Pragmatic Security: Modelling IT Security Management Responsibilities for SME Archetypes

Simon Parkin
University College London
United Kingdom
W1CE 6BT
s.parkin@ucl.ac.uk

Andrew Fielder
Imperial College London
United Kingdom
SW7 2AZ
andrew.fielder@imperial.ac.uk

Alex Ashby
University of Oxford
United Kingdom
OX1 3QD
alexander.ashby@stcatz.ox.ac.uk

ABSTRACT

Here we model the indirect costs of deploying security controls in small-to-medium enterprises (SMEs) to manage cyber threats. SMEs may not have the in-house skills and collective capacity to operate controls efficiently, resulting in inadvertent data leakage and exposure to compromise. Aside from financial costs, attempts to maintain security can impact morale, system performance, and retraining requirements, which are modelled here. Managing the overall complexity and effectiveness of an SME's security controls has the potential to reduce unintended leakage. The UK Cyber Essentials Scheme informs basic control definitions, and Available Responsibility Budget (ARB) is modelled to understand how controls can be prioritised for both security and usability. Human factors of security and practical experience of security management for SMEs inform the modelling of deployment challenges across a set of SME archetypes differing in size, complexity, and use of IT. Simple combinations of controls are matched to archetypes, balancing capabilities to protect data assets with the effort demands placed upon employees. Experiments indicate that two-factor authentication can be readily adopted by many SMEs and their employees to protect core assets, followed by correct access privileges and anti-malware software. Service and technology providers emerge as playing an important role in improving access to usable security controls for SMEs.

CCS Concepts

•**Security and privacy** → **Formal security models;** *Economics of security and privacy; Usability in security and privacy;*

Keywords

SME Security; Cyber Essentials; Security Effort

MIST'16, October 28 2016, Vienna, Austria
© 2016 ACM. ISBN 978-1-4503-4571-2/16/10...$15.00
DOI: http://dx.doi.org/10.1145/2995959.2995967

1. INTRODUCTION

99% of UK businesses are Small-to-Medium Enterprises (SMEs) with 250 or fewer employees, where 95% are micro-businesses with fewer than ten employees [32]. The picture is similar across the European Union [13] and the US [10]. These small companies use IT in different ways [23], and may lack the appropriate skills to manage IT security [12]. The role of service providers and IT manufacturers is critical: SMEs may use leased services and premises over which they have no control and little oversight, otherwise relying on security controls intended for the home market rather than corporate solutions [27]. Here we consider how these conditions contribute to insider vulnerabilities which must be managed to limit data leakage and exploitation by external attackers.

For security controls to be used effectively in smaller companies, they must be cost-effective but also make reasonable demands on staff time and effort [20]. Adoption of user-centric security controls in SMEs has the potential to remove some of the barriers to effective management of related risks [27].

In 2014 the UK government published the Cyber Essentials Scheme [19] (referred to here as CES), as a guide to basic protection of businesses from cyber threats. Here we build on prior models of security investment costs for CES controls [14], to consider the *indirect costs* of controls for staff for achieving a *baseline* level of security coverage to limit the potential for data leakage.

Here indirect costs are modelled to determine: (i) whether there are specific security controls which offer the best protection for limited available manpower, and (ii) if the impacts of control usability can identify current or potential controls for limiting unintended or malicious information leakage. Low-tech attacks are one of the means by which malicious insiders can compromise an organisation [34]; conversely, complex and highly-specialised user-facing controls may overwhelm general users, resulting in them being used incorrectly.

The model described here is informed in two ways: firstly, we characterise the usability costs and knowledge demands of basic security controls through examination of related literature in the human factors of security. CES controls may differ in the time required for implementation and maintenance [20]; employees may be unable to operate security controls generally if their use is not clear or approaches being impossible [24]; cumulative security effort can risk increased security costs for the organisation as well as heightened risks of information compromise [3], and; stressful workplace conditions and cognitive overload can increase employee vulnerability to social engineering attacks [16].

Secondly, we relate operation of security controls to the potentially diverse needs of SMEs. A representative set of SME *archetypes* is modelled, differing in size and use of security in daily activities. These archetypes leverage the experience of a collaborating provider of IT and security services to SMEs, with dozens of customers ranging in 1-250 employees across various sectors. This informs the modelling of SME activities relating to use of and access to data, technology restrictions, and how modelled data leakage scenarios can impact each SME archetype. The model is intended as a framework for examining the management of security controls by assumed non-experts in diverse, resource-constrained SMEs. A goal of the model is to motivate focused collection of real data about the experiences of SMEs in staying secure and preventing data leakage.

Section 2 describes Related Work. Section 3 outlines the Background to the work, using the CES as a framework. Section 4 describes our modelling approach, where Section 5 describes specific archetypes, controls, and associated indirect costs which appear in the model. Results are found in Section 6, with Analysis in Section 7. Concluding remarks and future work are in Section 8.

2. RELATED WORK

A number of works model security investment alongside the capacity of controls to mitigate threats, with an emphasis on the cost of controls and their effectiveness in mitigating specific vulnerabilities. Viduto et al. [38] provide a model of cyber security investment, where a defender seeks an optimal defensive strategy for a limited budget. The authors consider that controls not only mitigate system vulnerabilities but can also exacerbate or introduce vulnerabilities, which may obscure the capacity to prevent data leakage. A similar approach is defined by Gupta et al. [17], where this challenge is represented as a set cover problem, seeking to match available security technologies to potential vulnerabilities.

Rees et al. [31] describe an investment model which accommodates the uncertainty as to the number and types of attacks against a particular system. The same authors explore scenarios and attacks to identify the impact of a worst case scenario [29], where preferred solutions are those that minimise the spread of risk between the expected case and worst case. Likewise, Sawik [33] considers uncertainty in security decision-making in terms of risk appetite, where the decision maker is able to make trade-offs based on budget, risk and confidence level.

Beautement et al. [4] model employee use of USB storage devices across various locations (and related risk profiles), and the impact of these behaviours upon confidentiality and availability. The model design is informed by interviews with employees in an organisation. A balance is considered between training, monitoring, and IT support costs, indicating constraints on available security budget and a need to provide employees with timely support and skills development. Employees in the model trade off security with successful data transfers and the potential for negative support experiences – bad experiences with security can promote behaviours which involve insecure treatment of data. Similarly, Shay et al. [35] model user interactions with password policy and helpdesk support in organisations. Benign and malicious users are modelled as part of the same system; where problems memorising a password can result in insecure practices (such as writing the password down on an insecure note), increasing the risk of compromise local to the user. In the model, both password complexity and limiting of workarounds reduce the likelihood of compromise, where overloading users has negative consequences.

In summary, prior models have considered the effectiveness of controls and the inter-dependencies between user behaviour and organisational security. Here we model how the usability of controls can impact the capacity for a group of individuals within a small organisation to collectively manage their own security and limit data leakage. Our model considers how best to limit demands upon available manpower while also limiting vulnerability to attacks. Effective and usable controls bring with them less disruption to – and distraction from – the productive tasks that sustain the business, where controls with these qualities have the potential to limit vulnerability to insider attacks [16, 39].

