Original Article

The role and importance of trust: A study of the conditions that generate and undermine sensitive information sharing

Martin Gill[a], and Stephen Crane[b]
[a]PRCI Ltd, Romary House, 26 Church Road, Tunbridge Wells, Kent, UK.
[b]HP Labs, Long Down Avenue, Stoke Gifford, BRISTOL, BS34 8QZ, UK.

*Corresponding author.

Abstract This article evaluates the role of trust in a specific area of security activity, sensitive information sharing. It begins by exploring the nature of trust, and then moves on to highlight on the one hand some of the security benefits when trust is evident, and on the other the risks that can accrue when trust is misplaced. It then moves on to report the findings from an empirical study by discussing how three key elements: process issues, people issues and technology can, when done well improve the security of information sharing, indeed, it can create additional security opportunities, and when done badly can undermine it. In conclusion the article asserts that the generation of trust is fundamental to effective sensitive information exchange but this poses real challenges including in deciding how much trust is appropriate.

Security Journal (2017) **30,** 734–748. doi:10.1057/sj.2015.13; published online 18 May 2015

Keywords: trust; sensitive information sharing; information security

Defining trust has long been held as conceptually problematic (Bailey, 2002; Haralambos and Cofta, 2010), at least in part because it is 'relative, fluid, and multidimensional' (Schneier, forthcoming, p. 6). Trust is typically viewed as a positive attribute and a key characteristic of a virtuous society (Fukuyama, 1995), where it is seen as a mechanism for generating perceptions of equity in service delivery (Nyaupane *et al*, 2009), as underpinning the effectiveness of the financial system (Mayer, 2008), and as a key component of establishing justice (Hough *et al*, 2010; see also Hough, 2012). Indeed, in the context of organisational analysis it has been interpreted as a contributor to the presence of higher levels of staff satisfaction (Driscoll, 1978); to greater staff competence at work; as facilitator and indeed a requirement of effective relationships across organisations (Tomkins, 2005) and with clients (Johnson and Grayson, 2005); and in generating competitive advantage (Newman, 1998; Young, 2006). Not surprisingly then, managing trust is seen as something to be good at (Eccles *et al*, 2007). Yet the presence of trust is not a given and its existence to the lesser or greater extent will vary with circumstance (Cook *et al*, 2005), with organisational and client cultures (Bierestaker, 2009), and will be tested by different circumstances such as rapid company development (Robinson, 1996), and the presence of a known or potential threat (Schneier, 2012).

Existing research has considered the issue of trust in relation to information systems/exchange specifically. For example, Kelton *et al* (2008, p. 372) conclude from their extensive review of the literature on trust and information that: '(t)rust is a necessary precondition for information sharing and e-commerce on line', and they call for more research on the topic. Other research has shown that a higher level of trust in technology and the outputs from technology have been linked to a better quality of security decisions that are made (Kirschenbaum *et al*, 2012). It has also been argued that the purpose of trust is to reduce the chances of negative consequences (see, Wang and Emurian, 2005; Kelton *et al*, 2008).

Moreover, Sasse *et al* (2007) have argued that building trust into security systems is desirable, even necessary, from an economic point of view. They note that without trust high levels of reassurance have to be built into systems that are costly and less flexible (see also, Keval and Sasse, 2010). Yet there are three key points that need to be made with regard to the above observations. The first is that there is considerable debate about what is meant by the word 'trust' (see, Mcknight and Chervany, 1996). Cofta (2011) makes a distinction between 'trust' and 'trustworthiness' and discusses 'trust assurance' 'trust management' and 'trust usage' and he also acknowledges the existence of 'trust creation'. Typically the use of the word 'trust' implies as a minimum, some type of expectation that what is intended to happen will happen. Often there is a requirement to collect evidence on the behaviour of entities and to ensure any controls are adequate. For example, data has passed to the people it was intended for and no-one else, and that those managing the process behaved as expected and required. Indeed, the discussion about what 'trust' is can quickly become complicated. Here, and recognising the actual complexity, we wish to focus on its core elements, that trust involves some expectation of behaviour of people and systems and that the flow of information is processed as intended.

A second point is that generating trust is typically a longer term process and not easily susceptible to the quick managerial fix (Denize and Young, 2007); it has to be planned for. Also, once that trust is lost it can take a long time to re-establish.

Third, the process of trusting means accepting risks (and managing them). The risk is that those who are trusted may abuse the trust placed with them. After all, there is a well-documented set of criminological studies that have highlighted how the abuse of positions of trust by employees has resulted in massive losses to organisations (for example, Levi, 2008; Gill and Goldstraw-White, 2010). Clearly the characteristics of the risk in question will vary with the characteristics and attitudes (to trust) of the people involved, the systems and cultures in which they operate, and with the competence of the technology and systems they use, albeit, that some argue that only people can be trusted, not machines that do not have a social conscience (see, Solomon, 2000). As far as sensitive information sharing within and between organisations is concerned, it has been argued that the risks can be reduced by creating trusted working environments, or trust relationships (see Toh and Srinivas, 2012).

