A socio-technical perspective to counter cyber-enabled industrial espionage

Moufida Sadok, Institute of Criminal Justice Studies, University of Portsmouth, UK

Christine Welch, Portsmouth Business School, University of Portsmouth, UK

Peter Bednar, School of Computing, University of Portsmouth, UK; Department of Informatics, Lund University, Sweden

Abstract

The ubiquitous digitization of information and the pervasive connectivity of work systems have inevitably facilitated cyber-enabled industrial espionage. Security failures explain most of cyber industrial espionage incidents, and insider threats represent a significant pattern in many case examples. Insiders can inadvertently or purposefully pose serious threats to organisations by facilitating access to or misuse of proprietary sensitive data. This paper argues that technical security solutions have rather limited scope to tackle this problem, and that a socio-technical approach has potential to provide a better means to address the challenge of preventing and responding to insider threats. Such an approach could bridge the gap between the design and implementation of security solutions and creation of an organizational culture that is security aware.

Key words: cyber-security, socio-technical, industrial espionage, work system, insider threat

Introduction

Desire for means to gain competitive advantage underpins the nature of most business research. This suggests that it is vital for businesses and organisations to anticipate early-warning topics - including competitor initiatives, technological innovation, and governmental actions (Lesca and Lesca, 2011).

Analysis of such early signs of change is at the core of competitive and/or business intelligence activities, allowing organisations to develop proactive and innovative capabilities. However, there are increasing issues of concern in relation to certain intelligence gathering practices, at least from a legal and ethical point of view, which make the boundaries between competitive intelligence and industrial espionage rather blurred (Wright and Roy, 1999).

The move towards more connected work systems, in which technological developments have enabled the movement of a plethora of data over networked systems, has sparked concerns about security. Poorly designed and configured work systems might provide a backdoor for internal and/or external hackers looking to break into corporate networks.

Research on security failures has acknowledged the central role of human factors in developing and sustaining resilient security capabilities (Alotaibi, Furnell and Clarke, 2016; Soomro, Shah and Ahmed, 2016). In particular, employees can pose serious threats to their organisations, either inadvertently or voluntarily, by facilitating access to or misuse of proprietary sensitive data.

A report published by the Centre for the Protection of National Infrastructure (CPNI, 2013) states that poor management practices and poor communication between business areas have contributed significantly to increases in employee disaffection and, in consequence, increased risk of insider threats. In addition, a study by PwC and the London School of Business (Global Economic Crime Survey, 2016) shows that a "get-tough" approach to the management of performance, as well as a rise in blame culture, have created a hostile social climate. This, in turn, leads to an increased tendency towards unethical behaviours.

In this paper, we argue that there are many reasons to explain malicious and non-malicious intent of attack, but it is relevant to include among them a lack of understanding of security controls, poor communication within organizations and a lack of shared values between employer and employee. All of these tensions create cracks that facilitate vulnerabilities. We consider that a socio-technical perspective on security may be helpful both to illuminate the causes and facilitators of insider threats, and to support design of more secure and resilient work systems.

Thus, the aim of this paper is to set out a case for socio-technical approaches to counter cyber industrial espionage. In the next section, we consider the nature and scale of this problem. We then go on to examine deficiencies in security practice that may contribute towards insider threats, before discussing the socio-technical perspective, with practical illustrations. Finally, we attempt to draw some conclusions on the application of this perspective in reducing vulnerabilities.

Nature and scale of cyber-enabled industrial espionage

Industrial espionage incidents appear in the news on a daily basis. According to the Commission on the Theft of American Intellectual Property (IP Commission, 2017), the cost of counterfeit goods, pirated software, and theft of trade secrets in the USA could be as high as $600 billion. In particular, espionage via hacking costs the US economy $400 billion per year and trade secret theft costs 1% and 3% of GDP. The Centre for Strategic and International Studies (CSIS, 2018) estimates the cost of cyber-espionage between $10 and $12 billion to USA and $50-$60 billion globally. In the UK, a report published by Cabinet Office on the costs of cybercrime suggests that £7.6 billion may be attributed to industrial espionage (Cabinet Office/Detica, 2011).

The 11th edition of the Verizon Data Breach Investigations report (Verizon Data Breach Investigations, 2018), based on a dataset of over 53,000 incidents and 2,216 confirmed data breaches, shows that 90% of breaches fall into two main motives: financial gain, followed by strategic advantage – or in other words espionage. Phishing and pretexting represent 98% of social incidents and 93% of breaches; Email continues to be the most common attack vector over 95% of the time; and motives for phishing are split between financial (59%) and espionage (41%). The modus operandi of phishing is quite simple and consists of installing malware to enable the theft of and/or the access to sensitive and valuable data. The same reports states that 70% of breaches associated with nation-state or state-affiliated actors involved phishing. Threat actors attributed to state-affiliated groups or nation states combine to make up 93% of breaches, with former employees, competitors, and organized criminal groups representing the rest. Unsurprisingly, the sectors that are more affected by cyber-espionage are Education and Manufacturing. In the public sector, cyber-

espionage remains a large concern, with state-affiliated actors accounting for over half of all breaches. Interestingly, privilege misuse and error by insiders account for a third of breaches (Verizon Data Breach Investigations, 2018). The growing involvement of state actors in targeting non-military data was also highlighted in the Ninth Annual Cost of Cybercrime Study recently published by Accenture and the Ponemon Institute (Bissell, Lasalle and Dal Chin, 2019). This study involved 355 companies across 11 countries and 16 industries and shows that economic espionage, such as theft of high-value intellectual property by nation-states, is on the rise.