3. BACKGROUND

3.1 The Cyber Essentials Scheme

We use the Cyber Essentials Scheme (CES) [19] as a framework for basic cyber-security protections. The CES is aimed at organisations large and small, identifying organisational controls to address basic online cyber threats, specifically *Phishing attacks* and *Hacking attacks*:

- **Boundary Firewalls and Internet Gateways.** Manage firewall connection rules and removing unapproved or vulnerable services.
- **Secure Configuration.** Limit vulnerabilities and enable only those services necessary to the business. Change default settings or credentials, remove unnecessary accounts and software, and manage personal firewalls (mirrored elsewhere in insider threat advice for managing remote connections [34]).
- **Access Control.** Manage user accounts on applications, computers and networks, principally by the principle of least privilege (correlating with insider threat advice for limiting internal access [34]). Implement strong password authentication.
- **Malware Protection.** Operate up-to-date malware protection software to protect against malicious emails, compromised website, or unknown malicious files. Prevent access to malicious websites.
- **Patch Management.** Apply the latest security patches to computers and network devices in a timely fashion, and remove unsupported software.

The CES acknowledges that (i) larger organisations may already do much of what the scheme recommends, and that (ii) smaller organisations may be restricted in what they can achieve on their own, requiring guidance and support from others.

The CES accommodates the implementation of alternative controls if a particular control is deemed impractical. These basic controls for instance protect against basic cybersecurity threats but do not directly address theft or fraud involving computers [20]. Here we begin to explore the capacity for small combinations of controls – including the basic control types outlined in CES – to provide a baseline level of security coverage with minimal effort demands.

3.2 End-user costs of security controls

SMEs can lack security expertise or an identifiable IT expert in their company to resolve issues [27]. Security management responsibilities may not be assigned to any one individual [12]. Well-intentioned employees in SMEs are concerned about their own level of computer security knowledge, and may make efforts to implement security controls despite being inadequately prepared. These efforts may empower an effective balance of security and productivity, but equally can introduce further vulnerabilities [25]. In terms of insider security threats, Wall [39] couches IT insider threats in the realm of criminology, where we primarily consider those employees who would be referred to as a 'well-meaning insider'. These employees may want to act securely, but at times might let security take second place to their primary productive tasks (their job). Here we explore the burden that security technologies place on users, as a factor in creating vulnerabilities when tensions with productivity arise.

As basic controls (such as those in the CES) may be identical for SMEs to those available for use in home environments [27], challenges faced by home and corporate users alike are of interest:

- **Boundary Firewalls and Gateways.** Ho et al. [21] found that amongst home wireless networks in residential areas most access points used encryption, but that the capabilities of networked devices determined the strength of encryption in use. Decisions made by manufacturers heavily influenced the use and type of encryption, where users would rely on default settings.

- **Secure Configuration.** Those with little security expertise may be unaware of a personal firewall on their machine [30], relying on default configurations. If prompts from a firewall cannot be readily understood they may be ignored, where users can otherwise find it difficult to make informed decisions. Creating and recalling complex passwords is a demanding task [3], where a person may manage many passwords. Basic protection against computer viruses can have a high entry cost – an underdeveloped understanding of how they create harm can mean that anti-virus software is not used [40].

- **Access Control.** Corporate access control systems can suffer from restrictive policies and over-entitlements [2]. Having more than one person managing an access control policy makes it difficult to maintain oversight when changes are made, and to keep abreast of exceptions [5]. Experience with access control does not always translate into skillful management [41].

- **Malware Protection.** Users can suffer from 'warning fatigue' [1], resulting in warnings – and any decisions required in response – being ignored. Phishing advice undergoes regular revision, requiring users to learn ever more rules [18]. Users can have difficulty in understanding what web scripts are and how they work (malicious or not) [40]. Malicious activity may not then be noticeable to end-users.

- **Patch Management.** Individuals may differ greatly in whether they are willing to disrupt their primary task to install software patches (including requiring a restart of a computer) [37], where a person's perception of the configuration may differ from reality.

There is a potentially strong interdependence between risk awareness and security affect [6], where existing skills and knowledge are critical to the adoption of IT in SMEs [23]. With a focus foremost on limiting unintended data leakage, it can be noted that SME employees need to be able to learn how to use IT and adapt it to their practices [8]. Resistance to change can happen if staff requirements are not considered in the specification of technologies intended for use as part of work activities. If security controls are difficult to comply with, make excessive demands on well-meaning employees, or are deployed without clear relevance to business processes, employees may use *workarounds* to modify or circumvent controls in a way that weakens security [24]. Burdensome security then contributes to the indirect costs of deployment and the continued maintenance of controls.

For SMEs, protection against basic cyber-security threats brings with it the responsibility for employees to collectively manage security controls, and with that the time and skills necessary to use controls efficiently without causing disruptions. If controls are burdensome and require a lot of specialised expertise to use, they can distract from productive tasks. Conversely, where the time and skills necessary to effectively operate controls is not available within the workforce of an SME, a sub-optimal level of protection can persist.

4. METHODOLOGY

4.1 Modelling security investment

Security controls are modelled as single actionable activities that an organisation undertakes to address risks to their IT systems. Activities can produce benefits to security but also have direct and indirect costs. The financial burden of controls is well understood, but *indirect costs* are not widely modelled in cyber-security decision-making; deploying a control can require changes to staff behaviour or otherwise impact upon the capacity to operate IT systems effectively.

The approach of modelling both direct (financial) and indirect costs for cyber security investment is explored by Fielder et al. [14]. This (and other work [36]) demonstrate that controls advocated by the CES can provide effective coverage when implemented correctly and properly maintained. The case study in [14] makes limited consideration of indirect costs, where here we aim to develop understanding of the indirect impact of security upon members of smaller organisations, where there is limited available manpower and expertise (Section 4.2).

Networked environments with fixed workstation–server configurations are well understood [14, 27], where SME infrastructure may diverge from this template (as explored in Section 4.3). Specific attack vectors and mitigations may or may not be viable for the IT configuration of a particular SME. The model represents a single defender attempting to devise an optimal strategy for combining controls to defend their IT systems from a series of known attack methods; insiders may deliberately or inadvertently compromise a system based upon the controls that are put in place (where specific scenarios explore these and other issues in Section 5.5).

4.1.1 Targets and attacks

A target is an asset that an (internal or external) attacker is seeking to exploit via the network (for e.g., financial theft or to create a bot machine) and that the defender wishes to protect. The attacker in this case is indifferent to the method used to achieve their objective, and will use whichever method has the highest expectation of success.

The model describes a clear definition of each attack, in this work defined as a method and an outcome. We then measure the damage of a successful attack by the outcome, specifically what is compromised.

4.1.2 Controls

Defining an attack method allows us to identify countermeasure controls. Each control is an action available to the defender to reduce risks from a specific class of attack. Each control protects one or more targets in the system. The coverage a control provides is based on what that control does to defend a system. Each control has some level of efficiency for defending every target, such that the implementation of a control will lower the risk of damage from an attack of a given type by some amount. This will range from providing no protection – because the control does not defend against the attack at all – up to stopping nearly all variants of an attack class (bar genuinely novel variants). The latter means that any one control can approach but never reach 100% efficiency.

