2011).
[2] Carried out by USCERT (US Computer Emergency Response Team), USSS (US Secret Service), Deloite and CSO (Chief Security Officer) Magazine.

These trends are replicated in surveys from previous years, by other researchers (see CSI/FBI Surveys 2001-2006)[3] and in a range of different jurisdictions using different methodologies. Hong, et al. (2010: 31), for example, argue that 90 per cent of attacks against organisations are insider attacks. Such concerns are heightened by the increasing practice of ethical and unethical 'whistle blowing', as illustrated by Wikileaks and other cases (see later). These concerns also raise questions about the nature of the 'attacks' and whether or not a deeper understanding of them will contribute to our criminological knowledge about insiders and outsiders? Furthermore, how will such understanding also inform information security policy which is increasingly becoming a social policy for the information age as it acquires the power to include and exclude sections of society and potentially to stratify it?

Bishop has broadly defined the insider threat as "… a trusted entity that is given the power to violate one or more rules in a given security policy ... the insider threat occurs when a trusted entity abuses that power" (Bishop, 2008: 1). The problem with such broad definitions is that they rarely capture the full dynamics of the problem and one of the major shortcomings of the overall security response to the insider threat is that it has become framed by the politics of organisational security and governance. The insider threat problem becomes 'externalised' and the insiders who threaten information security are instinctively regarded as outsiders by proxy or redefined as 'criminal others' (Garland, 2001). Not only is this assumption misguided, but this perceived threat of 'the enemy within' engenders distrust within the organisation; distrust that is often (consciously or unconsciously) used as a tool of 'governance' (see Simon, 2007 and Garland, 2001). Ironically, this paradox becomes intensified when the construction of the enemy within subsequently becomes a 'site of entrepreneurship'; a resource that can be used by managers to garner additional resources and increase their power base[4]. As a consequence, the general mis-conceptualisation of the 'insider' tends to reduce the insider threat to a technical problem[5]. Once configured as a technical problem, then only technical solutions, such as access control software and other 'threat mitigation techniques' (Probst, et al. 2010), are perceived as resolutions. In short, the prevailing security paradigm frames perceptions of the insider threat in absolute terms rather than as a relative threat that is the product of a range of dynamic and situationally determined processes; processes that can also contribute to resolving the problem.

In pursuit of a more dynamic model for understanding the insider threat it will be argued in this article that the insider issue is far more complex than is often described in computing science, security and other academic literature. It will be

[3] See Richardson (2003) and Gordon, et al. (2003; 2004; 2005; 2006).
[4] Simon (2007), Garland (2001) and others were largely focused at a level of statehood, this article focuses upon the organisation, though some are very large and transglobal.
[5] As is the case more generally with cyber-crime that involves information theft.

argued that it encompasses a range of different motivations, including some that are certainly malicious, but also others that are the knock-on effects of organisational cultures and even the organisations' own policies. A more sophisticated and multi-disciplinary understanding of the insider threat is not only important for informing organisational information security policy and for creating rules for the application of software controls such as those mentioned above, but also for responding legally to related problems when they arise and for preventing them from reoccurring. This article draws upon the findings of a number 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. The first part looks at the prevailing organisational data loss threat model and introduces the problem of the insider threat and disaggregates it from the outsider threat with which it has been linked. The second part deconstructs the insider threat in order to map out the respective risk profiles of non-malicious and well-meaning insiders. The third part discusses the various options for security policy, especially the challenges created by the new insider threat model. The fourth part then looks to the future and at data spillage, insecurity and the Stuxnet warning. The fifth part draws some conclusions about how the insider threat might be reduced by identifying some building blocks for information security policy.

