Strathprints Institutional Repository

Renaud, Karen and Weir, George R S (2016) Cybersecurity and the unbearability of uncertainty. In: 2016 Cybersecurity and Cyberforensics Conference (CCC). Institute of Electrical and Electronics Engineers Inc., Piscataway, NJ, pp. 137-143. ISBN 9781509026579 , http://dx.doi.org/10.1109/CCC.2016.29

This version is available at http://strathprints.strath.ac.uk/58922/

Cybersecurity and the Unbearability of Uncertainty

Karen Renaud* and George R S Weir†
*University of Glasgow. Corresponding Author: karen.renaud@glasgow.ac.uk
†University of Strathclyde

***Abstract*—Cyber criminals increasingly target Small and Medium Sized Businesses (SMEs) since they are perceived to have the weakest defences. Some will not survive a cyber attack, and others will have their ability to continue trading seriously impaired. There is compelling evidence that, at present, SMEs do not seem to be implementing all the advisable security measures which could help them to resist such attacks.**

Many in the security industry believe that this is because SMEs do not take the threat seriously. This paper reports on a study to find out whether this is the case, or not.

The primary finding is that most SMEs do care about the threat but that very few implement even a small subset of the available security precautions. One contributory factor seemed to be the uncertainty caused by the wealth of conflicting and confusing online advice offered by industry and official bodies. This seemed to be hindering rather than helping SMEs so that they did not know what actions to take to improve their resilience. The conclusion is a recommendation for actions to be taken to better inform SMEs and help them to secure their systems more effectively.

I. Introduction

The security industry is reporting a major increase in cyber crime, and indications are that such crime is increasingly targeting SMEs [1], which make up 99% of UK businesses [2]. The criminals' new focus is probably because SMEs are an easier target than large companies [3]. Donnelly [4] predicts that 41% of all ransomware attacks will be aimed at small businesses in 2016.

The risks to SME assets include disclosure, corruption, destruction of the data, denying access to data and data theft, all with the potential to disrupt business activities. Some attacks on SMEs have appeared in the media [5] but it seems that many business owners are too worried about reputational damage to publicise attacks, preferring instead to absorb the loss [6]. With the low reporting rates it is difficult to gauge the actual size of the problem. There are strong indications, however, that in reality SMEs are at serious risk of becoming cyber attack victims.

The average cost of recovering from an attack was £1000 in 2015, but the long term impact is much more serious. Large companies increasingly cut off SME suppliers who have experienced an attack [7]. This means that the reputational damage that results from a cyber attack can have long-term impacts on the business. The business could lose customers, be removed from supply chains and lose government contracts, thereby impairing long-term sustainability. 83% of customers that KPMG surveyed were concerned about their data, and the care businesses took with their data [7]. Small businesses who neglect this duty of care might well go out of business, perhaps without being fully aware of this eventuality.

This paper reports on a study which explored Scottish SMEs' risk perceptions with respect to cyber attack as well as their current security practices. The research question explored in this paper is:

Do SMEs take the Cyber Security threat seriously?

II. SME Risk Perception and Security Management Stance

There is plenty of evidence that points to a significant number of Scottish SMEs not implementing sufficient security measures, and underestimating the risk of cyber attack. KPMG carried out a survey late in 2015 and found that 1 in 5 businesses took no security measures at all to resist attack [7]. Aviva's 2015 survey [8] also found that two out of five small businesses did not believe they would fall victim to a cyber attacker while Zurich's survey of 3000 SMEs found that 11% of UK businesses did not believe themselves to be a target [9]. Even those who *are* aware of their vulnerability often do not seem to implement sufficient measures to protect their businesses [7].

In order to find explanations for why SMEs could adopt a particular risk perception stance, and to explore different risk management approaches, a systematic search of the research literature pertaining to SME "decision making", "risk denial", "risk communication" and "threat appeal" was carried out. Google Scholar, ScienceDirect, SpringerLink and DBLP were consulted to find relevant papers for "information security" together with risk communication/risk denial/SME. The themes that emerged from the research papers informed the rest of this discussion.

A. Risk Perception

Threat appeals are "*persuasive messages designed to scare people by describing the terrible things that will happen to them if they do not do what the message recommends*" [10] (p. 329). People's perceptions of the risk will be impacted by the way they process any threat appeals that they encounter. People do not necessarily react in an objective way to the threat appeal: individuals will react differently depending on their life experiences, their attitudes, personality and many other aspects [11].

