tripwire

The Changing Role of the CISO

Cybersecurity in a More Complex World

RANT

A RANT WHITE PAPER

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

The chief information security officer, or CISO, is essential to the smooth and safe operation of any large organization.

Over the past few years, though, the scope and scale of the CISO's task has increased markedly. No longer simply a head of IT security, the CISO is responsible for a far wider range of cyber defenses and protective measures that extend well beyond the organization's perimeter.

Today's CISO can be tasked with protecting data in the cloud, with compliance and often data protection, business resilience, and even elements of physical security. And, following the acceleration of the trend for remote and home working, they will be looking after assets and employees who could be anywhere in the world. These changes also come at a time when the threats organizations face are developing rapidly, and as more business activity operates in the digital realm.

Organizations need to be more agile, and more responsive to customers and stakeholders. They need to embrace new technologies and enter new markets. They need to protect their data from malicious actors. And they need to do so by balancing opportunity and risk.

This makes the CISO's remit wider, and their role more complex. But by working with the business, the CISO can contribute directly to the organization's strategic development in a way that was never possible when the job was simply IT security.

Remote Working, Flexible Working: Managing a More Complex Environment

Remote and flexible working are now mainstream—and security has to keep up

In 2020, a quarter of people in the UK worked from home at least some of the time, according to the Office of National Statistics. The number of remote and home workers doubled since 2019, driven by the Covid-19 pandemic and lockdown restrictions. In some sectors the figures are much higher—a number of high-profile businesses have said employees can work continue to flexibly, including from home, for as long as they want.

But the growth in home working during the pandemic is part of a longer-term trend, driven by the growth of cloud computing and high-quality data communications. Indeed, industry experts observe that had the pandemic happened 10—or even five—years ago, businesses would have been in a far worse position.

New infrastructure, new possibilities

Software-as-a-Service technologies, including Microsoft Office365 and Google Workspace (formerly G Suite), cloud storage and online collaboration tools, and the proliferation of powerful personal devices were already driving up productivity. Organizations moving enterprise applications to SaaS, or opening them up to remote users, completed the picture.

These newer ways of working are about more than survival. Organizations that were quick to adapt to the pandemic included those that already had remote or home working as part of their business continuity plans, and those that already had successful remote and flexible working schemes in place. The task was to scale these up; they did not have to build infrastructure from scratch. Organizations without that grounding faced more of a challenge, including acquiring and deploying laptops and upgrading VPN infrastructure. But it is a challenge they have largely met.

In both cases, this infrastructure is likely to stay, even when firms reopen their offices. It supports business goals through greater flexibility, employee retention, and greater resilience. After all, the current pandemic might not be the last.

And today's knowledge worker is far more likely to access the network through a browser or a web-based API than a desktop application or a conventional client or endpoint device. Instead, they could move between mobile and desktop, hot-desking and smart home devices, all within the working day.

Mixed environments

As a result, organizations face maintaining two parallel sets of infrastructure: on-premises systems, devices and networks for staff who are in the office, and a range of mobile and remote technologies for when they are not. These technologies will no longer be restricted to a "road warrior" class of salespeople, engineers, and senior executives.

So far, we are only at the start of this journey. Mixed environments could scale much further, as people who have had a taste for home working realize that "home" could be anywhere, and offices start dealing with more part-time and more mobile workforces.

This will bring greater flexibility to the workforce, but it also brings more complexity. That complexity runs the risk of weakening security. It also makes the CISO's role more wide-ranging and, arguably, more difficult. Security itself needs to be more agile.

Security questions

Inevitably, more diverse and more complex technology creates new security risks. The organization's attack surface is larger, and there is evidence that cybercrime groups have exploited the move to remote working—as well as the pandemic itself—to target businesses.

Clearly some organizations found remote working a challenge from

a security and data protection standpoint, especially those that had focused on office-based work. Organizations were forced to invest in technology and additional infrastructure to remain effective in business.

Over a year on, most have adapted to remote working, by adjusting their security policies and introducing new security measures to keep employees safe while working remotely. Those new measures should stand them in good stead in other areas too, including as business travel restarts.

But there is no avoiding the fact that IT and security teams have more infrastructure to protect and manage. Protecting it will cost money and time. Security in general is a lot more difficult. In all, this leads to increasing workloads for the CISO.

Securing Technology, Everywhere

The CISO has a broader remit than ever, as IT touches everything

How then does today's CISO define their role? The CISO's areas of responsibility are broader than ever. At the core, IT security is still vital, but the last decade has seen a shift from securing IT systems to securing data and information. CISOs are increasingly tasked with monitoring and responding to external threats, including cybercrime and state-backed actors, as well as malicious hackers.

The most high-profile threats might be purely digital, but the role also crosses over into physical security, through the Internet of Things, SCADA and critical systems, and even protecting personnel operating remotely.

