Looking for cyber security workers? Join the queue!

11 September 2017

By Mark Lueck, Chairman, ClubCISO

For many years the debate has raged on about the stark skills shortage in the information security field, with many seasoned infosec veterans claiming there is no visible light at the end of the tunnel just yet. It seems, according to ClubCISO's Information Security Maturity Report 2017, that they may be correct. The study of top UK CISOs has highlighted that at least half of their organisations are struggling to attract and retain good quality staff in the information discipline. To make matters worse, just last year the same group of CISOs reported that staff retention had taken a downturn in 40% of companies.

With regulatory change firmly on the horizon, coming in the form of the General Data Protection Regulation (GDPR), and what seems like an eternal uncertainty around not only Brexit itself, but also the potential changes in the free movement of European workers—these issues are rearing their head at a critical time for businesses of all sizes. In all likelihood, more cyber security skills will be needed in order to mitigate the multitude of risks for businesses at this time of drastic change.

There is no doubt that a skills shortage in any sector can be exacerbated by organisations which overwork their current employees, and don't provide them with the tools and support they need to do their jobs properly. Thanks to infosec budgets being squeezed, this is happening abound in a variety of organisations, with many looking for security professionals—in an already finite market—who can tick every single infosec box.

This isn't just a problem from a resourcing standpoint (these people really aren't easy to find) but also increases an organisation's risk profile. After all, having information security rest on the shoulders of one person will surely make an organisation more vulnerable. If, for example, this person was to leave, then with them goes any notion of maintaining a viable level of security.

READ MORE; Does cybersecurity need a makeunder?

A safer option for companies is to invest in a team that has a good spread of skills in various areas of protection and risk mitigation. Although this can prove difficult for many organisations, taking this step builds in a big safeguard for the future of their infosecurity capabilities.

So, the idea of building a team is all well and good, but where should businesses start?

Exploring lateral sectors

A common thought process when securing cyber security talent is to only look in the field of cyber security. Makes sense right? Well, confronted with the fact that 69% of today's CISOs claim they started their careers in technology or engineering and with some even coming from armed forces, operational management, financial or even physical security—it's fair to say this net can, and should, be widened. After all, only 8% of CISOs have a dedicated degree in information security.

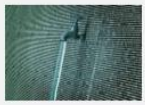
RECOMMENDED


INFORMATION SECURITY / NEWS / THREATS
Major spike in credit card fraud cases following Equifax data breach

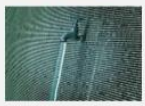
CURRENT AFFAIRS / INFORMATION SECURITY / NEWS
Best Buy shelves Kaspersky Lab products, cites 'too many unanswered questions'


INFORMATION SECURITY / NEWS / THREATS
Security flaws in HMRC website could let hackers steal citizens' tax filing details


CURRENT AFFAIRS / FEATURES / NEWS
Will PSD2 prove to be a cyber security nightmare for banks?


FEATURES / INFORMATION SECURITY / NEWS
Equifax data breach: all you need to know

MOST POPULAR


FEATURES / INFORMATION SECURITY / NEWS
Equifax data breach: all you need to know

INFORMATION SECURITY / NEWS
Equifax officials sold $1.7m in stock prior to data breach announcement


INFORMATION SECURITY / NEWS / THREATS
Hackers targeting UK universities to steal valuable research and IPR data


CURRENT AFFAIRS / FEATURES / NEWS
Will PSD2 prove to be a cyber security nightmare for banks?


INFORMATION SECURITY / NEWS / THREATS
Hackers targeting students with phishing emails to steal personal information


INFORMATION SECURITY / NEWS / THREATS
Energy firms beware! There's nothing Dragonfly wouldn't do to breach your networks


INFORMATION SECURITY / NEWS / THREATS
Major spike in credit card fraud cases following Equifax data breach

Given the fact that the role of "information security isn't exactly clear cut, due to the relative youth of the industry itself, and the complexity of the evolving digital landscape, each organisation has a different perspective on how the role should function. This diversity provides opportunity. Companies can go looking outside of the traditional IT realm when hiring infosec people.

One key factor that is required in the role is the ability to consult upon, and handle, various risk factors in their daily jobs. This is a challenge faced constantly by facility managers, legal professionals, HR executives and crisis comms managers, who would have readily available skills to transfer to the infosec strategy of an organisation.

READ MORE; Nine tactics for cyber security training that sticks

Admittedly, the deep technical element of the job is something that would need to be learnt, as it wouldn't be on par with someone from a more traditional IT background. However, with cyber crime transitioning to more social engineering-led model—this potential hurdling block is becoming less of an issue. Having this business-led perspective within employees, who are used to dealing with these responsibilities is an efficient way to reduce risk within the organisation and provide vital support to the operating CISO.

Brick by brick—building through people

Whilst opening up different organisational areas in this way should be encouraged, the fact is that a CISO will not be able to build a successful information security team by poaching from other fields alone. So, to build an adequate cyber security workforce, existing infosec pros need to begin investing in knowledge transfer, as eventually it will pay dividends.

For example, by giving opportunities to IT apprentices and investing in their future growth and development, they will ultimately be more engaged with the company and far more likely to grow with the organisation, rather than try their luck elsewhere.

"It's not my fault it's the industry!"

The unfortunate truth in the industry is that the shortage of cyber security talent is blamed on the labour pool, however it is really up to companies to adapt and be more willing to invest in people to generate effective cyber security roles. Companies that take this step are often more successful at recruiting top quality cyber security professionals, the type of workers who are able to solve unconventional problems and deliver outside of the normal realms of thinking. The alternative is an inactive approach of complaining about the state of the market and refusing to do anything about it.

READ MORE: Cyber insurance: Why is it important and do you need it?

When budgets are tightened and times are tough, cyber security is often an area overlooked. However organisations can bolster their staff numbers and quality through adequate training and knowledge transfer, alongside widening the goalposts when looking for staff. The ultimate benefit of organisational resilience will undoubtedly be worth it in the long run.

CULTURE / FEATURES / NEWS
Looking for cyber security workers? Join the queue!

INFORMATION SECURITY / KNOWLEDGE BASE / LEGISLATION/GDPR
Are you ready for GDPR?

INFORMATION SECURITY / NEWS / THREATS
Security flaws in HMRC website could let hackers steal citizens' tax filing details

INFORMATION SECURITY / NEWS
Did Wetherspoons delete all customer data for fear of GDPR's imminent arrival?

CURRENT AFFAIRS / INFORMATION SECURITY / NEWS
Best Buy shelves Kaspersky Lab products, cites 'too many unanswered questions'

FEATURES / NEWS
Top five biggest cyber-attacks in the UK

CURRENT AFFAIRS / NEWS
Chinese national arrested by FBI for orchestrating 2014 OPM data breach

CURRENT AFFAIRS / INFORMATION SECURITY / NEWS / THREATS
German election software can be hacked by novices, claims hacker group