4.2 Modelling indirect end-user costs

Informed by the discussion in Section 3.2 and related modelling described in Section 4.1, an indirect cost can impact three areas:

- **Morale.** Users will altruistically exert security effort for the protection of the organisation. If security becomes burdensome, this effort becomes less efficient and more costly to the organisation [3].
- **System Performance.** If a control is deployed with little or no fit with business processes, it can become that much more difficult to use properly, or can disrupt other tasks [24].
- **Retraining.** User-facing controls may require specific skills, or the ability and time to make informed decisions at critical points in a security process. User training is important for reducing insider threats [34]. However, excessive training can in itself cause upset amongst employees if it appears irrelevant or takes time away from the work that employee pay and performance is measured by [3].

4.3 Modelling SME diversity – archetypes

A 'typical' SME network is difficult to define – here we differentiate SMEs by size, as this has been identified as a determinant of ICT adoption [23]. We also consider use of IT-based systems and services: some UK-based statistics for instance indicate that 88% of SMEs operate from a single site, with 37% of micro and 32% of SMEs overall operating from the owners home [9]. 8% of SMEs pay rates within their rent, which implies use of a serviced/shared office arrangement [15]; a further 4% are listed as mobile, that is without office or home, again implying the use of shared infrastructure. Informed by the partner IT services provider, we consider the most diverse SMEs, with particular focus on micro-companies:

- **Single-person companies (1 user).** Most SMEs lack a dedicated office or network infrastructure (as noted elsewhere [27]). There may be at least one computer containing company data, which can be a person's home computer. Cloud services may be used to store data and act as off-site backups.
- **Micro companies (2-9 users).** Newer companies will make almost exclusive use of cloud services for email and file-sharing, with a flat file-sharing policy allowing all users to access all files. Firewall and device configuration are either controlled by others or follow the provider's default configuration. Employees may use personal devices in the workplace, and not necessarily just for work purposes [36]. Single-person and micro-companies alike may make use of a small office or home network.
- **Small companies (10-50 users).** Networks are likely to be based around corporate user accounts and a single server for file-sharing and email. The company may have business applications running on database servers. PCs are mostly corporate-owned desktops. Wireless networks are nearly universal. Most will have a part-time internal IT staff member or outsourced IT support.

We define a template for an SME *archetype*, where each instantiated archetype may benefit most from a different set of controls. The diversity of SME network configurations has been considered elsewhere [27, 36], where here archetypes act as input to a model of security effort investment. Each archetype defines:

- **Size.** Single Person (SP), Micro (Mi), or Small (Sm).
- **Network Design.** The devices and services used by the SME. This identifies requirements for security controls and bounds the range of available controls.
- **Daily Interactions.** A range of daily or regular interactions that the SME and its employees have with IT systems, and which might be a source of potential weaknesses.

5. EXPERIMENTAL DESIGN

5.1 Experimental archetypes

For this work, we derive a set of SME *archetypes* to represent groups of SMEs with diverse needs. This range of archetypes allows us to explore whether a coarse distinction of 'big' and 'small' organisations is adequate enough to provide meaningful support for the control of an organisation's data. The archetypes described in Figure 1 and the Appendix serve as general cases, built on the experiences of a partner company with 10+ years of experience providing IT devices and services (including security) to SME customers of various sizes. This experience includes provisioning of computer systems, configuration of security software and management of secure communication between devices. In providing maintenance support to clients, service provision will also touch upon how an SME interacts with business partners. Each archetype may be seen across a range of industry sectors.

For each archetype, the kind of devices used are defined, as well as how those devices interact as a business network, where devices and their connections have been used to drive analysis of SME security coverage in other work [36]. Regular daily activities are also considered, as security controls must not block productive tasks or this may promote workarounds or result in sub-optimal use of security controls [24]. To be able to scope regular activities, we restrict to specific modes of working; Single Person companies as in Figure 1 can include lone consultants or contractors, for instance.

5.2 Targets and attacks

The targets modelled here – and associated attacks – are informed by Brian Krebs' analysis of the uses for hacked PCs [26]. This analysis catalogues the different uses an attacker may have for a machine or online account (the assets belonging to a person or organisation), and the compromise of these assets by generally automated – i.e., *basic* – commodity-style attacks (as per the CES). The catalogue has been informed by the author's interactions with companies of various sizes. Attacks modelled here fall into three categories: Malware, Phishing and Vulnerabilities. Malware attacks rely on components being installed on a device to perform a malicious action. Phishing acts to convince a user to wilfully provide credentials. Vulnerabilities in this model are considered to be any security flaw in technology which might be exploited.

The damage associated with a particular target ranges on a scale from 0 to 1000. A value of 0 represents an attack that would not be possible. A value of 1000 represents an attack that, if successful, would likely cause a significant financial loss assumed to cause the company to cease business.

5.3 Controls

Controls in this model build on the Cyber Essentials Scheme and a range of *alternative controls* (as per the scheme). A *variant* of each control may be implemented, as determined by the archetype it is applied to. For example, making exclusive use of a data-plan for Internet connections would not apply to an organisation that has a leased network.

For simplicity, we have taken a single control variant for each archetype that is representative of the archetype's capability. This allows us to more naturally model the control choices taken by the defender. Each control variant will operate at one of four different efficiency levels; *Complete* (0.95), *Partial* (0.5), *Incidental* (0.1) and *None* (0.0).

5.4 Indirect costs – responsibility budget

Security experts such as IT-security administrators must plan how time is allocated to security responsibilities [7]. Here we consider a security responsibility as a basic measure of the need to manage controls within an SME. An unwieldy control requires more time and effort to use effectively, as would controls which demand precise application of skills. A control that is deployed in an organisation is less effective if the workforce lacks the capacity and capability to manage it. Such shortcomings can be more of a critical factor for SMEs which may often lack support from a dedicated expert (see Section 3.2).

The consequences for data leakage of staff being overburdened by security controls are for instance explored in our model as a case of 'overload' (described in Section 5.5). Minimising cognitive overload has been suggested as a means to reduce susceptibility to social engineering attacks [16]. Other models of socio-technical systems have shown that there can be a close relationship between a potential victim being vulnerable and the courses of action that an attacker can then take to exploit them [11].

Each control brings a responsibility in the organisation to manage it, taken on collectively or individually. The capacity to manage controls is an organisation's Available Responsibility Budget (ARB). Each control variant has an indirect cost score which draws on ARB. A score is in the range of 0 to 4, where the highest value represents a significant impact on morale, retraining and system performance as a whole.

Indirect cost values are estimates based on factors identified both in related research (Section 3.2) and the (albeit limited) experiences of the partner IT services company in managing SME security. These include knowledge requirements for correct operation of a control, time and effort to maintain a control, and the capacity for a control to distract from or prohibit work tasks. Where a characteristic of a control variant clearly exhibits one of these traits – resulting in one or more of the impacts described in Section 4.2 – a 'point' of 1 is added to the control's indirect cost.

