

CYBER SECURITY

---

# Buy in From the Board



## The challenges of convincing your organisation to invest in cyber security

**At some point most companies will invest in cyber security to ensure that their business does not fall victim to a cyber-attack. For some organisations this is mandatory to abide by government regulations, however for others it is because preparing and protecting their business before a hack is a cost-effective time-saving solution.**

For many organisations the journey into purchasing cyber security solutions is often met with objections and blockers before it even begins. There are unfortunately a lot of reasons for this but usually it's due to a lack of understanding of the benefits that a complete security posture can provide to an organisation.

In many cases, senior stakeholders in an organisation may not understand the direct business return that a cyber security program can provide. Shareholders and stakeholders in your business probably find it hard to quantify a return on investment when spending on cyber security. However, with ransomware and phishing attacks on the rise and multiple

reports of high profile breaches, even CEOs are beginning to recognise that their business must continuously focus on cyber risks to protect assets and customers.

It can be hard to explain why your organisation should invest if there is no obvious return and the company is unaware of its vulnerabilities - meaning the budget is not approved and your organisation remains exposed to security threats.

When considering an organisation's security, improvements are usually driven by the IT department and improving the technology stack. Alternatively, senior management, including the CIO are usually focused on company growth and revenue objectives. There is often a lack of communication between the departments, leading to cyber security being overlooked. But it's not just the CIO or CISO who should be championing cyber security in the organisation. To prevent such an important aspect of the business's growth ability being overlooked, a top-down approach will bring IT and management together so communication flows and budgets can be allocated accordingly. This is the only way to build a true security first culture throughout the organisation.

Both the technical teams and business stakeholders speak their own language - and do not always understand each other. To mitigate this issue technical teams and stakeholders need a common language which is accessible and understandable to both, this will enable clear informed decisions to be made.

### **Risk = Threat \* Vulnerability**

Risk is the common language which will bring the business and technology together. Risk is only present if there are two other factors; these are threat and vulnerability. Any reduction in either threat or vulnerability is a direct reduction of risk and increase in protection for your business. Risk is the possibility of a threat that exploits a vulnerability to cause damage to the business. The more likely a threat will occur, the greater the risk.

The primary objective of a cyber security program is to reduce your risk by identifying and mitigating vulnerabilities and blocking any threats.

## How to approach your stakeholders

**Approaching the board and stakeholders of your organisation to secure cyber security budget can be a daunting subject. A good avenue is to tackle the most obvious blocker head-on.**

The expense of cyber security is usually the leading objection when convincing stakeholders to buy into the idea of securing their organisation, as the outward cost often outweighs the risk of being breached. Directly approaching the issue is often the best way to convince the board to take cyber security seriously.

Explain that cyber security is a cost-effective way to implement a proactive approach to protecting your organisation, which would save you money over the expenses required to repair the damage caused by a cyber related incident where financial losses can be quantifiable. A breach can cause a drop in share price, fines, legal expenses, increased insurance premiums, loss of contracts, and much more.

However, some financial impacts cannot be quantified, and an exact monetary value is hard to determine. The economic impact a hack could have on your organisation is far reaching and instrumental as a persuasive argument you can use with your board or stakeholders in favour of a cyber security program. The reputational damage could make customers and partners less likely to want to purchase your products or services or be associated with your brand in the future.

There have been studies conducted to help to provide some insight as to what an appropriate cyber budget would be. The research conducted by Deloitte and the Financial Services Information Sharing and Analysis Centre discovered that around 10% of IT budgets were dedicated to cyber security, with an average spend per employee between £1000 and £3000.

These figures are not set in stone, and an appropriate budget for one company is just not the same for another. These figures illustrate a benchmark when implementing a defence-in-depth cyber security program that focuses on people, process, and technology.

The challenge that technical leaders face is that it's often hard to quantify the return on investment when spending on cyber security. Cyber security ROI is not always easy to understand and can challenge the company's status quo.

Businesses are looking for any expenditures to bring in a return, which of course is fundamental for a business to succeed. However, communicating the risk factor of a cyber security attack in a risk-based approach will help place a monetary value on the financial impact caused if this risk were exploited. If senior leaders in your organisation do not understand the benefit or return of cyber security, the often expensive spend is not approved.



**10%**  
of IT budgets were  
dedicated to cyber  
security, with an  
average spend per  
employee between  
**£1K-£3K**





## The Sliding Doors Moment

Let's imagine that a company invests in new technology to support the improvement of business processes.

This investment has been attributed to a direct return on increased efficiency and bottom-line revenue. Senior stakeholders can see the financial benefit to the business and attribute a clear ROI.

Now let's accelerate five years into the future, where the organisation has made the decision not to make investments into cyber security – well, everything is working well so why would they waste budget.

The system that has been implemented has had a lack of support over the last 5 years. While the system is working well, this is a long time in the world of technology. Without the support and patching that should have been deployed, the system has introduced many vulnerabilities. The technology team are aware of these. They've explained that it would require a £120,000 investment to remove these vulnerabilities. Unfortunately, the vulnerabilities and their potential impact are not fully understood at a senior level, so the budget needed to mitigate these was not seen as a priority, they cannot attribute an ROI to this


investment, and therefore it was not approved.

This seemingly inconsequential moment can drastically alter the trajectory of future events.

Unfortunately, the system vulnerabilities have caught the attention of a hacker. The Hacker has exploited the vulnerability and has uncovered that they can shut down the entire business. The Hacker demands a large ransom payment before allowing the business to operate again, and has ultimately ground the company to a complete stop.

The cost of a security breach is enormous. It will cost in the millions to get the system back online. The losses will include a combination of downtime, employees not able to work, violation of service level agreements, contract termination, specialist cyber consultants, drop in share price and more. Once the business is back in full operation and the vulnerability removed, the post-breach costs will still be mounting.

