IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

Getting Your Security Budget Right

Alastair Hartrup

Alastair Hartrup
Founder and
Global CEO
Network Critical

Biography

Alastair Hartrup is the Founder and Global CEO of network security experts, Network Critical (https://www.networkcritical.com).

Founded in 1997, Network Critical has been providing high-quality Network TAPs and Network Packet Brokers.

CEO and founder Alastair Hartrup has been at the helm since its foundation and under his leadership the company has grown from zero to a global multinational business.

Alastair blogs at https://www.networkcritical.com/blog

Keywords Cybersecurity, Budget, Planning, Ransomware, Information technology (IT), Packet brookers
Paper type Research

Abstract

For many technology organizations, seeing headlines on a daily basis with reports of data breaches and cyberattacks from all corners of the globe is highlighting the need to ensure they are protected. Boardrooms and executive management are more aware of the need for effective cybersecurity today than they ever have been. This awareness may be driving action as organizations look at frameworks for guidance on building effective security programs, but as the author of this article explains, many companies now need to ensure that the right budget is set aside to undergo the task.

Introduction

We know that a strict security regime, rigorous employee training and sound accounting policies can help prevent costly attacks. Yet, it is surprising how few companies are deploying robust cyber security mitigation and remediation processes. One big reason for this lack of security diligence is the difficulty in justifying the expense.

According to the *2018 Hiscox Cyber Readiness Report*[1], most businesses lack cyber-expertise to prevent attacks. The reason for this is first, a lack of investment in streamlined technologies and secondly, a shortage of talent is both barriers to fine-tuning data security programs.

The budget justification question for IT security is difficult to answer. How much is saved by not getting hacked? Well, if an event does not occur, it cannot be


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

quantified. However, we can look at instances where companies with lax security policies that have been successfully attacked and extrapolate potential liability from their experiences.

According to the same report[1], the average cost of cyber-crime across the globe, amassing all incidents, to each business over the past year was £250,000. Behind this number masks some wide variations to businesses on the different scales. For the largest organizations in the report (those with 1,000-plus employees), the average costs ranged between £394,000 in Spain and £1.4 million in the US. Some organizations faced still higher costs – here in the UK and our neighbours Germany the cost was £25 million.

A study Ponemon Institute's *2017 Cost of Data Breach Study: Global Overview*[2], highlighted regulated industries such as healthcare, education and financial organization suffer higher data breaches.

Last year, the WannaCry ransomware cryptoworm was one of the biggest cyber-attacks in the UK. The worldwide attack happened in May and targeted computers that were running Microsoft Windows OS by encrypting the data and demanding ransom payments in Bitcoin cryptocurrency. In the UK the most damaged business by WannaCry was the NHS, with over 80 practices in England alone being taking down. This resulted in almost 20,000 cancelled appointments, 600 GP surgeries having to abandon the use of their computers and five hospitals that could not accept any more patients due to the influx of emergency cases.

So, when a CFO asks what benefit network security and training can be brought to the company, it is the CIOs that oversees the accessibility, confidentiality and integrity of files and systems. Therefore, CIOs are responsible for securing and allocating budget.

Here are a couple of key components to ensure your security budget provides best practice for your business.

- **Understand your current systems** – We recommend you consider investing in a full risk assessment, which includes vulnerability scans and an in-depth penetration tests. Working with a reputable information security firm with proven business acumen will provide a stake-holder readiness report as well as a remediation plan from which you can derive budget numbers.

- **Understand regulatory bodies and compliance requirements** – Many regulatory requirements, such as PCI, HIPAA, and the soon-to-be introduced GDPR pose a very real threat to the company bottom line in the form of fines. These regulations require data security implementations, regular penetration tests and system monitoring. Failure to comply can also lead to heavy fines and damage to brand.

- **Align your plan with the CFO's vision** – Since IT purchases can be costly, big time technology spending in one quarter versus another can mean the difference between a good year and a bad year for the entire company. I

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

recommend aligning spending with the CFO and the calendar. Purchasing on a relatively even scale throughout the year makes forecasting easier for the CFO and limits any year-end surprises that may come about from overruns or unplanned purchases

In conclusion

Once budgets tend to get to the finalized stage it is also important to include access and visibility to the initial budget and plan. Taps and Packet Brokers are critical components providing the necessary security appliance connectivity and accurate visibility to network traffic. These relatively low-cost devices can actually save money overall by being able to combine traffic from multiple links and reduce the number of high cost security appliances that need to be deployed.

Taps and packet brokers can help keep your budget in line without compromising the protection provided by security appliances. They can also provide the scale necessary to grow without going off-budget. In both budgeting and design, diligent planning and disciplined execution can save, not cost.

Reference

1 https://www.hiscox.co.uk/cyberreadiness
2 https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN