MANAGING CYBERSECURITY RISK

CASE STUDIES AND SOLUTIONS

EDITED BY

JONATHAN REUVID

PA
AXELOS GLOBAL BEST PRACTICE
PGI

1.6 IF SMES ARE THE LIFE BLOOD OF THE BRITISH ECONOMY, WE'VE CUT AN ARTERY

Brian Lord, PGI Group

THE BRITISH CYBER SECURITY SYSTEM SIMPLY DOESN'T HELP SMES

The most frustrating, patronising, and ill-informed regular comment that emerges whenever a group of cyber security consultants and practitioners are put together is: "… companies have to understand that cyber security is a business enabler…".

Sigh. To every business, of any size, cyber security is an overhead; just like other security risks, it has always been an overhead, and it will always be an overhead. And to every business person there is a single rule regarding overheads. Keep them as low as you possibly can. Start at £0.00 and build upwards – only accepting the absolute essential after heavy scrutiny.

And before those cyber security experts throw their hands up in horror and bemoan how that is because "they don't really understand the risk or threat…", I can safely say that most DO understand the threat – at a headline level at least. Cyber security specialists care passionately about their area of expertise: it is the most important risk in their lives. Business owners simply care about it alongside all the other risks inherent in running a business, many of which have a greater proximity and risk of damage. It doesn't make it unimportant, it simply takes its place alongside other risks.

This overhead rule applies to all businesses, but to Small and Medium Enterprises (SMEs), it is often the difference between business success and failure. The reason SMEs don't buy cyber security services is not because they aren't aware of the threat or risk, it is because there is no clarity whatsoever over what they actually need to protect them from the specific risk they face. Moreover, the price tag that comes with whatever services they actually do try to pursue is so eye-wateringly expensive it puts them beyond reach.

Many SMEs often carry on trading and operating unprotected because so few organisations are prepared to help deliver them what they need, in the form they need, at a price they need. This of course significantly undermines the admirable UK Government's aspiration to make the UK 'the safest place in the world to do business'. But perhaps more significantly, it continues to facilitate an opportunistic and mass criminal free-for-all which dilutes and distracts the ability and capacity of limited national law enforcement and intelligence resources to counter what is an evolving and mutating threat. We are still some way away from a UK where "petty" cyber theft has become just too difficult to carry out at scale, and thus allows national resources to be focussed on the deeper more malevolent criminals and threat actors. And we are probably about three years behind where we should be at this point.

So, where and how does this square become circled? Let's look at the four corners of those who can help. Firstly, the Government (in the form of the National Cyber Security Centre [NCSC] and other government bodies), who still struggle to understand the world of the SME. Secondly, the cyber security industry, who still prefer to keep their nose in the trough, only serving those who can pay the preposterous prices they charge and doing everything possible to preserve the status quo. Thirdly, the large corporate industry, who can reduce their own risk from a supply chain of SMEs and an SME client base, through facilitating and supporting measures. Finally, there are the SMEs themselves whose cyber security stasis simply cannot continue.

GOVERNMENT

The NCSC, now a year old, has a department dedicated to the SME market. Just last month, they launched the hugely digestible *Small Business Guide to Cyber Security*, aimed at giving straightforward advice to SMEs as to how they should address the threat in a way that made sense and was affordable to them. It is clear, it is concise, but still focusses on technical controls and it is very unlikely that most SMEs will be able to implement the measures suggested without some alternative help and advice (back to the affordability again). And if we consider beyond the technical controls to the primary vulnerability of the human, it was only in May this year that Joe Siegrist, the VP of Last Pass, called upon the NCSC to produce some education for small businesses, and there still remains a large gap in education (rather than availability of information) that needs to be promulgated and made available to SMEs. The point being is it wouldn't take too much of the £1.9 billion allocated to the National Cyber Security Programme (certainly no more than 1%) to make cyber security education available to the 99.3% (2016 figures) of all UK businesses, who produce 47% of the UK private sector turnover. (Federation of Small Businesses, 2017).

But these measures are destined to stay in the realm of facilitation, rather than intervention. So where else can the UK Government adopt a policy approach that

reflects the realities of the SME world, where the rules and considerations are different to public sector organisations and large industry?

