Chapter

TOWARDS CYBER-RESILIENT & SUSTAINABLE SMES: THE CASE STUDY OF ADDED VALUE FROM A LARGE IT RE-SELLER

Dr Mils Hills & Louise Atkinson***

Associate Professor in Risk, Resilience & Corporate Security / Research Fellow

Northampton Business School

University of Northampton (UK)

ABSTRACT

This chapter reports on and discusses an extensive interview conducted by the authors with the head of pre-sales at a hardware and software re-seller. The Pre-Sales division of the reseller provides advice based on end-to-end solution for IT infrastructure and technology management. Within the team there is expertise spanning a plethora of specifically defined technology areas to support end customers in the decision making process on their capital expenditure in IT equipment. Areas include Software licensing, Server infrastructure development, data storage and management, systems security, and networking infrastructure (and more). The business of being a re-seller may not initially strike the reader as being relevant to cybersecurity in general, and socio-technical matters at all, but we discovered the rather vital role that such an intermediary performs through their added value and corporate ethics.

Specifically, this reseller's team of customer service agents provide advice and referral to colleagues and end customers for subject-matter expertise as well, naturally, for opportunities to up-sell – specifically with that important core of any economy: Small and Medium-Sized Enterprises (hereafter SMEs) - usually defined as companies with up to 250 employees. In other words, the business both responds to requests for solutions from existing customers (pull) and actively engages with customers to grow awareness about, for example, security risks in order to sell products and services (push).

The authors – drawing on a background of research in corporate resilience and SMEs (with a commercial background in the IT sector) were interested to learn from an individual

* Corresponding Author Email Address: mils.hills@northampton.ac.uk

with his finger very firmly on the pulse of SME cyber-security awareness, just what his view was on the general level of cyber-security awareness amongst SMEs and what his company offered in the way of assistance.

Keywords: Sales, Customers, Reseller, Business, Solutions

INTRODUCTION

> "Only two things are valuable in business: people and data. Everything else is an insurable risk" (Head of Pre-Sales, Large IT Reseller)

The authors of this chapter recognise the importance of SMEs to a stable and sustainable economy – after all, they employ over 60% of private sector employees in the UK (BIS UK 2015) and most of the people who have jobs in liberal democratic states. The European Commission definition of an SEM is widely accepted on an international basis and is presented in the below table (fig.1). Approximately 95% of business in Europe is of SME scale, with the figure rising to 99% globally. It is therefore important to examine smaller companies in order to understand the challenges they face in terms of their cyber security risks and what opportunities they have to enhance their levels of protection.

Company Category	**Employees**	**Turnover**	**Balance Sheet Total**
Medium Sized	<250	≤ € 50 m	≤ € 43 m
Small Sized	< 50	≤ € 10 m	≤ € 10 m
Micro Sized	< 10	≤ € 2 m	≤ € 2 m

Fig. 1 SME size definition – European Commission 2015

The authors are cognisant that many SMEs operate on narrow margins and / or have little appetite or interest in investing in unnecessary security measures. Whilst frugality is often a virtue, anecdotal knowledge (and many of the so-called statistics about business failure after cyber and other incidents are no more than frequently repeated anecdotes) suggests that a data protection, Intellectual Property loss, fraud, reputational damage or other directly cyber or cyber-enabled attacks could easily push an SME into difficulty or even oblivion. With a substantial customer base of SMEs, the reseller which is the focus of this chapter has visibility to business issues facing smaller organisations across multiple sectors within the umbrella 'SME'. SMEs are – numerous surveys show – both the least knowledgeable about cyber-risks and yet the most likely to suffer serious harm or existential threat from them occurring. With such a client base, accumulated from successful trading over several decades,

our interviewee's company utilises its "team of solution specialists and architects responsible for proactively supporting sales with solutions designed to meet our customers' needs and to reactively respond to requests from our sales teams for quotes and solutions".

