Knowledge Transfer Network

ICT

Security Lancaster | LANCASTER UNIVERSITY

Small Business Cyber Security Workshop 2013

Towards Digitally Secure Business Growth

Dr Daniel Prince and Mr Nick King

Security Lancaster

Foreword

Contents

Introduction 1

Key Outcomes 3

- Agility vs Security 4
- Thinking About the Types of Business 5
- Cyber Security and Digital Business Risk 9

Conclusions 11

Appendix A: Responses 13

Authors 14

References 15

Mr Tony Dyhouse

Director Cyber Security
ICT Knowledge Transfer Network

Persistent problems are rarely easy to solve else they would not remain such. Sometimes it is necessary to go back to grass roots and question accepted assumptions and theories in order to make progress against stubborn issues. That is what ICT KTN and Security Lancaster found themselves doing on 28th January 2013.

Much resource and advice has been levied at all organisations in the UK over the last few years. We hear about an ever-increasing range of attacks against UK industry, trying to steal identities and intellectual property. Yet despite increasing assistance, large organisations keep falling victim to such attacks; usually as a result of human gullibility rather than technological genius. This is understandable due in part to the large number of people they employ; each being a target results in a large attack surface. So, surely, a smaller organization should find it easier to adopt appropriate protection. Sadly, our Small Business Survey 2012 indicated that this was not the case, and that even cyber-savvy SMEs were failing to adopt the measures being regularly suggested.

So, ICT KTN and Security Lancaster went back to basics to find out why.

Executive Summary

This report identifies the key findings which were developed during a workshop involving a number of regional micro, small and medium enterprises from a range of industrial sectors and experts in the field of cyber security and business. The purpose of this dialogue was to establish the issues that businesses classed as an SME face with respect to Cyber Security. The output from this workshop, along with this report identifies the market failures that key stakeholders, such as universities and government, need to address in order to support the industry and help to grow a secure digital economy. This workshop follows on from CSC2012 and also the report SBCSS2012 which highlighted the significant problems SMEs are facing with regard to receiving support with regard to cyber security. Security Lancaster partnered with the ICT KTN and sought to work with a diverse group of SMEs in facilitated teams, taken through a series of guided exercises, to first and foremost identify their concerns around cyber security and subsequently capture any potential ways forward.

Key findings

In summary the following are the key findings developed from the output and discussion undertaken during the workshop:

- SMEs are in fact three different types of businesses (micro, small, medium) with different needs and cannot be treated as one sector.
- There is a need to understand that security although significant needs to be balanced against business agility and market responsiveness.
- Risk exposure and appropriate requirements are related to organisation size
- Cyber security Fear Uncertainty and Doubt is damaging giving a need for clear communication

Ultimately we propose three basic principles that should be undertaken by any organisation seeking to provide advice to businesses classified as a Small to Medium Enterprise.

1. ***If you are small then Agility is more important than Security***
2. ***They are not SMEs they are micro, small and medium businesses***
3. ***Stop talking about cyber security start talking about digital business risk***

Security Lancaster and the ICT KTN would like to thank the delegates of the workshop who gave their time and effort to tackle this tricky problem. Without your efforts and insights this report would not have been possible and we look forward to working with you all again in the future.

Introduction

At the Cyber Security Conference 2012 the conference team ran the Small Business Cyber Security Survey in order to understand the business related issues and business impact of cyber security to businesses with less than 250 staff. It has been identified by the UK government that this business sector is at risk from attack due to a lack of relevant information for their business needs on how to protect them.

The results from the survey (Prince & King, 2012) provided both positive and negative feedback. On the positive there was considerable interest and concern around cyber security, however this rarely translated into the respondents following the best practice identified by the government and other SME dedicated cyber security organisations such as IASME (Information Assurance for SMEs) (IASME Consortium, 2013). The survey clearly identified a market failure in the provision and consumption of the material around cyber protection. While the message that cyber security is a problem for small businesses was being heard it was clear that information being put out, despite being the best there is to offer, somehow fell short of providing appropriate advice for those targeted businesses to take action. The CSC team in conjunction with the ICT KTN put together a workshop to collaborate with a range of key stakeholders to understand this market failure and propose a range of solutions that could be taken up by policy makers and experts to extend appropriate advice and support to the small business community.

Methodology

The workshop was held on the 28th January 2013 and provided an open facilitated space to understand and get to grips with the problems. The delegates ran through a series of exploratory, self-guided exercises that were intended to probe beyond conventional wisdom and common responses in order to reveal the deeper underlying issues that are preventing SMEs from adopting cyber security principles and approaches. This ultimately drove a reflective learning process for the businesses and seasoned security experts in the room in order to arrive at a consensus on how the situation for all involved could be improved.

What resulted was the development of a series of simple strategies to model approaches and responsibility for cyber security. It also revealed a number of underlying misconceptions around the way the cyber security field, support agencies and the policy makers, view the small business approach to cyber security. The most important of these is the misconception that the lack of cyber security implementation is down to a lack of resource or appetite on the small businesses part. In some cases this may be true, but arguably it is a symptom of a fundamental risk trade-off by the business owner between security and agility. This trade-off has been well documented in a digital economy where networking effects dominate and it is important for product adoption to appeal to complementors in order to achieve and incumbent position in the market place (Varian, 1999).