Security controls by their nature constrain use of IT systems and also need to be managed. A business running exclusively on a smartphone may leverage the device as a (near implicit) second authentication factor (score of 1), whereas a professional services company may provide staff with physical tokens which must be carried and would add extra effort (score of 2). To have staff maintain genuinely unique passwords for all corporate accounts is difficult to achieve [18] (hence a score of 4), whereas having separate password sets for work and personal accounts (score of 1) is pragmatic as attacks on the home environment are not then a route to valuable business assets.

We consciously model indirect costs as a single, limited scale. Values are subjective and informed by related security usability research (described in Section 3.2). A number of our case studies (Section 5.5) act as sensitivity analyses (e.g., Patching costs) to determine the impact of subjectivity upon the control combinations which emerge. The ultimate goal would be to directly measure the indirect cost of a control, where the analysis of security usability is presently capable of providing only some of this information. The ARB values associated with each control variant in the model are available at the URL listed in Section 5.5.

5.5 Controls – alternative cases

A range of alternative security deployment scenarios are modelled, exploring the impact of factors which restrict either the capacity to use specific controls effectively or the effort available in a company to manage security (and hence limit leakage of data):

- **Phone-only business.** Isolated use of phone data plan, with few distinct controls.

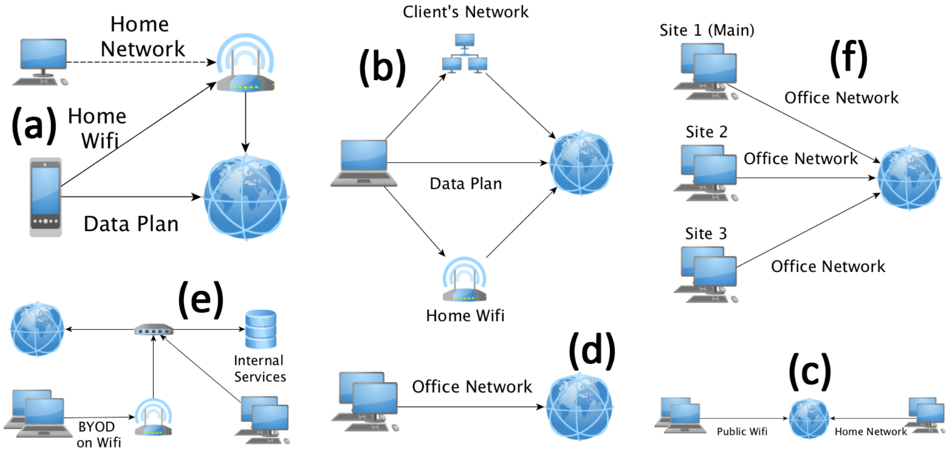

Figure 1: Network designs for archetypes: (a) Single Person, (b) Consultant, (c) Small Distributed Team, (d) Small Professional Services Team OR Single Site Public-Facing Business, (e) Medium Professional Services Team, (f) Multi-Site Public-Facing Business

- **No two-factor authentication.** Access (or not) to strong or innovative controls (given that SMEs may use off-the-shelf solutions).
- **Sensitive data.** A company whose data is regarded as being just as important as their finances, where data can be more difficult to track within the system [34].
- **Old system.** Aspects of the system are ill-suited to up-to-date controls; some SMEs may build systems gradually and maintain them over time.
- **Fake anti-virus.** Malicious entities may look to leverage any market for security controls, exploiting uninformed companies. This is analogous to an insider tampering with a security control through placement of malicious code [34].
- **Overload.** Explores the potential for controls to overwhelm an SME and its employees. The security responsibilities of employees pushed beyond their 'Compliance Budget' become generally harder to maintain [3].

Complete details of the data sets used for the experiments can be found at http://www.imperial.ac.uk/people/andrew.fielder/research.html. This includes control variants for each archetype, and the associated indirect cost scores.

5.6 Insider vulnerabilities

A number of the actions listed in the attack space would come about as a result of unintended mistakes by an insider. To identify if the distribution of residual risk after control implementation is as a result of accidental insider actions, the attack space has been divided amongst attacks that would impact the business from being an insider and those that would not. More specifically, attacks which exploit a software vulnerability or non-data extraditing malware (such as a zombie P.C. for Distributed Denial-of-Service attacks) are not considered an insider risk, as these are either the direct result of a hacking attempt or are deemed to result in no strategic loss for the company.

5.7 Solver

Optimal selection of controls can be viewed as a traditional knapsack problem. The defender aims to minimise expected damage to targets from attacks, by implementing a number of controls. The defender is constrained in their decision-making by the ARB of the system (see Section 5.5). Defence is further informed by the combined efficiency of all deployed controls, as a multiplicative reduction in expected damage. The optimisation can be represented as follows:

$$Min \frac{\sum_{i=0}^{T}(\prod_{j=0}^{C}(1-eff_{jk})d_i)}{T}$$

$$s.t. \sum_{j=0}^{C} c_{jk} < B$$

$$where, k \in \{0,1\} and, 0 <= eff <= 1$$

T is the set of targets, C is the set of controls, and B is the maximum ARB of the organisation. The damage for target i is given as d_i and eff_{jk} is the efficiency of control j when either implemented ($k = 1$) or not implemented ($k = 0$). The optimisation problem is implemented in Python and solved using a Genetic Algorithm.

6. RESULTS

This section presents experimental results, first considering the reduction in average expected damage an SME archetype can afford with a given Available Responsibility Budget (ARB). The damage for a single potential attack is in the range of 0–1000, where 1000 represents an attack that would cause the organisation to cease operations. The charts presented here represent the average expected damage from an attack across all possible vulnerabilities. This is governed by the likelihood of related attacks being prevented by a combination of security controls, dictated by an SME's ARB.

Figure 2 shows the reduction in damage that each archetype can achieve as ARB is increased (i.e., as more capacity becomes available to manage security, and do so efficiently).

At low ARBs, the expected damage across all attack vectors is in the range of a minor security breach (a value in the range of 175–275). With no controls present, a Small Professional Archetype experiences less average damage per attack relative to it's defence capability.

As capacity becomes available to manage security, all archetypes experience a decrease in expected damage. This should be considered relative to the size class of each archetype (see Section 5.1). All archetypes address major weaknesses first, after which controls are adopted to address less critical attack classes. The additional reduction in damage lessens with each extra control, where these act to fill gaps in the coverage already provided by existing controls.

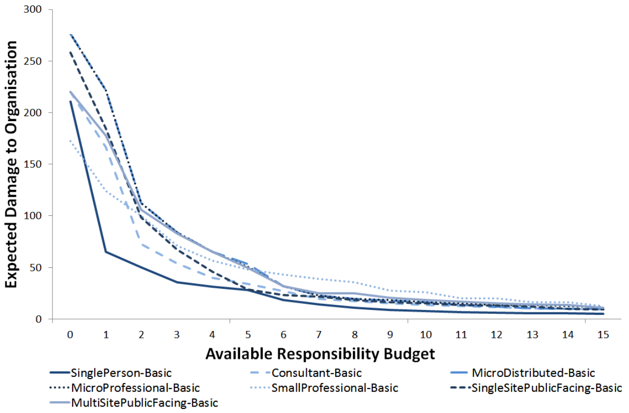

Figure 2: Expected Damage for each Archetype across all Available Responsibility Budget (ARB) Ranges

Organisations will have a limit to how much effort they can devote to security; in Table 1 we consider an ARB limit of 10, i.e. ten distinct security duties spread across the organisation.