The threat of cyber-espionage targets also small and medium-sized enterprises (SMEs), which are vulnerable mainly because of insufficient technical and investment capacities to counter cyber-risks. The WISKOS research project on industrial espionage in Germany and Europe reveals that one-third of Germany's SMEs have been victims of industrial espionage, sabotage or data theft (Carl, 2017). The scale of the problem is significant given the SMEs' importance for an economy.

It is worthy of mention that many organisations do not know they have been victims, as espionage breaches, by their nature, typically take longer to find. In addition, organisations who suffered are rather reluctant to report breaches because of concerns about reputation and consequent effect on share price.

From a legal point of view, there are a number of national, regional and international initiatives that have been developed to address industrial espionage. Examples of initiatives to protect trade secrets against theft in the context of industrial espionage include the EU Directive 2016/943 on the protection of undisclosed know-how and business information against unlawful acquisition, use and disclosure; and international obligations within the framework of the World Trade Organisation, such as the Agreement on Trade-Related Aspects of Intellectual Property Rights.

However, the implementation of these directives and treaties is rather challenging and problematic because of a number of legal issues with enforcement and jurisdiction (see, e.g. Baron and Pigeon, 2017). In addition, it is difficult to investigate industrial espionage cases when cyber-attacks are used to root out sensitive data, as it is often difficult to identify the attackers.

Having considered the nature and extent of the problem, in the next section we consider ways in which such security breaches are currently facilitated.

Understanding deficiencies in security practices

It is clear that designing and developing robust, secure information systems is one line of defence to counter cyber-enabled industrial espionage. While there have been significant technological advancements and a considerable investment in information systems security, cyber-security continues to be a big challenge for businesses and governmental organisations.

While security risks and financial costs of cybercrime continue to escalate, advances in security practice and strategy have not been adequate to keep up with dynamic and challenging attacks (e.g. The Global State of Information Security Survey, 2016; Symantec Internet Security Threat Report 2015; Global Economic Crime Survey, 2016). In particular, enterprises experience difficulties in assessing and managing their security risks, applying appropriate security controls that match the requirements of their real business processes, and preventing security threats.

Research in information security has shown that an exclusive emphasis on a technology-centred view induces flaws in the design and implementation of security solutions, and this points to the necessity of including people and processes as a core part of secure and usable work systems (Baskerville, 1991; Bednar and Katos, 2009; Siponen and Willison, 2009). One of the fundamental problems is to balance conflicting requirements of security and usability in the context of everyday priorities in real world work systems and practices (Sommerville, 2011; Furnell, 2016; Dhillon *et al.*, 2016). There are many reasons that can explain conflicts between security and usability, but it is relevant to include among them a lack of involvement of professionals with operational knowledge in risk assessement and security policy development (Shedden et al., 2011). In order to demonstrate the importance and necessity of the contextual dimension in the design of a secure information system, the study of Spears and Barki (2010) provides a particular application of this view in the context of regulatory compliance and confirms the conclusion that the engagement of users in risk analysis process contributes to more effective security measures and better alignment of security controls

with business processes. As such, the existence of a security policy does not in itself guarantee its effective implementation or, indeed, relevance from the perspectives of those who use organizational systems (Dhillon and Torkzadeh, 2006). Applying a critical analysis of security policies, Stahl et al., (2012) have advocated that these policies can privilege certain groups of stakeholders, particularly managers and IT professionals. There is also a need for management to communicate effectively the relevance of security controls to employees who are involved in their implementation in everyday work practices (Albrechtsen and Hovden, 2010). Consequently, questions about security failures in context need to address the relevance of security policies from the perspectives of professional stakeholders. In many cases, it has been found that professionals attempting to improve their effectiveness will work around security compliance or bypass security measures altogether (Albrechtsen, 2007; Koppel et al., 2015; Kolkowska and Dhillon, 2013).

Sadok and Bednar (2016) conducted a survey involving 33 SMEs in the UK on their approach to information security risks. Key findings of this survey indicate that, while there is a wide agreement about the importance of security and its potential impact on company performance, understanding of security is rather focused on a technology-oriented perspective. However, the actual work practices and routines of most employees were either ignored or insufficiently intertwined with security management efforts. While security practices may vary by industry and company size, the challenge for most SMEs is the integration of security functions into business processes through an active engagement of all internal stakeholders in risk analysis and security policy definition. Such engagement cannot be approached via top-down managerial instructions and policies, or through reliance on the competencies of the IT department or the security specialists.