Thinking Ahead

The workshop identified a number of deficiencies in the current approaches which policy makers and experts are using in tackling the cyber security issues for those businesses that total less than 250 staff. However, we believe that future policies and approaches should adopt the following three principles in order to ensure that they are suitable for this particular sector.

1. ***If you are small then Agility is more important than Security***
2. ***They are not SMEs they are micro, small and medium businesses***
3. ***Stop talking about cyber security start talking about digital business risk.***

Key Outcomes

The workshop recognised that cyber security is a key business challenge that needs to be tackled by businesses and government working in collaboration to produce consistent advice and support. Further, it also recognised that despite considerable appetite to take action, there was a lack of undertaking on the part of the SME sector.

Positively, this reveals that the reasons why cyber security is an important business concern are well understood and accepted, and that it is information on how the business should respond appropriately that is suffering a market failure. Common reasons for this cited during the workshop were; cost, complexity, problem size, language and applicability to their business. While all valid reasons, upon scratching the surface of these arguments significant complexities in the makeup and business approaches of micro, small and medium businesses became apparent. Simply addressing these issues head on may not be prudent.

The workshop revealed that a key barrier to the adoption of cyber security measures was a fundamental business risk trade off between being agile in order to respond to the market and being secure enough to operate in that market. Ultimately the workshop discussions exposed that the risk of not being agile, due to implementing stricter security, created a higher risk exposure for the company than not being secure. Further, it is only when the company reaches a certain size that these exposures cross and the cyber protection becomes more important than agility.

Another barrier identified was that current methods of imparting advice lump all size of businesses together as an SME. However, the diversity in culture, business approach and organisational structure is radically different and in a constant state of flux, when comparing micro, small and medium businesses. It is really only when a business becomes large enough to require well defined and fulfilled roles in a functional organisational hierarchy that formal holistic processes for managing cyber security become appropriate. Protection advice should therefore take this into account, and focus on delivering the best advice for the size of the company. Further, the advice should consider empowering businesses owners to successfully and securely manage the transitions in their digital business as the company grows. We argue that managing these transition points is vital for sustainable and secure digital business growth as they set the foundation for what comes after.

The final inhibitor that needs to be dealt with is the use of language. The common use of fear, uncertainty and doubt to motivate businesses to take up cyber protection measures is actually inhibiting the uptake of the advice. This issue is further compounded by the technocratic language used in the cyber security literature. Care must be taken with future advice to ensure that it demonstrates the positive benefits and is also framed in ways that are applicable to business owners.

The remainder of this section presents a more detailed discussion of the key points above and relates it to the discussions had during the facilitated workshop by the delegates.

Agility vs Security

There are many attempts to define why small businesses fail to adopt cyber security strategies to protect themselves. This uptake failure is often classed in the following ways:

- **Cost:** Implementing cyber security measures draws resources away from the main business in both cash and human resource.
- **Complexity:** In order to implement appropriate measures requires a significant amount of expertise and dedicated technology in order to achieve appropriate levels of security
- **Terminology:** The information and language surrounding cyber security is impenetrable to the average business person.
- **Applicability:** Cyber security does not relate to them and that the information and advice that comes out focuses on large companies and enterprises.

These four key concepts were also highlighted in the first round of discussions during the workshop. While we do not dispute that these are all real explanations for not adopting cyber security approaches, further discussions and analysis identified they are merely symptoms of an underlying rationale business trade-off of agility vs. security.

It can be argued that the number of threat agents, those individuals or organisations who would attack a business, and the ways in which those agents might attack a business is increasing regardless of the size of that business. It is also clear that attackers are often indiscriminate in terms of who they go after. What is not clear is whether the probability of attack is equal across the board. Conventional wisdom tells us that every business with a digital presence is equally likely to be attacked. We would argue that more work needs to be done in order to refute or confirm this “wisdom” in more detail. However, given this conventional wisdom, what we can say is that the size of the business does directly link to the attack surface of the business. For example, if a company is a sole trader who has one externally hosted website and one home PC for accounts and ordering, the potential number of vulnerabilities and the complexity in the way that this example business can be attacked is drastically different to a 10 person business, each with their own PC in an office containing server equipment and a significant number of outsourced services. Therefore, a clear argument relating business size, as measured by the size of the IT infrastructure, to the security exposure can be made in general terms. Given that network effects dominate in information technology it is not unreasonable to assume in this first instance that the attack surface is proportional to the square of the number of network devices operated by the business. However, work needs to be done to understand this aspect of complexity, but our purpose here is to illustrate the concept rather than provide a definitive answer. The likelihood of attack (which is consistent) coupled with the ability to undertake an attack (power law proportionality with number of devices) combined with the “at risk” value (The total loss of the business) provides a basic measure of risk exposure. However this is not the only risk that a small business is exposed to.