Table 1 shows a tally of the seven archetypes (Section 5.5) which include a control in the optimal configuration, for each ARB value. Two Factor Authentication (2FA) reaches '7' (all archetypes adopting it) from an ARB of 3, remaining thereafter – financial data risks are the first that SMEs of any size would mitigate, where restricting access to financial accounts is a priority. After 2FA, organisations adopt Correct Access Privileges and Anti-Malware. Correct Access Privileges mitigate against attacks on sensitive data. Anti-Malware covers a wide set of consistently dangerous attacks which impact multiple archetypes.

We see fluctuation amongst the optimal allocations, where some *combinations* of controls are favoured more than others. Firewalls and White-Listing share similar mitigation capabilities, and as such are traded in and out of configurations as ARB changes.

After core controls, combinations diverge as archetype-specific factors influence choices. Experiments performed here imply that Patching is a critical control for archetypes where there is personal control over individual devices. However, for larger SME archetypes running multiple applications, the overheads of patch maintenance across an organisation for end-users become much higher, favouring instead a combination of other controls with the same coverage and less draw on ARB.

6.1 Residual risk

For each of the archetypes tested, the percentage of residual risk from insider threats was analysed to see if the implementation of basic controls would alleviate the risk from accidental insider actions. Across all of the attack vectors, 50% of attacks were considered to be the result of mistakes by an insider – with no controls, this accounted for an average of 67% of possible damage. With an ARB of up to 7 units, this percentage dropped to 55%, as a result of usable controls that are designed to insulate the business from the damage caused by the theft of a number of the more valuable data assets, where these activities exploit user mistakes. As the number of controls available increases, the emphasis of the residual risk is placed back on the users, where at an ARB of 10 the distribution places over 70% of the risk on the user, increasing to a maximum of 80% with a budget of 15. This is caused by a number of the other attack methods being more comprehensively managed, while those relevant to the exploitation of a system user are not protected against to the same degree.

6.2 Alternative cases

Here we explore the consequences of specific restrictions, imposed by the business, to available controls and ARB (see Section 5.5).

6.2.1 *Phone-only business*

The first case represents a single-person organisation, where all business is conducted on a smartphone. We modelled users of two kinds of devices: Phone-Old represents a phone which is less supported (and more vulnerable), whereas Phone-New represents the latest phone hardware. For Phone-New the only risk of attack comes from phishing, assuming that any applications in use are assumed to be vetted by a central trusted app store. Reliance on in-built security may introduce an overhead in staying up-to-date with advances in technology, such as being sure to purchase the latest model of phone on or soon after release. Results suggest that phone-only users are less at risk of malware, so the optimal control configuration replaces anti-malware controls with those related to passwords and account settings. This shift in controls is more pronounced for those with the latest hardware.

6.2.2 *No 2-Factor authentication*

We consider the case where a Consultant SME does not have access to 2FA, with results presented in Figure 3. While other controls may cover aspects of the theft of financial data, not having or using a directly applicable and strong control limits effectiveness, especially against phishing. The optimal control set includes Anti-Malware and Correct Access Privileges with smaller ARB, and attempts to make up the shortfall in other ways such as with adoption of Patching and Password Management. In this case, it can be noted that security capabilities are achieved through a larger set of distinct, user-facing controls.

6.2.3 *Sensitive data*

This scenario considers the relationship between organisation size and the sensitivity of the data that supports the business, focusing on a micro professional organisation managing (for example) medical records. The value of data to the business is then high – here we increase the damage

Table 1: Total Control Uptake Across All Archetypes

Budget	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Anti-Malware	4	1	1	5	5	6	7	7	7	7	7	7	7	7	7
Firewalls	1	1	3	5	3	5	6	5	5	5	5	5	7	4	5
Patching	0	0	0	0	1	0	0	3	4	4	5	5	5	6	5
Removal of Old Software	0	0	0	0	0	0	0	0	0	2	1	1	2	2	3
Removal of Unnecessary Accounts	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Correct Access Privileges	1	1	2	2	5	6	6	6	7	7	7	7	7	7	7
2-Factor Authentication	1	6	7	7	7	7	7	7	7	7	7	7	7	7	7
Data Encryption	0	0	0	0	0	0	3	2	3	4	4	2	5	4	4
Offsite Back-Up	0	0	0	0	0	1	0	0	1	1	4	5	4	6	6
Whitelisting	0	0	2	4	5	4	7	6	6	6	6	6	5	6	7
Secured Hardware	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Password Management	0	0	0	0	0	0	0	1	1	2	3	4	5	5	7

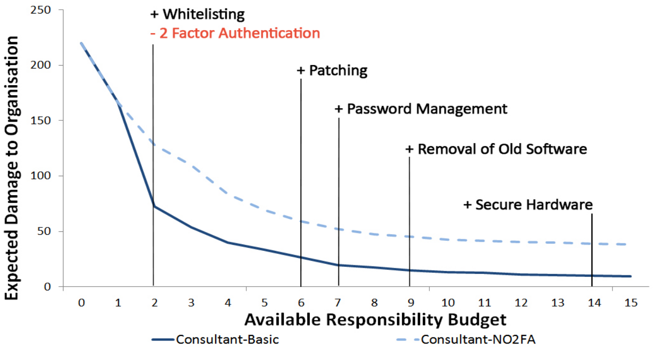

Figure 3: Expected Damage for A Consultant with and without 2-Factor Authentication

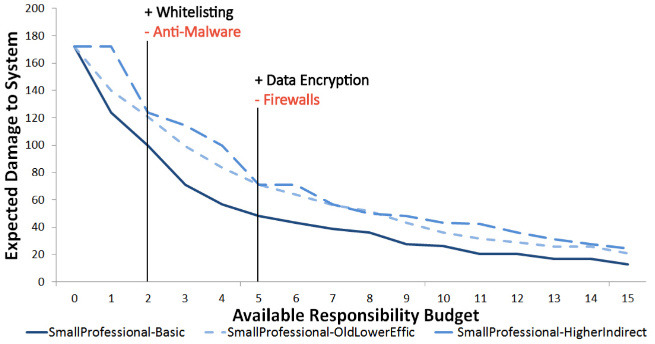

Figure 4: Expected Damage for a Medium Professional Archetype with an Old System

of data loss as equivalent to theft of financial credentials. There is a much larger level of damage relative to an increased ARB requirement, favouring Data-Encryption and Password Management to restrict access to the data.

6.2.4 *Old system*

We consider two possible cases of 'older' IT systems (as in Figure 4), where (i) the protection provided by controls is generally lower (efficiency lowered by one grade, see Section 5.3), and (ii) controls require more effort to maintain (ARB requirements of all controls are increased by 1).

