The CISO & the board: A love-hate relationship?

By Marc Lueck 2 hours ago Features

A third of CISOs aren't involved at all with their company's key strategic business decisions. It is clear something has to change.

Today, it seems like you are unable to pick up a paper without reading about a high profile hack, data breach or cyber criminal arrest. In the past, information security teams within large enterprises have always been the unsung heroes, working behind the scenes, often in isolation, to keep their businesses safe against these types of news stories — and maintaining a relatively low profile in the process. However, at a time when organisational security is getting compromised more and more, it is only natural that infosec professionals are finding their practices analysed and criticised more than ever.

Massive crises such as WannaCry and GoldenEye have shocked the business world into realising that cyber security isn't something that can happily tick along at the back of an organisation in isolation. It needs to be integrated into the business strategy as a whole. Concerningly though, ClubCISO's Information Security Maturity Report has revealed that a third of CISOs aren't involved at all with their company's key strategic business decisions. It is clear something has to change.

"What does my CISO actually do?"

Firstly, it is important for business decision makers to establish early: what does a CISO actually do, and why should they have a greater involvement than they commonly do in today's boardroom?

A CISO is involved with the day-to-day dealings of risk, threat and breach prevention — to put it simply, it is their job to keep the bad guys away from precious company data. Moreover, it is a CISO's core responsibility to keep on top of the latest policies and regulations, as well as keeping a hawkish eye over trends in user behaviour. The complexity of the issues CISOs deal with on an ongoing basis can often leave them isolated, and removed from vital aspects of corporate governance.

The divide between boards and CISOs, that has been raised by the ClubCISO report, has been around since the inception of the role. In order to strive forward and reduce organisational risk, companies will need to identify why this divide exists, and more importantly how to rectify the issue.

Despite lines of communications drastically improving in recent years, CISOs still think that boards have infosec priorities all wrong. With the deluge of cyber security-related stories hitting the headlines, the knee jerk reaction from company boards has been very much focused on dealing with visible threats and securing perimeters. What is needed however, is a far more holistic approach, weaving security and recovery into the very fabric of the organisation as a whole.

The language barrier

A key issue that has presented itself time and time again is the fact that company boards are often short of the time it takes to fully understand the multitude of threats facing their businesses. These issues they focus on are the ones they read about on their morning commute, rather than the long term strategies seasoned CISOs have devised using their extensive knowledge of the threat landscape.

It is important to note however, that the divide of understanding is rarely a result of friction between the ranks. It is usually a case of misunderstanding and confusion. This is why, in response to the cyber attacks making front-page news, 78 per cent of company boards place their focus purely on the prevention of cyber attacks, rather than recovery, which is a focus for only 22 per cent of companies. Recovery, the majority of boards say, is the major responsibility of a CISO, despite often not being brought to the boardroom table when discussing infosec and risk mitigation strategy.

The communication maze

Considering this, it is easy to understand exactly why the disconnect between CISO and the company board exists. The CISO is often expected to act as the clean up crew lead, without sufficient scope and resources to effectively manage the aftermath of a breach.

Over the past few years research has consistently shown that information security is struggling to really embed itself into company hierarchy, with CISOs reporting into matrix structures where influence is lost. However of late, there have been drastic improvements in this area, with just under two thirds of CISOs now reporting directly to CIO/CTOs, a figure which has doubled compared to the figures in the 2016 ClubCISO Information Security Maturity Report.

Infosec teams in 2017 have also been shown as operating more independently, rather than being combined into the IT department, further defining the role of the CISO. Despite this however, there is still much work to be done in giving information security a well-defined role within enterprise.

Attracting and retaining talent

Asides from enhancing infosec communication and collaboration from the top-down, boards also need to think about how any contention could be impacting employees. Worryingly, a massive 83 per cent of CISOs admit that they have difficulty retaining and attracting security staff. With employee retention proving to be such a massive issue in cyber security, it is very possible that the lack of understanding from C-level execs has a knock on effect in this regard.

The reality is, an employee will never be happy and motivated when they feel frustrated by internal processes that make their lives difficult, so streamlining these and removing unnecessary bureaucracy is one way in which organisations can improve the employee satisfaction levels of security staff across the industry.

Working towards rectifying this, companies are also indirectly addressing the overarching issue of 'kneejerk security' mentioned previously. More infosec staff has the positive effect of increasing cyber risk understanding and awareness across the entirety of an organisation. Quite simply, more people to spread best practice.

Ultimately, miscommunication and fragmentation in any part of any business will slow productivity and increase risk. Having a CISO that is disconnected from key business decisions has the inevitable knock on effect of poorer threat prevention, and compliance issues further down the line. But, as evidenced by this year's report figures, the situation is certainly improving. As ever though, there is still more than needs to be done in terms of inter-departmental communication and collaboration, before information security fully embeds itself as an invaluable facet of the modern day organisation.

Marc Lueck, Chairman, Club CISO
Image Credit: Uber Images / Shutterstock

TOPICS

CISO BOARD SECURITY CYBERATTACKS