A key aspect of small business success is their ability to be agile and adapt to the current market trends (Klien, 2012). As they are small they are not in a position, except for very niche markets, to be able to provide market direction, hence the need for co-operative groups such as the Federation of Small Businesses. Once a business passes the mark from being classed as an SME into a large organisation, they are much more able to control market direction; until that point they must respond in order to survive. Arguably, the smaller the business the more agile they need to be. However, it has been argued by a number of academics that security often inhibits the ability of businesses to respond and dominate a market, as it makes it harder for complementors to be able to access them. (Varian, 1999) has shown that a digital market place is dominated by network effects, the consequence of this is that the faster a business can build a network of consumers and complementors then the quicker it will achieve market dominance. (Anderson, 2008) put this in context with Microsoft’s approach to their software and showed it made perfect sense to develop insecure software initially in order to make it easier to build a dominant market position. Once the business is the incumbent it can then retrofit security in

order to differentiate and provide value add. Security significantly hinders the ability for complementors to work with others in a supply chain, the requirements for audits of partners and the adherence to standards such as ISO 27001 inherently make it harder for an organisation's neighbours in the supply network to work with that organisation. This adherence also stops a business from being agile as every time it wants to do something new it would have to go through a significant testing and compliance process. This slows the innovation process, which is the lifeblood of successful small businesses (Waldeck & Callahan, 2009). However, as we have argued once a business moves into a directing position rather than a responsive position with regard to the market the need for agility tails off in that sector.

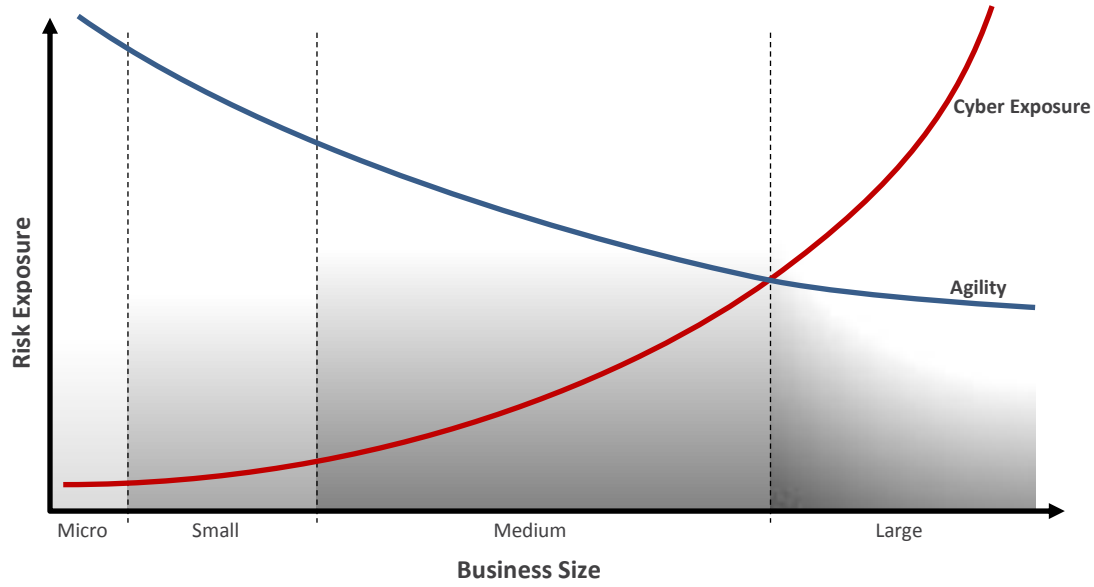


Figure 1 Risk Exposure Due to Cyber Security vs Lack of Agility Plotted against Business Size

In conclusion, when a business is in the micro category, the need for business agility is very high in order to mitigate the risk of business collapse, whereas the risk of loss of business due to a cyber attack is very small. The risk presented by not being agile reduces as a function of the size of business while the exposure from cyber attack increases in a power law relationship to the size. There naturally forms a point of transition where the risk posed by a lack of cyber security outweighs the risk of not being agile and it is at this point of inflection that cyber security should become a key business consideration; this can be seen in Figure 1. For simplicities sake, and based on the discussions from the workshop, we place this point of inflection where a medium enterprise moves to being classed as a large enterprise. Given this premise, the question then becomes what should micro, small and medium enterprises do in terms of cyber security until this point of inflection.

Thinking About the Types of Business

What became very apparent was the lack of applicability that cyber security advice had to the micro end of the business community. If a business is a sole trader or a two man organisation there are much more effective mechanisms to manage security. For example, do two people really need a comprehensive security policy, or do they just need to know a series of business principles that would protect their customers, and therefore their business? One result from the survey was the overwhelming majority of the small businesses respondents had outsourced their information technology capability. In this situation, is it about being able to assess your own security measures or being able to enforce or evaluate the security assurances given by the outsource provider? This led to several important key points:

- Cyber security business advice should be dictated by the business size,
- As a business you are responsible for cyber security, and you have the **Authority** to take action.