The prevailing 'outsider' data loss threat model and the insider threat

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 the organization. The debates have distinguished between the hack (by brute force or evasion of security), the social engineering of insiders and information holders, and access prevention through DDOS (distributed denial of service) attack. In recent years these debates have broadened to include malicious insiders after they entered the threat landscape; almost to obsess on which of the two groups (insider or outsider) 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 upon 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 and contribute to 'the culture of fear' about cybercrime, heightening public concerns about internet safety in the process (Wall, 2008/11). Malicious insiders and outsiders are, however, not the focus of discussion here because there already exists a considerable amount of literature about them – see, for example, the reports by Symantec (2008; 2009a), Verizon (2010) and many other cyber-security companies. But also see the relevant chapters and references in books about cybercrime and criminals, for example, Jewkes and Yar (eds, 2010), McQuade (2006), Wall (2007), Williams (2006), Yar (2006). 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 – which is the focus of this article. Furthermore, the tendency to orient information security policies primarily against the 'bad guys' (as they are so often referred to in security debates); 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 unjustly feel as though 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. In the bigger picture it also begins to change the relationship between the worker and their workplace.

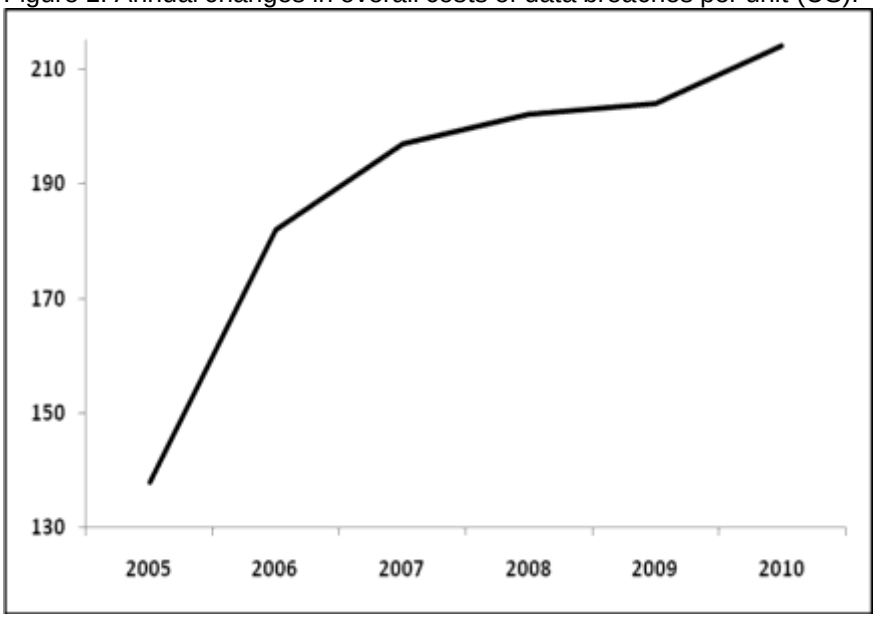
The nature of the insider threat

Data losses incurred by insiders through damage or misappropriation are very costly to organizations. The cost of losses has increased over the past decade along with the overall number of incidents. 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 and $7.2million in 2010, with the cost of each compromised customer record rising from $202 to $204 to $214 respectively (Ponemon, 2010a: 3; 2011). After beginning to tail off in 2008 and 2009 the US average loss began to rise again slightly in 2010 to match the longer term trend. In the U.K. (the lowest losses)[6] the trend-line was roughly similar rising from £60 to £64 to £72 from 2008 to 2010 inclusive. (Ponemon, 2010b: 3). Some cheer may be drawn from these relatively small changes when they are compared with the rises in previous years[7], see Figure 1 which indicates a steep rise from 2005—2007 with a lesser rise thereafter. This tailing of the increase in data loss costs after 2007/8 indicates the possible impact of improvements in security policies and associated training, although, such improvements take place in the face of an increase in data loss threats (see Ponemon, 2011: 2).

[6] Compared with the US ($214/£134), Germany ($191/£119); France ($136/£85); Australia ($123/£77); UK ($114/£72)

[7] 2005=$138; 2006=$182; 2007=$197; 2008=$202; 2009=$204; 2010= $214

Figure 1: Annual changes in overall costs of data breaches per unit (US).



