Give CISOs a Say: The Cyber Security Paradox

By Marc Lueck, Chairman at ClubCISO

+ INCREASE / DECREASE TEXT SIZE −

5TH SEPTEMBER 2017

Add to favorites

ClubCISCO Chairman Marc Lueck looks at how companies should be handling the latest cyber security issues facing companies.

In 2017, organisations have a growing list of cyber security challenges they need to face up to, in order to keep the enterprise secure. Not only has there been a sharp rise in the number of cyber attacks in the past six months, but companies also need to deal with an ever more fragmented and geographically spread workforce — working on multiple devices.

On top of this, new malware threats are increasingly sophisticated, and it takes a lot more technology and investment for the enterprise to overcome these threats.Set against this backdrop of rapid change, ClubCISO Information Security Maturity Report 2017, reveals many companies still do not have the right priorities in place when it comes to cyber security. In fact, it shows that as much as 78% of senior business executives still place their focus squarely on prevention of attacks, rather than organisational response and remediation after one happens.

The catch, in a highly connected modern business environment, it is no longer acceptable to have incorrect priorities in place. This is because it is common knowledge among CISOs and senior information security professionals, that any cyber defence is only as strong as its weakest component, and of course the stakes are higher than ever before. Companies do not only suffer financial loss during a cyber breach, but also possibly irreparable reputational damage.

Marc Lueck, Chairman at ClubCISO

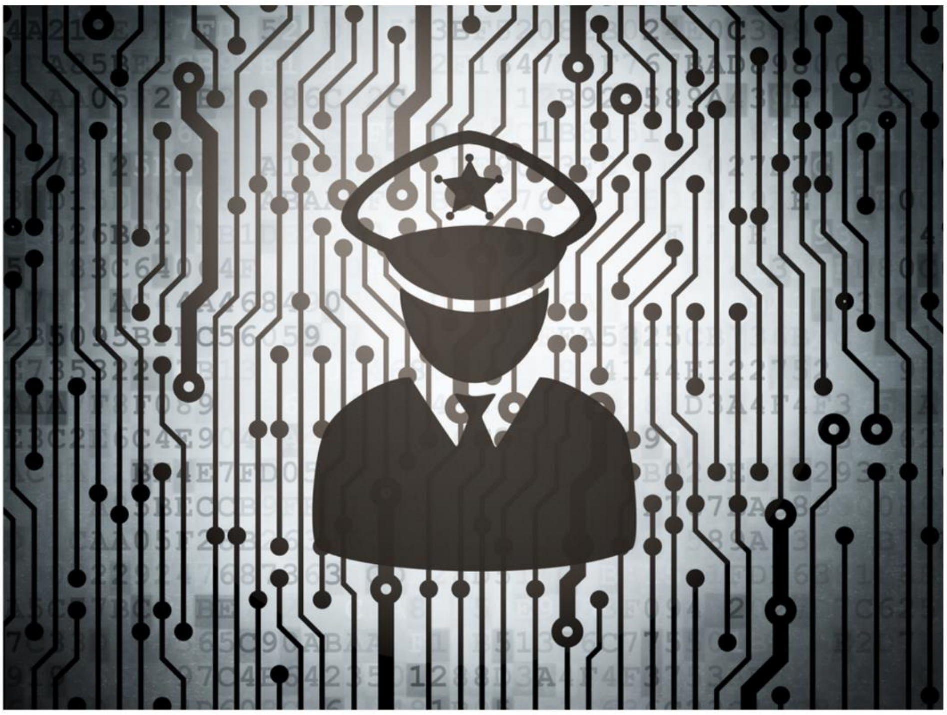
Communication, not isolation

ClubCISO's latest report shows that key board members prioritise cyber protection over response and recovery. Given the increasing media attention on cyber attacks this is not surprising. However, it also reveals that breach response, it seems, is considered a responsibility for the CISO without any added assistance.

Put bluntly, despite the fact that board members are not taking a balanced approach to investing in recovery after a cyber attack, 63% of board members want CISOs to take care of the aftermath of a breach. Not only does this seem a bit paradoxical, it is also reflective of a far greater problem that is present in company boards across the country, and that is the chasm between the reality of IT management and the board's expectations.

The lack of communication between the board and the CISO is partly owed to the fact that the role of the CISOs quite frankly haven't existed for very long in the enterprise. But with an increasing risk being presented, that falls right under the CISO remit, it can be argued with the growing threats that companies face, that these individuals are one of the most important of all of the tech stakeholders in any given business. On a day-to-day basis they deal with multiple threats, and data protection policies, while also juggling in changes in regulations and user behaviour.

Without a doubt these jobs have massive importance when it comes to managing infosecurity across the enterprise, therefore it is worrying that CISOs often find themselves on the other side of a significant divide in corporate governance and understanding, finding themselves isolated.



"Well then what does my CISO do?"

Despite the increasing relevance and prevalence of the CISO role in the enterprise, the role of the CISO is constantly under question, and there maintains a distinct lack of understanding as to what CISOs actually do. Despite common similarities between CISOs in their responsibilities, there is not a cookie cutter list of roles and responsibilities for all CISOs.

Of course their core responsibilities lie in mitigating cyber risks, and they hold a senior position on the board (although not always as some report into the CISO), however, the differing approaches and strategies, which are often decided by the expectation of individual boards, can create a massive variation between roles. It is therefore integral for the advancement of enterprise cyber security that CISOs work together.

A clear step that is being made is by the CISOs themselves boosting their visibility in the rest of their organisations. Nearly half (47%) of CISOs surveyed consider themselves to be actively involved in strategic business decisions outside of their core technology remit. Despite cuts that are taking place across multiple roles, CISOs continue to enjoy a boost in resources. This is exemplified by the fact that only one in ten CISOs have seen a budget cut this year, with 14% of CISOs seeing a massive 100% boost to their budgets.

How to spread the security bug throughout the company

In order to safeguard businesses and their data, there are clear changes that need to be made in the overall strategy companies are taking. Boards need help to reprioritise response and recovery on an equal level as prevention. But the only way to do this is for the CISO and the board to work together. In order to effectively safeguard a business, and mitigate risk, CISOs' opinions need to be heard and heeded at the board level.

If this does not happen, especially for the many executives who are not well versed in the world of cyber security, there is a very real threat that the focus on only the most visible and tactical threats to the company will be their downfall.

It is up to CISOs to help their organisation make this change. They need to proactively engage the board, and learn more about the intricacies of each role of their peers. At the same time, they have to get their peers to do the same with them. It is only when everyone is on equal footing, and that priorities are aligned, that the enterprise will be safe.