The Size of the Business is Fundamental

The information and advice for the businesses, which would be classed as SME, typically treats all businesses in this category as one thing, an SME. The natural tendency is to produce a single piece of advice in a "one size fits all" manner. However, it was clear from the workshop the striking differences between the SME classes of Micro, Small and Medium. As alluded to in the previous section there is a fundamental difference in the attack surface of these businesses as measured by the number of systems and there are also significant business risks outside of those posed by cyber security. Beyond this however, there are significantly different changes in the culture of the business. For example, some workshop delegates identified that a key indicator that a business is moving from micro to small is the employment of people other than your friends or people you know prior to the creation of the company. An important factor to consider is the speed of change at which a business must operate at when it is smaller in size. Some workshop delegates indicated that speed and agility were very important considerations for them in a globalised digital commerce environment, as they have to respond quickly to international customers, bidding against international businesses on the rapidly changing World Wide Web.

From the discussion with the key stakeholders present at the workshop the following background for business sizes in terms of structure and speed is presented.

Business	Structure	Speed
Micro	Informal, employees have multiple roles, employees tend to have been there from the start and have a more "friends and families" type relationship with each other. Very low turnover of staff, if any.	The business model is rapidly evolving with constantly changing markets and customer demographics. The company is much more likely to provide bespoke offerings around a set of core concepts.
Small	Largely informal but there is typically well-defined roles which usually only have on individual assigned to them. There is typically some sort of hierarchy of at least two levels, however, this is largely notional and there is still a friends and families type of relationship. Some staff turnover, but typically less than 1% or 2%.	The business has a well-defined set of products that are prepared of the customer. At this stage the business is less likely to accept highly customised jobs due to the cost implications over and above producing standardised products. As a result the company is more likely to try to respond to market changes by developing new products.
Medium	Well-defined formal roles and hierarchies are introduced, but team dynamics are more fluid enabling resources to be deployed dynamically. Much more of a formal working atmosphere and working relationships. Teams are much more statically defined and formal processes to manage employment, staff performance and progression. Typically around 5% staff turnover.	The company is transitioning into a market leader able to define the marketplace and the products that should be consumed. As a market leader the company is informing the consumer more on what to buy and has limited customisation beyond configuring a product or service line for a specific customer. Changes in products and customer demands are slower as the business is now influencing the marketplace.

Table 1 understanding the dynamics of Micro, Small and Medium Enterprises

Given this information it is clear that one size does not fit all and there are radical differences between each of the three subcategories. Therefore, the advice must be tailored and focused for at least the three categories; micro, small and medium. Importantly, an approach should be taken such that it uses these traits as an advantage. For example, a dynamic and creative three person micro business is much more likely to take risks and adopt new approaches, where as a 200 person medium enterprise is much more willing to develop formalised repeatable process and information. What is clear is the ease with which cyber security can be managed is inversely related to the size of the business, i.e. when there are two hundred employees telling people a common file server password is impractical and undesirable, but for three people in an office, this approach is more suitable.

This type of thinking showed up as part of the discussion between a security professional and a micro enterprise that attended the workshop. The micro enterprise indicated it was not through a lack of desire to implement cyber security but the description of current approaches was too overwhelming for them, even those that purported to be designed specifically for SMEs. The question the micro enterprise posed was what were the smaller individual steps that they could take to protect themselves. The response from the security professional was to say that piecemeal ad hoc approaches were not suitable for security, instead the enterprise had to take a holistic view first. The micro enterprise indicated a holistic approach was not feasible for all of the reasons this report has highlighted thus far. The exchange highlighted the gulf between current thinking of the professionals and the applicability of that advice for the small end of the SME sector. While a holistic approach may be applicable for medium enterprises it certainly is not appropriate for micro and small enterprises. The questions therefore become:

- How do you create advice for micro and small businesses who undertake cyber security measures in an ad hoc and organic way and support them as they grow in order to move them towards a more holistic and structured approach to cyber security that would be expected from a medium to large enterprise?
- How do you react appropriately to the support market failure rather than a failure in appetite in the market place?

We propose this be addressed in two ways; thinking about operation at each stage, and thinking about the key points of transition. The majority of advice present in the market place advises on what to do when you are operating in a stable state with a stable business model, or considers that the horse has already bolted and security measures are being retrofitted. This advice is perfectly legitimate and very useful for businesses, especially those that are operating in known markets with known or well-developed product and service concepts. However, it misses a key and highly disruptive phase in the business lifecycle which is the transition, an example of which is the transition between classifications; micro to small to medium. There is plenty of advice available for business in other areas to help manage important business transitions, such as employing your first person (Barclay Card, 2013) or setting up a new office (Dept. Business Innovation and Skills, 2013). Getting this transition right and managing it appropriately is just as important, if not more so, than appropriate management when the transition is over. In this context security transitions could be considered as:

- Commissioning outsourced or cloud based digital services
- Buying your first server
- Setting up your own client database
- Handling electronic financial transactions

By approaching the security advice with an understanding of who will consume in terms of their capability and capacity, coupled with a focus on whether the advice is targeting a transition or current operation will provide a more nuanced and sophisticated approach to support micro, small and medium businesses. A key recommendation from this report therefore is to develop tiered advice for micro, small and medium enterprises which provides advice not only on normal operation but on transitioning advice for each tier. However, further work needs to be commissioned in order to validate these workshops findings in terms of the information given in Table 1, and determining the best way to approach each target group

Modelling Responsibility

During the workshop the attendees were asked to complete a set of cards in teams identifying what needs to be done in order to improve the cyber security situation for all key stakeholders. A summary of these responses can be found in Appendix A. Subsequently the whole workshop worked together to place these responses on a grid as shown in

Figure 2. This grid broke the response categories down into classifications of Strategic vs Operational and Self vs Other and the diagram shows a heat map of where those responses were placed.