There are two key goals for this article. The first is to help better understand the role of trust in sensitive information sharing as a means of providing security. This has been the focus of attention both because security measures have been seen to be wanting (Schneier, 2012), and because the threat is emerging as a significant one for modern organisations (Ponemon Institute, 2012). The second is to contribute to the debate which argues that 'to reduce the immediate threat an organization must address the issues of people, policy, and technology together' (Janes; 2012, p. 144; see also, Andress, 2003; Hamou-Lhadj and Hamou-Lhadj (2009).

This article seeks to explain how process, people and technology both contribute to (when done well) and undermine (when not fully effective) the establishment of trust. Specifically the article looks at the role of rules, human factors and technology and its limits. This is not intended to be a review of all possible influences, rather those that emerged from interviews with representatives from an empirical study focused on these points.

Methodology

The study reported here was part of a first stage commitment to empirically research trust (and distrust) in action. Later stages, more technical in nature, were primarily focused on developing models for better understanding trust (see, Crane and Reinecke, forthcoming). We were specifically interested in those who worked, in some way, in sharing information, particularly where this was sensitive, high value and we included discussions about information at rest and in transit. Our primary focus was to understand the main risks to business in engaging in information exchange, and in this context to gain an appreciation of what constitutes trust and to what extent trust is a business imperative. In so doing we looked at how organisations use information to enhance confidence and improve interactions, how organisations react when forced to share information in uncomfortable situations and the role played by technology in information exchange. Topics covered included:

- Attitudes to taking risks
- The extent of ownership with regard to information and security
- The tension between choosing internal controls versus external, outsourced controls, for example, the Cloud
- The degree to which compliance (legislation, policy) is achievable in practice, and in general the role and effectiveness of enforcement techniques
- The breadth and depth of understanding that organisations have about modern day threats to information
- Evidence that information sharing can be described in terms of flows (or processes), a concept of understanding that would later emerge as a building block of the project's modelling capability
- The role of technology in establishing (or undermining) trust

Our empirical study was conducted in two phases. The first stage from May 2011 to January 2012 involved interviews and focus groups with representatives from different levels in organisations including the most senior levels of management and those involved in day-to-day operations. Our study was qualitative in nature; we wanted to understand the nuances of the role of trust in information sharing. Clearly we wanted to discuss sensitive issues. There were two main influences or considerations that governed our choice of who to approach for interview. The first was that we wanted to include a broad cross-section of business verticals. This was not in order to report findings on each vertical – that would have required a very different approach – rather to understand a broad variety of contexts in which issues around trust emerge and are managed. The seven verticals we selected covered the public and private sectors, high risk areas such as policing and protection of the national infrastructure, regulated and unregulated industries, and some working in areas where information sharing was contextualised by competition, both internally and with rivals. The verticals were:

Table 1: Table to show number of organisations represented in each vertical

Vertical	*Government*	*Education*	*Utility*	*Technology provider*	*Finance*	*Manufacturing*	*FMCG*
Number of organisations	✓✓✓✓	✓✓✓	✓✓	✓✓	✓✓✓	✓✓	✓✓

Government, Education, Utilities, Technology Providers, Finance, Manufacturing and Fast Moving Consumer Goods (FMCG). In all we met with representatives of 12 organisations, some of which were large organisations that covered more than one vertical; these are summarised in Table 1. The second factor influencing who we approached related to the fact that gaining support from top-tier organisations is always challenging and not least when there is sensitivity (often for both legal and commercial reasons) hence the choice of organisations approached relied largely on prior professional relationships and snowball sampling (see, Gomm, 2008). In each organization we asked to speak to those who were involved in information sharing and this generated representatives working at different levels. It is important to stress that our sample is not necessarily representative, indeed it is unlikely it is, rather it includes a variety of individuals engaged in the very different aspects and contexts in which trust is an element of information sharing.

In all but one case the empirical work was conducted by both authors and interviews with individuals ranged in duration from 45 mins to up to a whole day although typically they lasted from 1 to 2 hours. While often just one person was involved sometimes two, three or four people took part in the interview. One organization permitted us to interview 12 people involved in different ways and at different levels in the sharing of data over 2 days, another institution hosted a visit and combined some personal interviews with the opportunity to conduct small focus group discussions with three to four staff representing different parts of the organization involved in different ways in sharing sensitive information. In all 32 individuals contributed to the study in this way. However, as the research reported in this article was part of a larger research project that included leading experts from the field of information security and trust, and during the project we benefited from the input of invited speakers, we were in the fortunate position of being able to discuss our findings with an engaged and informed peer group. This process certainly enabled us to develop our thinking and clarify our insights. All participants were promised anonymity.

The interviews and group discussions mostly took place in the first half of the project (which started in April 2011). Interview transcripts were checked by both researchers and then analysed systematically by hand. Key themes were identified that suggested levels of trust were heavily influenced by a range of people, process and technology issues themselves influenced by the organisation setting (see, ISACA, 2009).