Rather than describe the depressing potentials, the authors hold a mind-set that academics have some duty to search for and publicise opportunities to improve the business world (sometimes defined as a 'ChangeMaker' ethos), and were this determined to identify practical and positive insights that could be of wider benefit. Through personal connections, we identified a likely source for both an unvarnished assay of the state of SME cyber-security and for constructive lessons for wider interest and value: the head of pre-sales at a major hard- and soft-ware re-seller.

The following sections of the chapter set out what re-sellers do, what pre-sales activity is and present some of the highlights of our interview which show that – in a self-organised way – this company is usefully and ethically helping SMEs better understand their cyber-risk exposure and invest to reduce it.

WHAT DOES A RESELLER DO?

Within the IT industry, the reseller is at the level of a retailer in terms of a supply chain. Often selling products and solutions to a blend of B2B and B2C customers, our interviewee primarily focuses on B2B sales. Resellers tend to seek specialisms within the IT Industry in order to offer USPs to their client base. Our reseller is categorised as a large reseller due to its international reach and sales revenue. As such, the business occupies no specific niche area of technical expertise, rather the reseller seeks to offer complete end-to-end IT solutions through their own expertise and Vendor (Manufacturer/Producer) accreditations, as well as carefully chosen partner organisations to support niche areas when needed. Accreditations at this reseller include Microsoft, HP, Citrix, Cisco, and more. The reseller works closely with IT vendor partners to ensure knowledge and solution provision within the organisation remains current. The reseller uses its combined knowledge of various IT partners in order to provide the best integrated IT systems for its customers. Resellers provide an important advisory link between IT vendors and end user customers, and this puts a level of responsibility and ethic of care upon them to offer best advice and guidance at all times.

WHAT IS PRE-SALES?

Pre-sales is an essential part of the decision making process for customers. By working alongside a general sales team, pre-sales offer second line support guiding customers seeking more complex advice. It is this division that acts as 'problem solvers' rather than mere order

fulfilment agents. Presales look to resolve business issues through consultancy, products and on-going services. Advice is freely available to clients at the initial point of contact, from which recommendations for consultancy/ sales are made in order to resolve the business issue in question.

Part of the solution offering process revolves around discussion of the additional needs of the organisation beyond the provision of IT products and software – namely the need for training and managing people behaviour in the use of IT equipment in order to be secure.

Given the paucity and complexity of official guidance from government and others, the pre-sales function has the ability to help its customers understand current and future risks, and (by so doing) help the overall business out-compete rival resellers.

EVOLVING SOLUTIONS TO ADDRESS CYBER RISK & SECURITY

Our interviewee noted that something that is both striking and overwhelming to SMEs and others is the pace at which the products and market moves as the risk and nature of security challenges and technological products evolve and change. Dynamic progression and innovation is constant in an effort to meet and address current risks, whether from hacking, spyware, or protecting systems from poor user practice. Traditionally security in IT terms meant the implementation of a firewall on a network and subscription to a reasonable anti-virus software package.

The diversity and creativity evident in cyber-crime (internally and externally-based) has led to the industry responding with increasingly fragmented and niche offerings that seek to combat specific security threats within the umbrella of 'cyber security'. This fragmentation of niche solutions makes it challenging for our reseller to remain current across the board, and to be fully trained in all aspects of security. This is where carefully chosen alliances and partnerships support the core knowledge of the reseller ensuring high quality product and service provision. It is common practice to engage services of penetration testing, security auditing and outsources data monitoring in order to help clients reduce risk of security threats. Through such a high level of engagement relationships are forged between client and supplier that are built on a trust basis and the ethics of this trust is something that is managed carefully by the reseller.

Building relationships with clients based on trust is extremely important to our reseller for customer retention and, from an ethical perspective, to support their reputation for resolving critical business concerns in a cost-effective way. This is something our interviewee was keen

to express- that is the need to provide the 'right' solution for clients, even when this may produce very little revenue.

We can evaluate from the fragmentation of the market, the pace at which the products evolve and the lack of inherent knowledge of clients there is a strong need for the expertise offered through the reseller channel via its trained agents and specialist partner organisations. There are, however, barriers to engagement with SMEs in terms of cyber risk and security and we turn to discuss them in the next section.