Unaware

The first possibility is that people are unaware of the threat. This seems unlikely, since hardly a week goes by without some cyber breach being reported in the news. In 2015, 480 million records were breached [12] including some that remained in the news for some time [13]. Pritchard [14] reports that awareness levels have risen over the last few years so complete unawareness, in 2016, is unlikely.

Minor or Medium Risk

There are broadly two reasons why SME owners might underestimate the risk. The first is that they do not fully comprehend the extent of the risk. The second is that they decline to acknowledge it — various psychological factors come into play that make it hard for them to see the risk for what it is. The former can happen if the message about the risk has been misunderstood completely, or become garbled so that they do not understand it.

On the other hand, the source of the risk communication may be mistrusted, especially if the source is an industry or government body [15] who appears to be promoting their own interests [16]. Frewer explains that mistrust of "experts" grew from the late 20th century onwards [17]. If the source is not trusted it is likely that the message will be rejected altogether.

Slovic *et al.* [18] explain that people assess risk primarily experientially, not purely using reason. They say "*We cannot assume that an intelligent person can understand the meaning of and properly act upon even the simplest of numbers such as amounts of money or numbers of lives at risk, not to mention more esoteric measures or statistics pertaining to risk, unless these numbers are infused with affect*" (p321). Hence, presenting people with figures and facts will often fail to gain their attention or interest. Their reaction will depend on how the information is presented [19] and because people do not understand probability very well they might easily misinterpret any figures that are presented to them.

Risk denial is a second possibility. Business owners may consider their companies too small to be significant, or they might not consider their data to be of any value [20]. Sometimes people may feel that there is no point implementing measures when the cyber criminals' skills are so superior to their own. They might not believe that their responses will have any efficacy [21]. Fromm [22] reported that some people acknowledge a risk but do not believe that the risk applies to them personally. This tendency was confirmed by [23]. Fromm referred to this as an *optimism bias*, which leads to a sense of invincibility [24]. Such invincibility often manifests when the link between risky behaviour and outcome is uncertain or delayed, as it is for people not implementing security measures. Getting people to take a risk seriously, especially when there is no immediate or testable feedback available to confirm the risk, is difficult [25]. A sense of invincibility could also come into being when people have not experienced an attack. The fact that others are attacked can actually exacerbate a sense of invulnerability, instead of acting to re-align risk perceptions as intuition would suggest [26]. Another explanation could be that acknowledging the threat would require a great deal of effort to be made to mitigate it, and this is somehow too uncomfortable. So, they become wilfully blind [27], simply refusing to acknowledge the existence of the problem. Kessels *et al.* [28] found that a threat communication could lead to an avoidance response, especially when the communication particularly emphasised the size of the threat, and the recipient considered the threat to be self evident. Ruiter *et al.* explain that people seem motivated to protect their self-image by denying threatening messages [29].

Finally, people have a desperate need to confirm their existing assessment of a particular hazard [19]. Slovic explains the tremendous difficulty of shifting existing preconceptions by giving people hard facts. If emotions are not acknowledged or addressed people might even use the facts to confirm their existing stance. Martha Nussbaum [30] says: "*Emotions are not just the fuel that powers the psychological mechanism of a reasoning creature. They are parts, highly complex and messy parts, of this creature's reasoning itself.*" (p. 3).

It is clear that one cannot address the problem of people underestimating the risk by providing them with the facts. We need to find ways to "add tears" to the cyber risk message [18] — what we cannot continue to do is to appeal purely to people's reason as if emotions either do not exist or are an inconvenient add-on. This has been effective in other disciplines, for example health [31].

Significant Risk

A personal experience of a cyber attack or a data breach is likely to have the desired effect of bringing perceptions into line with the reality of the risk. Fromm [22] confirmed this, finding that personal experience was extremely influential in realigning perceptions and encouraging behaviour change. This is the worst way for people to realise the reality of a risk since it is likely to involve a financial or reputational cost, let alone the harm caused by the privacy invasion that is likely to result from a breach.

This state, then, is probably inhabited by those who have either experienced an attack, forcing them to evaluate the risk realistically, or those who were able to process and accept the risk message when they heard it. There are a number of individual factors that influence whether people take risk messages seriously or not, including personality, for example [32], so this is difficult to accommodate in design.

B. Risk Management

People can be lax about security, basically ignoring it and doing nothing to address the threats. They could also be concerned, taking some measures, but being satisfied with a minimum of measures instead of transiting to the concerned stance, where they do as much as possible to protect themselves.

