LEXEL™

Security Posture Framework

lexel.co.nz

Contents

Setting the scene

Cybercrime has been on the rise every year since the first “worm” was made by a grad student in 1988 as a curious project. Now it is estimated that cybercrime will cost as much as 10.5 trillion dollars yearly by 2025. Furthermore, cyber threats have grown by 600% percent since the start of the pandemic, making the current cybersecurity landscape very hard to navigate safely.

With more and more organisations completing their digital transformation and moving their workloads to the cloud, the potential likelihood and impact of data breaches are becoming more severe each day. New viruses, malware, exploits and other methods to breach organisation’s security, are developed on a daily basis.

As a result, even the smallest companies and individuals are at constant risk of data breaches. With the new phishing methods, it only takes one breached account to infiltrate the whole organisation. How did we get to this place?

It is estimated that cybercrime will cost as much as 10.5 trillion dollars yearly by 2025. Furthermore, cyber threats have grown by 600% since the start of the pandemic.

Old ways – the castle

When most of our work used to be done on-premises, you could imagine an organisation's cybersecurity as a castle of sorts. Everything important was hidden from attacks with firewalls and other cybersecurity initiatives. While cybercrime evolved constantly to find new creative ways to breach firewalls, the IT team had an easier time managing endpoints. As a result, both sides constantly improved their methods, and most devices were accounted for, being on-premises.

Additionally, the number of devices that needed to be managed was much lower than in today's workplace. For example, every printer, Wi-Fi router, smart watch or tablet can be breached by a cyberattack. This historically allowed IT teams to react to threats and breaches with relative ease.

New ways – the city

With digital transformation and remote work, the cybersecurity landscape changed rapidly. You can picture a modern organisation's cybersecurity as a sprawling city that sometimes does not even have a centralised on-premise infrastructure. A lot, if not all work is happening in disparate locations and in unprotected home settings.

That means that firewalls can no longer protect organisations fully. It is exponentially harder to secure devices that are dispersed around the city, country, or the whole world. Firewalls are ineffective, as you cannot deploy them in everyone's house. Organisations use endpoint security software and internal policies to combat the issue. However, these initiatives need to be constantly reviewed and updated to stay effective. Otherwise, their impact quickly starts to decline over time, resulting in outdated and ineffective cybersecurity posture.

As a result of this organisation sprawl, cybercrime is doing better than ever, and a lot of organisations are struggling to keep up.

What does all that mean for your business?

As a result of the growth of cybercrime, combined with the new off-site work model we outlined above, every organisation is under constant threat of data breaches, big or small. However, small and medium organisations have not yet caught up with new trends and developments in the cybersecurity space.

Large enterprises typically have huge budgets and well-equipped cybersecurity teams, while smaller organisation have not been able to prioritise security to that extent yet. They often lack appropriate budget and team size/expertise to adequately manage the cybersecurity risk. Additionally, there is often a disconnect between what the actual cybersecurity risks are and the funding available to combat this risk.

Conversely, these organisations are constantly under cybersecurity breach risk without even realising how big of a risk they are taking. The transformation into the new remote everything way of work, was not so much designed as thrown together very quickly. There was limited time for best practice deployment and user security training around this new environment was either limited or did not happen at all.

Organisations are constantly under cybersecurity breach risk without even realising how big of a risk they are taking.

Risks vs ROI in cybersecurity

A big part of the problem for small to medium businesses is understanding the relationship between cybersecurity risks and the multiple investment options available to mitigate that risk. A lot of organisations do not realise the actual risk they are taking at any given spending level.

Risk vs ROI relationship is quite simple, there are two main points we need to understand:

1. You can never get to 0% risk, no matter what you do and how you do it. However, there are some tricks to getting to your target ROI balance.

2. You have to spend exponentially more to reduce risk once you have addressed the basics.

Security Posture vs Risk & ROI

The biggest problem for many is not accurately realising how much your organisation needs to spend to get to your desired risk level, or even understanding you have a decision to make. For example, if your budget is $20,000/ year, but you are looking to deflect 90% of cyberattacks, you might be setting unattainable goals for your team.

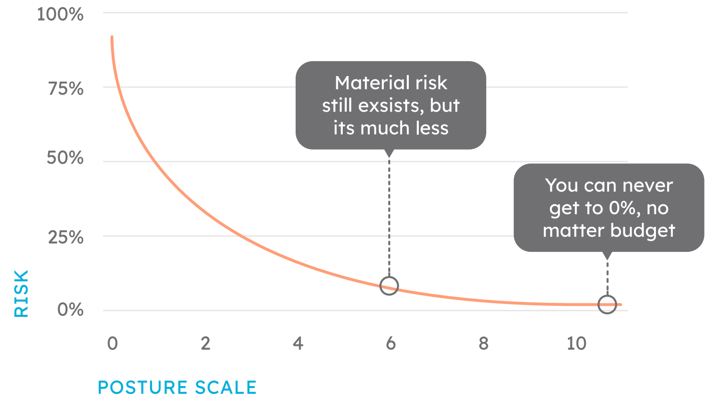
It is quite hard to assess your organisation internally. Your team might have a budget set up historically for your cybersecurity needs. However, as the workplace shifted to digital, new challenges and threats started to appear. Has your cyber-security budget increased to address this or are you expected to do more with the same total IT spend?