Results show a reduction of the damage mitigated at low budget levels, where an ARB of 5 is required to approach coverage similar to an ARB of 3 in a newer system; the cumulative efficiency simply has less impact. Between the two 'old' systems, SMEs using controls with a lower efficiency fare better than SMEs attempting to use controls that are more difficult for users to apply to the system. The cumulative efficiency of a higher number of less efficient controls provides better protection than fewer controls that have high efficiency but similarly high ARB requirements. The scenario with lower efficiency favours white listing, offsite-back-ups and Data Encryption over Anti-Malware and Firewalls, to lower the risk of theft and loss of data with minimal adjustments to the existing system. Both 'old' systems are exposed to risk which may in time encourage renewal of all their IT.

6.2.5 *Fake anti-virus*

We model an optimal set of controls for a small distributed organisation, where an employee has unwittingly installed Fake Anti-Virus (AV) software. There are two scenarios (as in Figure 5): one where the software is functionally useless, and an extreme case where it is actively malicious. If we consider that a malicious insider can install the software, this also represents a technology-based attack upon the organisation.

The benign AV significantly weakens defences and opens up the system to damage otherwise assumed to be mitigated. The malicious AV has a negative impact on the system, where other controls are then needed to reduce the damage it can potentially cause.

6.2.6 *Overload*

Figure 6 considers controls with a high indirect cost, combined with an ARB capped at 7 and a penalty function applied when the cost of defence exceeds this cap. The solid line represents the optimal defence for the budget. The remaining lines show the impact of a 5% and 10 % reduction in the efficiency of controls (representing delays that exacerbate work tasks) for every unit that exceeds the ARB cap, which would promote adoption of insecure attempts to circumvent unworkable controls. Workarounds such as this may at first glance appear similar to 'IT sabotage' [34], where there is a need to distinguish between malicious insiders and those legitimate users for whom the existing security infrastructure is unusable. A reduction in security can result in either case.

Considering the residual risk to the system, we found that when overloaded, there was an additional 5-10% of the sys-

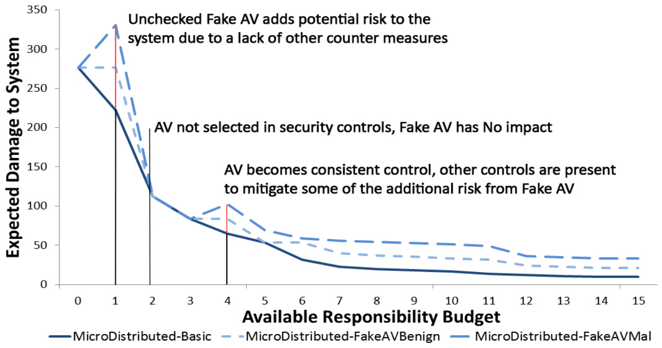

Figure 5: Expected Damage for a Small Distributed Team with Different Kinds of Fake Anti Virus

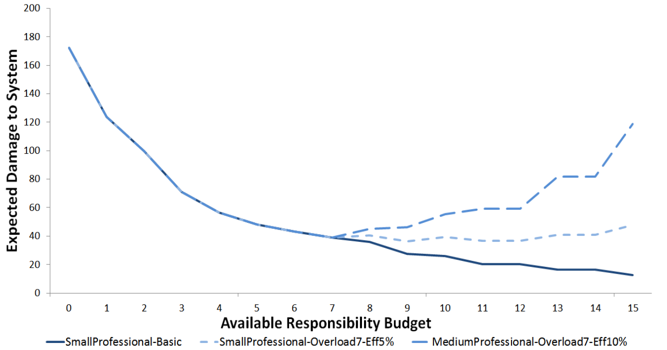

Figure 6: Expected Damage for a Medium Professional Archetype with a Maximum Budget of 7

Table 2: Uptake of Patching per Archetype based on Available Responsibility Budget for Different Indirect Costs

Cost of Patching	1	2	3	4
Single Person	3	5	8	11
Consultant	4	8	12	-
Micro Distributed	5	8	10	14
Micro Professional	7	9	13	14
Small Professional	10	14	-	-
Single Site Public	4	7	8	11
Multi Site Public	3	8	9	12

tem damage that was attributed to attacks that involve the user. This is due to the reduction in efficiency of the controls that were intended to protect the most valuable assets, given that there is no discrimination over which controls see the reduction in efficiency.

6.3 Sensitivity analysis

We isolate Patching as an under-utilised control, altering the indirect cost then modelling uptake according to available ARB. Managing the patching of systems is a challenge in preventing insider threats [34]. This case acts as sensitivity analysis but also considers the impact of the varying visibility of a control – patching may be wholly automated, or require manual intervention and force device restarts. Table 2 shows the point of uptake for Patching according to the associated indirect cost. Even with a low indirect cost, Patching is not an optimal control for micro and small professional systems. For other archetypes, uptake of Patching is consistent with other critical controls, such as 2-Factor Authentication and Anti-Malware.

Sensitivity was also examined for 2FA, where we set the indirect cost to the maximum value of 4. For each archetype the control is implemented on its own as soon as the Available Responsibility Budget can accommodate it.

7. DISCUSSION

Results imply that the control that is most effective and usable for small organisations is 2-Factor Authentication (2FA), as it directly addresses theft of financial credentials. 2FA is widely offered by providers of banking services and may be broadly interchangeable with passwords, especially for single-user businesses. 2FA may not be manageable for companies with less available capacity for security, suggesting a need for less effortful protection measures to mitigate theft of credentials.

Of the basic controls suggested by the CES, the greatest protection for the archetypes modelled here comes from Anti-Malware and (Personal) Firewalls. As noted in the 'Overload' scenario, these controls manage the majority of malware and vulnerabilities when combined with 2FA. This result is encouraging for smaller companies, as it suggests that a relatively small set of controls can begin to approach adequate protection. This also highlights the role of software providers, as devices come with personal firewalls which often remain with default settings [30].

When considering patching policies (Section 6.3), as an organisation grows there are more assets to be patched, and costs increase relative to other controls. Patching is adopted earlier by archetypes that experience a lower associated indirect cost (for instance if it can operate automatically without user intervention), with a lower impact on system-wide security for implementing the control. Other work has highlighted the role of software providers in releasing patches in an effective manner to support SMEs in staying secure [36].

The remaining controls are broadly interchangeable based on an archetype's needs; those using valuable data deploy Data Encryption and Back-ups rather than account controls, whereas those with valuable accounts focus on the reduction of vulnerabilities that may facilitate theft of credentials.

Correct Access Privileges are an unavoidable control, however once a security responsibility is delegated it is rarely reassigned (see Section 3.2) – usable security solutions are then key. Anti-malware solutions are also important, and Ho et al. [21] stress that manufacturers of consumer-level networking devices play a critical role in network security.

The percentage of risk associated with an insider threat is notable; despite the absolute risk to the system being reduced, as the number of controls increases the amount of that remaining risk that is transferred to users increases. This becomes more noticeable in the results – when considering the potential to overload users with controls – as not only does the risk to the system increase, but the source of that risk increasingly originates from user interaction with IT and IT-security systems.