Government standards, certification and accreditations continue to emerge out of the NCSC (previously CESG) with the laudable intent of providing something against which the private sector can measure what is good when they buy or assume protective measures and services. However, there appears to be an inability to differentiate what really is the skill level and certification standard necessary to measure service levels to a large complex organisation and that are required by the majority of SMEs. 'Gold Standard' or not, obtaining these certifications and accreditations continues to be hugely bureaucratic and very expensive for service deliverers to obtain and sustain. As we will see (below), these organisations need no excuse to justify extraordinarily high prices.

We recognise that it requires high-end and complex skills and knowledge to protect parts of the Critical National Infrastructure, and so means of certifying these to a reassuringly high level are right. But what is lacking is a set of routine, affordable service benchmarks which help an SME determine the difference between 'cowboy' and 'competent' and measure what:

(a) is good enough to protect them;

(b) assures their insurer that responsible judgements have been made (because, yes, insurance is the primary mitigation measure);

and

(c) demonstrates to the ICO, should the worst case scenario happen, that they took reasonable and informed measures to meet their legal and regulatory responsibilities.

If the SME department of the NCSC achieves anything in the coming year, it would be to drive a coach and horses through the self-licking certification and accreditation lollipop and set some affordable standards for services and training to SMEs. This would take a massive step forward in defining and creating an affordable envelope for SME cyber security standards.

The NCSC is a force for good, but needs help in understanding exactly what drives an SME's decision making.

THE CYBER SECURITY INDUSTRY

Ever since 1999 and the Y2K cash cow, the IT security/information security/cyber security industry has rubbed its hands, over-complicated and over-teched the risk and threat, bought the national supply of mirrors and smoke and proceeded to try to create

a fear culture that has simply served to produce a stasis and drag on proportionate adoption and normalisation of measures. And along the way led CESG by the nose in the co-creation of a cyber world of over-complicated standards, skills, service levels and faux-qualification hierarchies.

The argument put forward is that there are too few qualified people to meet the national demand for skills and certification. Basic economics lays out the straightforward concept of supply and demand on cost and sale. The skills and certification levels are co-created by the Government, who have an altruistic reason to make the nation safe, and an IT/cyber security industry who want to make a lot of money. When it comes to protecting critical infrastructure and organisations against whom there is a multi-layered threat, it is quite right that standards are very high and, as in all professions, the highest skills demand the highest prices.

But SMEs look on and wonder why they seem to have to pay a doctor or a surgeon to deal with a cut finger, or help avoid catching flu. The information (and the pricing point) available seems not to differentiate much between the equivalent of a First Aider, a St John's Ambulance Officer, a Nurse, a GP, a Senior House Officer, a Registrar, a Surgeon and a Consultant. And there is no benefit to industry in explaining there could be a difference. Not being able to afford it, the SMEs go away with no idea how to stop catching flu and their finger's still cut. And of course, many catch flu and their fingers go septic and have to return to a smug "I told you so" doctor and surgeon. Q.E.D.

But it seems there should be no real downside to creating a more dynamic and flexible approach to these issues in a way that helps an SME afford to counter what is a persistent 21st century threat. Well, inevitably there is a risk that the very large multi-national companies and CNI providers, who do pay top dollar, will then realise that not ALL their cyber security risks need to be dealt with at the same level and could readjust downwards accordingly.

One of the leading organisations trying to supply affordable services to SMEs, the London Digital Security Centre (LDSC), has a number of service delivery partners. However, with the honourable exception of Sophos and Symantec (since the AV vendors matured and grew out of scaremongering pricing several years ago), the number of major providers of cyber security products, consultancy and services are noticeable by their absence.

In October this year the LDSC took themselves to Birmingham to demonstrate the model and provide the same type of help they routinely offer to London SMEs. The issue remains not one of just providing information – but one of implementing practical solutions, including training that allows SMEs to protect themselves in an affordable, continuous and sustainable way.

Development of automated services, including on-line training, testing, protection, certification, maturity modelling and online Information Security Management Systems remains the end-state for the bulk of the SME market. And it is only when the

industry service providers can branch out from rarefied gold-plated selling and apply a pragmatic solution to a basic model, with appropriate, proportionate and affordable kite-marking, delivered through an annuity revenue approach, will the SME market really be able to protect itself... And the ability to reach a market of that scale needs to be through an increased national number of public and private bodies, such as the LDSC, in which the large service providers will play properly, at the right price, with staff at the right level of skills to conduct the level of work required.