Lax About Security

Some SMEs might be able to rationalise the risk away altogether, and choose to take no measures at all. For solo businesses making minimal use of Information Technology (IT) this might well be a reasonable strategy, but for larger businesses and those heavily reliant on IT this is an unwise option.

One explanation was put forward by Njenga and Jordaan [33] who discovered, in their study, that some SMEs did not want to follow advice, preferring to follow their own inclinations.

Care About Security

Businesses need to implement a suite of security measures. They tend to know about strong passwords and about anti-virus software [34]. The problem is that the cyber threat landscape changes all the time, and relying solely on these tools will not prevent cyber attacks. So, while the use of an incomplete set of measures will help to a certain extent, it does leave businesses more vulnerable than they realise [35]. SMEs could well be labouring under a misapprehension that they are indeed secure. This will mean they do not look for more information or advice, and live under a false sense of security.

An SME that acknowledges the likelihood of attack is still at risk of implementing insufficient measures. The literature suggests a number of factors could lead to this state.

(1) Lacks Skills

An SME being presented with a fear appeal will assess it based on (a) the perceived magnitude of the event; (b) the perceived probability of the event happening; and (c) whether a response will be efficacious [36]. Maddux and Rogers [37] argue that efficacy is the most important of these, in terms of persuasion. A fear appeal, in other words, will fail if the recipient does not have the necessary expertise to respond, and does not know what advice to follow to deal with the fear. The SME might not have the required expertise or have employees with the requisite skills [21], and might have to rationalise the fear away as a way of dealing with it.

(2) Lacks Resources

A full quarter (24%) of a recent survey's respondents considered cyber security to be too expensive [38], which seems to lend support to this possibility.

It could also be that SMEs feel that the required security measures are too arduous and not warranted by their perceptions of their vulnerability. They may also genuinely lack resources to implement all the measures [39]. The real issue, as West [40] points out, is that the costs are immediate but the benefits nebulous and hard to quantify. West also argues that people will prefer to gamble for a loss than accept a sure loss. An expense is a certain loss and in the face of an uncertain loss that might result from not being protected, they are likely not to implement measures and, of course, other business priorities can crowd out security considerations [41].

(3) Lacks Perseverance

A business could implement a number of security measures and then, over time, become lax, especially since there is no visible benefit that accrues from the extra effort and expense [42], or simply because they inhabit a sense of false security because they have not kept up with the emerging risks.

Concerned About Security

This implies an understanding of the measures to take, and the wherewithal to implement them. No one is ever 100% secure, but these measures will significantly reduce the likelihood of falling victim to an attack, or breaching confidential data.

A one-off implementation is never the end point. Businesses have to re-evaluate regularly, keep informed and be prepared to make security a journey and not expect a one-off inoculation. Otherwise they might well transition to being serious about security.

C. Interaction Between Risk Perception and Risk Management

The previous two sections considered each of these separately but this does not mean that they are independent. Witte [43] says that if people receive a message about a potential threat they will seek to maintain control, in one of two ways:

- If they know how to protect themselves, they will take action to do so. This is a danger control process;
- If they do not know how to protect themselves, they will reject the message, and act to control the fear in that way.

Thus people could initially accept the message, but if they are unable to take the correct protective action they will reconsider the message and reject it, or rationalise it away, in order to re-establish control over the situation. If the advice is unclear or inaccessible people are likely to reject the message altogether, simply because of a deep human need to maintain control [44].

Witte's findings have been confirmed by [11]: all agree that the person's perceptions of their own efficacy in dealing with a threat have a significant impact on their behavioural response to a threat. Latour and Rotfeld [45] also found that efficacy in dealing with the threat had an impact on the person's attitude towards the message. Watson *et al.* [46] (p. 213) argue that "*The most consistent and definitive conclusions appear to be in relation to the importance, not of fear arousal but, of relevance (i.e, vulnerability) and provision of coping strategies and recommendations that an individual can effectively enact to avoid or prevent a threat from occurring (i.e., efficacy).*"

Another aspect is the person's pre-existing behaviour with respect to the threat. Cho and Salmon [47] found that people who were already in the habit of taking precautions were much more open to taking further actions to mitigate a threat. Those who had not previously contemplated taking precautionary actions were much harder to convince. Hence advice that is overly voluminous or comprehensive will probably be rejected by those who unused to taking any precautions at all: the very people who need most to be convinced of the need to take action.

The clear conclusion to be drawn from these findings is that unless people know how to reduce a threat, and have confidence that their actions are reducing the threat, they will deny the threat, and take no or very little action to ameliorate it. It seems that the way advice is provided is almost more important than the threat appeal itself.