(Source: based upon statistics in Ponemon, 2011; 2010a: 3; 2009a: 3)

The percentage of losses specifically attributed to insider negligence was found to have declined slightly along with the overall number of insider caused breaches. This decrease could 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 costs of losses are significant, but also significant is that they result from the actions of a number of different types of insider which each have different threat profiles. This point is brought out later in the analysis of research data on incidents.

The Ponemon research makes a 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 to 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[8] prioritised by the President's Critical Infrastructure Protection Board in the 2003 *The National Strategy to Secure Cyberspace* (White House, 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 the primary motivation of most offenders 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). In 2005, a second U.S. Secret Service/ CERT® research team (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 in terms of status, psychology and motivations of malicious insiders. As might be expected, the findings confirmed that a negative work-related event triggered most actions, however, perhaps the most striking finding of the second CERT/ USS study was that the majority of the incidents were technologically un-sophisticated (Keeney et al., 2005: 17). In over three fifths of the cases (61 per cent), the insiders used relatively simple methods of attack, for example, user commands, information exchanges, and exploitation of physical security vulnerabilities. The remaining two fifths (39 per cent) 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 2011 CERT® annual data on insider threats (a different series of data to the above) compares its most recent survey with previous years [2004-2010]. It shows a slight drop in the percentage of organizations that fall victim to insider incidents, from two thirds (66%) in 2007 to three fifths (58%) in the 2011 report (2% down on 2010). It is debateable whether or not the drop in the number of insider incidents is significant or not. On the one hand, it may reflect improvements in security policies and training (as also found in Ponemon 2010b) as nearly one third of respondents (32%) said they monitored the online activities of disgruntled employees who had tendered their resignations or had been fired or laid off (CERT, 2010: 2). On the other hand, 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

[8] The complete list being: banking and finance; information and telecommunications; transportation; postal and shipping; emergency services; continuity of government; public health; food; energy; water; chemical industry and hazardous materials; agriculture; defence industrial base (Randazzo et al. (2005: 3).

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 (Verizon, 2010).

It is hard, if not impossible, to perfectly match the statistics and findings of 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 by request of the victim to perform an investigation 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. In contrast, the Open Security Foundation (OSF) data[9] used later 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 are not yet in the database and update and verify incidents they have already logged. There is some bias here towards the larger and more public facing incidents, but it nevertheless adds an important independent source of quantitative and qualitative data. Finally, the LMRMC (LM Research & Marketing Consultancy) 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 in insider breaches over the past five years 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

	Insider	Outside	Unknown
Pre-2005	34%	59%	7%
2005	23%	74%	4%
2006	32%	63%	4%
2007	22%	75%	2%

[9] See OSF site at: http://datalossdb.org/about.

2008	31%	63%	6%
2009	40%	52%	8%
2010	47%	47%	6%
Totals	**33%**	**62%**	**6%**

[Data analysed from raw OSF data. Total n=3001 cases]

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 to the problem by corporate security departments and other interested parties – through reports produced at that time, such as CERT (2005). The implication is 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 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

	Insider-unknown	**Inside-Accidental**	**Inside-Malicious**	**All Insiders**
Pre-2005	4%	19%	11%	34%
2005	1%	16%	6%	23%
2006	1%	25%	6%	32%
2007	3%	15%	5%	22%
2008	4%	18%	9%	31%
2009	1%	30%	9%	40%
2010	3%	31%	13%	47%
Totals	**2%**	**22%**	**8%**	**33%**

[Data analysed from raw OSF data. Total n=3001 cases]

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, as reflected in the good guy/bad guy binary described earlier. 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 protect the public and maintain order by managing or prosecuting these dangerous others, who were not to be deemed part of mainstream society (see Reiner, 2000). 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[10]. Threat profiles are therefore reduced to 'good guy'/ 'bad guy' binaries that reflect contemporary criminal stereotypes that subsequently define the relationships between security personnel and the rest of the organisation.

Mapping out the risk profiles of non-malicious and well-meaning insiders

The fly in the ointment here is that not all insider precipitated incidents are malicious, so they do not neatly fit into the perceived offender stereotype; for example, some insiders may be negligent as illustrated earlier, or may simply skip security measures to make life easier for themselves (or be more efficient). Yet, the dogged pursuit of the conventional offender 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 known demons invariably tends to miss those falling outside the stereotype, which is why it is so important to distinguish between the different types of insider 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 a 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 respond to the different types of insider.