What would this mean for your business if it happened to you? If these senior stakeholders could go back in time to the security meeting and approve the £120,000 budget, they would.



“ The cost of a security breach is enormous. It will cost in the millions to get the system back online. ”

## Explaining the quantitative risk factor

Another way to explain the risk-based method is using 'quantitative risk analysis', which will clarify the financial impact caused by an attack if your company should be breached.

If you are trying to secure a budget for cyber security, then calculating the risk-factor is the best approach as it produces data which provides an undeniable truth why a cyber security program should be implemented.

Quantitative risk calculations provide a report which can be presented to senior stakeholders, demonstrating the risk, potential losses, and cost of countermeasures to mitigate threats and vulnerabilities.

It is possible to put a monetary value on both the financial loss that a security breach could cause, and the initial cost it would take to mitigate it. Calculating risk starts with identifying the value of an asset or assets that you need to protect, and understanding the threats that could harm those asset/s.

There are six steps to calculating the monetary value of quantitative risk which you can then present to your board to persuade them to allocate budget for cyber security.



## Step 1: Asset Value (AV)

This is the method of apportioning a monetary value to your asset/s. This is because if the cost to protect an asset is more than the actual cost of the asset there is a risk the security control cost, compensating or otherwise, could be incorrect. It is important not to overlook how lower value assets could be used as a pivot or launching point into more valuable assets. Completing regular penetration tests would highlight this through the attack kill chain.

## Step 2: Calculate Exposure Factor (EF)

Exposure Factor is the percentage of loss that would be suffered if the asset were compromised. In most cases, the loss is not total and is a percentage. The Exposure Factor of small hardware devices such as laptops would be relatively low. However, for assets such as architectural designs or Intellectual Property, the exposure factor would be high.

## Step 3: Single Loss Expectancy (SLE)

The single loss expectancy is the costs incurred by a single event that compromised the asset. This monetary value is the total loss the company would be impacted by a single event that compromised the asset. To calculate the SLE use the following formula  $(SLE) = (AV) * (EF)$ .

## Step 4: Annualised Rate of Occurrence (ARO)

The annualised rate of occurrence is the probability of the number of times in a single year a threat or risk will occur. For example, a company has experienced a significant security breach once in ten years; the calculation would be  $1/10 = 0.1$ . The ARO can be challenging to calculate and will be based on historical data, industry averages and guesswork.

## Step 5: Annualised Loss Expectancy (ALE)

The annual loss expectancy is the total financial loss within twelve months caused by threats against a specific asset. To calculate ALE, use the formula  $(ALE) = (SLE) * (ARO)$ .



## Step 6: Cost Benefit Analysis of Countermeasures/ROI.

This can be complicated to understand, and a new Annualised Loss Expectancy (ALE) must be calculated. You will also need the annual cost of implementing the safeguard which should incorporate purchases, ongoing management, license fees, depreciation, administration, etc. The ROI of a cyber security program can be achieved by calculating the Pre and Post Safeguarded Annualised Loss Expectancy (ALE), the formula for ROI is  $ALE1 \text{ (Pre-Safeguard)} - ALE2 \text{ (Post-Safeguard)} - ACS$ .

A positive figure would show the annual savings made from implementing the safeguard to protect the asset, highlighting an evident ROI from the security spend. A negative figure would indicate it would not be worth implementing the safeguard to mitigate this risk, and risk acceptance would be the better option.

*Below is a table with the calculations for the above steps:*

Steps/Models	Formula
Exposure factor (EF)	%
Single loss expectancy (SLE)	$SLE = AV * EF$
The annual rate of occurrence (ARO)	# / Year
Annual loss expectancy (ALE)	$ALE = SLE * ARO$ or
The annual cost of safeguard (ACS)	£ / Year
Cost-benefit of safeguard/ ROI	$(ALE1 - ALE2) - ACS$

Why go through all these calculations? It may seem like a lot of leg work however if your result is a positive figure it would show the money your organisation would save by implementing a cyber security program.

Using these risk calculations above shows that if the company had made a different decision in their Sliding Doors Moment, an investment of £120,000 would have reduced the risk to the business and saved over £456,000 in revenue loss caused by the cyber threat. This is calculated purely based on the loss of service. However, many factors can cause loss and financial impact and should be incorporated into the overall risk assessment.

By highlighting the potential financial loss that your organisation could face if no action is taken, and the savings you could make if the recommended security controls were implemented, you are providing concrete evidence why your organisation should implement a cyber security program.

When communicating to senior stakeholders, you must speak a language they understand, ensure it's not technically led, and highlight the risk and supporting numbers; this will secure your cyber budget.

It's important to also mention to senior stakeholders that the quantitative risk calculated is only covering loss of service. There are still other factors which can cause loss and financial impact on your organisation, which should be incorporated into an overall risk assessment.





## What to do next:

**It can be a challenge to persuade your board, stakeholders, and shareholders that cyber security is worth the expense.**

Make sure that they understand the importance of complete security protection for the business and the risks to your organisation if they do not invest, adopting the top-down approach. Involve them in the process and use approachable non-jargon language. It is important that you remind the rest of your board how a cyber security solution benefits the business financially, and that it is not an inconsequential expense that can be overlooked.

If you would like further information, help regarding your cyber security, or support in making the case to your stakeholders and shareholders to gain buy in for a cyber security solution, then get in touch today. We're here to help.



**Need the Best Defence  
Against Cyber Threats?  
Call us now on 0800 090 3734**

---

**info@digitalxraid.com    digitalxraid.com**

---



IASME<sup>®</sup>  
Consortium



IT Health Check Service