III. Current Attempts to Help SMEs

The USA government, whose SMEs are also at risk, propose a number of mitigations [48]. Here we list their suggestions, along with the existing mitigations in Scotland and the UK.

- *Provide more guidance* — the Scottish Business Resilience Centre (SBRC)[49] publishes advice and informative videos online. The Federation for Small Businesses [50] also make a number of resources available online, as do the Scottish Government and Information Commissioner.
- *Find ways of fostering economies of scale for SMEs* — the Scottish Business Resilience Centre provides

a sponsored service to SMEs to help them to test their security provision. Innovate UK provided grants in 2015 to help SMEs to improve their security [1], and Scottish Enterprise is shortly launching a scheme to fund accreditation efforts[2].

- *Provide additional resources* — The UK government is promoting the Cyber Essentials accreditation [51], trying to get businesses in the UK to take the first steps towards greater cyber resilience. A website called Cyber Streetwise [52] provides advice to people on a personal and business level.
- *Devote additional resources to fighting cyber crime* — The Scottish Government take cyber crime very seriously, as evidenced by their development of a Cyber Resilience Strategy for Scotland[3], informed by a widely-publicised consultation process[4].

A. *Security Measure Classification*

Security measures can be classified as [53]:

- *Deterrent* — these reduce the possibility of attack. This entails keeping up with the threat landscape and implementing preventive measures as they become necessary.
- *Preventive* – these defend vulnerabilities. For example, access controls, backups, patching and firewalls.
- *Corrective* – alleviates the consequences of an attack. For example, reporting of an attack, investigation and mitigation of risk.
- *Detective* — these actively seek evidence of an attack and activate corrective or preventive controls.

B. *What Kinds of Advice are SMEs Likely to Find?*

It is worth considering what people find if they use Google, since Google is the most used site in the UK[5]. (Gov.uk is 24th on the list). Renaud [54] demonstrates the profusion of conflicting advice that results from such a search.

It is challenging to filter the good advice and to know what to trust when confronted by such a wealth of information.

In reviewing available online advice, aggregated data was derived from sites listed on the first page of a Google search for "security measures small business" as well as advice offered by official UK and Scottish bodies.

A number of studies have shown that when people have too many options to choose from, they often decline to choose at all, especially when there is no clear way to differentiate the options from each other [55]. This situation might well lead to an "intention-behaviour gap" [29], where people either don't know how to start, or get confused and then implement only those measures they can understand or are already aware of. This point is also made by Richard Hollis from the Risk Factory, that SMEs find it very hard to figure out what their priorities ought to be[6]. He also explains that the terminology used by advice-givers can confuse rather than help. What SMEs really need is a single set of clear steps they should take. The advice providers must come together to agree on a unified set of advice that will constitute an agreed "Best Practice" for SMEs. While the experts disagree to such an extent it is likely that the ensuing confusion is leading to uncertainty and inaction.

IV. Research Study

A study was carried out to explore SME risk perceptions and security management practices[7]. A number of one-to-one interviews were carried out with small businesses to explore their perceptions and practices. The researcher discovered that businesses would not grant interviews unless they either knew the researcher or had a recommendation from someone they knew. This is understandable in a world where many scammers try to trick people out of their hard-earned money. The researcher only gained access to business owners via recommendations from acquaintances or University contacts.

Paper-based surveys were then posted to randomly chosen businesses across Scotland, to allow them to respond anonymously via postage paid envelopes. In order to ensure an even coverage of Scotland's businesses a database of businesses was constructed by harvesting business details from various sources across the Web, including the UK small business directory, Chambers of Commerce and trade finder websites. Over 18 000 business details were accumulated, and validated in terms of number of employees. Where it was possible to ascertain this, businesses with more than 100 employees were removed from the database. The researcher then used the SQL randomiser to randomly choose 600 addresses as targets for mailed surveys. When surveys were returned because the business was no longer trading, the survey was mailed to another randomly chosen business. The businesses were located in towns ranging from Kelso in the east to Arran in the west, from Dumfries in the South to Lerwick in the north.

V. Findings

110 people participated in the study. 32% were solo businesses, 63% had 30 or fewer employees and 5% had up to 100 employees. 35% operated their businesses from home.

When asked to rate the importance of IT to their business on a scale of 1(unimportant) to 5(very important), the average rating across all participants was 4.3. When asked to rate how concerned they were about the security of their company's information, on a scale of 1(unconcerned) to 5 (I lose sleep), the average was 2.09.