People Issues: The Role of Human Factors

We focus in this section on humans, their attitudes and their behaviours, before switching in the next section to processes (including rules and policies).

The role of ‘human factors’ (Sasse *et al*, 2007) is important. Attitudes towards rules can be a crucial determinant for whether rules work or do not. It is much easier to protect information when security is the only priority, but in practice this is rarely the case. Information exists to be used, and security is just one of the conditions that governs its use. Tension arises when security 'interferes' in the smooth flow of the process.

As a Chief Information Security Officer (CISO) from a global financial risk management company noted, 'Security will always lose to convenience' and that 'there is not a single security solution that is not based on the integrity of the people using it. You give it a best shot and it will not always work'.

Many references were made to this particular issue, for example:

> Some policies do not enable you to do your job and then you get around them by different ways. The policies are too strong in some cases and they do not work. (Chief Finance Manager, ICT company)

> Controls are inconvenient to use, encryption policies hard to follow. (Cyber Forensics Manager, bank)

> I wanted to share data with the local University, we were working on a project. I removed various fields to anonymise it, but I thought I had better seek advice before sending on, I just thought that since this was data that was potentially sensitive I better had. The information person I spoke to said I could not share by email because they did not have secure email. So I had to put everything on an encrypted memory stick and take it down personally. So that took a morning of my life. (Deputy Head, policing unit)

> Do some people see security as a pain and try and get around it? Yes, they do. (Information Risk Manager, bank)

One human factor that undermined effective data transfer was competition between groups. Even within the state sector, competition is a serious issue. For example, the head of information security for a group of local authorities summarised that the main impediments to sharing data are, 'a lack of information sharing protocols and policies, common standards for information classification, and the lack of trust between organisations'.

The deputy head of a policing unit highlighted data sharing problems within a police force, 'I have come across situations where one constable will withhold information from another officer because he wants to make the arrest and get the credit'.

One chief finance officer from an ICT company noted that:

> We have an ongoing problem with HR, they do not understand our role and what we have to do. But then you have a friendly relationship with someone in HR who will send what you need. Ridiculous because the system, if it was good, would facilitate this and avoid the problem of us all breaking the rules.

Knowing individuals personally was frequently cited as a reason and a facilitator for breaking rules on information sharing. When people interact with someone they know they get around rules and technology controls by giving information verbally, typically over the phone. Individuals were prepared to risk personal admonishment to get the job done, albeit with the expectation that they will not be caught, and if they are can argue that they are working in the 'best interests of the company'.

Knowing someone well enough to call them trusted was an important criteria in determining whether to share information. When sharing with another organisation, trust was sometimes more important than brand and reputation (including reputation of their technology and information sharing processes).

There is usually an assumption that employees will consistently act in the best interests of their employer, but sometimes they do not. Schneier (2013, p. 159) gives the example of the 'defecting employee: someone who doesn't think of his employer's best interests while doing his job'. Employees can be careless and/or lazy in their attitudes to work. Several interviewees noted that training is given to employees on how to share data effectively, particularly when the information is sensitive and/or the risks are high. The expectation is that individuals will then act responsibility, but not all do, giving rise to the 'insider threat'.

Insider threat relates to an employee who exploits an opportunity by virtue of the status and/or autonomy they hold within the organization (Gill and Goldstraw-White, 2010; Capelli *et al*, 2012). This directly undermines processes that rely on an element of trust, a reality recognised as serious by a majority of IT security professionals (Aleem and Sprott, 2013). While employees recognised this as a criminal act, others pointed to an interpretation that saw this as a means by which the 'disaffected' breached rules rather than contravened laws.

The head of information management for an international data protection organisation felt that his company had used due diligence in creating a 'trust awareness' culture, and focused on good risk management, internal structure and effective use of technology. Yet they recognised the danger of insider threat as serious, especially when offenders colluded with outsiders. Other interviewees highlighted similar dangers, and felt that their organisation did not have a culture and procedures that would manage the insider threat well, and that while process and technology can be audited, audit is only effective up to the point of collusion.

The culture of the organization clearly has a bearing on attitudes towards information flow. A financial crime director for an insurance brokers noted that 'strong cultural values govern how staff share information', while others, including a CISO for an international energy distributor, highlighted the existence of many sub-cultures within an organisation.

Sometimes the culture is well developed. The CISO for an international engineering manufacturer noted that the culture in their organisation was somewhat relaxed. This is in contrast to the more heavily regulated and controlled culture evident in the financial sector.

Process Issues: Formal and Informal Governance Frameworks

Typically, organisations create rules that describe how information should be shared, and with whom. When information carries a sensitivity classification, the rules take this into account. Rules reflect an organisation's values, but are also influenced by legal and societal values. For example, the laws of the land, statutory and voluntary regulation, and industry best practices.

However, although the motivation for having rules is clear, difficulties in the way that they are implemented and interpreted can lead to a lower level of adoption than expected.

