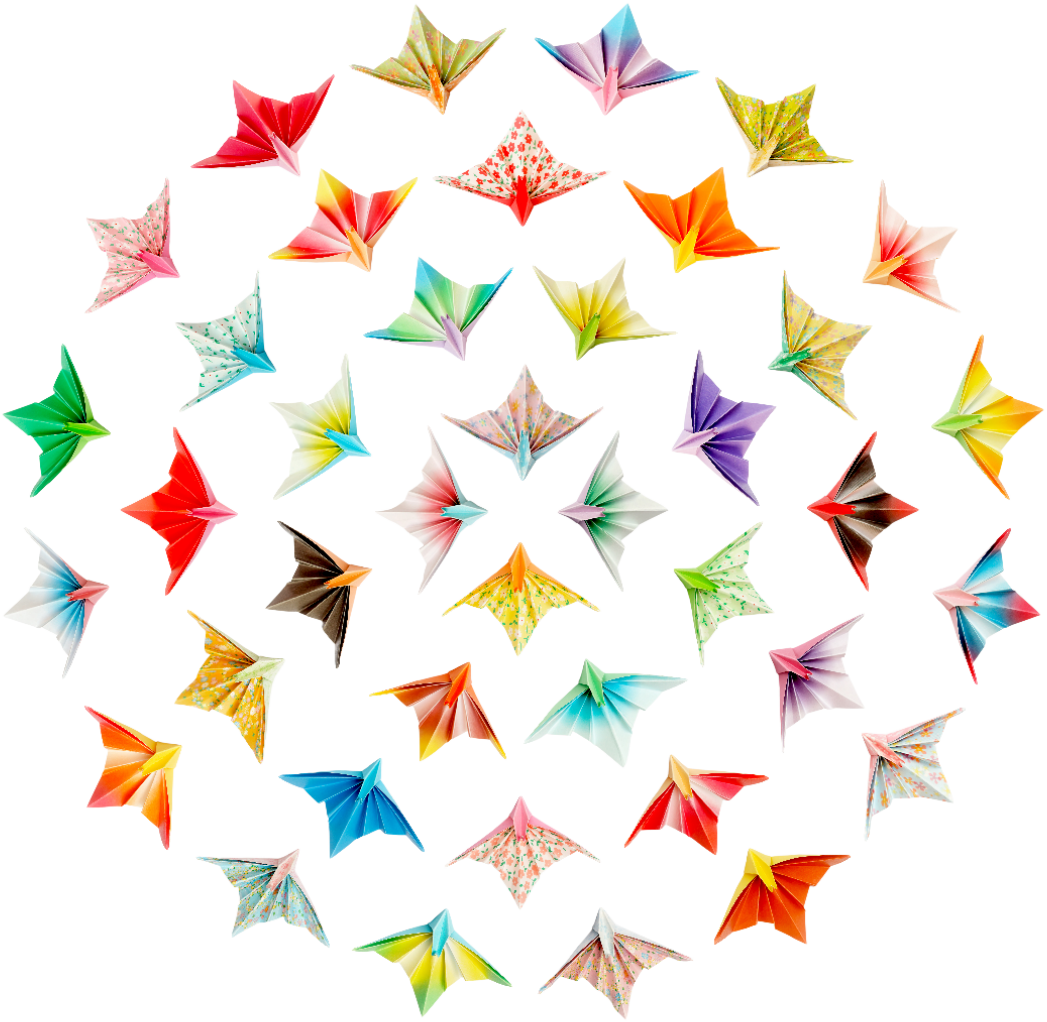
Deloitte.



The ascent of the CISO

Cyber everywhere. Succeed anywhere.

2019

The chief information security officer (CISO) of the present is a different breed from that of the past. It has rapidly changed from a technology-oriented position to a business leadership-focused one, and it is an evolutionary process that is far from over.

By Sir Rob Wainwright
Partner, Risk Advisory, Deloitte.

This article has been authored by Sir Rob Wainwright who has been a Partner with Deloitte since June 2018, working in its cyber and financial crime practices. He was previously the Executive Director of Europol, from 2009 to 2018. Sir Rob has had a 25-year career in intelligence, policing, government, EU and international affairs, including at the Serious Organised Crime Agency, National Criminal Intelligence Service and the British Security Service. and in June 2018 he was awarded a Knighthood by HM The Queen for his services to security and policing.

Contents

Introduction

Just as the scale and seriousness of the cyber threat facing businesses has evolved in recent years, so too has the role of the chief information security officer (CISO). Cyber aggressors, including hostile states, organised crime gangs and lone hackers have become more numerous, focused and sophisticated. The methods at their disposal have become more innovative, varied and destructive.