Best practice is to to have a security framework to easily assess where you are, and where you want to be. Only then can you make meaningful strides towards achieving your target cybersecurity goals vs the business appetite for "Informed" risk.

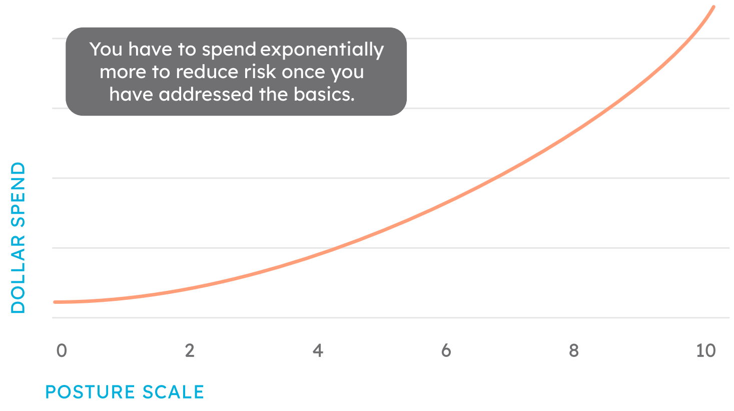
Once scale 7 is reached, additional protection costs exponentially more.

lexel.co.nz

Risk Level



Increasing Cost



Security Posture Framework from Lexel

That is where Lexel comes in. We have developed our own cybersecurity framework to help IT managers and decision makers translate their business risk appetite into a cybersecurity posture and plan, at the corresponding ROI level.

The process begins with defining your target business risk profile. Most organisations are aiming quite high, without realising the real economic cost of achieving that risk profile. As discussed in the previous section, it becomes exponentially more expensive to achieve the lower cybersecurity risk profile.

Next step is to assess your organisation's actual cybersecurity posture. For that, we go through a checklist that has requirements for each business risk profile. For example, if you are looking to achieve true Zero Trust, you need to make sure you have deployed the Full Framework, rather than purchasing a product that may only be partially deployed.

From our experience, a lot of organisations land way lower on our Security Posture Framework, which means that there is a disconnect between "where we are" and "where we want to be". In a lot of cases, they used to be in a perfect place, but have failed to update their solutions and policies to stay ahead of the curve. In other cases, cyber-security budget is just not high enough to be able to implement all required solutions and practices.

We also see cases which are well invested in some areas, but completely neglect others and are unaware they are doing so. This leaves them vulnerable to attack in these weak areas.

Applying the framework

Lexel's Security Posture Framework also provides an invaluable instrument to align IT staff and executive teams on cybersecurity, all based upon the agreed risk profile selected.

After you have assessed and selected your cybersecurity posture, the framework outlines the actions needed to reach that posture level.

Actual and effective cybersecurity technology is made up of three core elements, only when all three have been fully achieved will you receive genuine cyber protection.

1. Products

Recommended trusted and proven products that meet your target business risk profile.

2. Configuration

A guide to configure the products to best industry practices including configuration templates from Lexel for the best ROI.

3. Policy

Creating cyber-related IT policy to be followed or audited against is essential to ensure cybersecurity is not only established, but maintained.

Applying the framework

For IT teams the Security Posture Framework:

- allows IT teams to clearly articulate the risk/ROI decision to the board
- provides a trusted set of templated actions to implement, in an order which provides the strongest ROI first
- educates on new technologies that are available and recommended
- provides a trusted architecture that avoids major security gaps
- takes a broad, holistic view to security including configuration, policy and technologies used.

For boards / executives the Security Posture Framework:

- allows boards to make key cyber investment decisions based upon acceptable levels of business risk, including the ROI options available without being drawn into technology detail
- allows definition of a ‘target’ for ICT Security Posture (the risk profile)
- provides confidence that best practice security requirements are being implemented
- provides independent confidence that the agreed plan will be fully implemented correctly.

Next steps

Sign up for a **free introductory workshop** with Lexel's team of experts to start your security transition. After this workshop you will have a full understanding of the next steps and a holistic overview of our framework. You can decide whether to progress with a roadmap or complete a formal assessment.

*subject to criteria

Contact us

LEXEL™

Founded over 35 years ago; Lexel is one of the largest privately-owned providers of ICT services and solutions in New Zealand. An agile and innovative organisation, Lexel has a staff of over 170 and revenues exceeding $80m.

With extensive expertise in services and ICT solutions, Lexel consistently delivers on both quality and innovation. Across both New Zealand and Australia, customers can rely on Lexel's commitment to service excellence, every time.