[10] Please note that there is no suggestion 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.

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 LM Research & Marketing Consultancy (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 above 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 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 driven by 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 two fifths (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 two fifths (18%) 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. 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[11], 1% PDA, 3% Cellphone, 3% USB stick).

The findings of the 2010 LMRMC research appear to contradict the larger losses found in the CERT and Verizon studies described earlier, however, a simple explanation for this disparity might be that both studies had very different respondent groups. As suggested earlier, the LMRMC data may be a 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. Despite these 'unknown unknowns', however, 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 findings discussed earlier all broadly suggest the presence of two main groups of non-malicious insider: the negligent insider and 'the well-meaning insider' which are distinguished by different motives. Negligent insiders primarily pursue their own goals, whereas well-meaning insiders are more likely to pursue those of the organization. Since an organizational security chain is only as good as its weakest 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

[11] 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.

organizational policy minimally and also in terms of their own interpretation of its spirit.

The well-meaning insider
Ever present, but rarely acknowledged in internet data breach research and organizational security debates, the 'well-meaning insider' is the proverbial elephant in the room. The 'well-meaning insider' is typically the valued employee who, unlike the other security threats (including the negligent insider), is dedicated to pursuing performance goals set for them by their organization. It is in the pursuit of such goals that they may regard security policies as less important, which can sometimes, inadvertently, cause them to become a threat to their organization. Data spilt 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, say, as more and more individuals are laid off because of the 2010+ public spending cuts in Western countries and the well-meaning insiders will unintentionally assist more vengeful colleagues (Shiels, 2009).

The process of demarcating these risk categories is further complicated by the presence of 'outsider insiders' or affiliates who are linked to the organization but are not formally part of it, for example, where a function has been outsourced. Also, by the 'Insider outsiders', those who work within the organizational boundaries, but who may be interns, or be either seconded into the organization from elsewhere or seconded out. These 'hybrid' insiders are acknowledged here as a group that require further study.

The introduction of the distinction between 'well-meaning' and 'negligent' insiders into security debates blurs the (now) conventional '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 article 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 in security debates vastly understates the current response to the insider threat, and yet, as outlined earlier the financial implications may be considerable. Because of this we need to map out what we understand by the 'insider threat' in much greater detail, 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 (Cited in EON, 2010) 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'. We have already discerned between 'negligent' and '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 risk groups 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.

Non-malicious risk groups

The underminers are the insiders who routinely undermine computer security systems in order to improve their own access to information. 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 be circulated amongst friends via social networking sites to allow them to check their emails whilst on holiday. 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 illustrate the security paradox whereby 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.

The over-ambitious understand the importance of security but 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.

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!

The data-leakers are the growing cadre of 'whistleblowers' who, for various ethical or unethical reasons, leak data to the public via social network technology, such as Wikileaks, 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 can be considerable (BBC, 2007).

Methods of non-malicious data spillage

The non-malicious data spillers are the employees of an organization 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 spillers may:

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. 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 realised.

De-secure 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.

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

Inadequately manage data that is 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.

Send unsecured data through public postal and delivery services. 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 U.K. data spill events (Raywood, 2009; 2010).

Not update 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.

Not review user 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-prioritisation of security.

Data spillage, insecurity 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 malware (malicious software) brought with it a serious warning about the importance of preventing spillage from and also into computers. Analysis of Stuxnet's structure and its pathways through computer systems shows that organizational insiders are likely to have provided information crucial to its creation, installation and propagation through various systems. A more detailed analysis of Stuxnet can be found in the research by 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 via insiders through infected 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 is mixed as to whether or not it has found its specific target and as to what impact it had (BBC, 2011).

Where Stuxnet contrasts with the design and function of preceding threats 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.