Our interview with the director of financial crime for an insurance brokers revealed that corporate policies designed to secure information were difficult to interpret. Yet, getting it wrong could have serious consequences for the organisation. Even those who enforce the law are not immune; warranted police officers interviewed noted that they too are bound to follow processes, the consequence of failure being imprisonment. Many others that we interviewed recounted events in which colleagues did not abide by the stated policy, and suffered accordingly. What they described as negative consequences were also said to keep people on their guard.

Part of the difficulty for those whose working responsibilities involve sharing sensitive information securely is that technical solutions alone are not enough; they need to be aware and able to follow the rules. Yet rules, which on face value seem straightforward, can be problematic:

First, the rules may be ineffective – they do not protect the information. This situation is complicated further if those following the rules consider them to be inadequate. One ICT manager lamented that rules put in place were 'idealistic' and only introduced to protect the company from litigation, and that some did not work at all. Another interviewee noted that their university had set aspirational policies (that is, policies that are set in the knowledge that not everyone/all employees can or will comply) on purpose to exploit the psychology of people. By encouraging their use, people would become aware of the need, but no attempt was made to enforce their use. Achieving partial adoption was considered to be a satisfactory outcome, reflecting the culture in which academic and personal freedom is highly valued.

Second, the rules are bad – bad in the sense that although they do protect information, they are not conducive to working practices, especially the practices of those on the front line. As a consequence users find ways to get around them, or ignore them altogether, on the justification that the needs of the business outweigh the need for security. Many interviewees admitted that they had broken rules when sharing information in order to 'get the job done', and that their actions could have had serious implications for their organisation. High on the list of reasons was difficulty in using information classification systems (frameworks); they were too complicated to use, and often used inconsistently within the same organisation. Sharing between organisations was even worse, with different terminology, interpretations of meanings and incompatible processes complicating the situation. In part, this failure was put down to poor communications (rules, categorisation), but also a degree of frustration arose from the time it would take to follow the requirements.

Third, awareness of the rules relating to sharing information is poor – few have sufficient knowledge of the processes, and consequently they are not followed.

A cyber forensics manager for a bank noted an example where the Board failed to promote awareness. There were even instances where individuals had been disciplined for breaches despite the individuals having no knowledge of the process and tools that should be used to protect the information. In the case of one risk management company, the CISO admitted that information that should have been encrypted was in fact not.

The CISO of a manufacturing multinational noted that within the organisation (consisting of more than a 'score of companies'), different security marking practices existed, and that there were few impediments to sharing because the organisation did not take information protection seriously; cyber-crime incidents were going unreported. However, there was evidence that situations similar to this are declining, with the creation of new CISO roles in direct response to poor security awareness. A more security-minded culture is emerging that gives greater attention to the development, implementation and adoption of policies and procedures.

These examples of seemingly straightforward rules being ignored are strongly influenced by the context surrounding the situation. For example, within a law enforcement unit that frequently shared sensitive information overseas, our interviewees reported that some foreign law enforcement organisations are less trustworthy. The level of trust may be based on prior interactions, where a rapport develops between individuals. However, even in these situations, where 'priority is to the victim', there was still a danger of sensitive information 'getting into the wrong hands'. The consequence of this had repercussions beyond the individuals of the organisation, for example, when an offender finds out:

> Sometimes we have to take a risk. If we knew a victim might be harmed, and the only way of intervening is to release information about a potential attack on a victim, then we would release the information. We would assess the risk – the victim could be attacked, the offender could get the information, it could ruin relationships … The report had said something which was not accurate and the person found out, maybe via freedom of information request and they (sic) complained. It was awkward. And it takes time away from dealing with other real cases where we are protecting access to victims. You have to be careful, I mean you have to check where information is coming from and grade intelligence. We can do this in the UK, but overseas it is not always the same. You have to be careful and it may not be corroborated. (Manager of risks posed by travelling offenders, policing unit)

A major impediment for organisations that aspire to implement systems that have trust at their core is the different regulatory requirements that apply internationally. An example of this is, as mentioned above, the various ways that information is risk assessed, classified, labelled and protected, vary with geography, cultural values and maturity of technology.

Technology and Its Limitations

Technology that tightly enforces a process, and that strongly directs people, relaxes the need for trust in humans. But as we have already heard, technology can be inflexible and not designed with every eventuality in mind (Peterson, 2010).

Technology provides a control point, one that underpins the processes that it is designed to support. And where those processes involve information sharing, each action that contributes to the sharing is in a sense guaranteed by the technology, whether that be identifying the parties involved, protecting the information during transmission using encryption or logging what takes place. This supports a common criticism of technology, that the very processes that the technology is designed to protect are sometimes undermined by the technology itself (Peterson, 2010).