In attempting to integrate security measures into business processes and practices, it is important to consider *meaningful use*. While most people engage with information systems to some extent in carrying out their work roles, it is a mistake for designers to consider them simply as ‘users’ – few of us, if asked what we do at work, would reply that we are users of IS – we are machine operators, accountants, surveyors, customer assistants, and so on (Nissen, 2002). It is important that professionals’ individual, contextual understandings of their work roles are channelled into design practice if appropriate security measures are to be incorporated. Too often, exploration of context of

use stops at a consideration for *usability* factors – what will make the system safe and comfortable in use for given, pre-defined purposes. While it is important to achieve a balance between usability and security measures, professionals also need opportunities to explore and express what factors will render a system *useful* to them in a context of practice. Checkland and Holwell (1998), make the point that not one, but two systems are involved in IS design endeavors – a system to be served (i.e. *people* engaged in activities), and a serving system containing elements which generate data useful to those people. When we use the objective term 'information system', this tends to focus attention on the second of these to the exclusion of the first. However, human agents are required to engage with such a system in order to interpret data and transform it into something meaningful to a work role or task. It may be preferable to think in terms of 'informing systems', i.e. means by which people can inform themselves or assist others to do so. People are an essential element in any informing system and, of course, it is not possible to design a person. Effective design of an informing system requires their involvement and understanding of the process of meaning creation (Bednar and Welch, 2009). Embedding of appropriate provision to promote security *within* an informing system must therefore involve opportunities to explore the context of meaningful use.

By failing to appreciate complex relationships between use, usability and usefulness, efforts to impose security procedures will not only result in potential for misuse, but are likely to create difficulties for work functionality and efficiency (Bednar and Katos, 2009). This, in turn, will create incentives to explore short-cuts and work arounds that will constitute new vulnerabilities (Alter, 2013; Alter, 2017). The weakest link is not necessarily to be found in the technical system, but in the difference between the formal model of usage and patterns of real usage of system and content (data) in a purposeful activity system. Consequently, designers have to find a balance between security, performance and usability (Sommerville, 2011) by involving professionals in shaping system and security requirements holistically. IT specialists should also continue to work on security methods that minimize inconvenience and delays (Oz and Jones, 2008) that could encourage deviation from desired security practice.

Another important issue is related to the implementation of a security policy. This is expected to change organisational procedures and to shape and monitor the behavior of employees, through

education and training for compliance. However, documented requirements and general training campaigns may have a minimal effect on user behavior and awareness in practice (Parsons et al., 2014; Bada, Sasse and Nurse, 2015). In the study by Sadok and Bednar (2016), many subjects indicated that they had received appropriate training and yet, when asked whether their job roles involved consideration of security, answered in the negative. This is in spite of the fact that, for instance, breaches of the General Data Protection Regulations can and do lead to individual prosecution (Information Commissioner, 2017).

Having considered the deficiencies that may arise in relation to information systems security practice, and some possible causes of these vulnerabilities, we now go on to consider how socio-technical perspectives may provide a way forward.

Socio-technical approaches

The socio-technical systems approach to work design has its origins in work by the Tavistock Institute for Human Relations in the period immediately after the Second World War. Emery and Trist (Trist, et al, 1997) believed that social sciences could be harnessed to influence the ways in which new technologies were harnessed in order to bring about radical improvements in working lives. The guiding values of these endeavours were a desire to improve job design and create safer, more humane systems, as well as promoting democracy in both workplaces and society more generally. They considered that a work system should be seen as a set of activities coming together to form an integrated whole, as opposed to a collection of separate tasks, i.e. an open system, interacting with an environment that influences its behaviour (Emery, 2000). Through Action Research projects in industry, and working with Systems Thinking (Ackoff and Emery, 1972) a set of principles for socio-technical design were developed (Cerns, 1976).

These principles, and their implications for security professionals, are represented in Figure 1 and also set out in Table 1. An overriding theme is that analysis, preparation and implementation of a socio-technical design is the property of no individual or set of individuals; it belongs to the members of the organization whose working lives are to be designed. Thus, also, development of security

policies and measures must be considered a socio-technical issue, to be addressed in all areas and at all levels in an organization.

