The Costs of Cyber Security

The Economic Argument for Information Security

A White Paper from:

Chris Cope MA, CISM, CISSP, MInstISP,

Senior CESG Certified Professional, PCBCM,

ISO27001 Lead Auditor

Security Consultant

Advent IM Ltd

Introduction

The Economic Argument for Information Security

How can you justify expenditure on something that hasn't happened? Ultimately, this is the management dilemma of security specialists across a range of organisations, and for the executives who are responsible for finding the money. Whilst security professionals will advance the benefits of improvements within their business area, the executives are left balancing the needs of the security team with those from other areas and financial constraints. Is there any point in developing world class security controls when the business is about to fail due to a lack of investment in Research & Development? Clearly not.

The modern polemic is cyber security; it is either going to radically undermine ecommerce and society, or its effects will be minimal. It's probably fair to suggest that most observers will hold positions somewhere in between those two extremes, yet when even experienced professionals struggle to determine the actual risks, what hope does the executive have and why should that investment be made?

I am going to argue three main points in this paper. First of all, the impacts of cybercrime can be highly significant, even if they don't happen to all organisations on a daily business. Secondly, the myth that cyber security is a hugely expensive technical domain will be challenged. And finally, I will address the point that good cyber security can be good for business. I don't intend to cover legal compliance; those areas where effective cyber security are a requirement, i.e. data protection and government contracts, are widely commented on. Rather, I intend to focus on why investment in information security makes good economic sense for you.

The Economic Argument for Information Security

The impact of cybercrime will clearly differ according to the organisation. Losses that would cripple a small to medium enterprise (SME) would hardly register on a huge multi-national. Yet whilst a larger organisation may be more resilient, they may equally face a higher degree of risk as they are seen as more of a target. For an example of the impact on a large business, look at TalkTalk.

When the TalkTalk hack broke into the headlines in 2015, it was one of several major cyber security news stories, many of which involved telecommunications. There is not the room here for a detailed analysis of the methodology used by the attackers, yet as the story unfolded it became clear that customer data in the care of TalkTalk had been compromised. Initial estimations of the scale of the loss were soon reduced, although just over 4% of TalkTalk's customers were compromised[1].

Quite unsurprisingly, this was referred to the Information Commissioners Office (ICO) and, after investigation, a fine of £400,000 was levied[2]. Yet whilst at the high end of the current range of sanctions available to the ICO, that was by no means the end of the financial impact for the company. TalkTalk lost over 100,000 customers[3] and saw a drop in share price of 30%[4], with growth slowing to 1.8%, compared to 4.2% prior to the attack[5]. In total, costs from the attack were assessed to be in excess of £60million[6]. It could have been worse. Under soon to be enforced EU data protection legislation the fine could have been in the region of £70m[7], up to 5% of company revenue. Even a major international company would have struggled to absorb losses of that nature.

Smaller companies may not suffer attacks of this nature, but they can be equally devastating. Ransomware attacks can result in bribes of several thousand pounds being demanded, yet the loss of operability may be significantly more expensive. Another common attack is where cyber criminals may exploit poor authentication methods to deceive customers. Again the costs can be significant against a smaller company.

---

[1] 20 May 2016 'Why TalkTalk's relatively minor cyber attack cost it £42 million', *Management Today* [Online],

[2] 5 Oct 2016, 'TalkTalk gets record £400000 fine for failing to prevent October 2015 attack', *ICO*, [Online], https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/

[3] Farrell S, 'TalkTalk counts cost of cyber-attack', The Guardian [Online], 2 Feb 2016

[4] Lewin J, 'Cyber attack cost TalkTalk up to £60m and 101k customers', Financial Times [Online], 2 Feb 2016

[5] Ibid

[6] Ibid

[7] Decision Marketing, 'TalkTalk could have faced £70m fine under GDPR', decisionmarkering.co.uk [Online], 6 Oct 2016.