Technology also enforces rules: users need permission to access the system; users do not have sign-off authority; users cannot share information with an organisation unless it is on the approved list. But as we have already heard from our interviewees, inflexible technology can give rise to rule breaking. In essence, while technology solves some problems, it also creates a new set of problems that need to be managed. As one interviewee remarked:

> I distrust technology. I never believe it when I am told things are safe and secure. I think there are some technical systems you can trust because we work in the best in the world in terms of encryption. Now adversaries don't have to go through hurdles to get what they want. There is always a human element to technology. Security systems are more comfortable in making humans not behave in a certain way. You can mitigate the risk

> but it will keep changing. Technology may give us a better control. We are talking about data and information, and we are talking about an activity in which people fail to comply and fail to do what they should, short cut, get things done quickly. (Director, specialist law enforcement agency)

The interviewees noted several problems that arise because of technology.

First, technology was poorly specified, placing the blame squarely with the security specialists. In part this was because the security specialists – technical people – ask technical questions of non-technical people. Being asked was better than not being asked at all, but the lack of shared understanding reduced the value of the question and the answer.

Interviewees also noted that whenever information sharing was present, the solution would be problematic. A university security and compliance officer noted that there exists a range of questions that needed to be asked when receiving information, which are easy to ask but hard to answer. For example: What is the source of the information? What conditions are attached to having it? How will it be processed? What controls were present at the origin of the data? Is the information part of a classification scheme, and if so, what is that? What will anyone getting hold of the information make of what they find?

A risk manager covering third-party risk for a bank made a similar point, suggesting that some key questions should in theory always be asked: how much data are there? What is the type of data? Where will it be held? Who will handle it? What controls are needed? How do they work? Do we trust the audit firm from the data source? Do we trust the vendor? What reassurance do we need? The problem is that the questions are important to ask but they do not always generate meaningful answers.

Second, technology quickly becomes out of date and unfit for purpose. It was noted that it was not easy for organisations operating in a continually changing threat landscape to know which technological was best. One interviewee admitted that as a consequence of weak technology, their organisation could address only a few threats, leaving them exposed to those that technology could not address.

Third, mergers and acquisitions, and variable procurement practices, meant that different parts of the same organisation use very different types of technology. A financial crime director from an insurance broker noted that one of the consequences for his company was that they were not able to support all the different systems fully, ‘We have grown through acquisition so it has not been joined up. This means technology does not always work as it should’.

Fourth, new technologies sometimes demand organisational change. For example, they may not be designed for the organisational structure in which they are deployed. Some pointed out that the normal procedure of testing products to ensure they can be safely deployed, and ensuring that user requirements were properly and effectively articulated, had to be relaxed when new technologies were ‘rushed in’ to replace old and failed system. The wide use of tablets was cited by interviewees as an example of new technology being adopted quickly, often driven by senior management. This had created the need for policy changes where the driver was convenience, which then came at the expense of security. As a CISO of a global financial risk management company noted, ‘We had to relax the policy to permit the use of these technologies. So many people were using these devices, people were able to get nicer devices than the company was providing, and this is happening top down too. We had to react and make exceptions’.

Fifth, and overlapping with people and human factors issues, is that technology was considered hard (cumbersome and/or complicated) to use. There were a number of references to this problem. One representative from a bank noted that she had had ‘to dig on the internet to find the solution and apply it. Then you have to train the person the other end to respond to controls’.

When asked about the main impediments to sharing information, some interviewees pointed to the time it takes to learn and use certain technologies. Often simple tasks such as writing to DVDs, uploading to Websites, installing new apps, getting external access and/or access to a specific system, logging into Web portals and even using email, delay the process. There was a strong link between technologies being hard to use and technology being perceived as not being fit for purpose.

Some interviewees noted that the nature of the information security team had a bearing on attitudes towards information sharing. Some took comfort from the fact that a team was ‘not outsourced’, while others were less sure. Those that favoured internal arrangements were largely suspicious of outsourcing because of issues of trust (in the people, processes and technology). Others held the polar opposite view, that outsourcing meant that the complications of technology would be in the hands of the experts.

Assessing the Context

Trust operates in a dynamic environment, indeed attitudes to risk varied; these were driven by a number of factors. One key factor identified was the importance of strong leadership in setting the tone for what was acceptable and then backing this up with action against those whose behaviour fell short of requirements (see, Janes, 2012). Another factor was the level of importance attached to the risk within the company. The CISO for an international energy distributor noted that the company philosophy was risk adverse, and although there was an approach which emphasised devolved responsibility with education and guidance being directed from the Board, in practice this was not communicated to best effect.

Another key factor is that trust can be difficult to measure and difficult in practice to create and this limited its appeal to some:

> People do business with people, I accept that, but good business is done without trust. You cannot afford for it to be based on trust in case you get it wrong. It is very difficult to reconcile. So when we discuss information sharing I would steer away from trust, I would base it on a need and an auditable process, just don’t worry about trust at all. The auditable bits are the things you rely on. Trust implies an exposure for the firm, I mean how do you say we trusted this guy as a defence when things go wrong? (CISO, Global financial risk management company)

A university security and compliance officer made a similar point, that ultimately people could not be trusted, especially where there was a high turnover of staff, and so there was a preference where it was possible and practical to place more reliance on technology that could be automated: ‘we prefer to focus on technology where we can … we like to automate processes, that reduces human risk’. Against this, a senior crime manager from an insurance broker noted that technology can be circumvented by staff and even automation has to be managed by humans. And a deputy director of a policing unit warned ‘technology doesn’t do sharing, people do that. Technology is a tool’.