Although Stuxnet is not unique in requiring insider complicity, see, for example, the Hydraq Trojan (Symantec, 2010). It has, however, raised the risk stakes and has highlighted the insider threat issue. The discovery of custom-built variants will likely continue this practice (Zetter, 2010). The Stuxnet 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, Stuxnet also illustrates the necessity to ensure that security measures are both effective and understood by all employees whilst being internalised 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. Algorithms 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; a problem that 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. As, Vint Cerf, one of the fathers of the internet once observed, '[t]here are no electronic filters that separate truth from fiction' (Cerf, 2003: 10).

Discussion and Conclusions: Reducing incidents of data loss

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 non-malicious insider threats are 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. 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 recognised 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. Categorising 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, a 100+ per cent

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.

In conclusion, this article has sought to redefine and re-theorise the insider threat in organisational security and has provided some general principles that should be considered when framing security policy. Moreover, it has shown both the diversity of the insider threat, but also how its roots can lie within organisational policy and culture and not necessarily predatory outsiders. In so doing these finding begin to change our understanding of the nature of the relationship between modern workers, their organization and ultimately their relationship with the state itself. Information brokering, as outlined earlier, is becoming central to the core operations of most modern organizations so that, intentionally or unintentionally (because we currently do not know which) their security policy is increasingly acquiring the power to include, exclude and stratify sections of society. Because of this innate power, then the formulation of security policy has to be more holistic than it is currently regarded and it has to adopt a more relative rather than absolutist approach to the insider threat because of its variable nature.

References

BBC (2007) ‘Six more data discs 'are missing', *BBC News Online*, 24 November. http://news.bbc.co.uk/1/hi/7111056.stm, accessed 1 August 2011.

BBC (2008) ‘Pension data was on stolen laptop’, *BBC News Online*, 10 October. http://news.bbc.co.uk/1/hi/uk/7664274.stm, accessed 1 August 2011.

BBC (2011) ‘US and Israel were behind Stuxnet claims researcher’, *BBC News Online*, 4 March, http://www.bbc.co.uk/news/technology-12633240, accessed 1 August 2011.

Bishop, M. and Gates, C. (2008) ‘Defining the Insider Threat’, *Proceedings of the Cyber Security and Information Intelligence Research Workshop*, article 15. http://nob.cs.ucdavis.edu/bishop/papers/2008-csiiw/definsider.pdf, accessed 1 August 2011.

Caputo D., Stephens, G., Stephenson, B. and Kim. M. (2009) *Human Behavior, Insider Threat, and Awareness An Empirical Study of Insider Threat Behavior*, Institute for Information Infrastructure Protection (I3P) research program Research Report No. 16, July 2009, Hannover: Dartmouth College. http://www.thei3p.org/docs/publications/134.pdf, accessed 1 August 2011.

Cerf, V. (2003) 'The internet under surveillance: obstacles to the free flow of information online', *Reporters Without Borders*. http://famguardian.org/Subjects/Computers/Articles/IntUnderSurv.htm, accessed 2 Sept. 2011.

CERT (2005) '2005 E-Crime Watch™ survey shows E-Crime fighters making headway: Average Company Loss Estimated at More Than Half Million Dollars', *Press release*, CERT/CSO. http://www.cert.org/archive/pdf/ecrime_watch05.pdf, accessed 1 August 2011.

CERT (2010) *Cybersecurity Watch Survey: Cybercrime Increasing Faster Than Some Company Defenses*, CERT Insider Threat Team, Pittsburgh: Carnegie Mellon University, Software Engineering Institute. http://www.cert.org/archive/pdf/ecrimesummary10.pdf, accessed 1 August 2011. (Summaries also available for 2004-2009)

CERT (2011) *Cybersecurity Watch Survey: How Bad is the Insider Threat?*, CERT Insider Threat Team, Pittsburgh: Carnegie Mellon University, Software Engineering Institute. http://www.cert.org/archive/pdf/CyberSecuritySurvey2011Data.pdf, accessed 1 August 2011. (Summaries also available for years 2004-2010)

EON (2010) '2010 CyberSecurity Watch Survey: Cybercrime Increasing Faster Than Some Company Defenses', Enhanced Online News (EON), 25 January. http://eon.businesswire.com/news/eon/20100125006500/en/CSO/Cybercrime/cybersecurity, accessed 1 August 2011.