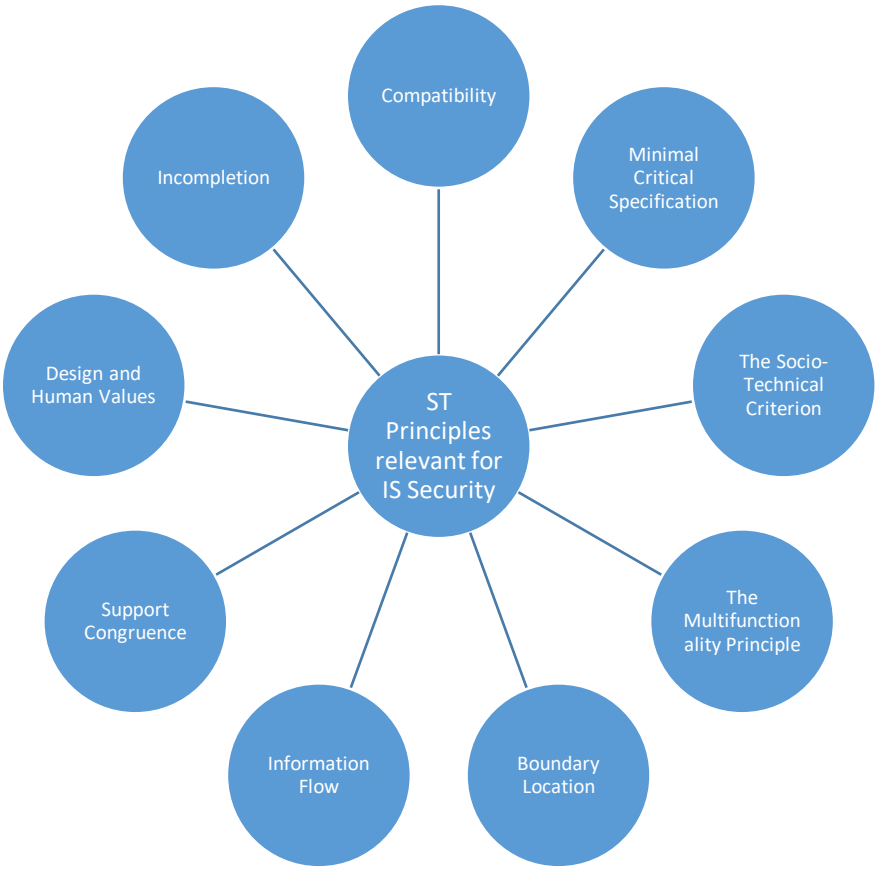

Figure 1: Principles for Socio-technical Design relevant for IS Security

Since the early years of the socio-technical movement, it has been widely recognised that capability is embedded in people (Nonaka, 1991; Davenport and Prusak, 2000), and it follows that an effective work system will be designed as a socio-technical whole, in which available technologies are considered in the light of the desires of those who will use them (Mohr and van Amelsvoort, 2016).

Table 1: Principles of Socio-technical Design (adapted from Cerns, 1976).

Socio-technical Principle	**Description**	**Relationship to IS Security**
Compatibility	The process of design must be compatible with the objectives to be achieved.	IS design processes must incorporate consideration of security in all stages and iterations.

Minimal Critical Specification	The essential aspects of the design must first be established but only those aspects that are absolutely necessary must be prescribed.	It is expected that systems will (co)evolve and change through use by engaged actors. Security must continue to be an on-going consideration.
The Socio-Technical Criterion	Variances, i.e. any unprogrammed event that can affect the outcome from the system, must be controlled as near their point of origin as possible. 'Management' is concerned with control of variances but too often is reactive – dealing with consequences of variance, rather than prevention.	This suggests that security matters should be considered by all staff members, and receive continuous attention from those with relevant contextual knowledge of the system, including managers, in a pro-active manner.
The Multifunctionality Principle	As environmental demands vary, it is more adaptive and less wasteful to design multifunctional elements in a work system. By combining elements in different ways, the same functions can be performed in different ways. Thus, work systems can be designed to be flexible and resilient.	This requires that all staff should engage in security mindfulness from multiple perspectives, so that switching of functions does not facilitate breaches.
Boundary Location	Organizational boundaries are usually drawn to reflect one or more of three criteria (technology, territory and time). These tend to create barriers, interfering with sharing of knowledge and experience. In contrast, autonomous work groups can manage their own boundaries more effectively. Responsibility for co-ordination should therefore rest within such groups. Managers should be seen as a resource of such groups.	Clearly, the inception of autonomous workgroups, with fluid boundaries in working systems and power to define these for themselves, could lead to a loss of focus on security and scope for breaches to be facilitated. Security awareness development and training are therefore an essential consideration.
Information Flow	Data systems should be designed to deliver information to the first point at which action is required. Too often, technology is harnessed to please budget holders rather than people involved in work systems.	This principle facilitates good security practice because by encouraging its implementation in the context of actual work practice.
Support Congruence	Systems of social support should be designed so as to reinforce the behaviours that the organization structure is designed to elicit. An example would be reward systems. If group working is required, then individual incentives will be counterproductive. Systems of selection, training, conflict resolution, work measurement,	An engaged workforce, focused upon achievement of excellence and appropriately rewarded may well be the best asset any organization can have in endeavours to promote effective security culture.

	performance assessment, timekeeping, leave allocation, promotion and separation can all reinforce or contradict the behaviours which are desired.	
Design and Human Values	The objective of organizational design should be to provide a high quality of work for participants, e.g. content should be reasonably demanding, work-based learning should be supported, and individuals should have a certain, minimal area of decision making of their own, together with appropriate support.	Employees who are motivated and enjoying job satisfaction are likely to identify with organizational ideals, which will include good security compliance.
Incompletion	Design is a reiterative process, in which closure of some options opens up new ones. As soon as design is implemented, its consequences will indicate the need for redesign, and the same multifunctional, multilevel and multidisciplinary approach needed for design is needed for evaluation, review and redesign.	This principle emphasises a need to take an iterative perspective. All security policies and measures are by their nature contingent. Change in organizational systems and environments is endemic and must be continually matched.

