CYBER SECURITY: *NOT* AN I.T. PROBLEM

Contents

Introduction

The emphasis on Cyber Security really came to the fore in the early year 2000's, it was around the time of the Dot com boom. organisations were designing eye catching e-commerce sites and web content, but not focusing on how secure they were. It's an old cliché but think of it as double glazing the windows to the front of your house and securing them but leaving the back door open for anyone to enter.

IT departments around the world were already responsible for the design, implementation and management of applications, and from that point onwards the whole responsibility for becoming a cyber secure organisation!

How many times have you heard this phrase?

"Cyber Security is an IT problem"

Organisations seem to forget that IT applications are there to support business activities. Without a business there would be no applications and what business' also need are people and processes to run these IT systems and applications. So now, not only are IT implicated with cyber security, you also have people and business processes that need to adapt and comply with cyber.

So, cyber is not just an IT problem, but how do we change this mindset amongst organisations and their C-suite and boards. Cyber risks are not just an IT issue, but a significant business problem to be solved. In this guide we will show you how to make cyber not an IT problem, but one for the business to solve.

.. A Case in Point

Before we get to the 'how', I'd like to take you through my own experience of how I have witnessed an organisation focus on cyber as an IT only problem and the ramifications that this attitude caused.

When I first started out in the cyber security world working for a large UK based organisation, our finance department were presented with a letter from our acquiring bank. We had to become PCI DSS (Payment Card Industry Data Security Standard) compliant through a formal external audit process. This standard was new to the world and the entity was targeted by their banking acquirer due to the volume of payment card transactions processed.

Our general manager in finance forwarded this letter to our IT department, thinking they will have a good idea of where and how to process this letter and give the acquirer all the answers they require. The IT department quickly noted around 11 IT applications that would fall into scope and formulated a letter back to the acquiring bank that the organisation believed they complied with the PCI DSS and that all in scope IT applications were compliant.

Just before the letter was submitted to the bank, the cyber security department caught wind of this letter doing the rounds internally and decided to take a vested interest in what was about to be submitted. The team questioned the contents of the letter and advised finance that all 11 applications need to be validated for compliance.

The PCI DSS is a contractual standard based around 12 high-level requirements and 250 plus sub-requirements. Each requirement needs to be validated by the entity and assessed as compliant against every requirement.

The standard covers People, Process, IT and Governance and compliance provides assurance to the acquirers and card schemes that an entity is taking precautions to protect themselves from a cyber-attack. Gaining compliance however does not ensure you won't be attacked!

The outcome was that the organisation realised they needed to invest significant cash and resources into this cybersecurity compliance programme. This important job was left to the IT leaders rather than the full C-suite and board.

Following a detailed analysis on the IT applications, the exercise unearthed other applications. IT subsequently reported a total of 75 systems and applications in scope.

The next 4 years were spent on remediating the applications and fixing Cyber issues in IT including, vulnerabilities in the IT Infrastructure, encrypting sensitive data and segmenting the IT network

It's not to say that business and people processes were not reviewed or fixed, but the priority and focus was on individual technologies to fix individual problems in IT as they, IT were leading the programme. The total cost to the organisation was in excess of £5m.

Had the people and business processes have been prioritised, this cost could have been significantly lowered with a potentially shorter timeframe to compliance and business activities protected.

Compliance was gained, but there were no results in business change to show for it.

The Breakdown

So, how do we move from cyber being an IT problem to one that the entire business needs to own and solve. The following is a guide on how to make this change in mindset and shift in business strategy and operation. It needs the business to take on an active role in the management of cyber within the organisation. Here's how it can happen:

1. **Understand your business risks and how a Cyber-attack could cause these risks to become a reality.**
2. **Change the perception in the leadership teams that cyber is complex and that only IT can understand it.**
3. **Train your employees on security awareness, but also ensure the employees of your third- party service providers have also been trained.**
4. **Move cyber security activities over to a Business orientated activity.**
5. **Implement a CISO (Chief Information Security Officer)**
6. **The Business teams need to own the IT applications and understand the risks and impact of a cyber-attack to them.**

Understand your Business Risks

and how a Cyber-attack could cause these risks to become reality.

It's normal to assume that getting non-technical business leaders involved in Cyber risks is difficult. They have been brought in to run a business and why should they be spending time on cyber when their KPI's are focused on driving the business.

What's important here is to change the narrative from cyber risks into business risks should a cyber-attack occur. If you engage with the business from the outset in this manner, then the conversation takes on a different form. The catalyst for initiating this dialogue is important with senior business leaders and the technical people in the organisation.