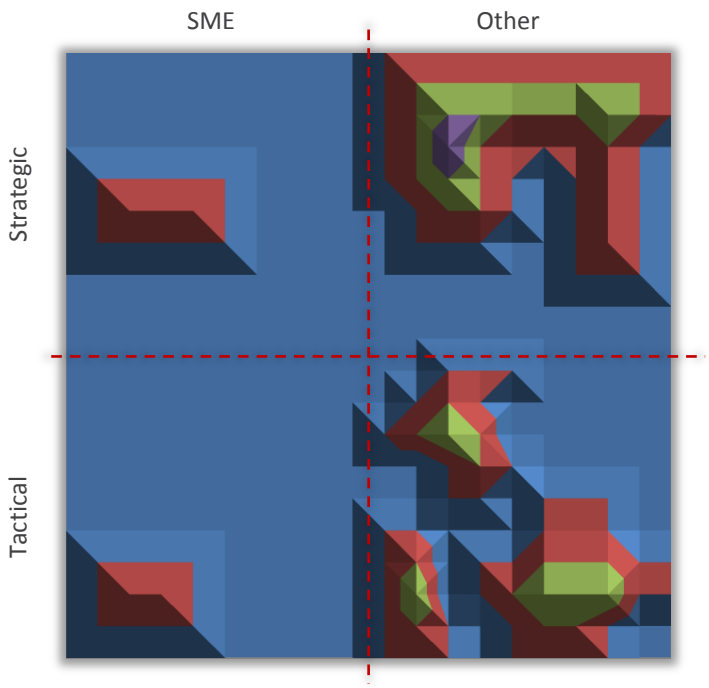


Figure 2 Grid placement of responsibility verses type of action

This exercise intended to reveal who should undertake the tasks previously identified and to understand whether those tasks should be considered at a tactical or strategic level. What it revealed was an underlying push from those present onto the "Other" category, which was considered to be government and affiliated departments such as BIS. The main focus of which was in the form of government endorsed standards, backed by enforcing legislation at the strategic level, coupled with awareness and outreach campaigns at the tactical level. The reason for this bias is uncertain but potentially identifies a significant hurdle that any organisation attempting to tackle this problem needs to overcome. Based on collating the thoughts of the workshop delegates, the authors suggest the following possible explanations:

- Businesses do not understand the complex messages and would like someone to resolve it for them
- Businesses are fundamentally not interested in solving the issue for themselves
- Businesses feel disenfranchised and feel they have no authority or limited capability to solve the problem for themselves.

Naturally other explanations exist and further research needs to be undertaken in order to identify the correct hypothesis. However, the dominant theory that many felt was that the issues cyber security present are beyond their control and yet they have significant responsibility in order to protect themselves, their customers and ultimately their business. This mismatch between responsibility and authority is an important inhibitor to action that needs to be examined in detail if real change and impact is to be delivered. Specifically we would recommend an empowerment approach that would help business owners to understand that they do have the capability and capacity to tackle the issue as ultimately it is potentially the whole business at risk not just the business assets in terms of information assets, hardware, service and reputation.

To conclude further advice needs to be issued cognisant of the fact that businesses which would be classified as an SME (less than 250 employees or turnover less than €50M or a balance sheet total of less than €43M) should not be treated as one type of business as the nature, culture and style of operation is radically different between micro, small and medium enterprises. Further, the advice should focus on empowering those businesses in order to be able to take some action regardless of how small in order to protect themselves. If as experts we keep stating that cyber security is a big problem, business owners may start to believe that the problem is too big for them to tackle.

Cyber Security and Digital Business Risk

One aspect that was prevalent during the discussion was the use of language and terminology around cyber security. It was highlighted that cyber security discussions are focused on fear uncertainty and doubt (FUD), which was identified as being very off putting rather than a driver for change. One delegate commented that:

"Cyber security is presented in such a scary way I am not about to poke the wasps nest to see how scary it actually is!"

More fundamentally, the context in which cyber security is presented is nearly always technical and as such unless a business is in an IT related field it would require considerable effort to understand the language used. Ultimately the discussion turned to presenting cyber security, not in terms of FUD or technology, but rather what it truly represents which is a set of risks that are encountered by businesses operating with a digital presence.