One well-known methodology based on ST principles is ETHICS (Mumford, 2006). The acronym stands for Effective Technical and Human Implementation of Computer-based Systems. This was developed through interaction of theory with practice in action research projects. Mumford and Wear (1979) detail nine such projects, ranging from work in Liverpool docks and the British coal industry to problems experienced in a bank and in senior management decision-making systems. What was clear from these interventions was the importance of participation by all those having an interest in the qualities of a resultant design, and a need to avoid separation of technical and social dimensions –these cannot simply be 'aligned' but are integral and indivisible from each other. During her lifetime, Mumford continued to develop her socio-technical thinking (Mumford, 2006). She recognized a need to develop methodologies that could support a holistic perspective and also address the impetus of change in all organizational systems (Mumford and Beekman, 1994). Others, such as Baxter and Sommerville (2011) and Bednar (2018) have taken up the challenge left by Mumford to carry this work forward. The next section contains examples showing the importance of socio-technical perspectives in management thinking.

Illustrating the need for a socio-technical approach

Mohr (2016) discusses the nature of High Performance Organizations (HPO) and the requirements for their design. An HPO is one which achieves both human and business goals to a great extent, and is able to show resilience to disturbances by adapting to changing requirements with minimal disruption or cost. In an HPO, the culture of the organization, its vision for the future and its supporting structures are all aligned, so that the energy for high performance comes from self-generated, individual commitment. Mohr contends that such organizations require an open, socio-technical systems approach to design. Mohr cites an example highlighted by Pava (1983).

The General Motors (GM) plant at Fordstown, in USA, was one of the most technologically advanced automotive plants in the world at the time. It was designed on Taylorist principles, for maximum efficiency. However, poor job conditions led to a strike. Over-optimisation of technical systems, and under-development of social systems by comparison, led to a watershed for GM management. It was recognised that there was a need to move away from traditional approaches to system design. It could be seen that technical systems analysis was focused upon steps, tasks and processes, measurement of variances and means by which these should be addressed. Social systems analysis, on the other hand, was focused on interactions among people, how co-ordination was to be achieved, and how staff were to be motivated. If these analyses are carried out separately, even if they are simultaneous, it seems unlikely that the results can be combined into one, homogenous and effective design in which all factors are optimal (Pava, 1983). This well-publicised case led to change in American management thinking, away from reliance on Taylorism. Commenting upon this case, Pava suggested that an approach called the North American Open Sociotechnical System (NAOSS) could address this issue. This approach combined theory with detailed procedure for design so that variances could be addressed as close to their source as possible, and operations could be set up on the basis of meaningful work tasks (as defined by employees). This would lead to situations in which people desired to carry out tasks, had the necessary capability to do so, and were permitted by the system to deliver the desired outcomes. Clearly, design of security would be included within such a collaborative approach.

Too often, in the past, struggling companies have focused on fixing operations affecting the bottom line first, postponing consideration of 'soft' issues until later, as they are seen as less crucial. Keller and Schaninger (2019) have disputed the wisdom of such a view. These authors argue that more effective organizational design results when both 'hard' and 'soft' issues are tackled at the same time and with equal emphasis, in a co-ordinated effort. To support this view, they cite experience at the CocaCola Company (Beasley and Isdell, 2011). In the early years of the 21st century, CocaCola suffered a downturn in shareholder value to -26%. During the same period, their greatest rivals, Pepsi, experienced an increase to 46%. A new CEO was appointed, who found that his predecessor had made great efforts to turn things around through brand development, creation of adjacent businesses and building of a corporate 'wellness' programme. All of this had been to no avail. The incoming CEO launched a new manifesto for growth. This set out the company's vision, how it was proposed to pursue these goals and how people would work together more effectively. Crucially, this manifesto was developed collaboratively. A team of 150 top managers wrote it up, following collaboration among 400 of their colleagues, who collaborated in turn with their teams. This meant that the implementation of new strategies were widely 'owned' among company employees. Performance improved markedly in the period that followed. Furthermore, there was a 25% reduction in staff turnover, and employee engagement improved to an unprecedented degree. Reflecting upon this, and other examples, Keller and Schaninger developed a five frame performance-and-health methodology that might be used as a guide to tackling large-scale change (see Table 2).

Aspire	Where do we want to go?
Assess	How ready are we to go?
Architect	What must we do to get there?
Act	How do we manage the journey?
Advance	How do we continue to improve?

Table 2: Five frames of performance and health – top level (Keller and Schaninger, 2019).

Each of these frames is considered in collaborative inquiry, in turn. Participants know when to move on to the next phase when they have answered the question posed. This will be an iterative process. Evidently, consideration of security will form one of the issues for work in each stage.