Falliere, N., Murchu, L. and Chien, E. (2010) 'W32.Stuxnet Dossier: September 2010, version 1.0', *Symantec White Paper*. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, accessed 1 August 2011.

Garland, D. (2001) *The Culture of Control*, Oxford University Press, Oxford.

Gordon, L, Loeb, M., Lucyshyn and Richardson, R. (2004) *2004 CSI/FBI Computer Crime and Security Survey*. Computer Security Institute. San Francisco: Computer Security Institute.

Gordon, L, Loeb, M., Lucyshyn and Richardson, R. (2005) *2005 CSI/FBI Computer Crime and Security Survey*. Computer Security Institute. San Francisco: Computer Security Institute.

Gordon, L, Loeb, M., Lucyshyn and Richardson, R. (2006) *2006 CSI/FBI Computer Crime and Security Survey*. Computer Security Institute. San Francisco: Computer Security Institute.

Hong, J., Kim, J. and Cho, J. (2010) 'The Trend of the Security Research for the Insider Cyber Threat'. *International Journal of Future Generation Communication and Networking*, 3(2) 31-40.

Jewkes, Y. and M. Yar (eds) (2010) *Handbook of Internet Crime*, Cullompton: Willan Publishing.

Keeney, M., Cappelli, D., Kowalski, E. Moore, A., Shimeall, T. and Rogers, S. (2005) *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*, Pittsburgh, PA Carnegie Mellon University Software Engineering Institute/ United States Secret Service. http://www.cert.org/archive/pdf/insidercross051105.pdf, accessed 1 August 2011.

LMRMC (2010) *Online Riskiness: Questionnaire Results – Overall*, LM Research & Marketing Consultancy, 20, September (Unpublished).

Mail (2008) 'Military laptop stolen from McDonald's as 'Army captain eats a Big Mac'', Mail Online, 12 April. http://www.dailymail.co.uk/news/article-559178/Military-laptop-stolen-McDonalds-Army-captain-eats-Big-Mac.html#ixzz13NxVuGd0, accessed 1 August 2011.

Mearian (2009) 'Survey: 40% of hard drives bought on eBay hold personal, corporate data: Buyers found data on everything from corporate spreadsheets to e-mails and photos', *Computerworld*, 10 February. http://www.computerworld.com/s/article/9127717/Survey_40_of_hard_drives_bought_on_eBay_hold_personal_corporate_data, accessed 1 August 2011.

McQuade, S. (2006) *Understanding and Managing Cybercrime*. Boston: Allyn & Bacon.

Ponemon (2008) *The Cost of a Lost Laptop*. Ponemon Institute. http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/Cost%20of%20a%20Lost%20Laptop%20White%20Paper%20Final%203.pdf, accessed 1 August 2011.

Ponemon (2009a) *Fourth Annual US Cost of Data Breach Study: Benchmark Study of Companies*, Ponemon Institute.

http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008-2009%20US%20Cost%20of%20Data%20Breach%20Report%20Final.pdf, accessed 1 August 2011.

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, accessed 1 August 2011.

Ponemon (2010a) *2009 Annual Study: Cost of a Data Breach*, Ponemon Institute. http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/US_Ponemon_CODB_09_012209_sec.pdf, accessed 1 August 2011.

Ponemon (2010b) *2009 Annual Study: UK Cost of a Data Breach,* Ponemon Institute, http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/UK_Ponemon_CODB%202009%20v9.pdf, accessed 1 August 2011.

Ponemon (2011) *2010 Annual Study: Cost of a Data Breach*, Ponemon Institute/ Symantec. http://www.symantec.com/content/en/us/about/media/pdfs/symantec_cost_of_data_breach_global_2010.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Jun_worldwide_idod_codb_9jun, accessed 1 August 2011.

Probst, C., Hunker, J. and Gollmann, D. (2010) (eds) *Insider Threats in Cyber Security, Advances in Information Security*, Vol. 49, New York: Elsevier.