You typically start off by bringing senior resources in to a business tolerance workshop The invitees should consist of a business owner, someone who runs a business department and someone who is responsible for managing the P&L (Profit and loss). The rationale behind this is to understand where the business risks in the organisation are.

You start off by identifying the critical assets that are important to run their business operation. You then begin to drill down to the business processes that compliment these assets and provide a competitive advantage to them, their business department and ultimately the organisation.

Once these have been identified you are then well equipped to engage with other resources in the organisation to help quantify what those business risks are, and then working with your IT department and cyber security team to understand what the cyber threat environment currently is and how this could impact the business should those risks occur as a result of the threats turning into a reality.

Change perception amongst leadership

that cyber is complex and only IT can understand it

As we have discussed, cyber security is seen as being so complex and that only the IT department or cyber security team can understand it. Non-technical business leaders just see it as being so difficult and very hard to comprehend. Well how do we change this perception?

Most organisations have an Information security policy rolled out and within it will be a section on cyber security training and awareness. Unfortunately, it's mostly seen as a tick box exercise and business departments are only ever given the very basics on keeping safe from cyber threats. Just ask anyone who has recently received training as to what value they derived from the training. The content is usually based around passwords do's and don'ts, handling sensitive data and adhering to security polices etc. When a real-life cyber security issue is brought in front of the business, it's treated like a difficult subject.

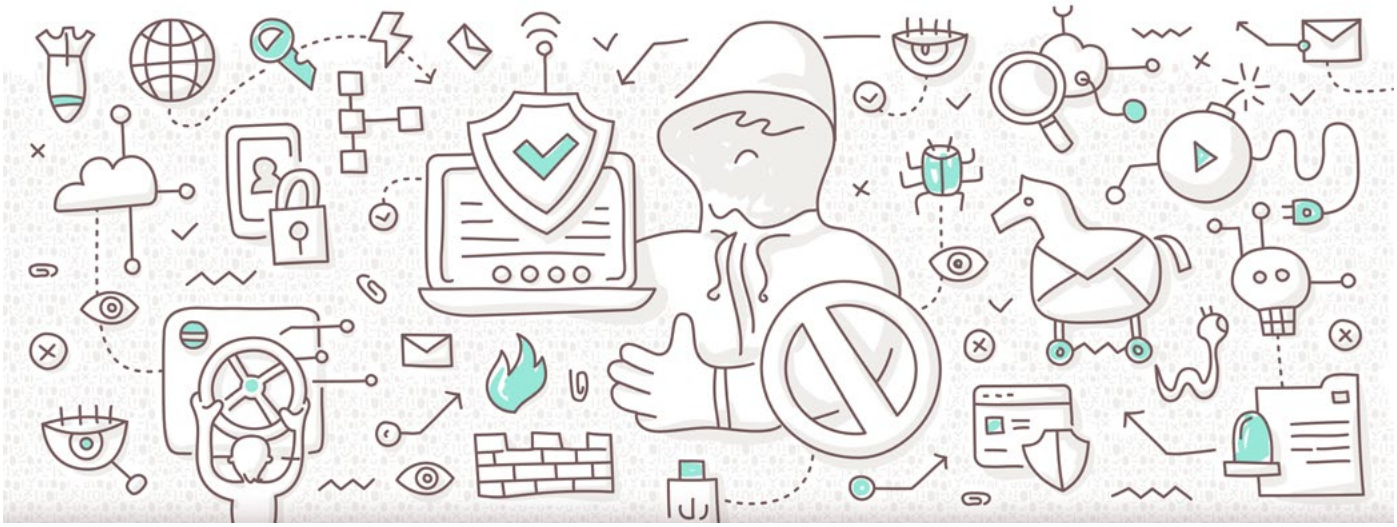
Motivation is also an issue. The business is paid for getting their job done and achieving results that will add to the bottom line of their business. Why should they even begin to try and understand cyber security complexities when there are experts on hand to deal with them.

You can't turn the business into Cyber security professionals but changing the content of the security awareness training and general good habits into real life examples and scenarios that could implicate their own work would be a start. The training needs to take on an interactive form. One example could be using a phishing attack on unsuspecting individuals in the business and then sharing the lessons learned.

The training needs to incorporate cyber issues that could impact the business in their day to day role. At Equantiis, we have seen a dramatic change in how cyber security is perceived within the business once individuals have learnt what the impact of a cyber threat could be on the business and how the business can mitigate the risk. The training brings on an inquisitive approach from individuals in the business to take risks into consideration in any business activity that would be outside of their day to day work. This learning will enable the business to understand that Cyber is much more than just IT.

Train employees on security awareness

Also ensure that third party employees are trained.