A further example of the need for socio-technical approaches can be found in the rise of applications of Artificial Intelligence (AI). It has often been suggested that one of the benefits in using AI is the removal of human bias from decision-making. However, it can easily be seen that the algorithms underpinning AI can lead to bias being 'baked in' if there is insufficient critical scrutiny of algorithm design; or if there is inherent bias in data that AI applications draw upon or the methods by which this is gathered and processed. Silberg and Maryilea (2019) suggest that two opportunities present themselves. The first is to use AI to identify and reduce the impact of human bias. The second is the opportunity to improve AI systems, how they leverage data, and how they are developed and deployed to prevent them from perpetuating human and societal biases. The need to take up the second of these opportunities is highlighted by recent inquiry into the impacts of data derived from social media. Organizations such as Cambridge Analytica have been able to take bodies of anonymised data from social media interactions, find patterns in that data, and make targeted interventions via those media that have arguably impacted negatively upon democratic processes in the USA and elsewhere (Naughton, 2018). This clearly shows the indestructible link between technological and social factors that means they must be tackled holistically. Human imagination must be exercised to consider what unintended consequences can arise from use of AI, what their impact might be and how to prevent and combat them.

Discussion

All of the examples above have highlighted wide recognition that systems development is a socio-technical matter, and that it is neither desirable nor advisable to attempt to separate social and technical strands. What is needed is a range of available methodologies, tools and techniques to support socio-technical design. It can be seen that all of the above examples are relevant for Information Systems security professionals to consider. Staff who are engaged and motivated, and

who take ownership of the objectives of their employing organization, will also be likely to be watchful and co-operative in protecting its interests through appropriate security measures. Their collaboration in design, using their contextual knowledge, is likely to lead to more effective security design. Consideration of socio-technical factors is vital in design of all systems, even those whose foundation is highly technical, such as application of AI. Engagement with staff, customers and wider society is necessary to design of systems that are safe and secure in use.

However, despite wide recognition that socio-technical design improves both productivity and quality of work, it has not gained prominence among the available approaches to development. Baxter and Sommerville (2011) argue that this is due to a number of factors. The desire to create more humane systems that underpinned the original research may be seen by some as naïve in a business context. However, the main problem may relate to lack of tools to carry socio-technical design principles into effect, or a perception among designers trained in more reductionist approaches that such methodologies are difficult and time-consuming to implement. There is clearly a need for more work in this area to bring a much-needed, socio-technical lens to issues of IS development and security for the future, with an appropriate armoury of methodologies, tools and techniques (Sarker, et al, 2019).

Education in socio-technical methods must be a priority, particularly for those concerned with information security. As the impact of artificial intelligence, robotics and cobotics in industry are realised, and separation between human and technological elements of work systems becomes ever less practical, it is likely that designers will increasingly turn to socio-technical methodologies (Moulières-Seban, Bitonneau, Salotti, Thibault and Claverie, 2017).

Conclusions

Research clearly shows that cyber-enabled industrial espionage is a growing problem. The volume and complexity of modern data systems, the inter-dependencies of work systems based in both human and artificial intelligence, and the pace of technological change, combine to make it difficult for designers to comprehend and anticipate all possible vulnerabilities and threats. It is clear that

insiders within organizations provide the weakest link in security measures, whether through choice to engage in nefarious practices or through inadvertent activities that facilitate a breach. Deliberate espionage by outsiders is known to focus on weaknesses in corporate security practice, and poorly-designed work systems that facilitate unauthorised access.

Concerns about espionage may also raise new issues of privacy and stress for employees. The temptation may be great for managers to introduce oppressive measures in the name of enhanced security, such as close surveillance and monitoring of performance; listening in to voice mail; searching of emails and computer files. Such measures are likely to be counterproductive in practice – any short-term gains in enhanced security will be off-set by destruction of trust, creativity and engagement with the culture and values of the business.

Attempts by legislators to address espionage through regulatory frameworks have suffered from difficulties in interpretation and application of rules, as well as difficulties with detection and reporting. While there have been successful prosecutions of individuals in relation to data breaches that resulted in financial gain, many organizations would be reluctant to report their own vulnerabilities for fear of reputational damage. Smaller organizations may lack the expertise or resources to mount a forensic investigation of vulnerability or breach.

Organizations would benefit from a two-way approach to information systems security: good system design and management practice to minimise vulnerability, coupled with appropriate detection and regulatory measures. Organizations of all sizes, and SMEs in particular, may benefit from adopting a socio-technical perspective. Such approaches can incorporate effective design of work systems to streamline risk management processes, involve relevant stakeholders in operational cyber-risk mitigation and promote a culture of security awareness. Training programmes can be designed and delivered to relate to actual, professional practice so as to be meaningful to stakeholders. Engagement and participation by professionals is needed to promote design of systems that are not only user-friendly, but genuinely supportive of meaningful use in context. Principles for good socio-technical design should be considered at all stages and levels, whenever desirable change is contemplated. Malleability should be built into systems so that they are adaptable in use without introducing

unanticipated weaknesses. In this way, professionals will be supported to carry out their roles without needing to by-pass procedures or develop work-arounds.

Clearly, appropriate tools and techniques for socio-technical design of secure systems will be needed. This highlights a requirement for continuing research into this crucial field.

References

Ackoff, R. L., & Emery, F.E. (1972). *On Purposeful Systems*, London, Tavistock.