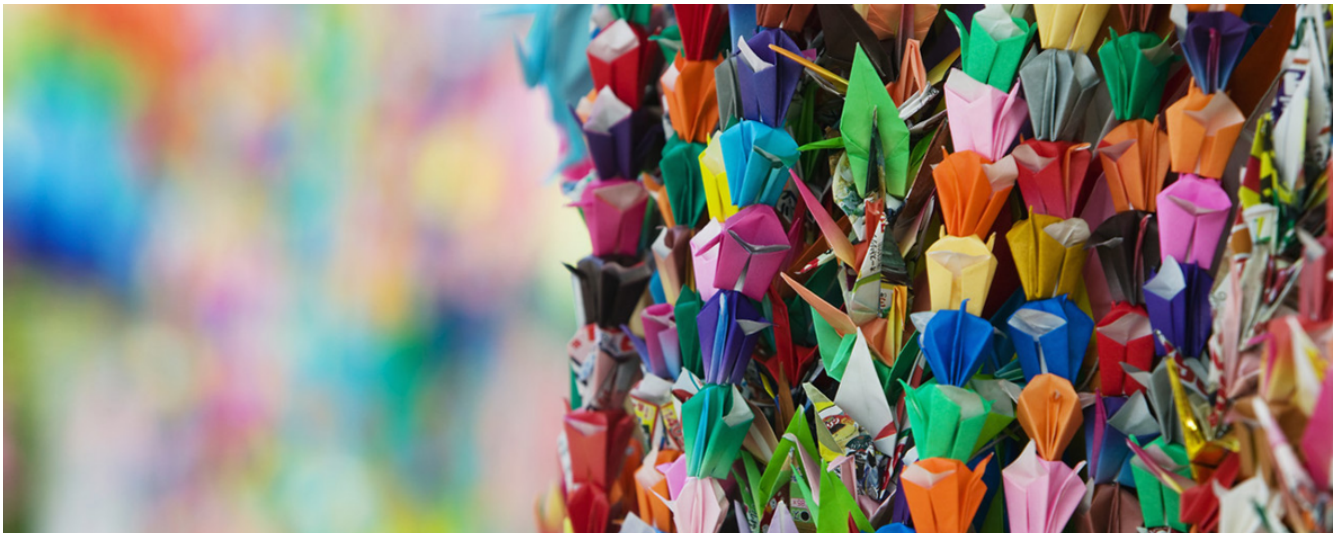
Many businesses, but by no means all, have adjusted to this more hostile cyberspace. Those that have adapted have re-modelled their short-term tactical procedures and long-term strategies to improve their defences. They have invested in the latest detection and prevention software. They have gotten better at responding to breaches and getting operations back to normal as soon as possible. And they have elevated their CISOs, giving them more authority and more budget.

Cyber security is now being dealt with higher up the corporate ladder. In many cases, the CISO has become a close peer of the chief information officer (CIO). The role now demands business leadership as well as information security and technical skills, and the CISO is now being seen as a business partner not just a business protector.

The CISO's department has become a much bigger cost centre than it ever was, and therefore has to demonstrate value for money. The argument has to be made that high security expenditure will, by reducing the incidence and severity of attacks, save the company money in the long run. If this argument is accepted, the CISO will be seen as a money saver.

Some companies, such as certain telecommunications and defence companies, have developed such sophisticated and effective security that they are able to sell their solutions to other companies and have spun off separate business to do so. In these cases the CISO has become a money maker, and thereby a good friend of the chief executive and finance director.

However, the rise of the CISO and is far from over. As the cyber threats to business increase, the role of the CISO will become even more important.



The cyber threats

The main cyber threats to businesses fall into several broad categories. One is the opportunistic, high-volume theft and use of data – data breaches – by criminal groups and individuals for commercial gain. Another is the targeted use of higher-end capabilities such as malware and ransomware by malicious state actors, "hacktivists" and crime gangs with the specific intention of disrupting banking networks and the operating systems of other global industries. Yet another is an attack that spreads from intended targets to unintended victims, disrupting or destroying business supply chains and causing catastrophic collateral damage.

Companies have adopted a range of tactical and strategic security measures to counter the threats they face in cyberspace.

None provides 100 percent protection. It is inevitable that breaches will happen. The best that can be hoped for is that the risk of breaches is minimised, and that when they do happen they are dealt with quickly and business continuity plans kick in immediately.

Defensive capabilities must be multi-layered, not flat. The basics must be in place. The UK's National Cyber Security Centre's *10 steps to cyber security*, complemented by its paper *Common Cyber Attacks: Reducing the Impact*, form a good basis for organisations looking to protect themselves, and are now used by most of the FTSE350.

The evolving role of the CISO

Understanding the threats and putting effective counter measures in place is the responsibility of the CISO but he or she depend on many others in the company. The board and top management need to be aware of the risks and approve a budget that provides the CISO with the necessary technology and human resources. Staff at all levels need to be educated about the critical roles they play in their company's security, and follow the established procedures on the use of passwords, data access rights and so on. But the brunt of the day-to-day responsibility falls on the CISO.