In terms of who they asked for advice, 53% of the participants consulted Google, and 7% consulted government websites. 23% consulted their IT service provider.

[1] https://vouchers.innovateuk.org/cyber-security

[2] http://www.scottish-enterprise.com/services/develop-new-products-and-services/smart-scotland

[3] http://news.scotland.gov.uk/imagelibrary/downloadmedia.ashx?MediaDetailsID=3708&SizeId=-1

[4] https://consult.scotland.gov.uk/cyber-resilience-policy-team/cyberconsultation

[5] http://www.alexa.com/topsites/countries/GB

[6] https://www.youtube.com/watch?v=6JkuEM126Ds

[7] Ethical Approval was obtained from the University of Glasgow College Ethics Committee

18% of participants did not make backups. Those who did make backups were asked about the frequency. The most likely answer was Daily (38% of respondents). 19% made backups as and when necessary so did not seem to do it regularly or reliably. When asked whether they thought they might become the target of a hacking attack, the majority did not think this would happen to them.

When asked who they would report it to if they were hacked, 15 mentioned reporting the police. Five of these said they would not report it, and one said he would only report it for insurance purposes.

When asked what the Scottish government could do, answers fell into the following categories:

- Funding, including subsidised access to security services and experts;
- Information and Advice tailored for SMEs, Workshops, Breakfast Talks;
- Better Policing of hackers;
- Advice about security software, free software.

A. Risk Perceptions

The first step was to determine which of the states the participants fell into. A broad stroke classification was carried out as follows:

Minor Risk: When asked if they could be targeted by a cyber attack they said it would never happen or that there was only a remote chance. 52% of participants fell into this category.

Medium Risk: These participants acknolwedged a likelihood of an attack but considered that there was a small chance of falling victim. 33% of participants.

Significant Risk: These participants considered themselves likely or extremely likely to be a target of an attack. 15% of the participants fell into this category.

B. Security Management Categories

To assess categories we used reports of implementation of a very small subset of existing security measures. We chose the most well-known preventive measures that did not require the use of jargon: *backups, access-control, anti-virus software* and *patching of operating systems*. Since all the indicators from other survey were that SMEs were generally unsophisticated in terms of security measures we considered that checking for implementation of a small subset of measures would give an indication of security stance.

Lax About Security: Participants were allocated to this state if they said they were unsure about whether or not they ought to be worried about their company's information. Other signals were being unsure about, or considering unimportant, the preventive measures: backups, using access control measures, anti-virus and patching their operating systems. Only 5% of participants fell into this category.

Care About Security: These participants implemented some measures but the coverage was often patchy. If they considered any of the preventive measures: backups, access control, anti-virus or patching, unimportant this was an indicator. Finally, if they said they were unconcerned about using WiFi this indicated a level of naïvety that seriously concerned participants probably would not demonstrate (81% participants).

Concerned About Security: We considered that these participants would make backups, and consider access control, anti-virus and patching to be important, or very important. They would be concerned or very concerned about using public WiFi. 14% of participants met these requirements. Ideally they would also have Cyber Essentials accreditation but if that requirement is added none of the participants can be classified as concerned.

Figure 1 shows how many participants inhabited each of the risk perception and security management states.

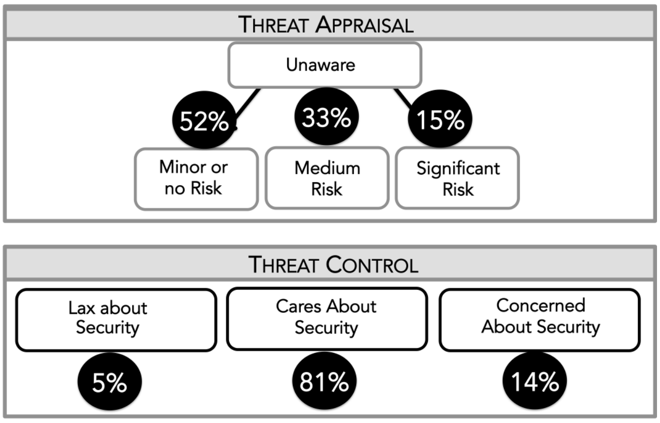

Fig. 1. Number of participants in each State

C. Other Findings

A number of themes emerged from the analysis that the literature review did not uncover.

The Role of IT Service Companies: 22 of the companies relied primarily on IT service providers to take care of the information security needs. When asked what action they would take if they realised they had been hacked 37 specifically referred to either their own IT service provider, or the fact that they would call in someone knowledgeable. Only 5 said they would ask a friend or family member to help them. This means that these companies are in a position to play a key role in improving resilience.