Another problem that information security professionals face, in fact, security professionals generally, is the low status of security within organisations (Cavanagh, 2005; Gill, 2013, 2014; Gill and Howell, 2014). There were two main sources of evidence sighted to support this. The first is the extent to which policies were overridden by senior managers or by staff (and backed up by business managers) in pursuit of what are justified as more important business objectives. This can lead to some fractious discussions. One university security and compliance officer highlighted some of the problems that come from a strong belief in academic freedom, which, he lamented, can evolve into ‘a sense of we do what we want, it is about academic freedom’. In addition to academics acting individually in this way, University Departments also acted autonomously (limiting the amount of oversight that is possible), arguing that it was up to them to do the real work while central information security personnel managed the risks albeit that ‘this is not realistic’.

The second issue here was what was perceived as the meagre resources devoted to protecting information. It was argued that this led to poor policy development, inadequate technology, and what one interviewee described as ‘contradictory policies’. There are real problems in being able to assign a value to information and the exchange of it, and to prove the return on investment. Indeed, some interviewees argued that ignorance about the value of secure information was common. Whether this is the symptom or the cause needs further research. Some interviewees noted that in services industries where people were crucial to the business model, IT may inevitably be viewed as a low priority. A director of a specialist law enforcement agency noted that: ‘the truth of the matter is that we as any organisation in the public sector will be behind the curve because we will never be able to invest in technology’, and because ‘we are but a tiny part of a much bigger system’.

Discussion

If, as seems likely, the presence of trust is endemic to conducting good business and to the effective sharing of sensitive information, then there is evidence to suggest that different types of organisations do not always adopt good practices. Indeed, some encouraged risky behaviour in the way they managed information that could, and in some cases did, result in serious consequences. Even organisations that considered themselves risk adverse often took risks with the management and exchange of data, not least because staff sometimes sought and found practical ways of circumventing rules they considered inhibited the process of doing business. The findings lead us to postulate three key characteristics of trust, all of which merit further research and analysis.

The first is to suggest that the generation of trust is fundamental to effective information exchange. Indeed, further research might explore the extent to which we can postulate that trust is in fact a security measure in its own right. So, just as an organisation may introduce access controls to protect against unwanted intruders so it may generate trust as a means of protecting its assets. A complicating factor is that trust is difficult to measure and to evidence, and difficult to enforce in practice. Where the generation of trust is pursued, it will always need to be framed with a clear definition, and backed up by objectives and policies that take account of the specific circumstances it is being introduced into and against the threats which it is intended to mitigate.

The second is to recognise that trust is fundamental to the effectiveness of other measures. Managing trust well is dependent on a well crafted relevant set of laws and rules to guide behaviour. These need to be supported with education and guidance to ensure they are implemented; policies for understanding when exceptions are acceptable (if at all) are required; and a culture that recognises rules and regulations as important. Well motivated humans are important too, geared to meeting the objectives of the organisation by behaving in a way that is legal, compliant and has the best interests of the business at heart. And supported by a range of technologies that are fit for purpose easy to follow and which can be relied on is also important. Knowing how and when to use them is a crucial part of the process.

The third is to recognise that more research is needed to identify and realise the right amount of trust. Approaches to achieving this are dependent on a good understanding of security risks, well thought through responses that mitigate threats in a proportionate way (Beautement *et al*, 2008; Moss, 2009, 2011; Gill, 2014); a leadership that sets an example and supports and enforces agreed approaches enthusiastically; a culture that is conducive to good business and good security on sensitive information sharing remains key. Indeed, the culture of an organisation, the priority attached to business process and the closeness and effectiveness of supervision of this area, the existence and quality of training and the levels of awareness all combine to create a context in which trust is a fundamental requirement for the organization to be able to operate. Sometimes the problem is the technology, not because of a security weakness *per se*, but because it is not fit for purpose, sometimes because the technology is cumbersome and/or complex, was poorly specified and/or installed, or the needs of the business and its users change. It is a key finding that the tendency to exclude organisational issues, alongside process, people and technology, or at least not to see them as a specific point of reference risks missing a key component of what makes information sharing effective, indeed the effectiveness of process, people and technology is mediated by organisational issues.

