Publication: Security Boulevard
Date: 04.05.20
URL: https://securityboulevard.com/2020/05/can-the-cco-and-ciso-work-in-harmony/
Title: Can the CCO and CISO work in harmony?
Author: Matt Cable, VP Solutions Architect and MD Europe, Certes Networks

Can the CCO and CISO work in harmony?

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

The roles of CCO and CISO are different, but each is tasked with protecting an organization from cyberthreats

Cast your mind back to the TalkTalk data breach in 2015. Before this, many organizations had suffered a data breach, but this one in particular was monumental. It resulted in the government recommending that a specific officer should be appointed with the sole responsibility of protecting computer systems from cyberattacks.

This breach was hardly the largest the industry had seen, however. With the data of "just" over 150,000 customers accessed and "only" 15,000 bank accounts and sort codes included within this, it was not the size of this breach that made an impact. Rather, it was the way in which the breach itself and the aftermath were dealt with that lead to the guidance being enforced.

Responsibilities of the CISO

Following this guidance, in a typical organization, this authority fell to the chief information security officer (CISO), with support from the CEO. The TalkTalk data breach, in particular, saw "free rein" given to the CISO to strengthen the organization's cybersecurity strategy in an effort to keep the hackers at bay.

At the time, the role of the CISO itself was certainly not a new concept; it actually dates back to 1994, when Steve Katz was given the title of CISO and tasked with running the world's first formal cybersecurity executive office. The CISO role has evolved to encompass many responsibilities: from cyber risk and cyber intelligence to security architecture, identity and access management, security operations, data loss and fraud prevention and governance, to name but a few.

Recent years and numerous data breaches later, however, and the role has come under increasing scrutiny. Research shows that more than two-thirds of organizations have suffered at least one cyber breach in the past year and that the entire C-suite believes the CISO is ultimately responsible for the response to a data breach. The CISO clearly has a lot of responsibility and the increasing threat landscape only heightens this. It's clear to see why many organizations feel that it's time to add another role to the mix, giving cybersecurity the attention it deserves.

Finding a Place for the CCO

And so, it was time for the chief cybercrime officer (CCO) to find their place within the organization. This role is responsible for ensuring the organization is cyber-ready and is in charge of mitigating breaches, taking the lead if a breach does arise and providing the much-needed link between the board and the rest of the company to reduce risk and work collaboratively to resolve issues as they occur.

With it being well-documented that cybersecurity must become far more central to C-suite strategies, this role eases the load on the CISO and makes sure the organization can get—and stay—one step ahead of hackers in the continuous cybercrime race. However, these two roles can't work in isolation; organizations must ensure that both the CISO and CCO work in harmony, with clearly defined roles and support from the board. But what should these roles look like?

New Job Descriptions

Both the CISO and CCO share a common goal of keeping the company's data safe from cyberattacks. However, how each role looks at doing that may differ in each organization. To define this, each role and the teams within them should have clear parameters and responsibilities so that in the event of a data breach, the organization clearly understands what steps to take and who should take them.

This is welcome news to many CISOs, who would identify cybersecurity as the greatest risk within their role. When they're also trying to juggle several other responsibilities, it's a lot to have on their plate. 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 both roles can't work collaboratively toward keeping the organization and its data safe.

Who Has Influence?

With both roles working side by side, the next step organizations need to consider is ensuring the CISO and the CCO have enough influence with the board to make critical decisions and resolve issues immediately. All board members should have visibility of the entire cybersecurity strategy, which should be reviewed and updated regularly in line with new threats and intelligence. With this in place, the CCO and CISO can be given the responsibility to report and respond to incidents in their own capacity and to make rapid decisions on behalf of the business. This is essential as, in the event of a data breach, removing unnecessary approval and authorization steps ensures the organization can respond quickly to minimize potentially disastrous consequences.

With new cyberthreats continuously arising, now is the time for the structure of organizations and the roles within them to be considered. Each role should be clearly defined and given enough influence with the board to ensure decisions can be made quickly. In turn, this will make sure that both roles can work in harmony. With the right roles and structure in place, organizations will be safe in the knowledge that their data will be kept safe and that their reputation will remain intact.