The role of the CISO has changed. In the past four or five years it has broadened, from being almost purely technology-oriented, to being more people-oriented; and from being a middle-management function, to being a business and technology leadership function. The role continues to accelerate in the same direction to meet these needs.

The CISO has to communicate the nature and extent of the cyber threats to all levels of the company. They have to influence senior management and the board to support the cyber security strategy and sign-off an ever-increasing budget.

We have seen how "information security" – which was always a niche corner of IT, and never important enough to get anywhere near the boardroom – suddenly in the past five years or so becoming a big concern, a potentially existential concern, because of the rapid increase in the number and seriousness of cyber attacks. Those managing information security have quickly been given more responsibility and the title chief information security officer or similar. Where they have not been up to the task, they have been replaced by those who have a higher level of the required technical and management skills.

In many cases even the new cohort of CISOs may not have the experience or skills to fulfil what the role now demands. The role therefore continues to evolve.

The prerequisites of a top CISO today demand that she or he is a dynamic leader of the function, is able to formulate and implement strategy and can speak to senior management and board in a confident manner. The CISO is more outward facing in communications in order to influence external stakeholders, reassuring regulators and able to think about the problems in a different way. Today's high-level CISO is fundamentally different from yesterday's information security manager.

In no organisation has the role of the CISO fully evolved. There are some organisations – in the banking sector for example – where the CISO is near the top of the evolutionary tree, but even there further development is likely. Additional progress might include senior appointments from other industries, from law enforcement or from national security agencies. It might include aggregating all security responsibilities – including physical security – into one role, to create the position of chief security officer (CSO), as some companies have already done.

The CISO still has some distance to travel up the corporate ladder, of that I am sure. In my role as a board member of the Centre for Cyber Security at the World Economic Forum (WEF) I have seen first-hand the encouragement and importance WEF gives to the sharing of cyber intelligence between organisations, creating new tools to protect against cyber attacks – and developing the role of the CISO. We intend to implement global capacity-building and training programmes to produce the next generation of cyber security professionals and set up a Global Rapid-Reaction Cyber Security Task Force of experts.

The CISO as a value-protector and a value-adder

Cyber security is expensive. The CISO's department is a cost centre, an increasingly major cost centre. The CISO has to be able to demonstrate to the finance director and other controllers of the purse strings that the costs are justified.

It is difficult, if not impossible, to quantify the return on investment of security spending. Perhaps the best approach is to draw attention to the many companies that have hit the headlines because they were victims of high-profile, financially damaging, reputation-ruining cyber assaults, and the point is made. Effective cyber security is essential, and in the long-run it will save the company money.

A little more difficult, but eminently possible, is to demonstrate how it can make money. Today's brightest CISOs are showing how cyber security not only protects the business, but can enable the business. They are being asked by their board to a) keep us safe, but b) make sure your security measures do not get in the way of our digital transformation programme, and c) can your technological know-how be used to create a frictionless customer experience? In many cases all three requests can be delivered. A good example is mobile payments.

First, a bank payments app on a mobile device will incorporate all the latest security features to keep the bank and its users safe. Second, those security features will not detract from the digital experience, because a mobile payment is often the easiest and fastest payment method. Third, a mobile payment app that requires a fingerprint or other piece of biometric information to gain access – instead of an online banking account that requires the customer to input a log-in number, PIN and password – is far more convenient for the customer.

This is a prime example of the benefits of "security by design", where robust security measures, far from slowing down and spoiling the customer experience, have sped it up and enhanced it. Happy customers lead to bigger revenues. So cyber security at this level of sophistication will make the company money.

The money-making potential does not stop there. Large telecommunications companies have for decades had to invest vast sums in security to protect their networks and the privacy of their customers, especially as those customers often include ministries of defence, national security agencies and other government bodies communicating sensitive data.

As cyber threats have increased, these telecoms companies have been able to package their CISO-generated expertise into specially created subsidiaries and sell their security technology and consulting services to organisations that have not been able to develop the same capabilities. This has created a profit centre for the telecoms companies which has gone a long way to defraying the costs of protecting themselves.

Strong cybersecurity is the foundation for a resilient company. With effective cyber risk management, businesses can achieve smarter, faster and more connected futures, driving business growth.

It is fascinating to see how the position of the CISO has evolved, from being a cost generator, to a value protector and, in certain cases, to a value adder. Different companies are at different stages of the evolutionary process, depending on a variety of factors such as management foresight, industry sector and country of operation. With a dynamic landscape such as cyber it calls for a new breed of cyber security leaders and there must be a continued acceleration of the CISO role in order to adapt to the ever-changing, cyber environment.

Contacts

Sir Rob Wainwright
Partner, Risk Advisory, Deloitte
The Netherlands
+31882880032
rwainwright@deloitte.nl

Acknowledgements

We are grateful to Chris Verdonck, Nick Seaver, Mark Nicholson, Vikram Bhat, Stephen Bonner and Michael Imeson for their insight and guidance, without whom this article would not have been possible.

Notes

Notes