Article

May 2021

Developing a Cyber Security Strategy - Where Do I Start?

We all know cyber security isn't a topic we can ignore. But how many of us are really prepared to face this evolving threat?

Stewart Hogg
Associate Director - Cyber

Email stewart.hogg@waterstons.com
Linkedin https://www.linkedin.com/in/stew-hogg/

The Government's 2021 Cyber Security Breach Survey tells us that 80% of business say cyber security is a top priority for their senior managers. Yet only 33% had established formal security policies, 13% set security standards for their suppliers and 10% had a formal incident plan . So, if cyber security truly is a top priority why have so few embarked upon the journey to protect their organisation from attack?

Headlines describing state-sponsored hackers, teenagers in their bedroom bringing large corporations to their knees and even the devices in your house being compromised to launch attacks on a global scale, most certainly plays a part in building a picture of a complex cyber security landscape. It's hard to know what steps to take first. For many senior managers and board members, the cyber security threat landscape and how to navigate it may be akin to the maps of ancient times marked with "here be dragons" and maybe that's why few have ventured on this path!

The good news is, every organisation can take simple steps to greatly improve their cyber security defences by identifying their key data assets, implementing a number of basic security controls and over time evolving their approach to provide a holistic defence against a range of security threats.

Before we get into that, let's look at what data security is really all about.

Where's your passport?

It's common to find organisations that don't treat their key data assets with the appropriate level of security they require. Consider the most important data asset in your organisation; it may be a commercially sensitive business plan, a brief for a new product or perhaps highly confidential personal information relating to your customers. Whatever it is, consider how many people have access to that data, the locations where it may reside and what would happen if it was compromised.

For many businesses the impact of a data breach of an asset this sensitive would result in severe brand reputation damage, potential loss of business and maybe even financial penalties, yet often little has been done to safeguard these vital data assets.

On the other hand, if you were asked where your own passport is, it's likely you'd have a good idea. To many of us it's a crucial document allowing us to pass through international borders for business trips or that well-earned break. It's a crucial asset and we protect it as such, checking its location every five minutes as we await check-in at the airport, locking it in a safe in our hotel room and always taking precaution to ensure it's up to date, valid and available when we need it.

Essentially we protect our passport's confidentiality (guarding it from those who shouldn't have it), its integrity (ensuring its details are accurate and up to date) and its availability (by ensuring it's available when we need it). These three aspects are often termed the 'CIA' of security and that's where all good security strategies start. The key is to take this same approach with our organisational data.

Identify what data you need to protect

The first step in protecting your organisational data is to understand what data you have. It may seem obvious, but as organisations grow, the location of different types of data and who has access is often not well known. Consider highly confidential spreadsheets which get emailed round an increasing number of staff, are received on personal devices and stored in a variety of repositories. The risk to these data assets is often far beyond what many organisations would accept if they knew the risks. Therefore, the starting point for any security strategy is understanding what data we have, its location and its value.

What is the value of the data you have?

Value can be defined in a number of ways in terms of sensitivity, legal and compliance requirements, cost to replace or better still, in terms of how valuable we consider the confidentiality, integrity and availability of that data to be.

Once we have a good handle on the data assets we hold, we can then perform a risk assessment of these assets. Consider the risks to confidentiality, integrity and availability which these may face. Risks could include external threats like unauthorised access to key IT services, such as email or the risk of data corruption e.g. a ransomware virus. However, it'll also include a large number of non-technical risks e.g. data accidentally being forwarded due to human error or a lack of user training resulting in data being available in the public domain.

Once we understand the risks and have identified those which we're happy to accept and those which we're not, we're now able to select the most appropriate steps (or controls) to reduce these risks and further protect our critical data assets.

Identify what cyber security solution works for you

There's a range of frameworks and best practice standards which can help determine the most appropriate security controls. Here are our three recommended approaches which we've used with a number of our clients to enhance their cyber security strategy:

1) 10 Steps to Cyber Security

A good starting point is often found in the NCSC's 10 Steps to Cyber Security framework which outlines ten key steps organisations should take to safeguard data from the most common cyber attacks. These include technical controls in addition to non-technical steps such as user training and awareness programmes.

While no certification exists against the 10 Steps to Cyber Security frameworks these guidelines align with best practice outlined by the Cyber Essentials and ISO 27001 standards described below.

2) Cyber Essentials and Cyber Essentials PLUS

The Cyber Essentials standard is based on a pre-determined risk threshold and therefore contains a number of prescriptive steps which must be applied to achieve certification against the standard. The controls are predominantly technical in nature however will ensure that the most likely vulnerabilities which could be exploited by internet borne attacks are secured.

The standard looks at five domains which include: access management, boundary firewall security, malware protection, secure configuration and patch management.

The Cyber Essentials badge can be gained through completion of a self-assessment questionnaire through a certification body (such as Waterstons). Upon successfully attaining the Cyber Essentials badge, organisations may also apply for the Cyber Essentials PLUS certification which involves an onsite audit of the in-scope security controls and a network vulnerability scan to validate that the organisation has indeed guarded against the most common security threats.

3) ISO 27001:2013

ISO 27001:2013 is often seen as the ‘gold standard’ in approaches to protect organisational assets. This standard sets out the requirements for an 'Information Security Management System (ISMS)' which is designed to ensure a robust and consistent approach is applied to safeguard organisational data. In addition to a risk methodology, the formation of security policies and training programmes, the standard also outlines 114 controls which organisations must evaluate to determine if they’re appropriate for each organisation. These controls range from encryption technologies, access control systems and backup processes to supplier chain vetting procedures, legal compliance measures and business continuity plans.

The standard is based on the 'Plan, Do, Check, Act' cycle which drives the process of continual improvement. Therefore, once the identified security controls have been implemented, the organisation must undertake internal audits and conduct management reviews to ensure the effectiveness of security controls are measured and identified improvements are tracked to completion in order to continually improve the ISMS.

Focus on continual improvement

Whatever approach you choose to adopt the key is that a culture of security awareness and continual improvement is established within your organisation. It’s crucial that security is not just seen as a job for the IT department but rather that stakeholders from across the business are engaged to develop a holistic, pragmatic and effective approach to guard against the evolving threats we face in our digital world.

If you are looking for more information on how to ensure your business is cyber secure, please read our blog on our 5 top tips to cyber secure your business.

Need some help?

Our dedicated cyber security team work with you to design, implement and optimise pragmatic controls to ensure your critical data and systems are always protected – helping you sleep easier at night. We recognise that no ‘one size ¬fits all’ when it comes to cyber security, so our services are tailored to suit your needs. Please get in touch today!