2017: THE YEAR OF THE CISO

Posted by: Dean Alvarez July 20, 2017 in EDITOR'S NEWS 0 Comments

The role of the Chief Information Security Officer (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 role of ClubCISO, a private members forum for European information security professionals, is to help understand, promote and shape the future of the profession. Powered by Company85, ClubCISO held its fourth annual survey this year, with 39 CISOs participating in the discussion, and published the findings in the new ClubCISO IT Security Maturity Report 2017. These CISOs represent all sizes of business, from rapidly-growing challengers to major FTSE organisations.

While the full results are enlightening and hugely optimistic across the board, we wanted to highlight three areas that sum up the challenges and opportunities for CISOs in today's enterprise: their role; the relationship with their company boards; and the importance of understanding people and their behaviours.

Trust me, I'm a CISO

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

TOP 10 STORIES AROUND THE WEB

Web application attacks accounted for 73% of all incidents says report
August 16, 2017

AP Moller-Maersk counts cost of cyber attack but swings to profit
August 16, 2017

Venezuela's public telcos collapse under cyber-attack
August 16, 2017

Scottish parliament hit by cyber-attack similar to Westminster assault
August 16, 2017

How Just Opening A Malicious PowerPoint File Could Compromise Your PC
August 15, 2017

Cloudflare is helping defend a neo-Nazi website from hackers, even as Google and GoDaddy are distancing themselves from it
August 15, 2017

If Anonymous 'pwnd' the Daily Stormer, they did a spectacularly awful job
August 15, 2017

US military spies: We'll capture enemy malware, tweak it, lob it right back at our adversaries
August 15, 2017

UK businesses "unprepared for a cyber shock"
August 15, 2017

A local securities firm has been hit by a cyberattack
August 14, 2017

one defined CISO role. Yes, they are all 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 the profession.

The trend, however, is for the CISO to become more visible in the organisation. Nearly half (47%) 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 9% of CISOs have seen a budget cut this year, while 14% have seen an increase of over 100%. The only thing that appears to be holding back further growth in the rise and function is the ability to find good people.

In past years the ClubCISO survey has shown that information security hasn't always had a natural home in a company, but most CISOs now report directly to CIO/CTO, rather than into matrix structures. In 2017 nearly two-thirds of CISOs report to the CIO/ CTO; this figure has almost doubled since 2016 (33%). Reporting via matrix structures has correspondingly fallen to 17% (2016: 37%). A number of CISOs pointed out that they report directly to the CIO but not as part of the IT department. This change in reporting structure will also, no doubt, further define the role of the CISO.

Board games

It's evident from the research, that there's a clear disconnect between expectation and reality of how information security can and should be managed. Despite the majority of CISOs having better lines of communication into boards, CISOs think many of their company boards still have information security priorities in the wrong order. Security is undoubtedly important for companies, but the temptation is to deal with tactical and visible threats rather than bake security and recovery into the organisation holistically.

Company boards are time poor and so tend to focus on the issues right in front of their noses. Perhaps that's why, in the wake of a growing number of cyber attacks, an increasingly fragmented (and therefore vulnerable) workforce, and a step-up in the complexity and effectiveness of malware, 78% of company boards still place their focus squarely on prevention capabilities, rather than response (just 22%). At the same time, these same boards contradict themselves by prioritising breach response very highly. In fact, 63% cite it as a major responsibility of the CISO. In other words, boards want CISOs to clean up the mess after a breach, but they're not necessarily taking a balanced approach in investing in solutions that enable them to do this quickly and effectively.

The CISO as a people person

IT security is not all ones and zeros. Insider threat and user behaviour (malicious or not) is one of the biggest challenges to an IT security strategy and policy. Time and again, ClubCISO's annual survey has shown that CISOs believe that people pose the greatest risk to an organisation. Respondents revealed that as many as 60% lack the confidence that internal security policies are actually implemented. As such, it is no wonder that CISOs are working ever more closely with HR to devise and implement solid policies and controls.

As one CISO says in the research: "I now spend more time with HR than I do at my own desk".

CISOs touch every part of their businesses and organisations. There are multiple reasons for this. Chief amongst these might be the fact that over one-third of organisations were certain they had suffered a material data loss incident during the past 12 months. It is becoming increasingly evident that security has to be embedded into every facet of the business to minimise risk. CISOs do however admit that 'security by design' is very hit-and-miss. More than half of CISOs surveyed said it is considered from the outset for all projects, but nearly one-third think it is hardly ever considered.

So what's next?

Ultimately, CISOs have made it clear that there needs to be a change in security strategy in order to safeguard businesses and their data. CISOs are concerned at how their boards prioritise prevention over response. ClubCISO believes this imbalance does not reflect the reality of breaches—it is an inevitability that every organisation will suffer a data breach at some point, therefore businesses need to do more to ensure they have good recovery plans in place to mitigate the potential damage.

What is clear is that now is definitely the time for change for the CISO. And those businesses that want to reduce risk will need to start changing according to the leaders in the industry who are stepping up to fulfil this role.

To find out if you, as a CISO, are on track with your peers we suggest downloading the ClubCISO Information Security Maturity Report 2017, here.

Tagged with: CYBER SECURITY TECHNOLOGY