Albrechtsen, E. and Hovden, J. (2010), "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study", *Computers & Security*, Vol. 29, pp 432-445.

Alotaibi, M., Furnell, S., & Clarke, N. (2016, December). Information security policies: a review of challenges and influencing factors. In 2016 *11th International Conference for Internet Technology and Secured Transactions* (ICITST) (pp. 352-358). IEEE.

Alter, S. (2017). Six Work System Lenses for Describing, Analyzing, or Evaluating Important Aspects of IS Security. *International Journal of Systems and Society (IJSS), 4*(2), 69-82.

Alter, S. (2013). Work system theory: overview of core concepts, extensions, and challenges for the future. *Journal of the Association for Information Systems*, 14(2),72-121.

Bada, M., Sasse, A. M., & Nurse, J. R. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? *Working Papers of the Sustainable Society Network Vol. 3, First International Conference on Cyber Security for Sustainable Society 2015, Coventry University, 26-27 February 2015*, 118-132. arXiv preprint arXiv:1901.02672.

Baron, R & Pigeon, M. (2017). *Adapting the EU Directive on Trade Secrets 'Protection' into National Law: A transposition guide for legislators and civil society organisations*. Brussels: Corporate Europe Observatory, February 2017.

Baskerville, R. (1991) Risk analysis: an interpretive feasibility tool in justifying information systems security. European Journal of Information Systems, 1, 121–130.

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers*, 23(1), 4-17.

Beadnar, PM (2018) The socio-technical toolbox. Portsmouth Craneswater Press.

Bednar, P.M. and Katos, V. (2009). Addressing the human factor in information systems security. MCIS2009. In Poulymenakou, A., Pouloudi, N., Pramatari, K. (eds), *Proceedings of 4th Mediterranean Conference on Information Systems*, Athens, Greece, September 25-27. pp. 900-912.

Bednar, P.M. and Welch, C. (2009). Inquiry into Informing Systems: critical systemic thinking in practice, Chapter 14 in G. Gill, editor, *Foundations of Informing Science*. Santa Rosa, California: Informing Science Press.

Bissell, K., Lasalle, R.M. and Dal Chin, P (2019). Ninth Annual Cost of Cybercrime Study, Accenture and the Ponemon Institute, accessed 16 July 2019 at https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

Cabinet Office/Detica (2011). The Costs of Cybercrime: A Detica report in Partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office, accessed 16 July 2019 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf.

Carl, S. (2017). An unacknowledged crisis – economic and industrial espionage in Europe. *Essays in Honour of Nestor Courakis*, pp 1316-1326. Athens: Ant. N. Sakkoulas Publications L.P. 2017.

Checkland, P. and Holwell, S. (1998). *Information, Systems and Information Systems: making sense of the field*. Chichester: J Wiley & Sons.

Cherns, A. (1976). Principles of Socio-technical Design. Human Relations, 29(8), 783-792.

CPNI (2013). Insider Threat Data Collection Study: Report of Main Findings. Retrieved from https://www.cpni.gov.uk/.../insider-data-collection-study-report-of-main-findings.pdf

CSIS (2018). Economic Impact of cyber Crime –No Slowing Down. p17. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

Davenport, T. H. & Prusak, L. (2000*). Working knowledge: How organizations manage what they know.* Boston, MA: Harvard Business School Press.

Dhillon, G. and Torkzadeh, G. (2006) "Value-focused assessment of information system security in organizations", Information Systems Journal, Vol. 16, pp 293-314.

Dhillon G., Oliveira T., Susarapu S., Caldeira M. (2016) Deciding between information security and usability: Developing value based objectives *Computers in Human Behavior*, 61, 656-666.

Emery, M. (2000). The Current Version of Emery's Open Systems Theory. *Systemic Practice and Action Research*, 13(5), 623-643.

Furnell S. (2016) "The usability of security – revisited", Computer Fraud & Security, September, 5-11.

Global Economic Crime Survey (2016). Adjusting the Lens on Economic Crime. Retrieved from https://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf

Information Commissioner (2017). Warning for workers after charity employee is prosecuted for data protection offences. *ICO News 8 November 2017*. Accessed 26 April 2019 at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/11/warning-for-workers-after-charity-employee-is-prosecuted-for-data-protection-offences/.

IP Commission (2017). The Theft Of American Intellectual Property: Reassessments Of The Challenge And United States Policy. The National Bureau of Asian Research. Retrieved from http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf

Keller, S. and Schaninger, B. (2019). A better way to lead large-scale change. *McKinsey & Company*, accessed 30 June 2019 at https://www.mckinsey.com/business-functions/organization/our-insights/a-better-way-to-lead-large-scale-change.

Koppel, R., Smith, S., Blythe, J. and Kothari, V. (2015), "Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient?", Studies in Health Technology and Informatics, Vol. 280, pp. 251-220.

Kolkowska, E., and Dhillon, G. (2013), "Organizational power and information security rule compliance", *Computers & Security*, Vol. 33, pp. 3-11.

