by Marc Lueck

September 14, 2017

InfoSec problems? Listen to your CISO, put more emphasis on recovery

For those businesses that want to reduce the brand risk of cyber-attack, Marc Lueck says more emphasis on recovery is the easiest place to start. It will also go a long way to future proofing organisations against upcoming threats.

InfoSec problems? Listen to your CISO, put more emphasis on recovery

A growing number of cyber-attacks.
An increasingly fragmented and geographically spread workforce.
A step change in the complexity and effectiveness of malware and malicious social engineering techniques.

These are the realities that organisations both large and small have to deal with on a day-to-day basis in 2017.

Despite the above factors, company boards still seem to have their information security priorities wrong. According to the ClubCISO Information Security Maturity Report 2017, 78 percent of senior business executives still place their focus squarely on prevention of attacks, rather than organisational response and remediation after one happens.

CISOs and senior information security professionals know however, that an organisation's cyber-response is only as good as its weakest link. With so many variables, attack vectors and misconceptions about the sanctity of certain types of data amongst employees — make no mistake, it really is a case of not if, but when an organisation will suffer a data breach.

Isn't that the job of the CISO?

Interestingly, the ClubCISO report also reveals that these very board members who prioritise prevention over response, actually cite breach response as a major responsibility for those in the role of CISO. In other words, 63 percent of board members want CISOs to take care of the mess after a breach, yet they are not necessarily taking a balanced approach to investing in solutions that enable this in an effective manner. It is evident that there is a clear disconnect between expectation and reality of how information security can and should be managed.

Part of the problem between this communication breakdown is the fact that the role of CISO is a comparatively new one in both the IT industry and enterprise. Yet, CISOs are arguably the most important technology stakeholder working in businesses today — dealing with a myriad of risks, threats, breaches, policies, regulations and user behaviour. These responsibilities are as complicated as they are important, and CISOs can often find themselves isolated and operating outside of the usual and well-understood aspects of corporate governance.

The present day lynchpin of cyber-security

As the role of the CISO becomes more mature, there are more points of commonality between job descriptions. Several fundamental questions however remain, including 'what do CISOs actually do, and what exactly is a CISO?' First and foremost, it is clear there is no one defined CISO role. Yes, they are often the most senior professional in their organisations for mitigating cyber-risks, but there is also huge variation between approaches and strategies — pending company and board expectations. CISOs must therefore work together to shape the future of their profession.

The trend, however, is for the CISO to become more visible in the organisation. Nearly half (47 percent) of CISOs surveyed consider themselves to be actively involved in strategic business decisions outside of their core technology remit. And they are also getting more resources, at a time where other roles are facing cutbacks. Only nine percent of CISOs have seen a budget cut this year, while 14 percent have seen an increase of over 100 percent.

A holistic view of breach mitigation

Ultimately, CISOs have made it clear that there needs to be a change in security strategy to safeguard businesses and their data. And it is evident that many are concerned at how their boards prioritise prevention over response. It is therefore essential for CISOs to communicate, at board level, the importance of baking in both security and recovery into the organisation in an overarching way.

Undoubtedly, it is very natural for executives whose job is not cyber security day-in-day-out, to want to deal with tactical and visible threats. But in a world ever more connected, and therefore at risk, even the biggest technology laggards must admit that change needs to happen in regard to the organisational response of current information security threats.

For those businesses that want to reduce risk, more emphasis on recovery is definitely the easiest place to start. It will also go a long way to future proofing organisations against upcoming threats. But for those that are still reluctant, or slow moving, make no mistake, the risks will increase, and brand reputation will become all the more fragile.

Within all of this lies the opportunity for the modern CISO to make a positive and fundamental organisational change, as the leaders in the industry who are stepping up to help their businesses mitigate risk through technology.

Contributed by Marc Lueck, chairman at ClubCISO

**Note: The views expressed in this blog are those of the author and do not necessarily reflect the views of SC Media or Haymarket Media.*

MOST READ ON SC

1. Sharing IOT malware rife, botnets now child's play as teen arrest shows
2. Risk management to strategic resilience: The evolution of cyber-security
3. New UK data protection bill to be published tomorrow
4. LinkedIn Premium accounts being used in phishing scam
5. The hidden danger of cryptocurrency mining in the enterprise