With the right model, within three years the not-for-profit nature of such bodies would have developed a cultural change within both the providers and the SME market to become a largely privately funded body, able to release the public funds back into public services. This is not altruism, it is a hard, commercial fact – there is an untapped market in annuitised, online solutions, like all services that help manage risk for SMEs. A solution of this type remains the only viable solution, but it is a solution that can be extremely profitable to those who deliver and affordable to those who buy. It just requires industry noses to be lifted out of a shallow trough, in which the food is rapidly going stale.

WIDER INDUSTRY

One of the most enlightening afternoons I have had recently, was when we invited a number of large industry partners to our offices and Cyber Academy. These partners were those who recruited their own cyber security professionals, either to work internally on their own corporate protection or those who could deliver services for others. The purpose was to launch our skills conversion programme through which they could recruit new members of staff who would become operationally viable (i.e. deliver independent cyber security capability) within 10 weeks. Not the "gold standard" (see below) but the basic, more procedural, systemic implementation that is an inherent part of any security process or compliance based service delivery.

As we wheeled out our own staff who had gone through our own similar internal programme, and were already delivering cyber security effect, the scales fell and the disbelief was suspended as it became hugely apparent to them that the cheque book recruitment they had hitherto been undertaking was not wholly necessary, and there were cheaper more effective routes through which the skills shortage could be addressed.

It doesn't just make obvious commercial sense for the companies concerned, but it also halts a strand of cheque book recruitment, which creates disproportionately high salaries which are passed on to the clients, place it out of reach of the SME market and limit the corporate willingness to build cheaper, more annuitised services, as described above.

And from another angle, as wider industry looks, as it should, at where and how different levels of service standard should be applied to different parts of the business

(i.e. where do they need a brain surgeon and where do they need a nurse), it becomes apparent that some of the swifter, cheaper, even annuitised models may be applicable to them in some part. It therefore becomes in their interest to ensure the development (and price) of such capability moves on apace.

So large corporate industry needs to look at how and where CSR and marketing budgets are currently being deployed in the cyber spaces, because, adopted smartly it will provide a return not only in profile and reputation, but it will massively reduce their own recruitment and service delivery costs, and take a major step towards influencing the speed at which their SME supply chain adopts sensible security measures that protect their own corporate assets and liabilities.

SMES THEMSELVES

While it remains absolutely imperative that the levels of service and solutions available to SMEs are proportionate and in line with the culture and business processes in the SME world, it is also not feasible to perpetuate the existing inertia in the SME world around protecting online assets and capability. The threat is inherent in the adoption of modern technologies which allow businesses to thrive in the 21st century. Now is the time to engage, both collectively and individually. The NCSC SME department, perhaps more than any other area of the organisation, depends upon input and engagement from those they seek to serve. Without it, they will get it wrong – not out of incompetence, but because they don't have the knowledge they seek for initiatives to work in the SME environment.

Engage in the bodies being set up, often with the help of the local police force, such as the LDSC, and take advantage of the services and support offered.

Be demanding from the cyber security industry. Collectively, through trade bodies, local business communities and other vehicles, challenge the pricing offered and demand more automated innovative solutions. Half an expensive solution is no solution at all.

It is a world in which SMEs will have to play, and only SMEs can really make the case for rules that work, because the rules of the game now aren't sustainable.

CONCLUSION

The current world of cyber security is not geared for SMEs. As already mentioned, the UK Government is investing 1.9 billion GBP into cyber security. (Osbourne, 2015). SMEs represent 99.3% of the private sector and generate 45% of the nation's private sector turnover at 1.8 trillion pounds. (Federation of Small Businesses, 2017). A comparatively small proportion of investment can secure a comparatively high proportion of UK economic interest.

The Government's aspiration can be met; the cyber security industry can thrive,

larger industry can be better protected for less, and the SMEs themselves can have the levels of protection needed in the 21st century. All it needs is for the UK Government to be slightly more SME sensitive, the cyber security industry to work for its returns, wider industry to challenge the status quo and SMEs to understand how to make it all work for them. Because it isn't at the moment.

REFERENCE LIST

Federation of Small Businesses. (2017) *UK Small Business Statistics*. Available at: http://www.fsb.org.uk/media-centre/small-business-statistics (Accessed: 28 November 2017).

Osbourne, G. (2015) *Chancellor's Speech to GCHQ on Cyber Security*. Available at: https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security (Accessed: 28 November 2017).