Absolute assurance is in practice so hard to achieve that incorporating an element of trust is an unavoidable component in all systems designed with security in mind. After all, trust needs to be placed in the crafters of rules that they are informed and well intentioned; in the communicators of the rules that they do so wisely and with good intentions; and that users of the rules have the best interests of their employers at heart. Where they break rules for what they would consider good intentions like sharing with a colleague (outside the trust domains) in the belief that this is beneficial to getting the job done, they need to be trusted to raise awareness of weaknesses, and be trusted to make good judgements in who they collaborate with. Similar points can be made about technology, people must be trusted to make the right specification; to implement/install systems effectively; to recognise weaknesses and implement effective remedies; users need to be trusted not to circumvent the purpose of the technology for illicit aims; and where they meet compliance problems to report them and seek guidance to follow rules. Organisations create cultures but people need to be trusted not to create sub cultures of deviance; senior managers have to be trusted to make good decisions about levels of risk and the correct investment in rules, people and technology to set examples of conduct that support and encourage trust. Clearly people are crucial. Good security including good information security is dependent on trust and most notably for the trust placed in and generated among people.

Concluding Comments

This article is based on a small scale study and its limitations need to be borne in mind. It is hoped that the findings and discussion will provide a basis for more critical thinking about the ways the concept of trust can be understood, in which sensitive information exchange can be researched, and better practices developed. There are some key characteristics of data sharing which will always be a challenge to good practice. These include (but are not limited to): the existence of inter and intra company/region differences (for example, in compliance requirements); not knowing who the recipients or distributors of data are; overcoming territory and competition between individuals/groups within and between organisations; weak classification systems; and motivating humans to follow rules when their priorities and the reasons for their employment are typically different (and these can sometimes be contradictory). There is then a diverse set of issues that impact on trust relationships, so much so that in some cases it seems it is only possible to set aspirational policies. It may be that the strongest trust relationships can only exist when there is a culture based on a set of prioritised shared values that says sharing information needs to be undertaken in a certain way. What is clear is that problems arise when trust is absent and opportunities arise when trust is nurtured. Yet questions still arise in defining how much trust is acceptable and in finding meaningful ways of measuring this. These are areas where more research is needed.

Acknowledgements

The project on which research for this study is based was funded by the Technology Strategy Board (Project TP/400206) and EPSRC. Project partners are: HP Labs, Perpetuity Research Limited, Oxford University, Birmingham University, Aberdeen University and University College London. We would like to thank colleagues from partner organisations who helped us develop the ideas in this article and specifically Philipp Reinecke (HP), Simon Arnell (HP), Ruth Crocker, Charlotte Howell, Sarah Webb (Perpetuity Research) and two anonymous referees for comments on earlier drafts of this article.

References

Aleem, A. and Sprott, C. (2013) Let me in the cloud: Analysis of the benefit and risk assessment of cloud platform. *Journal of Financial Crime* 20(1): 6–24.

Andress, A. (2003) *Surviving Security: How to Integrate People, Process and Technology*. Auerbach Publications.

Bailey, T. (2002) On trust and philosophy. The philosophy of trust, Open University Reith Lectures 2002, http://www.open2.net/trust/on_trust/on_trust1.htm, accessed March 2013.

Beautement, A. *et al* (2008) Modelling the human and technological costs and benefits of USB memory stick security, http://homepages.abdn.ac.uk/d.j.pym/pages/pym-weis-2008.pdf, accessed 14 June 2013.

Bierstaker, J.L. (2009) Differences in attitudes about fraud and corruption across cultures: Theory, examples and recommendations. *Cross Cultural Management* 16(3): 241–250.

Capelli, D., Moore, A. and Trzeciak, R. (2012) *The Cert Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud).* Upper Saddle River, NJ: Pearson Education.

Cavanagh, T.E. (2005) *Corporate Security Measures and Practices.* The Conference Board, SR-05-01, Conference Board: London, March.

Cofta, P. (2011) *The Trustworthy and Trusted Web*. Foundations and Trends in Web Science. Vol. 2. No. 4. Delft: The Netherlands.

Cook, K., Hardin, R. and Levi, M. (2005) *Cooperation without Trust?* New York: Russell Sage Foundation.

Crane, S. and Reinecke, P. (eds.) (forthcoming) *Trust Domains Guide: A Guide to Identifying, Modelling, and Establishing Trust Domains.*

Denize, S. and Young, L. (2007) Concerning trust and information. *Industrial Marketing Management* 36(7): 843–1018.

Driscoll, J.W. (1978) Trust and participation in organizational decision making as predictors of satisfaction. *The Academy of Management Journal* 21(1): 44–56.

Eccles, R.G., Newquist, S.C. and Schatz, R. (2007, February) Reputation and its risks. *Harvard Business Review* 85(2): 104–114.

Fukuyama, F. (1995) *Trust: The social virtues, and the creation of prosperity*. New York, NY: The Free Press.

Gill, M. (2013) Engaging the Corporate Sector in Policing: Realities and Opportunities. *Policing: A Journal of Policy and Practice* 7(3): 273–279.

Gill, M. (ed.) (2014) Exploring some contradictions of modern day security. In: *The Handbook of Security*. 2nd edn. London: Palgrave Macmillan.

Gill, M.L. and Goldstraw-White, J.E. (2010) Theft and fraud by employees. In: F. Brookman, M. Maguire, H. Pierpoint and T. Bennett (eds.) *Handbook of Crime*. Uffculme, UK: Willan.