The CISO is also likely to have compliance responsibilities, and responsibility for dealing with insider threats and, along with HR and internal communications, end-user security awareness and education. This can even extend to helping senior executives manage their social media presence.

Traditionally, the CISO or head of IT security role has been internally facing, focusing on areas such as compliance and keeping data secure. But CISOs are now providing services that are more outward looking, including SOC as a service or consultancy. These services might be provided only to internal customers, or to external stakeholders as well. Either way, it is a new discipline for IT security teams. As well as this, they will be involved in purchasing decisions, and with software development—the idea of "DevSecOps"—and addressing security much earlier in technology projects.

Few of these were part of the CISO's role, even 10 years ago. And CISOs now face dealing with a far more fluid setup than when most IT was neatly behind the firewall.

The Changing Business Perimeter

Until recently, most remote workers accessed critical IT assets from behind the perimeter, or via a VPN. Cloud services, including Office365 and other business applications outside the perimeter of the organization, reduce the dependency on VPN services. These allow organizations to extend the corporate network into remote locations—including the home—with little in the way of physical security controls.

For those organizations that do rely on VPNs, there are security risks. Attackers have targeted VPN concentrators. Adopting hardening standards and enforcing software policies is a must if organizations are to remain secure.

And IT security also needs to move away from its focus on the endpoint. Endpoint security is starting to look like an outdated concept. Security, instead, must be continually verifying user access. But defenses for servers and traditional IT infrastructure will remain. These could even become more important as more machines are required to serve up web services for users to access on the move.

CISOs will need to address this requirement, as well as the need to "harden" cloud applications. Cloud security might not have been the first priority early in the pandemic. But with cloud technologies now firmly embedded in most organizations' ways of working, security needs to catch up. And there is a further challenge: the convergence of IT and operational technology (OT).

IT and OT: Converged Security

As well as digital transformation, the CISO's role is expanding because of the way OT is increasingly connected. Industrial control systems, manufacturing machinery, vehicles, and buildings and facilities are increasingly networked. The growth of the Internet of Things (Iot) might attract the most attention, but OT is as important from a security point of view. And often, IoT is used together with OT in order to bring more visibility into operational systems.

As OT converges with IT, organizations are using IT teams to secure OT environments. Here, misconfigurations could occur. The risks are made worse though the need to share infrastructure. Ideally, from a security point of view OT environments would remain segregated from the IT network. But that is not always possible—or even desirable. Plus, IT and OT have different priorities and work at a different pace.

OT and IT have a different emphasis on risk and reliability. IT might be able to update a system in a matter of a few clicks. However, OT teams must plan, often months in advance, to run a single patch on a single system. This can lead to a mismatch between security across the two pillars. Again, these are vulnerabilities malicious actors will find, and exploit. Not all CISOs—or security teams—will have a background in OT, its constraints, and its requirements. There is far more collaboration now between

OT and IT than ever before, but even so, a one-size-fits-all approach to security is unlikely to work.

IT and cybersecurity functions have become used to a fast pace of change to stay ahead of threats. But can result in a fragmented set of security solutions. This needs to be addressed to ensure consistency of internal security processes across mixed IT/OT environments.

CISOs will need to spend more time on OT security, especially as it becomes more instrumented—through the IoT and smart devices—and linked into other business objectives (such as a reducing environmental impact through smart buildings). These are all areas that are increasingly networked, and so need to be secure at the same time that CISOs are addressing the needs of digital business transformation.

Digital Business

Digitalization of business, or digital transformation, potentially extends the CISO's role into every area of operation. This can lead to mission creep, an IT or cybersecurity team that is overwhelmed by work requests, and a SOC that is overloaded.

Security teams are also being pulled into areas where they might not have operated before and might lack expertise, the cloud being just one example. Even very experienced "traditional" security experts are finding gaps in their skillset that need to be filled.

Growth in cloud and SaaS is spreading security knowledge thin and putting more pressure on security teams at a time when it is hard to attract suitable candidates with the right skills. Talent and skills development becomes another item to add to the CISO's to do list.

And there is a further trend at work: for the CISO to become one of the business's most important advisers on risk.

Building a Business Case for Cybersecurity

Investments in cybersecurity need to lead to business value. Part of the extended role of the CISO is to demonstrate how it can support the wider business. However, it is notoriously difficult to prove a return on investment from security.

Calculations around security incidents focus most often on direct costs, such as damage caused, loss of business, or regulatory penalties. Or else they focus on indirect costs, such as reputational damage, loss of customer confidence, and impact on share prices. Security spending is viewed as an insurance premium—a way to avoid these costs.

Base-level technical security measures are a cost of doing business. But security can—and does—enable new ways of working and, potentially, new products and services. Innovations, from electric cars to smart meters to music downloads and online banking, depend to a great extent on effective security.

So, too, do new ways of working, from digital business processes to predictive maintenance in factories or intelligent supply chains. The CISO can contribute to all these areas, even as they increase the scope of their role.