No Faith in Police: There was very little faith in the police to remediate. Some said they would report it to cover their backs, but that they did not expect the police to be able to help. One business who had experienced a ransomware attack said that the police had been of very little assistance to him. One said "the police are overstretched and stressed. What would they be able to do?" Another said: "they would not know what to do".

Low Levels of Expertise: The participants demonstrated a knowledge of well-known measures such as strong passwords, anti-virus and firewalls. The majority had no concept of the risks of using public WiFi or of installing Apps on their Smartphones. One said: "I am learning as I go along", which demonstrates an admirable openness, but probably means they are currently insufficiently protected.

VI. Discussion & Recommendations

The question explored by this study was whether SMEs were taking the cyber threat seriously. Certainly we confirmed that a significant percentage were not doing so. Only 15% of the participants had anything close to an accurate perception of their vulnerability to attack. Moreover, this study checked whether participants were implementing a small subset of the available security measures, whether they were concerned about their information and whether they understood the dangers of public WiFi. Only 14% of participants covered all of these. The rest implemented only some of the measures or were not very concerned.

One possible contributor both to poor risk perception and poor risk management is that the message about the magnitude of the cyber threat risk was not being communicated effectively to SMEs. If they do not understand, or are able to rationalise the fear away, they will not accept the seriousness of the risk. We also noticed that even those who had a realistic idea of the risk did not reliably implement all the required measures. A contributing factor here could be the fact that the available advice is often overly technical, complex and overwhelming.

In terms of reaching SMEs, some viable (inexpensive) options emerged from the analysis.

One source of advice: Provide a security advice website, with one set of SME-targeted advice agreed upon by all stakeholders. Ensure that it appears on page 1 of Google.

Structure the advice to answer the main questions to keep things very simple (details can be linked to for those who are interested):

What extra measures could I take to be even more secure? What are the advantages of outsourcing to an IT service provider? Where can I get funding? What do I do if I have been hacked?

1) Why bother? (Risk Message "with tears")
    a) What is the risk of being hacked as an SME?
2) What should I do and how? (Security Management)
    a) What basic security measures must I take?
    b) What extra security measures would make me even more secure?
    c) What are the advantages of outsourcing to an IT service provider?
    d) Where can I get funding to help me with security?
3) What do I do if I have been hacked? What actions should I take? (Incident Response)

Engage Locally with SMEs: Arrange SME-specific events, dealing with something they care about, like business continuity, specifically not advertised as security events. When people attend these, tell them about cyber security. Find a way to inject emotion, but be careful of overhyping and always ensure that they know where to get advice. Provide inexpensive reminders of the advice website on something they use in their everyday lives (keyring, stickers). Provide a newsletter they can sign up to that provides up to date advice at regular intervals, so that they are apprised of new risks, and measures they ought to take to mitigate them.

Empower IT Service Providers: Local IT companies have an important role to play. We should focus on improving their security knowledge and directly supporting them.

VII. Conclusion & Future Work

The study reported in this paper was carried out to find out whether Scottish SMEs were taking the risk of cyber attack seriously, and were implementing sufficient measures to protect their systems and information. We discovered that many took at least some security measures but very few were implementing all of the security measures in the small subset we asked them about.

The reasons for this are two-fold. The first is that the risk communication messages are primarily fact based and human nature prefers to reason emotionally and experientially. The second problem is that there is far too much advice available. SMEs are becoming overwhelmed by the multitude of available advice, the exhaustive nature of the recommendations and disagreements between security experts. It is vital for official bodies to get together to issue one set of advice and for such advice to be simple and easy to comprehend.

Acknowledgement

This research was carried out while the first author was seconded to the Scottish Business Resilience Centre, funded by a Royal Academy of Engineering Grant. A shorter version of this paper will appear here [54].

References

[1] M. Smith, "Huge rise in hack attacks as cyber-criminals target small businesses," 2016. [Online]. Available: http://www.theguardian.com/

[2] C. Rhodes, "Business statistics," 2015, 7 December. House of Commons Library.