The phrase *Digital Business Risk* was coined to better describe what the group was actually talking about. This concept quickly became adopted as the majority of the business representatives present had a sound understanding of business risk and business planning, some had additional experience in open new markets, such as in different countries. Put in the context of working in a new business market therefore created a more positive attitude, where the opportunities that operating in cyberspace could be more easily balanced against the risk of this new market. This approach enabled the creation of a more comprehensible model for business owners to consider business risk of operating with a digital footprint.

In part the discussion natural focused on business risk management with the follow as examples of the typical questions that were asked:

- *"What's your appropriate level of spend for IT Security? How valuable are your 'crown jewels'?"*
- *"How can we maximize our cyber security spend to protect the business and how to make it more profitable?"*
- *"How much do you need to spend to have effective cyber security?"*

Ultimately as a group the workshop delegates concluded that for a micro, small or medium business the cessation of trading was the fundamental loss exposure as these classes of business would potentially be unable to absorb the impact on reputation or financial loss as a result of a digital risk materialisation, unlike larger organisations, for example Sony and the Playstation network hack (BBC, 2011). However, it is important to be aware that this maximum loss of total business value is only exposed if the business has a digital footprint and as we have argued the total exposure would be related to the attack surface available to the attacker, as calculated by the probability of attack multiplied by the total loss expected.

The question of how much to spend is similar to the question of how long a password should be. Simple responses to the latter question of 10 characters with a mix of upper and lower case plus special characters misses the fundamental issue of what is it you are trying to protect with that password? Should you be using a password at all or some other strong form of authentication? Similarly the former question misses the point of what are you trying to protect. It is not the case that micro businesses need to implement the same level of security as large international corporates or even, as we have discussed, the same level of security as a small business. Rather the workshop concluded that it should not be about implementing the Gold Standard in cyber security but the *highest* standard *appropriate* to you. As an example, consider a local business providing a paid for child play gym/park. The business has 8 employees operating in shifts, operating the gate, taking payments and running the café. Enter and exit is operated on a paper based sign in book, it is a cash only business (no PCI-DSS compliance), it has a static website and a Facebook page, accounts run using spread sheets and free WiFi provided to the patrons. In this case there is clearly no need to go beyond only the measures that a home user would be expected to undertake.

It is clear that the language used is vital to the uptake of the advice regarding cyber security. Scaring individuals to take action is not working and is actually having a negative effect. Further, the technocratic language used to describe cyber security is counterproductive, further driving individuals away. Business owners understand business concepts and it is rare that businesses at the smaller end of the spectrum would have the technical capability to understand complex technical discussions on the merits or lack thereof of cyber security protection. Therefore, future advice needs to couched in terms that business owners understand and can relate to in a positive way.

Conclusions

The workshop revealed a mixed bag of positives and negatives. Most importantly it is clear that the message regarding cyber protection is getting through and that business owners and employees alike are understanding why cyber security is important and that they have a responsibility to protect themselves, their customers and ultimately their business.

However, there exists a gulf in translating that acceptance into action. Businesses struggle to understand how they should protect themselves and what they can actually do. Arguably this has led to frustration and disenfranchisement on the part of the businesses, which is compounded by the negative rhetoric of the cyber security profession. While there are clear lines of attack in order to help businesses tackle this issue the workshop exposed that the gulf between appetite and action may be amplified by a lack of understanding by the cyber security profession seeking to apply their existing knowledge and skills as used with large organisations, who can afford their services, to the SME market place without fully realising the drastically different operating culture and environment. In this report we have argued the case that a key inhibitor for cyber security uptake is a fundamental business trade off between the risk of business agility and the impact suffered from cyber losses. It is only when the complexity and risk exposure of a businesses digital footprint reaches a size that pushes that risk exposure higher than the risk of loss of agility that cyber security becomes a fundamental business concern. Therefore, advice for the SME grouping of companies should focus on how to manage the transitions in digital business approaches so that as the company grows the businesses security approaches grow in line and proportionally with the digital business requirements as show in Figure 3.