Randazzo, M., Keeney, M., Kowalski, E., Cappelli, D., and Moore, A. (2005) *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*. Philadelphia: Carnegie Mellon University, Software Engineering Institute. http://82.138.248.200/hcs-temp/teaching/GA10/lec4extra/certreport.pdf, accessed 1 August 2011.

Raywood, D. (2009) 'MBNA confirms data loss after laptop containing personal details of thousands of customers was stolen from vendor', *SC Magazine*, 23 December. http://www.scmagazineuk.com/mbna-confirms-data-loss-after-laptop-containing-personal-details-of-thousands-of-customers-was-stolen-from-vendor/article/160217/, accessed 1 August 2011.

Raywood, D. (2010) 'Stolen laptop leads to the loss of details of around 13,000 UK dairy farmers', *SC Magazine*, 2 July. http://www.scmagazineuk.com/stolen-laptop-leads-to-the-loss-of-details-of-around-13000-uk-dairy-farmers/article/173843/, accessed 1 August 2011.

Reiner, R. (2000. *The politics of the police* (3rd ed.), Oxford: Oxford University Press.

Richardson, R. (2003) *CSI/FBI Computer Crime and Security Survey*. Computer Security Institute. San Francisco: Computer Security Institute.

Schneier, B. (2003) *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*, New York: Springer.

Shiels, M. (2009) 'Malicious insider attacks to rise', *BBC News Online*, 11 February. http://news.bbc.co.uk/1/hi/technology/7875904.stm, accessed 1 August 2011.

Simon, J. (2007) *Governing Through Crime: How the War on Crime Transformed American Democracy and Created a Culture of Fear*, New York: Oxford University Press

Symantec (2008) *Anatomy of a Data Breach: Why Breaches Happen and What to Do About It*, Mountain View: Symantec. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-anatomy_of_a_data_breach_WP_20049424-1.en-us.pdf, accessed 1 August 2011.

Symantec (2009a) *Internet Security Threat Report Volume XIV*: April, 2009, Symantec. http://www.symantec.com/business/theme.jsp?themeid=threatreport, accessed 1 August 2011.

Symantec (2009b) *SMB Protection Gap: SMB security and data protection: survey shows high concern, less action*, Symantec White Paper. http://eval.symantec.com/mktginfo/enterprise/other_resources/b-SMB-Protection-Gap_WP_20094842.en-us.pdf, accessed 1 August 2011.

Symantec (2010) 'The Trojan.Hydraq Incident', *Symantec Security Response Blog*, 18 January. http://www.symantec.com/connect/blogs/trojanhydraq-incident, accessed 1 August 2011.

Verizon (2010) *2010 Data Breach Investigations Report*, Verizon. http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf, accessed 1 August 2011.

Wall, D.S. (2007) *Cybercrime: The transformation of crime in the information age*, Cambridge: Polity.

Wall, D.S. (2008/11) 'Cybercrime and the Culture of Fear: Social Science Fiction(s) and the Production of Knowledge about Cybercrime', *Information, Communication & Society*, 11(6): 861-884 (Revised Feb. 2011). http://ssrn.com/abstract=1155155, accessed 1 August 2011.

Wall, D.S. (2011) *Organizational Security and the Insider Threat: Malicious, Negligent and Well-Meaning Insiders*, White Paper: Data Loss Prevention, Reading, UK: Symantec. https://www4.symantec.com/Vrt/offer?a_id=108920, accessed 1 August 2011.

Williams, M. (2006) *Virtually Criminal: Crime, Deviance and Regulation Online*, London: Routledge.

White House (2003) *The National Strategy to Secure Cyberspace*, White House, February. http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf, accessed 1 August 2011.

Yar, M. (2006) *Cybercrime and Society*, London: Sage.

Zetter, K. (2011) 'DHS Fears a Modified Stuxnet Could Attack U.S. Infrastructure', *WIRED*, 26 July, http://www.wired.com/threatlevel/2011/07/dhs-fears-stuxnet-attacks/, accessed 1 August 2011.