Gill, M. and Howell, C. (2014) Policing Organisations: The Role of the Corporate Security Function and the Implications for Suppliers. *International Journal of Police Science and Management* 16(1): 65–75.

Gomm, R. (2008) *Social Research Methodology: A Critical Introduction*. Basingstoke, UK: Palgrave Macmillan.

Hamou-Lhadj, A. and Hamou-Lhadj, A. (2009) A governance framework for building secure IT systems. *International Journal of Security and Its Applications* 3(2): 15–20.

Haralambos, M. and Cofta, P. (2010) Practitioner's challenges in designing trust into online systems. *Journal of Theoretical and Applied Electronic Commerce Research* 5(3): 66.

Hough, M. (2012) Researching trust in the police and trust in justice: A UK perspective. *Policing and Society: An International Journal of Research and Policy* 22(3): 332–345.

Hough, M., Jackson, J., Bradford, B., Myhill, A. and Quinton, P. (2010) Procedural justice, trust and institutional legitimacy. *Policing: A Journal of Policy and Practice* 4(3): 203–210.

ISACA. (2009) An introduction to the business model for information security, http://www.isaca.org/Knowledge-Center/Research/Documents/Introduction-to-the-Business-Model-for-Information-Security_res_Eng_0109.pdf, accessed March 2013.

Janes, P. (2012) People, process, and technologies impact on information data loss, http://www.sans.org/reading_room/whitepapers/dlp/people-process-technologies-impact-information-data-loss_34032, accessed 14 June 2013.

Johnson, K. and Grayson, D. (2005) Cognitive and affective trust in service relationships. *Journal of Business Research* 58(4): 500.

Kelton, K., Fleischmann, K. and Wallace, W. (2008) Trust in digital information. *Journal of the American Society for Information Science and Technology* 59(3): 363–374.

Keval, H.U. and Sasse, M.A. (2010) Not the usual suspects: A study of factors reducing the effectiveness of CCTV. *Security Journal* 23(2): 134–154.

Kirschenbaum, A., Mariani, M., Van Gulijk, C., Lubasz, S., Rapoport, C. and Andriessen, H. (2012) Airport security: An ethnographic study. *Journal of Air Transport Management* 18: 68–73.

Levi, M. (2008) *The Phantom Capitalists: The Organisation and Control of Long-Firm Fraud.* Aldershot, UK: Ashgate.

Mayer, C. (2008) Trust in financial markets. *European Financial Management* 14(4): 617–632.

Mcknight, D. and Chervany, N. (1996) The meanings of trust. Carlson School of Management, University of Minnesota, http://misrc.umn.edu/workingpapers/fullpapers/1996/9604_040100.pdf, accessed 12 July 2013.

Moss, K. (2009) *Security and Liberty: Restriction by Stealth*. Basingstoke, UK: Palgrave Macmillan.

Moss, K. (2011) *Balancing Liberty and Security: Human Rights and Human Wrongs*. Basingstoke, UK: Palgrave, Macmillan.

Newman, J. (1998) The dynamics of trust. In: A. Coulson (ed.) *Trust and Contracts*. Bristol, UK: Policy Press.

Nyaupane, G., Graefe, A. and Burns, R. (2009) The role of equity, trust and information on user fee acceptance in protected areas and other public lands: A structural model. *Journal of Sustainable Tourism* 17(4): 501–517.

Peterson, G. (2010) Don't trust. And verify: A security architecture stack for the cloud. *IEEE Security and Privacy* 8(5): 83–86.

Ponemon Institute. (2012) 2011 cost of data breach study United States, http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf, accessed 14 June 2013.

Robinson, S.L. (1996) Trust and breach of the psychological contract. *Administrative Science Quarterly* 41(4): 574–599.

Sasse, A., Ashenden, D., Lawrence, D., Coles-Kemp, L., Fléchais, I. and Kearney, P. (2007) Human Factors Working Group White Paper: Human Vulnerabilities in Security Systems Knowledge Transfer Networks, University College London: London.

Schneier, B. (2012) *Liars and Outliers*. New York: Wiley.

Solomon, R.C. (2000) Trusting. In: M. Wrathall and J. Malpas (eds.) *Heidegger, Coping, and Cognitive Science: Essays in Honor of Hubert L. Dreyfus*. Vol. 2. Cambridge, MA: The MIT Press, pp. 229–244.

Toh, S. and Srinivas, E. (2012) Perceptions of task cohesiveness and organizational support increase trust and information sharing between host country nationals and expatriate coworkers in Oman. *Journal of World Business* 47(4): 696–705.

Tomkins, C. (2001) Interdependencies, trust and information in relationships, alliances and networks. *Accounting, Organizations and Society* 26(2): 161–191.

Wang, Y. and Emurian, H. (2005) An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior* 21(1): 105–125.

Young, L. (2006) Trust: Looking forward and back. *Journal of Business and Industrial Marketing* 21(7): 439–445.