So, now we have trained your employees and brought the benefits to your organisation on security awareness, the general belief would be that the organisation is now secure. The business has been trained and your IT department have secured the IT network so that any potential external attacks have been mitigated. Or have they?

Chances are, like other organisations you may have outsourced some of your business and/or IT processes to an external third-party service provider. They will conduct your business on your behalf and so that question asked is, how secure are they as an organisation and do they understand cyber?

The third party supplier could be the weakest link in the chain of command and therefore it should be a requirement that they also train their employees on cyber security awareness.

The business eco-system needs to think alike in order to avoid any misunderstandings further down the line. The benefits here are two-fold. The third party also has an appreciation of the cyber risks to the business they are working on behalf of and there is an opportunity for them also to possibly win further business as a compliant service provider.

our organisation should not only treat its employees as their own, but also of their third parties who operate on your behalf. The third party may be conducting business processes for you today or sometime in the future and they need to provide you with assurance that cyber security is not just an IT problem.

Move Cyber activities into business areas

Nominate representatives

The cyber security team have a role and a purpose for protecting the organisation, but they have limited resources to manage the cyber activities across an entire organisation. This is where Equantiis have worked with organisations to ensure that all individuals in an organisation are responsible for the cyber security of their organisation.

We have worked to instil a level of understanding that ensures that the cyber security teams can continue to monitor threats and prevent attacks, but the business provides input into this.

Work with each business unit and nominate a single point of contact within the department to represent security as cyber champions.

This process ensures cyber is at the forefront of everything the business department does and reports any cyber risks or issues up the chain.

The IT and cyber security departments will also have a point of contact now within each business area to manage and discuss any risks before they become cyber issues. The business will also take on responsibility for owning their business risks and not IT.

Implement a CISO

A Chief Information Security Officer

For an organisation to deploy an Information security role is a step in the right direction. It shows that the organisation understands their security responsibilities and has allocated a specific person to manage and maintain the security of the organisation. However, this comes at a cost and the organisation needs to not only employ this person for this specific role, but also manage the role holder's ongoing training programme and the management of their security certifications. They also need to subscribe to third party channels for security news and updates which can add to the ever-growing burden of security tasks.

Added to this, the role owner may need to be on 24/7 alert for any security threats or incidents to the organisation. The role owner also needs to have a place at the C-Suite table to present cyber risks and issues as a priority. We've probably listed so many challenges here for this role that you are beginning to think why you should even bother. Well there is light at the end of the tunnel.

You could opt for an external third party to provide you with resource to cover the role of the CISO. This has many advantages but can also bring dis-advantages if the CISO doesn't understand the business or sector they are required to work in.

The fact of the matter remains that the CISO, whether internal or external, needs to manage cyber security within the organisation and fundamentally report into a senior member of the organisation that owns the biggest number of business risks from a cyber-attack.

Too often you see organisations get it wrong by getting a CISO role to report into an IT Director or Chief Technical Officer. At Equantiis we believe that the CISO role holder should report into a senior business head. Ultimately the CISO has the interests of the whole organisation, but if the highest priority area with the greatest number of business risks can be endorsed by an internal member of the team being the CISO, then you will begin to move away from Cyber security being an IT problem, but a business problem.

Business teams must own IT applications

and understand the risks and impact that a cyber attack may pose to them.

Cyber security is different to Information security and this is because cyber is generally associated with computer systems and hardware. The focus is usually on the IT department to manage Cyber.

Information security is much wider and varied. It not only refers to computer systems, but also the security of assets. These assets can be hardware or paper based.

IT applications within an organisation are usually developed in house or procured from a third-party developer. This activity is usually led from an IT department and therefore the perception is that IT should fix the IT application when things go wrong, cyber or non cyber related. Even the onboarding of new users being given access to use the application is nearly always an IT service desk activity.

At Equantiis, we believe that IT do have a place in the lifecycle of an IT application being administered in an organisation, but the business needs to own the application.

As we said at the beginning of this guide. An IT application exists in an organisation because the business has a need for the application to conduct a part of their business for them.

Once it has been established that a business team owns an application, you then take them through the onboarding process and look at all the interactions with business users that the business can administer. For example, the joiners, leavers, movers process should be owned by the application owner in the business to grant access to the system and then IT can provide the access. Once the ownership is agreed and managed from within the business, you then run a risk workshop to take the business through all the risks to the application they own that could become a reality if a cyber attack was to impact the application.

The true cost to the business of an application down time will become immediately prevalent and we are sure that the business will then begin to understand why cyber security is not an IT problem.

Author

Paul Forrest

Executive Chairman

www.equantiis.com

hello@equantiis.com

+44 (0) 203 376 7447

EQUANTIIS