If deliberate attacks were not enough, consider the potential costs of an accidental loss of IT services, or information. What is the impact on your company's reputation if you are unable to fulfil customer expectations for several days? What is the impact of a deliberate or accidental incident on your reputation?

For any organisation that relies on IT, an incident involving systems will clearly have an impact. The key, however, to reducing either the impact of the incident, or the potential for it occurring in the first place, is not to spend significant amounts of money on technology, but to assess the risks properly. If your potential exposure to a cyber incident is high then you will probably want to spend more on mitigating those particular risks. Yet, whilst fancy technology can be a solution to some risks, there are two major points to be made about technical security controls. Firstly, they do not counter all of the risks; a holistic defence in depth approach is needed for best effect. Most importantly of all, security controls are hugely undermined by poor governance.

No matter how well established security controls are (be they technical, physical or procedural) they must be supported by good governance within the organisation where security is seen as a legitimate business activity and given the attention it deserves. This also means holding the security staff to account – are they delivering against the key objective of protecting the organisation? Are the risks against the organisation understood and assessed? Without a robust risk assessment, you may be spending too little in combatting key risks, or even too much. Just because attacks of a certain nature happen to other organisations, this does not mean they will happen to you.

Some reading this will probably think that this is irrelevant as they use a service provider for their IT, yet don't forget that whilst the service provider should be providing a good level of security, the information remains yours. You still need to be assured that your information is being protected in a competent manner.

It's also crucial to remember that one size does not fit all. ISO27001 is growing in popularity as a global information security standard. Yet this approach may not suit a small organisation. If that is the case, then Cyber Essentials may provide a better platform for managing your information security. A look at the 10 principles of Cyber Essentials demonstrates that it does not take huge sums of money to implement; there genuinely is a solution out there for all budgets.

So can effective security be good for business? Well on the one hand, not suffering £60 million losses due to a cyber-attack is an obvious bonus, but what of the less dramatic examples? The hardest quantifiable in a risk assessment are risks against an organisation's reputation. How many potential customers are dissuaded from taking up your services due to an attack? Yet, how many can be persuaded to become new customers if your organisation appears to be taking its security obligations seriously? When buying a product, does the presence of the BSI Kite Mark reassure you? If there is a choice between 2 products, could the Kite Mark be the deciding factor? Perhaps it's time for security certifications like ISO27001 or Cyber Essentials to be viewed in the

same way. Putting a logo on your correspondence and website could be enough to reassure potential customers, yet a greater effort in highlighting how seriously your organisation takes security will potentially reap far greater rewards. After all, the risks from cyber-attack, even if often misunderstood, are frequently newsworthy and the growing sense of customer unease in how their information and transactions are managed must be a concern. A further consideration must surely be the potential for government direction. Slovakia is in the process of drafting cyber security legislation for critical business areas, whilst the US is about to debate a bill which will force companies to disclose their cyber security expertise and governance. If the continued assault on ecommerce within the UK does not relent, will the UK government look to legislation to plug the gap rather than risk damaging a key commercial area? It may be better for the private sector to grasp the mantle themselves rather than wait for legislation to be imposed.

If you belong to an organisation where there is absolutely no use of IT whatsoever, then hopefully you have found this to be of some academic interest. For everyone else, ie the majority of British companies who are increasingly reliant on IT to some degree, then adopting an effective program of information security is a key business requirement. That program does not have to involve highly expensive technology, nor an army of staff and consultants, but it does need to be appropriate to you and your organisation. With some careful marketing, your investment in information security need not be seen as a financial drain; it can be turned into a business benefit for you.

Executive Summary

- Cyber-crime poses a real threat to the UK private sector,
- Mitigating the risks from cyber-crime do not have to involve significant amounts of money,
- Promoting good cyber-security within your business can be a positive and boost customer assurance,
- If companies do not grasp the opportunity, governments may legislate and force compliance with standards.

advent-im.co.uk

0121 559 6699

0207 100 1124

@Advent_IM

bestpractice@advent-im.co.uk