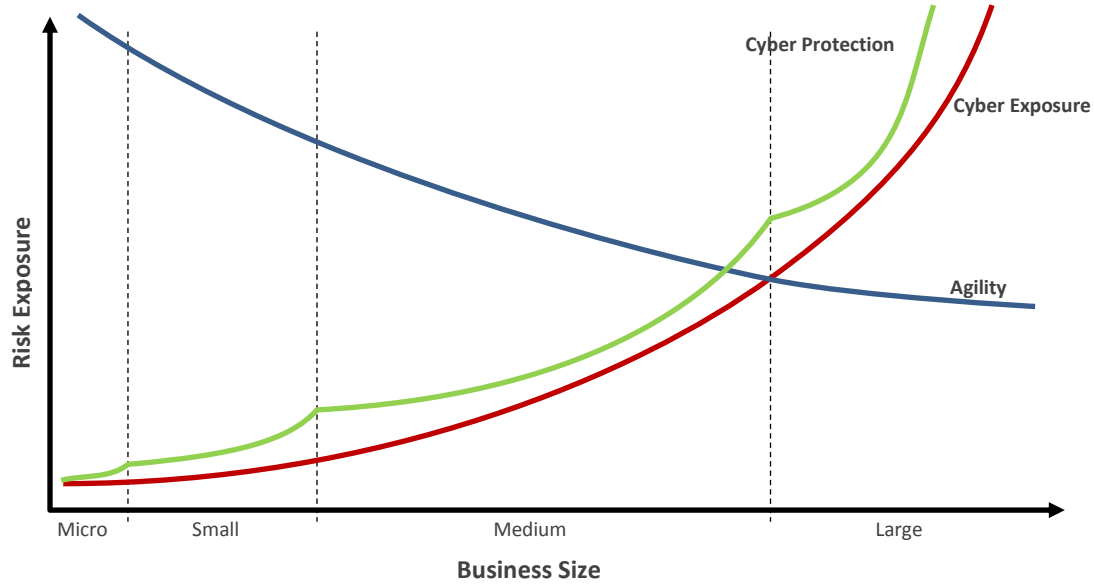


Figure 3 cyber security capability aligned with business growth

The Workshop also highlighted how dominated cyber security is by technologists and cyber security experts (who potentially have their own products or services to sell). Yes there is clearly a problem and potential risk exposure to companies regardless of sector or size, but not every micro, small or medium enterprise is a high

tech hub of digital innovation, and it is clear at times that this is lost in the hyperbole and rhetoric. In the 2012 BIS Business Population Estimate report, it was projected that there were 3.6M businesses with no employees, i.e. sole traders, which accounted for 16.3% of private sector employment and 6.6% of private sector turnover (£208B) (Dept. Business Innovation and Skills, 2013). As sole traders they likely have a computer to run office style applications, a mobile phone, a website and a social media presence. How is this different to the average individual in the street? Clearly the size of the business must dictate the type of advice it receives.

The workshop also revealed the delegates preference for a governmental and legislative response in order to tackle the problem in the national interest and that an individual SME is too small to act alone. The authors wonder if the announcements by the government regarding the fact that cyber security is a critical national risk (HM Government, 2010) has reinforced this view. Reasons suggested for this cover the complexity of messages, not being interested or disempowered to solve the issues themselves. This certainly highlights a significant barrier to companies in these classifications taking ownership and driving forward their own solutions. The authors suggest that given the size and the complexity of the target audience that a way forward may be to crowdsource community groups in order to create a self-sustaining resilient business community.

Open questions

Inevitably the workshop identified more questions than it answered. Now however, those questions have found a voice and are being asked and it is incumbent upon the government, universities and other influential stakeholders to start to answer them in order to protect the future of our digital economy. Some of the more pertinent questions identified during the workshop are:

- Can a free market economy drive cyber security requirements or do we need to legislate?
- How do SMEs accept and manage their risk in the national interest, mandatory or self-regulating?
- What are the cyber threats we will face in 5 years time and how do we get ahead of the game?
- What should Universities be proactively doing to help small businesses address cyber/IT issues/threats?
- How to collect a strong evidence base for cyber security exposures suffered by SMEs?

Hopefully the workshop and this report have started to highlight the complexities as to why it seems the message for cyber protection does not seem to be getting through. Further, report has started to chart the potential start of the pathways to tackle these issues and look at the problem domain from a new vantage point and with more nuanced understanding of the domain.

Ultimately we need to stop talking about cyber security talk about digital business risk.

Appendix A: Responses

SME: Strategic

- Should the CEO/CFO be responsible for the consequences of a data breach
- Preferred supply chain (list of cyber secure companies)
- Subsidise certification

SME: Tactical

- Ask staff to list digital vulnerabilities – reward for most beneficial improvement
- Promote local groups to collaborate on best practice, ie CMI
- Produce a BIS guide for SME on how to identify and value their crown jewels

Other: Strategic

- Industry led standards; Gold, secure, silver secure, bronze secure.
- Tiered standard i.e. ISO27001 1 – 5
- Establish tiered approach to digital business risk adoption – appropriate to sme size/risk
- Establish standards at appropriate levels to enable an sme to establish and maintain customer and supplier confidence
- Legislation to require adherence to minimum standards
- Reinforce directors responsibility towards business continuity planning which would include digital security.
- Mandate legislation (corporate governance – Companies House) to require risk register including digital business risks
- Cyber security becomes a condition of directorship
- Tax incentive for companies

Other: Tactical

- Value SME corporate information in the UK
- Cyber Security Support Network
- Education
- Establish a single source of information relating to digital business risk easy to find, easy to read and understand, actionable cyber security support network
- The creation of a toolkit to track + quantify attack to enable a personalise response -> Secure UK like the green cross code
- Businesses need to be made aware of the threats. To counter the “it won’t happen to me” approach
- Mainstream media move output on impact of IT security breaches from technology pages to business pages + big story on govt not doing enough to support SME’s
- Media Campaign (HMG and BIS)
- Need to change cyber to digital business security
- Awareness of risks around self i.e. mobile devices in business premises
- Make the business case for investing in systems

Authors

Dr Daniel Prince: Security Lancaster Associate Director for Partnerships

Dr Daniel Prince is an associate director and business partnerships manager for Security Lancaster. Prior to this he was the course director for the multi-disciplinary MSc in Cyber Security teaching penetration testing, digital forensics and information security risk management.