[3] FireEye, "Why SMBs are a Prime Target for Cyber Attacks," 2015, 7. [Online]. Available: https://www2.fireeye.com/WEB-WP-Not-Too-Small-To-Matter_LP.html

[4] S. Donnelly, "41% of all ransomware attacks aimed at small businesses," 2016, march 16. [Online]. Available: http://is4profit.com/41-of-all-ransomware-attacks-aimed-at-small-businesses/

[5] BBC, "Scottish hairdressing firm warns of cyber attack threat," 2015, 27 October. [Online]. Available: http://www.bbc.co.uk/news/uk-scotland-scotland-business-34647780

[6] K. Palmer, "Businesses keep quiet over cyber attacks, as EU cracks down on underreporting," 2016, 3 March. [Online]. Available: http://www.telegraph.co.uk/

[7] KPMG, "Small business reputation & the cyber risk," 2016. [Online]. Available: www.kpmg.com

[8] Aviva, "UK: Businesses don't believe they are at risk of cyber crime, says Aviva," 2016. [Online]. Available: http://www.aviva.com/media/news/

[9] Zurich, "SMEs' concerns over cybercrime have doubled," 2015. [Online]. Available: https://www.zurich.com/en/media/news-releases/2015/2015-1203-01

[10] K. Witte, "Putting the fear back into fear appeals: The extended parallel process model," *Communications Monographs*, vol. 59, no. 4, pp. 329–349, 1992.

[11] V. Cauberghe, P. De Pelsmacker, W. Janssens, and N. Dens, "Fear, threat and efficacy in threat appeals: Message involvement as a key mediator to message acceptance," *Accident Analysis & Prevention*, vol. 41, no. 2, pp. 276–285, 2009.

[12] L. Morgan, "List of data breaches and cyber attacks in 2015 – over 480 million leaked records," 2016, 8 January. [Online]. Available: http://www.itgovernance.co.uk/blog/

[13] BBC, "TalkTalk hack 'affected 157,000 customers'," 2015, 6 November. [Online]. Available: http://www.bbc.co.uk/news/business-34743185

[14] S. Pritchard, "Navigating the black hole of small business security," *Infosecurity*, vol. 7, no. 5, pp. 18–21, 2010.

[15] M. J. Palenchar and R. L. Heath, "Strategic risk communication: Adding value to society," *Public Relations Review*, vol. 33, no. 2, pp. 120–129, 2007.

[16] L. J. Frewer, J. Scholderer, and L. Bredahl, "Communicating about the risks and benefits of genetically modified foods: The mediating role of trust," *Risk analysis*, vol. 23, no. 6, pp. 1117–1133, 2003.

[17] L. Frewer, "The public and effective risk communication," *Toxicology letters*, vol. 149, no. 1, pp. 391–397, 2004.

[18] P. Slovic, M. L. Finucane, E. Peters, and D. G. MacGregor, "Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality," *Risk analysis*, vol. 24, no. 2, pp. 311–322, 2004.

[19] P. Slovic, B. Fischhoff, and S. Lichtenstein, "Behavioral decision theory perspectives on risk and safety," *Acta psychologica*, vol. 56, no. 1-3, pp. 183–203, 1984.

[20] N. Amrin, "The Impact of Cyber Security on SMEs," Ph.D. dissertation, Faculty of Electrical Engineering, Mathematics and Computer Science, 2014.

[21] M. Siponen, S. Pahnila, and A. Mahmood, "Employees' adherence to information security policies: an empirical study," in *new approaches for security, privacy and trust in complex environments*. Springer, 2007, pp. 133–144.

[22] J. Fromm, "Risk denial and neglect: studies in risk perception," Ph.D. dissertation, The Economic Research Institute, 2005.

[23] B. Fischhoff, P. Slovic, and S. Lichtenstein, "Facts versus fears: Understanding perceived risk," 1982.

[24] W. Ashford, "Lack of security knowledge limiting business initiatives, survey shows," 2016, computerWeekly, 9 May.

[25] N. D. Weinstein, "Misleading tests of health behavior theories," *Annals of Behavioral Medicine*, vol. 33, no. 1, pp. 1–10, 2007.

[26] J. T. MacCurdy, *The psychology of emotion: morbid and normal*. Routledge, 2013, vol. 12.

[27] M. Heffernan, *Wilful Blindness: Why We Ignore the Obvious*. Simon and Schuster, 2011.

[28] L. T. Kessels, R. A. Ruiter, L. Wouters, and B. M. Jansma, "Neuroscientific evidence for defensive avoidance of fear appeals," *International Journal of Psychology*, vol. 49, no. 2, pp. 80–88, 2014.

[29] R. A. Ruiter, L. T. Kessels, G.-J. Y. Peters, and G. Kok, "Sixty years of fear appeal research: Current state of the evidence," *International journal of psychology*, vol. 49, no. 2, pp. 63–70, 2014.

