Publication: Security Magazine
Date: 08.04.20
URL: https://www.securitymagazine.com/blogs/14-security-blog/post/92092-the-rise-of-the-chief-cybercrime-officer
Title: The Rise of the Chief Cybercrime Officer
Author: Matt Cable, VP Solutions Architect and MD Europe, Certes Networks

The Rise of the Chief Cybercrime Officer

Matt Cable, VP Solutions Architect and MD Europe, Certes Networks

The TalkTalk data breach in 2015 was monumental for the cybersecurity industry. At the time, data breaches were hardly new, but this particular breach resulted in the government recommending that an officer should be appointed with day-to-day responsibility for protecting computer systems from a cyber attack.

This governmental guidance was not a consequence of the size of the breach. With the personal details of 157,000 customers accessed, including bank account numbers and sort codes of more than 15,000 customers, it certainly was not the largest the world had seen. Rather, the guidance resulted from the way in which the immediate situation and the following aftermath, were handled. In most organizations, the responsibility of following this guidance has historically fallen to the Chief Information Security Officer (CISO), with support from the CEO. In the wake of the TalkTalk data breach in particular, the CISO was given 'free rein' to strengthen the organization's cyber security capabilities.

The Many Faces of the CISO

Yet, the role of the CISO was not a new concept. In fact, the CISO dates back to 1994 when Steve Katz was hired to run the world's first formal cybersecurity executive office, and was subsequently given the title of CISO. Unsurprisingly, the role has many aspects to it, from security operations, cyber risk and cyber intelligence, data loss and fraud prevention, security architecture, identity and access management, program management and compliance and governance, to name but a few.

Recently however, the role has come under increasing scrutiny and with the rise of cyber crime and the sophistication of cyber attacks, it's easy to see why. Research shows that more than two-thirds of organizations have experienced at least one security breach in the past year and that the majority of both CISOs and the entire C-Suite believe the CISO is ultimately responsible for the response to a data breach. However, with so many 'hats' to wear and multiple day-to-day responsibilities, it is clear to see why, with the increasing threat landscape, many organizations feel that it's time to add another role to the C-Suite.

Enter the CCO

Enter the Chief Cybercrime Officer (CCO), whose remit will entail ensuring the organization is cyber-ready and who will bear the responsibility of mitigating breaches, taking the lead if a breach does occur and providing the necessary link between the Board and the rest of the company to mitigate risk and work collaboratively to resolve issues as they arise.

With the need for cybersecurity to become far more central to C-Suite strategies, this new role should ease the load on the CISO and ensure the organization can get one step ahead of hackers in the cyber crime race. However, organizations must take into account the need for both the CISO and CCO to work in harmony, with clearly defined roles and support from the Board.

Aligning to Boundaries

With both the CISO and CCO working towards keeping the company's data safe from cyber threats, it is essential for each role to be clearly defined. This definition may look different to each organization: each role, and the teams working with them, should have clear parameters and responsibilities so that in the event of a data breach, the organization clearly understands the steps that should be taken and who should take them.

In practice, this should make every CISO breathe a big sigh of relief. Many CISOs would identify cybersecurity as the greatest risk within their role, and when they're also trying to juggle multiple other responsibilities, it's a lot to have on their shoulders. With the CCO focused on the system architecture and the CISO focused on the security of the information within the organization, there should be no reason that both roles can't work collaboratively towards keeping the organization safe.

Making Decisions

With both roles working in tandem, the next step that organizations need to take is ensuring the CISO and the CCO have enough influence with the Board to make critical decisions and resolve issues immediately. By ensuring that all members of the Board have visibility of the entire cybersecurity strategy and that the strategy is regularly reviewed and updated in line with new threats and intelligence, the CCO and CISO can be given the responsibility to report and respond to incidents and make rapid decisions on behalf of the business. In the event of a data breach, removing unnecessary approval and authorization steps ensures that the organization can respond quickly and put remediating measures in place to minimize potentially catastrophic repercussions.

In a world where cybersecurity threats can't be ignored, now is the time for the structure of organizations to truly be considered. Has cybersecurity been given enough prominence at Board level? Can decisions be made quickly? Can space be made for both the CISO and CCO to work in harmony? By asking these questions and making changes, organizations can ensure they are in a far better position to keep their data safe and protect their reputation.