7.1 Limitations

The indirect cost of a control is modelled as being shared collectively by all members of an SME, where one person may be responsible for each control or indeed for all controls. Other work has shown that security responsibilities can in fact go unassigned [12], meaning that a small company may collectively coordinate responses to security events as and when needed in an ad-hoc fashion.

The model focuses on day-to-day security management, whereas activities such as removal of unnecessary accounts may not occur regularly in organisations with fewer staff. Likewise, high staff turnover may be concentrated in roles with limited access to systems, where proper implementation of Access Control can to some extent alleviate concerns about implementing proper account termination [34], for instance.

The emphasis of the work presented here has been on the potential for vulnerabilities to basic commodity cyber attacks to emerge within smaller companies. This may be as a result of sub-optimal management of security, constrained by available time amongst normally non-expert employees and the skill demands of the controls. By focusing on basic controls and security threats, we anticipate that a next step would be to collect system-level information about security coverage and data leakage, but also to consult employees within SMEs to gather qualitative evidence of their experiences of working and interacting with security controls and data assets. These data collection efforts would become more complex in scope were we not limiting the model to a basic, restricted set of security considerations. They may also become less transferable, for instance if organisation-specific systems were analysed in isolation without comparison to other SMEs. One potential way to scale data collection would be to examine SMEs on a sector-by-sector basis, presuming that there will be similar business practices and regulatory expectations informing regular security-related behaviours.

8. CONCLUSION

Here we model the indirect costs of deploying combinations of basic cyber-security controls in small-to-medium enterprises (SMEs). SMEs and their staff often work without formal security training or in-house security expertise, where unwieldy security controls can overwhelm staff and may not be applied effectively. A security investment model uses the Cyber Essentials Scheme as a framework, exploring how the capacity and capability of an SME and its staff – the Available Responsibility Budget (ARB) – can govern prioritisation of controls to limit exposure of data to basic attacks. Human factors of security are considered, to understand the weight of indirect costs for a variety of controls. The model is driven by a set of SME archetypes based in practice, informing the viability of controls for a range of typical IT infrastructures (differing in size, complexity, and daily activities). Realistic scenarios explore how ARB can be best applied to achieve effective security coverage in the face of IT restrictions, such as deploying controls to older IT systems.

Results suggest that two-factor authentication, correct access privileges and anti-malware controls can be combined to provide smaller companies with a level of security that minimises the collective burden on staff. In the model outcomes, up-to-date patching of systems becomes more demanding as an organisation grows in size and complexity, being adopted only in much smaller companies where it remains relatively easy to maintain. Service and technology providers are in a position to reduce the indirect costs of security where SMEs rely on their products.

Future work will engage with SMEs and their employees directly, through interview and survey exercises. This will inform a richer and more granular set of realistic SME archetypes which can be modelled. It will also identify not only security requirements and restrictions, but also opportunities to match the implementation of security to regular business activities to limit the potential for insider-related data leakage. Regular review of security usability research can further inform the indirect costs modelled for with existing and emerging controls.

Acknowledgments

Simon Parkin is supported by UK EPSRC, grant nr. EP/K006517/1 (“Productive Security”). Andrew Fielder is supported by UK EPSRC, grant nr. EP/K005790/1 (“Games and Abstraction”).

9. REFERENCES

[1] D. Akhawe and A. P. Felt. Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness. In *Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13)*, pp. 257-272. 2013.

[2] S. Bartsch and M. A. Sasse. How Users Bypass Access Control and Why: The Impact of Authorization Problems on Individuals and the Organization. In *ECIS 2013 Completed Research*, 2013.

[3] A. Beautement, M. A. Sasse, and M. Wonham. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 workshop on New security paradigms*, pp. 47-58. ACM, 2009.

[4] A. Beautement, R. Coles, J. Griffin, C. Ioannidis. B. Monahan, D. Pym, A. Sasse, M. Wonham. Modelling the human and technological costs and benefits of USB memory stick security. In *Managing Information Risk and the Economics of Security*, pp. 141-163. Springer US, 2009.

[5] L. Bauer, L. F. Cranor, R. W. Reeder., M. K. Reiter, K. Vaniea. Real life challenges in access-control management. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 899-908. ACM, 2009.

[6] O. Beris, A. Beautement, and M. A. Sasse. Employee Rule Breakers, Excuse Makers and Security Champions: Mapping the risk perceptions and emotions that drive security behaviors. In *Proceedings of the 2015 New Security Paradigms Workshop*, pp. 73-84. ACM, 2015.

[7] T. Caulfield and A. Fielder. Optimizing time allocation for network defence. In *Journal of Cybersecurity*, 2015.

[8] S. Chinedu Eze, D. Yanqing, and C. Hsin. Examining emerging ICT’s adoption in SMEs from a dynamic process approach. In *Information Technology People 27*, no. 1, 2014: 63-82, 2014.

[9] Department for Business Innovation & Skills: Small Business Survey 2014: SME Employers. BIS Research Paper Number 214, March 2015.

[10] U.S. Bureau of Labor Statistics: Distribution of private sector firms by size class: 1993/Q1 through 2015/Q1, not seasonally adjusted. http://www.bls.gov/web/cewbd/table_g.txt

[11] N. David, A. David, R. R. Hansen, K. G. Larsen, A. Legay, M. C. Olesen, and C. W. Probst. Modelling social-technical attacks with timed automata. In *Proceedings of the 7th ACM CCS International Workshop on Managing Insider Security Threats*, pp. 21-28, ACM, Otober 2015.

[12] V. Dimopoulos, S. Furnell, M. Jennex, and I. Kritharas. Approaches to IT Security in Small and Medium Enterprises. In *AISM*, pp. 73-82, 2004.

[13] European Commission: What is an SME. http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition/index_en.htm

[14] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi. Decision support approaches for cyber security investment. In *Decision Support Systems*, 2016.

[15] Federation of Small Businesses (FSB): Voice of Small Business. FSB Member Survey, 2013.

[16] F. L. Greitzer, J. R. Strozer, S. Cohen, A. P. Moore, D. Mundie, and J. Cowley. Analysis of unintentional insider threats deriving from social engineering exploits. In *Security and Privacy Workshops (SPW)*, pp. 236-250, IEEE, May 2014.

[17] M. Gupta, J. Rees, A. Chaturvedi, and J. Chi. Matching information security vulnerabilities to organizational security profiles: a genetic algorithm approach In *Decision Support Systems*, 41,3, Elsevier, 2006.

[18] C. Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop*, pp. 133-144. ACM, 2009.

[19] HM Government, UK: Cyber Essentials Scheme: Requirements for basic technical protection from cyber attacks, June 2014.

[20] C. Heitzenrater and A. Simpson. Policy, Statistics, and Questions: Reflections on UK Cyber Security Disclosures. In *Proceedings of the 14th Workshop on The Economics of Information Security*, 2015.

[21] J. T. Ho, D. Dearman, and K. N. Truong. Improving users' security choices on home wireless networks. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, p. 12. ACM, 2010.

[22] M. E. Jennex and T. Addo. SMEs and knowledge requirements for operating hacker and security tools. In *IRMA 2004 Conference*, 2004.