[30] M. C. Nussbaum, *Upheavals of thought: The intelligence of emotions*. Cambridge University Press, 2003.

[31] I. M. Lewis, B. Watson, and K. M. White, "Response efficacy: The key to minimizing rejection and maximizing acceptance of emotion-based anti-speeding messages," *Accident Analysis & Prevention*, vol. 42, no. 2, pp. 459–467, 2010.

[32] J. Shropshire, M. Warkentin, and S. Sharma, "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior," *Computers & Security*, vol. 49, pp. 177–191, 2015.

[33] K. Njenga and P. Jordaan, "We want to do it our way: The neutralisation approach to managing information systems security by small businesses," *The African Journal of Information Systems*, vol. 8, no. 1, p. 3, 2015.

[34] J.-Y. Park, R. J. Robles, C.-H. Hong, S.-S. Yeo, and T.-h. Kim, "It security strategies for sme's," *International journal of software engineering and its applications*, vol. 2, no. 3, pp. 91–98, 2008.

[35] A. Gupta and R. Hammond, "Information systems security issues and decisions for small businesses: An empirical examination," *Information management & computer security*, vol. 13, no. 4, pp. 297–310, 2005.

[36] A. C. Johnston and M. Warkentin, "Fear appeals and information security behaviors: an empirical study," *MIS quarterly*, pp. 549–566, 2010.

[37] J. E. Maddux and R. W. Rogers, "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *Journal of experimental social psychology*, vol. 19, no. 5, pp. 469–479, 1983.

[38] Gov.uk, "Cyber security 'myths' putting a third of SME revenue at risk," 2015, 25 February. [Online]. Available: https://www.gov.uk/government/news/cyber-security-myths-putting-a-third-of-sme-revenue-at-risk

[39] L. Kelly, "IT security considerations for SMEs," 2011, computerWeekly. 13-19 September.

[40] R. West, "The psychology of security," *Communications of the ACM*, vol. 51, no. 4, pp. 34–40, 2008.

[41] T. Kurpjuhn, "The SME security challenge," *Computer Fraud & Security*, vol. 2015, no. 3, pp. 5–7, 2015.

[42] S. Furnell and K.-L. Thomson, "Recognising and addressing 'security fatigue'," *Computer Fraud & Security*, vol. 2009, no. 11, pp. 7–11, 2009.

[43] K. Witte, "Fear as motivator, fear as inhibitor: Using the extended parallel process model to explain fear appeal successes and failures." in *Handbook of Communication and Emotion: Research, Theory, Applications and Contexts*. Academic Press, 1998, no. 16, pp. 423–450.

[44] D. H. Pink, *Drive: The surprising truth about what motivates us*. Penguin, 2011.

[45] M. S. LaTour and H. J. Rotfeld, "There are threats and (maybe) fear-caused arousal: Theory and confusions of appeals to fear and fear arousal itself," *Journal of advertising*, vol. 26, no. 3, pp. 45–59, 1997.

[46] I. Lewis, B. Watson, R. Tay, and K. M. White, "The role of fear appeals in improving driver safety: A review of the effectiveness of fear-arousing (threat) appeals in road safety advertising." *International Journal of Behavioral Consultation and Therapy*, vol. 3, no. 2, p. 203, 2007.

[47] H. Cho and C. T. Salmon, "Fear appeals for individuals in different stages of change: Intended and unintended effects and implications on public health campaigns," *Health communication*, vol. 20, no. 1, pp. 91–99, 2006.

[48] L. A. Aguilar, "The need for greater focus on the cybersecurity challenges facing small and midsize businesses," 2015, 19 October. [Online]. Available: https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html#_edn6

[49] "Scottish Business Resilience Centre." [Online]. Available: www.sbrcentre.co.uk

[50] Federation of Small Businesses, "Are you underestimating the impact a cyber attack could have on your reputation?" [Online]. Available: http://www.fsb.org.uk/

[51] Cyber Essentials. [Online]. Available: http://www.cyberessentials.org

[52] "Cyber StreetWise." [Online]. Available: https://www.cyberstreetwise.com

[53] G. B. Gokhale and D. A. Banks, "Organisational information security: A viable system perspective." in *AISM*, 2004, pp. 178–184.

[54] K. Renaud, "SMEs are Lost in an Advice Thicket," *Computer Fraud and Security*, 2016, to Appear.

[55] R. Greifeneder, B. Scheibehenne, and N. Kleber, "Less may be more when choosing is difficult: Choice complexity and too much choice," *Acta psychologica*, vol. 133, no. 1, pp. 45–50, 2010.