Mr Nick King: Business Development Manager, School of Computing and Communications

Nick King is Business Development Manager in Lancaster University's School of Computing and Communications, located at InfoLab21. In addition to leading the Schools' Business Development Team Nick also Manages one of the Schools key Business Support Projects: ISTEP. Prior to his time at InfoLab21 Nick was UK Business Manager with a UK IT Solution Provider with a specialism in information assurance and security products/services.

References

Anderson, R. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems* (2nd ed.). John Wiley & Sons.

Barclay Card. (2013). *Employing a member of staff for the first time*. Retrieved April 24, 2013, from Barclay Card Business: http://www.barclaycard.co.uk/business/sme/getting-started/employing-a-member-of-staff-for-the-first-time/

BBC. (2011, April 25). *http://www.bbc.co.uk/news/technology-13192359*. Retrieved April 24, 2013, from BBC Technology News: http://www.bbc.co.uk/news/technology-13169518

Dept. Business Innovation and Skills. (2013). *Business Population Estimates*. Retrieved April 24, 2013, from Inside Government: https://www.gov.uk/government/organisations/department-for-business-innovation-skills/series/business-population-estimates

Dept. Business Innovation and Skills. (2013, April 4). *Choosing your business premises*. Retrieved April 24, 2013, from UK Government: https://www.gov.uk/choosing-your-business-premises

HM Government. (2010). *A Strong Britain in an Age of Uncertainty: The National Security Strategy.* London: The Stationary Office.

IASME Consortium. (2013). *Home Page*. Retrieved April 24, 2013, from Information Assurance for SMEs Consortium: http://www.iasme.co.uk/

Klien, K. (2012, june 27). *From Bed Bugs to Mini-Brownies, Business Adapt to Change*. Retrieved April 24, 2013, from Bloomberg Businessweek: http://www.businessweek.com/articles/2012-06-27/from-mice-to-bed-bugs-businesses-change-with-the-times

Prince, D., & King, N. (2012). *Small Business Cyber Security Survey 2012.* Lancaster: Lancaster University.

Security Lancaster. (2012). *Cyber Security Conference 2012: Protecting your business in an insecure world*. Retrieved April 24, 2013, from Security Lancaster: http://www.security-centre.lancs.ac.uk/events/conferences/csc2012.php

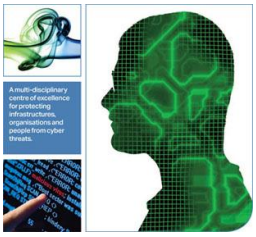
Varian, C. S. (1999). *Information Rules.* Harvard Business School Press.

Waldeck, A., & Callahan, R. H. (2009, February 3). *Innovation Lessons From Small Business*. Retrieved April 24, 2013, from Forbes: http://www.forbes.com/2009/02/03/apple-innovation-customers-leadership-clayton-christensen_0203_small_business.html

This page intentionally blank

About Security Lancaster

Security Lancaster delivers research and education that innovates and creatively challenges the way that individuals, organisations and societies secure and protect themselves. We achieve this via engagement and collaboration with companies from a range of sectors and governments. Our approach delivers the very best use-inspired and pure research alongside cutting edge education that delivers real impact.



Our Strategy

- Deliver World leading Research in Security Sciences by balancing basic research with use-inspired and applied research to ensure its work remains both theoretically rich and relevant to societal needs and priorities.
- Cultivate Innovation and Entrepreneurship in Security by facilitating the exchange of ideas and information through the sharing of facilities, the creation of networks of like-minded individuals, and through the development of a 'social infrastructure'
- Deliver Excellent Security Education through multi-disciplinary training programmes for future scientists and industry practitioners

The overarching aim for the Centre is to derive additional capability for collaborative, multi-disciplinary research and education. The research in the Centre will be driven by an ethos of undertaking theoretically rich, use-inspired research. The latter will be achieved through close collaboration between the scientists in Security Lancaster and our industry and practice partners, facilitated by a dedicated partnership management team.

About Security Lancaster's Cyber Security Research Theme

Our cyber security research is multi-disciplinary and puts the person at the heart of security decisions. We work across a wide variety of sectors to help businesses, other organisations and individuals to gain an understanding of cyber threats, how to counter them, embed cyber security practices and establish a cyber security culture to help support and protect the UK economy.

About the ICT KTN Co. Ltd

The ICT KTN Co. Ltd was established in 2007 as a not-for-profit company with the specific aim of delivering knowledge transfer activity on behalf of the Technology Strategy Board. It was previously known as the Digital Communications KTN Co. Ltd, and has hitherto been promoting knowledge transfer in this important element of the wider ICT sector for which it now has responsibility.

Knowledge Transfer Network

ICT

For more information regarding the event related to this report and for further details of other associated events and information please visit

http://www.security-centre.lancs.ac.uk/sbcsw2012