SMEs, Cyber Risk & Security: 'the last thing on their mind'

Our interviewee was frank in evidencing our assumption that SMEs had neither the time nor resources to consider cyber-security as anything like a priority. Pithily expressed, our interviewee stated that for those running such companies, this was "the last thing on their mind". In particular for companies where Information Technology is not recognised as core to their business – for example in a small engineering company – these SMEs are unaware of just how reliant they actually are on computers.

We understand how this situation arises – IT has become a utility, we are easily tempted to worry about it only when its performance is degraded or availability ceases altogether. The authors speculate that those who own and operate SMEs are much more interested in 'the work' *rather than what makes that work possible and sustainable*. However, in an era where intellectual property (at the level of tangible product or service, in terms of trust and confidence, price or even client list) is red meat that competitors and others seek out to appropriate or, potentially, contaminate – this attitude needs to change.

Our interviewee referred to research from the University of Texas which found that:

> 94 per cent of companies suffering from catastrophic data loss do not survive, 43 per cent never reopen and 51 per cent close within two years, according to stats from the University of Texas (Burns 2015).[1]

In terms of the levels of risk that are 'out there' – pre-sales companies have a better appreciation than their SME customers of it, but they also have a richer picture of the risk exposure and perceptions of risks taken (or unappreciated) that customers have.

Our interviewee provided the example of the massively popular domain of cloud services. Whilst such offerings enable very easy set-up and demonstrable savings in terms of efficiency (easy access to information and applications by many people in a business) and

[1] We understand that this report references the following journal article: Christensen, S. R., et. al, "Financial and Functional Impacts of Computer Outages on Businesses", Center for Research on Information Systems, The University of Texas at Arlington.

cost (cheaper to outsource storage than own the physical assets): those buying and implementing cloud services often do not consider such vital aspects as how the data gets to / from the cloud and issues of rights access to that data once uploaded. The weakest link, he concluded, is less likely to be the cloud service itself (if a major brand has been chosen) – but the corporate route to it and the users involved. In any case, our interviewee encourages his customer agents to interact with SMEs to enable them to review their real, as opposed to imagined, level of cyber-security and to empower them with the right questions to ask to the vendors of, say, cloud solutions.

An additional complication was also raised. As SMEs struggle, perhaps, with legacy IT systems where there is limited storage space – despite Information Security and other policies being in place, individuals or groups may choose to use commercial cloud services as a workaround to clunky, slow or impossible to use IT infrastructure. The SME (at owner or director level) may not realise it yet, but *it may already be dependent on cloud services and may already have been exploited through insecure links between the enterprise and the cloud*. Former employees, stakeholders (such as contractors) those with network privileges and others may also retain access to the cloud and may be using corporate and non-corporate devices to access it.

Given that all of these activities operate outwith the policy of the company and that there is unlikely to be any activity monitoring to detect unusual behaviour – we would suggest that it is not an exaggeration to state that the lifeblood of the SME is now critically exposed.

UNTETHERING + FLEXIBLE WORKING = CAN COMPROMISE SECURITY

Aware of the increase in the sale and use of hybrid notebooks, our interviewee indicated that a major human factor problem that is emerging in SME cyber security is the blurring between home / office security psychology. Business activities are likely to be conducted through – for convenience –notebooks, even if this is not permitted. Equally, the leisure use of business notebooks could expose the user to technical and human attacks. The transformation away from desktop computing to ‘bring your own device’ (or, the authors might add, ‘hack your own device or cloud service to enable easier work’) computing is laced with complications. Users may have the best intentions at heart – more efficient working – but the collateral effects could be horrific.

Whilst USB ports can be blocked and other technical measures implemented, the use of apps on - or cloud services to circumvent forced use of - business machines and their security

protocols and counter-measures means that the focus of attention and responsibility shifts to humans as the centre of gravity of (in)security.