[23] P. Jones, G. Simmons, G. Packham, P. Beynon-Davies, and D. Pickernell: An exploration of the attitudes and strategic responses of sole-proprietor micro-enterprises in adopting information and communication technology. In *International Small Business Journal 32*, no. 3, 2014: 285-306, 2014.

[24] I. Kirlappos, A. Beautement, and M. A. Sasse. "Comply or Die" Is Dead: Long live security-aware principal agents. In *Financial Cryptography and Data Security*, pp. 70-82. Springer Berlin Heidelberg, 2013.

[25] I. Kirlappos, S. Parkin, and M. A. Sasse. "Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security.". In *Workshop on Usable Security (USEC)*, 2014.

[26] B. Krebs. The scrap value of a hacked pc, revisited. Krebs on Security, 2012.

[27] E. Osborn. Business versus Technology: Sources of the Perceived Lack of Cyber Security in SMEs. CDT in Cyber Security, CDT Technical Paper 01/15, 2014.

[28] E. Rader and R. Wash. Identifying patterns in informal sources of security information. In *Journal of Cybersecurity 1*, no. 1, 2015: 121-144, 2015.

[29] T. Rakes, J. Deane, and L. Rees. IT security planning under uncertainty for high-impact events. In *Omega*, 40, 1, Elsevier, 2012.

[30] F. Raja, K. Hawkey, P. Jaferian, K. Beznosov, and K. S. Booth. It's too complicated, so I turned it off!: expectations, perceptions, and misconceptions of personal firewalls. In *Proceedings of the 3rd ACM workshop on Assurable and usable security configuration*, pp. 53-62. ACM, 2010.

[31] L. Rees, J. Deane, T. Rakes, W. Baker. Decision support for Cybersecurity risk planning In *Decision Support Systems*, 51, 3,Elsevier, 2011.

[32] C. Rhodes. Business statistics. Economic policy and statistics, 2015.

[33] T. Sawik. Selection of optimal countermeasure portfolio in IT security planning In *Decision Support Systems*, 55,1, Elsevier, 2013.

[34] G. J. Silowash, D. Capelli, A. Moore, R. Trzeciak, T. J. Shimeall, and L. Flynn. Common sense guide to mitigating insider threats. 4th edition. CMU/SEI-2012-TR-012, Technical Report, Carnegie Mellon University, 2012.

[35] R. Shay, A. Bhargav-Spantzel, and E. Bertino. Password policy simulation and analysis. In *Proceedings of the 2007 ACM workshop on Digital identity management*, pp. 1-10. ACM, 2007.

[36] J. M. Such, J. Vidler, T. Seabrook, and A. Rashid. Cyber security controls effectiveness: a qualitative assessment of cyber essentials. Lancaster University, 2015.

[37] K. Vaniea, E. Rader, and R. Wash. Mental models of software updates. In *International Communication Association*. May 2014.

[38] V. Viduto, C. Maple, W. Huang, and D. Lopez-Perez. A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem. In *Decision Support Systems*, 53, 3, Elsevier, 2012.

[39] D. S. Wall. Enemies within: Redefining the insider threat in organizational security policy. In *Security journal*, 26(2), 107-124, 2013.

[40] R. Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, p. 11. ACM, 2010.

[41] T. Whalen, D. Smetters, and E. F. Churchill. User experiences with sharing and access control. In *CHI'06 extended abstracts on Human factors in computing systems*, pp. 1517-1522. ACM, 2006.

APPENDIX

The following Archetypes inform the mapping of security technologies to business activities. Each Archetype includes an indicator of sieze, a description of the business infrastructure, the Network Design ('ND'), and regular Daily Activities ('DA') involving use of IT.

Single Person (SP): Highly mobile, making use of a phone data plan, with some cloud services. Uses few vulnerable services. Any attack is critically disruptive to a lone employee with one or two devices and service accounts.

- **ND:** The individual's mobile phone, connected by data plan or home wi-fi network, to cloud-based or internet-based services. A 'home' computer may also be used.
- **DA:** Regular use of *e-mails* and *phone calls* is central to the business. Business supplies ordered *online* through trusted suppliers. Payments and expenses may be made at any time, most readily by *internet banking.*

Consultant (SP): Engages with clients on their premises, with basic access to their network/systems.

- **ND:** Active on a single computer, i.e. a laptop used on home/home-office network or during travel on a mobile data plan. Laptop would also connect to client networks.
- **DA:** Much of the business relies on *phone* and *e-mail* communication, and potentially spontaneous *voice communication.* May interact with potentially insecure *networks* (i.e. clients, or wi-fi during travel). Most banking done by *internet banking.*

Micro Distributed Team (Mi): A small team, geographically separated. No fixed office space; individuals work remotely, either from respective home networks or public spaces (such as cafes).

- **ND:** A set of devices connected to cloud services. Most devices connect through home networks or public wi-fi. Employees may connect to a client's network.
- **DA:** Checking *emails* becomes a larger risk, given the number of employees with access to sensitive or valuable data. *Voice communication* via Skype or *messenger systems* used for rapid team communication. Broad interactions with a wide range of *cloud services*, from storage to banking.

Micro Professional Service (Mi): A small group of employees in one physical location. Offer a single highly specialised service, using a suite of sector-related applications.

- **ND:** A static network design; a number of computers connected through a small local network, linked to cloud-based services predominantly for data storage and file-sharing.
- **DA:** *E-mails* are the driver for business. May operate using *non-standard software* specific to the sector (i.e., not from a large vendor), where this software may have its own vulnerabilities.

Small Professional Service (Sm): A larger variant of a *Micro Professional Service* company, with more assets hosted locally in dedicated facilities.

- **ND:** Likely that the company deals with potentially sensitive data and wishes to keep the data on-site, although other cloud-based services may be used.
- **DA:** Internal *e-mails* will be relayed frequently as separate teams emerge, where spoofing-based approaches then gain traction. *Non-standardised software* specific to the sector may be used. Clients and contractors may connect *uncontrolled devices* to the network.

Single Site Public Facing (Mi): A small business, such as a shop or restaurant, operating a web front for a physical service. Much of the business relies on preserving availability and access to web services, such as an online booking/appointments system.

- **ND:** Consists mainly of a limited number of computers based principally on one site, used to access the web and cloud-based resources.
- **DA:** An *online booking system* is maintained, with reduced use of *e-mails*; as a public-facing entity there may still be risks. Booking system requires secure connections. *Online payment systems* are key to day-to-day business interactions, used more frequently than in smaller businesses.

Multi-Site Public Facing (Sm): An expansion of the *Single Site Public Facing* business. A small number of distributed locations, with information held in cloud services and accessed publicly through a single portal.

- **ND:** Based on a number of similar sites connecting via a set of web resources. There is a main site where most business functions are managed (equivalent to a head office); satellite sites access resources remotely as needed.
- **DA:** Bookings maintained by *online booking systems.* E-mails are traded between sites, opening up avenues for spoofing of payment requests. Booking systems require secure connections. Credentials may provide increasing levels of *remote access* not only to data assets but also to business systems.