Lesca, H. and Lesca, N. (2011). *Weak Signals for Strategic Intelligence: Anticipation Tool for Managers*. Chichester: J. Wiley & Sons.

Mohr, B.J. (2016). Creating High-Performing Organizations: The North American Open Socio-technical systems Design Approach. Chapter 2 in B.J. Mohr and P. van Amelsvoort (editors), *Co-creating Humane and Innovative Organizations: Evolutions in the Practice of Socio-Technical System Design*. Portland: ME, Global STS-D Network Press.

Mohr, B.J., & van Amelsvoort, P. (editors) (2016). *Co-Creating Humane and Innovative Organizations Evolutions in the Practice of Socio-technical System Design*. Portland, ME: Global STS-D Network Press.

Moulières-Seban, T., Bitonneau, D., Salotti, J. M., Thibault, J. F., & Claverie, B. (2017). Human Factors Issues for the Design of a Cobotic System. In *Advances in Human Factors in Robots and Unmanned Systems* (pp. 375-385). Springer, Cham.

Mumford, E. (2006). The story of socio-technical design: reflections on its successes, failures and potential. *Information Systems Journal*, 16(1), 317-342.

Mumford, E., & Beekman, G. J. (1994). *Tools for change & progress: a socio-technical approach to business process re-engineering*. Leiden: CSG Publications.

Mumford, E. and Weir, M. (1979). *Computer systems in work design – the ETHICS method*. NY: John Wiley.

Naughton, J. (2018). How Facebook got into a mess – and why it can't get out of it. *The Observer*, 28 April 2018, accessed on-line 30 June 2019 at https://www.theguardian.com/technology/2018/apr/07/facebookgot-into-mess-cant-get-out-of-it-mark-zuckerberg-surveillance-capitalism.

Nissen, H-E (2002). Challenging Traditions of Inquiry in Software Practice, Chapter 4 in Y. Dittrich, C. Floyd and R. Klischewski, editors, *Social Thinking – Software Practice*. Cambridge Mass: MIT Press.

Nonaka, I. (1991), The Knowledge Creating Company, *Harvard Business Review*, 69 Nov-Dec 1991.

Oz, E., & Jones, A. (2008), Management information systems, Cengage Learning EMEA, London, ISBN: 978-1-84480-758-1.

Parsons K., McCormac, A., Butavicius, M., Pattinson, M., and Jerram, C. (2014), "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)", Computers & Security, Vol. 42, pp 165-176.

Pava, C.H.P. (1983). Designing Managerial and Professional Work for High Performance: a Socio-technical Approach. *National Productivity Review*, 2(2), 126-35.

Sadok, M., & Bednar, P. M. (2016). Information Security Management in SMEs: Beyond the IT Challenges. In Proceedings of International Symposium on Human Aspects of Information Security & Assurance, Frankfurt, Germany, July 19-21, 2016, pp. 209-219.

Sarker, S., Chatterjee, S., Xiao, X., & Elbanna, A. (2019). The Sociotechnical "Axis Of Cohesion" for the IS Discipline: its Historical Legacy and its Continued Relevance, *MISQ* (forthcoming).

Shedden P., Scheepers R., Smith W., Ahmad A. (2011), "Incorporating a knowledge perspective into security risk assessments", *VINE Journal Information Knowledge Management System*, Vol. 41, No. 2, pp 152-166.

Silberg, J. and Maryilka, J. (2019). Tackling bias in artificial intelligence (and in humans). *McKinsey Global Institute*, accessed 27 April 2019 at https://www.mckinsey.com/featured-insights/artificial-intelligence/tackling-bias-in-artificial-intelligence-and-in-humans.

Siponen, M. and Willison, R. (2009), "Information security management standards: Problems and solutions", *Information & Management*, Vol. 46, pp. 267-270.

Sommerville, I. (2011), *Software engineering*, Pearson Education Inc, ISBN: 978-0-13-705346-9.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), 215-225.

Spears, J. L. and Barki, H. (2010), "User participation in information systems security risk management", *MIS Quarterly*, Vol. 34 No. 3, pp. 503-522.

Stahl, B. C., Doherty, N. F. and Shaw, M. (2012), "Information security policies in the UK healthcare sector: a critical evaluation", *Information Systems Journal*, Vol. 22, pp. 77-94.

Symantec Internet Security Threat Report 20. (2015). Accessed 16 July 2019 at https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf.

The Global State of Information Security Survey (2016) "Managing cyber risks in an interconnected world", www.pwc.com/gsiss2015

Trist, E., Murray, H. and Emery, F. (1997).*The Social Engagement of Social Science: A Tavistock Anthology : The Socio-Ecological Perspective (Tavistock Anthology)*, University of Pennsylvania, accessed 26 April 2019 at http://www.moderntimesworkplace.com/archives/ericsess/sessvol1/sessvol1.html.

Verizon Data Breach Investigation Report (2018). Accessed 16 July 2019 at https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf.

Wright, P.C., & Roy, G. (1999). Industrial espionage and competitive intelligence: one you do; one you do not. *Journal of Workplace Learning*, 11(2), pp.53-59.