Security Spend – How much is enough?

Some of the best leaders I've met actively seek knowledge and insights to help inform decisions. They also like to make comparisons with others in the same market or of a similar size to bring relevant context to their decision making. When they consider how much should be budgeted for IT security the same applies and I am frequently asked how much is enough, how much do competitors spend and where do they spend it. These seem quite straightforward questions because much research has been published on the subject however things are a rarely as simple as the one size fits all ratios that float around.

In this article I have included some commonly reported figures as a broad guide, however I've also introduced a few discussion points that highlight how comparative figures alone might not be the best measure when determining security budgets.

How much do your competitors spend and where?

Information security spend is often expressed as a percentage of an organisations IT budget and varies according to who you ask and what sector you are in. However, figures between 4% and 7% of IT spend are frequently quoted. These figures are only meaningful if you understand what the spend is on and how much the IT budget is.

IT budgets currently sit at around 2.5% of an organisations revenue with approximately 70% of the annual budget being attributed to operational rather than capital expenditure. As for where the budget is been spent, it can broadly be thought of as hardware (18%), software (18%), the cost of employing and housing IT teams (40%) and outsourced consultancy, cloud services and connectivity (24%).

How much is enough?

Although we know an average spend to be between 4% and 7% of an organisations IT Budget, this isn't a guarantee of adequacy. Consider the following scenarios where it might be appropriate to spend more than the average.

- You are at the start of an IT improvement journey or have under invested in IT security over many years
- You have a low threshold for risk and want to adopt a best of breed security posture
- You operate in a heavily regulated market and regardless of your appetite, you are obligated to do more than the average
- A large percentage of your income is derived by a small number of high value clients and their expectation or your contracted obligation requires higher levels of security than other customers
- You operate in a sector where a security breach could impact lives

- You are involved in merger and acquisition activity and cannot afford an incident at any cost
- Your clients are unlikely to be forgiving of an incident
- Your organisation is likely to attract a higher number of motivated attackers because of its activities

A further consideration in the suitability of the 4% – 7% spend is whether emerging attacks methods will demand a higher level of investment to prevent. For example, over the last few years there has been a steady increase in denial of service and social engineering attacks. Denial of Service attacks have been met with the adoption of new cloud-based defence services and social engineering attacks have been met with the wider adoption of outsourced phishing and vishing exercises. I doubt these new costs have been met with cost savings in other areas.

So, if the IT and security spend figures can only be used as a guide and may not be an entirely guaranteed figure, how do you arrive at the right figure? In earlier articles I talked about the benefit of understanding what you are protecting by conducting a risk assessment. A good risk assessment will consider a range of items including, appetite, regulation, attackers and attack vectors, current controls maturity and the impact and likelihood of an incident. With this information, it is possible to identify your security controls and furthermore map the daily, weekly, monthly and annual IT & Security activities that will need to be undertaken. Using this information, it will be possible to identify your unique requirements for security or at least understand the variations to the ‘average’ and allow extras. In my experience of heavily regulated sectors and heavy technology providers, the extras can double the average spend of other sectors.

So in answer to the original question – ‘how much is enough’ I can only suggest ‘ it depends on the size of the risk and your appetite towards it, both of which should be determined through a formal assessment.

If you are happy to apply averages then my best estimate would be 5 – 7% of IT spend unless special circumstances apply (see bullet list), at which point a figure of 12-14% might be appropriate. – remember though, without undertaking an assessment of risk, you may still be unclear about how best to direct that spend.

Want to understand more about this subject ? Get in touch at info@cortida.com