BRIEFING

At the Intersection of Risk and Security: It's Time to Fireproof, not Firefight

Today's organisations are laser-focused on driving success through digital innovation and growth. This is where spending is focused, and rightly so. But digital infrastructure needs securing. There's just one problem: without a clear ROI it's hard to know how much to spend on cyber-tools and processes, and where to focus that investment. That can make it tempting to play the odds when it comes to cybersecurity, but it's a dangerous game to play.

At Panaseer, we understand that there's no such thing as 100% security. But to avoid becoming the next TalkTalk, or Yahoo, you first need better insight into your IT Risks and then you need to be able to translate those into business risks to ensure you have the appropriate level of controls in place. Without this insight into your Risk Appetite you can't start to drive a risk-based approach to security or even begin to understand if you have the right budgets or ROI measures in place.

IN THE DARK

Modern boardrooms increasingly understand the importance of cybersecurity to the business. A recent report by insurer Hiscox claims that two-thirds of organisations in the UK, US, Germany, the Netherlands and Spain rank cyber as the top risk to their business alongside fraud . However, that same report reveals the majority of firms as "cyber-novices" when it comes to the quality and execution of their security strategy.

A major challenge is defining how much time, budget and effort you need to spend, and in what areas of the cyber landscape. The problem here is that if cybersecurity is working well, you won't see any obvious return on your investment. The fact that nothing is happening is precisely the result of good security: no impact on staff productivity, no breaches of sensitive data, no service outages. In these terms, spending money on a cyber-attack that 'might' happen can be difficult to justify when there are many other digital priorities to consider. It has often lead to organisations having a flat or minimal budget approach.

This could be an expensive mistake.

JOINING THE DOTS

Organisations should instead think more clearly about risk. What's your risk appetite? How many customer records would your business need to lose, or how many hours of downtime could it tolerate, before it becomes a serious issue? Once you've established this risk appetite, you need to translate IT Risks into those business risk appetites. What's your level of acceptable cybersecurity risk and what controls do you need in place to support this? How much budget is required?

To do all this effectively you need to break down those communication silos and connect the dots across the company — from the executive suite to security and IT. Everyone must be working in alignment against that agreed acceptable risk.

Unfortunately, many organisations don't work this way. They don't make the crucial connection between the business risk levels and IT, to make sure the business is protected to the level required. This means when a breach or serious cyber-incident happens, they can end up having to throw more money at the problem than if they had worked out what was required before, protected themselves accordingly and avoided the risk in the first place.

A case in point: TalkTalk's former CEO claimed the firm had "significantly increased" security spending following a major 2015 breach. Why did this happen? We can safely make the assumption that as a major telecoms provider its risk appetite would have been low, but spend on security was also low when in reality it should have been much higher. Organisations that have a low risk appetite need to spend more on security, but at TalkTalk that disconnect between business and IT meant risk and spend weren't aligned.

John Gamble of the US credit agency giant Equifax in November 2017 forecasted "between $60 and $75 million in spending that will include information technology security in the fourth quarter" after occurring a one-time charge of $87.5m due to a cybersecurity incident. That's in addition to the $17m in consulting fees it's said to have spent following a monumental breach of over 145m customers' records.

What can we learn from these cautionary tales? That when it comes to cybersecurity, you need to understand risk and fireproof it, rather than firefighting after the event.

[1] HISCOX Cyber Readiness Report 2018

ESTABLISHING YOUR RISK APPETITE

So, how do you establish your risk appetite? Here are a few key points to consider:

1. **Translate the business risk appetite into the IT risk model.** This isn't easy, but you need to understand what is important to the business and what you can afford or not afford to happen. For example, is client data more valuable than a financial loss? Or is a financial loss or down-time more critical to the ongoing business? Depending on the case this will drive where to place emphasis within your security approach. Allowing you to draw a base-level of success in the security areas you perceive as key to achieving the associated level of risk.

2. **Consolidated data driven view of your security:** A single source of consolidated data from across your security estate becomes mandatory when reviewing your risk model. Without a single source of truth by which to get a true understanding into your actual risk levels you have no hope in starting to prove where you are, let alone measure your Risk Appetite.

3. **Automate visibility:** Many CISOs rely on manual processes to generate insight into security systems. But as the number of — often siloed — products rise in the enterprise and complexity increases, this is no longer viable. It's time to move away from manual and adopt automated, on-demand visibility. It's the only way to get that single source of the truth at your fingertips.

4. **Leverage frameworks:** Existing resources can help to provide the structure via which to align key areas of focus for security investment and prioritisation. Good examples include the Center for Internet Security's Critical Security Controls (CSCs) and the cybersecurity framework produced by the US National Institute of Standards and Technology (NIST) .

5. **Build relationships:** Business, IT and security teams must work together. With limited budget, headcount and time you need to co-ordinate to work out priorities. Having trusted data from a single source of the truth is a vital first step, ensuring that separate teams are all working from the same page for the same goals.

[2] TalkTAlk profits halve after cyber attack, BBC News 12 May 2016
[3] Massive data breach has cost Equifax nearly $90 million, Phys. Org, 11 November 2017
[4] Equifax spends $87.5 million on data breach, more expenses on deck, Larry Dignan for Between the Lines, ZDNet, 9 November 2017
[5] https://www.nist.gov/cyberframework

Prevention is better than cure in security. So, don't wait until it's too late. Be proactive and take steps to better understand your business risk appetite. Then ensure you meet IT in the middle to translate that risk.

Ultimately fireproofing is always preferable to firefighting.


Jim Doggett

Jim Doggett is the Senior Vice President of US Operations and our own CISO. Having leaded the development of the information security practice at EY, Jim developed a deep understanding of the intersection of controls, risk and cybersecurity. Taking this insight, Jim moved to roles as Chief Technology Risk Officer at JP Morgan, Kaiser Permanente and AIG. At AIG he built a bespoke system to help automatically unite security data into a single view to measure risk and drive re-mediation. Recognising the power this type of approach brings, joining Panaseer was an opportunity for Jim to continue to develop a solution to solve the challenge.

ABOUT PANASEER

Panaseer headquartered in London, with US operations in New York and Houston. We exist to empower enterprises to conduct business in the digital world with confidence and control. Our diversity is our strength. The team hails from a wide range of backgrounds and skillsets, with degrees covering everything from Astrophysics and Computational Chemistry to Mathematical Biology, High-Performance Computing and everything in-between.

We love to hear from you. Reach us at **Success@Panaseer.com**

panaseer
www.panaseer.com

CargoWorks
ET101, 1-2 Hatfields, London
SE1 9PG, UK

Work-Bench
5th Floor, 110 Fifth Avenue, New York
10011 NY, USA