Pre-sales organisations can, then, provide SME customers with the wake-up call that they should look for evidence that unauthorised cloud services have been implemented and then provide the software and hardware means to mitigate the damage and prevent further risk exposure. These re-sellers can also help clarify what SMEs are protected against through, for example, the investments they have made in solutions (e.g. firewalls) and insurance (e.g. that data integrity cover may well be invalidated by actions taken by users to date).

NOT ALL RESELLERS ARE EQUAL

The authors were profoundly struck by the ethical care taken by this reseller and his team of around thirty pre-sales agents to find out more about SME customers and work with them to mutual best interest. Obviously, the reseller wishes – ultimately – to sell equipment, software and (a new offering) consultancy and there is, for SMEs, the helpful role of pre-sales to help educate them in terms of their security exposure, engage with their assumptions and support them in preparing for emerging challenges.

There is a danger for less scrupulous resellers to be motivated primarily by short term sales revenue. The SME customers of *this* reseller are fortunate that they are safe from such exploitation – others will not be so lucky. Customers, as we have seen can easily become bamboozled by the extensive options available to create an unaffordable but robust system of security that would be comparable to a much larger company's solution. It is abundantly clear from the interview that the training given within the presales team is ethically directed towards selling solutions to meet the customers' needs- without attempting to sell the vast range of options on the market. This is extremely important in building the trust of SME organisations to make the investment required (and no more) to meet their risk appetite

The authors were impressed by the fact that our interviewee was committed to building a pre- and sales force that coached SME customers towards immunity to the promises of security confidence tricksters and unscrupulous sales agents. The re-seller is also proactively educating customers about some of the emerging risks that lie ahead. A specific example referred to was the use of power lines for data communication: against something which, on the face of it, offers considerable benefits but that requires a very rounded appreciation of deeply technical threats and very attractive cost-saving opportunities.

CONCLUSION

Pre-sales contacts within resellers such as the employer of our interviewee are perhaps uniquely placed to raise and / or respond to cyber-security concerns of SMEs. It is accepted wisdom that the multiplicity of advice provided by government, trade bodies, insurers, the media, consultancies and others amounts to a cacophony that no SME could be expected to extract signal from noise, de-crypt it and then understand exactly what they ought to do in their operational context.

Driven by frugality – and inspired by the cost savings and efficiency benefits that can flow from emerging and established technologies such as cloud computing and the 'Internet of Things' – SMEs are unwittingly exposing themselves to new risks, neglecting established ones (e.g. the insider) and making investments based on patchy understandings of the threat surface or deliberately false claims of unscrupulous vendors.

Pre-sales companies can – when underpinned by an ethical code which mitigates against 'sales for sales sake' – perform a vital role in building on a trusted relationship with a customer to advise on their current status, raise awareness about risks that may have been overlooked or generated and enable a pragmatic, confidential 'balance of investment' solution.

Although the authors regard themselves as relatively well-sighted on current and emerging trends in cyber-security, we both learned a considerable amount from our interviewee. At the nexus between advanced insight into emerging technologies and trends and the current state of implementation and behaviour in the SME customer base, he provided us with a unique assessment of a gulf between best practice and actual practice in the real world. The re-seller has detected a major change with SMEs who increasingly see security as a matter of pro-active rather than a re-active concern. This is a heartening move which, as well as a business opportunity for re-sellers and others, indicates that there is a good prospect that many of those SME enterprises that comprise the core of the economy could well be resilient to, and sustainable against, current and future technical and socio-technical cyber threats and risks.

ACKNOWLEDGEMENT

Both authors would like to formally record our appreciation to our anonymous interviewee for their generosity in terms of time and analysis.

REFERENCES

Burns, S, (2016) Data AWOL? Thank God for backup. You backed up, right? (2015), *The Register*, available at: http://www.theregister.co.uk/2015/06/18/missing_data_backups_crisis/ (accessed on 28 June 2016)

Christensen, SR, Schkade, LL, and Smith, A, (1998) *Financial and functional impacts of computer outages on businesses*, Center for Research on Information Systems, The University of Texas at Arlington.

European Commission, (2015) *What is an SME?*, available at http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition/index_en.htm (accessed on 23 June 2016).