A focus on cybersecurity as opportunity cost misses the efficiency gains that come from good security processes (such as Zero Trust). These processes can reduce friction by replacing overly simple access-based controls with the introduction of seamless security checks—cybersecurity that seamlessly ensures a device is up to date in the background and does not interrupt the user. It works towards the goal of letting employees focus on the task in hand, not managing security.

Of course, a strong cybersecurity posture reduces threats and potential data loss and makes the delivery of new products and services safer and easier. Communicating this, however, demands new skills from both the CISO and their team.

Security as an Enabler, Not a Barrier

The CISO has a further challenge: to overcome the perception that security is an obstacle to doing business. This means moving security beyond a technical or compliance-focused function and involving CISOs earlier in key decisions. Two areas that are making this change possible are in development (where DevOps is moving towards DevSecOps) and automation.

Security should never be seen as a barrier. Security teams need to work with, and compromise with, developers to ensure they are releasing secure code. Automated DevOps solutions can tie into workflows to identify potentially vulnerable systems before they are deployed. Regular testing on projects and engagement from security managers at an early stage of the project should be compulsory to maintain a good and strong relationship.

Automated security testing also needs to be a core area of investment for any software development business, and skilled staff are required to really take advantage of this; without someone "selling" security in your development workflows, it is unlikely to be given the importance it deserves. For those advocating security in development, the key is to position security as a method of making your product more robust and more available, and therefore more profitable.

Automation is also the simplest way to make sure that security is not bypassed for simplicity and ease. If security is baked into every process, and people were not even aware that it is taking place, then they would be open to including it in everything that they can. Nobody with good intentions would ever suggest security be ignored if it had no impact to their everyday lives.

The Changing Role of the CISO

The CISO as an IT expert, or an expert on risk?

The most marked change in the CISO's role over the last decade is less about technology and more about where they sit within the wider business. In forward-looking organizations, the CISO is one of the business's risk advisers, if not a risk officer. The CISO is no longer primarily there to manage technical IT security, although they are likely to manage teams with that responsibility. Instead, the role is focusing more on monitoring threats and understanding risk, and communicating those to the business, and to the board.

Over the last few years, as cyber threats have grown in their scope and impact, cybersecurity teams have moved away from the notion that they can block all attacks—the "ever higher walls" approach—to an understanding that attacks will happen and breaches are likely. If attacks cannot be prevented, then the focus turns to resilience. The organization needs to know if it can continue to operate, and if there is a breach, how quickly normal operations can be restored.

The growing attention paid to cyberattacks and security breaches might even have bolstered the CISO's position. CISOs are more involved in key decision making and their voices are being heard more often than they were in the past; boards are increasingly aware of the financial, regulatory, and public perception consequences of attacks.

This gives the CISO the opportunity to highlight positive security approaches to problems. That, in turn, might drive a greater emphasis on security in environments such as the cloud, or OT, and a better appreciation for the ROI that security can bring to the business. This understanding leads to a more nuanced approach to business risks. Security decisions are no longer clear-cut, or that an attacker is blocked, or breaks through.

In a mature organization, boards will balance the potential security threats and risks of an initiative with the likely rewards. CISOs should be at the heart of this process, advising the business, so boards can make informed decisions on whether they can accept the risk, or if not, how to reduce or mitigate it.

The next step is for the CISO to demonstrate that security is about reward, as well as risk.

A New Model for the CISO

Taken together, the trends in how business operates, regulatory pressures, and, above all, changes in the threat landscape have significantly expanded the CISO's areas of responsibility. Organizations are responding in a number of ways. On the surface, some of these might seem contradictory.

For some organizations, the CISO is clearly a single, board-level appointment with overall responsibility for information security, and quite often other aspects of security too. In others, business functions have their own security teams and CISOs, responsible for IT security. And in yet others, the CISO sits under the IT department, or the chief technical officer. There is no single approach.

Elsewhere, the move is towards a team of security leaders, reporting to a single overall CISO, or even an "office of the CISO," where multiple information security officers report to an executive who manages the team and reports to the board. This approach might also bring together specialists in areas adjacent to IT security, including resilience and business continuity, crisis management, and physical security.

New Approaches

Other organizations are moving towards a single CISO, focused on both the OT and IT estates. Often this involves a steep learning curve, no matter if the CISO comes from an IT or OT background.

But, as is seen in other areas of convergence (including DevOps, digital transformation, and physical security), this is an inevitable part of the business's growing awareness of the threats it faces. The business needs to understand and control risks across the organization, and the CISO function needs to be organized in a way that supports that.

Drawing Lessons From a Riskier Environment

In the world of IT security old threats rarely disappear, even as they become less prominent. As in all areas of technology, cybersecurity does focus on the latest greatest (or more accurately, worst) threats. New threats will always come along, but methodologies that worked five, 10, or even 15 years ago are still being used today. Techniques such as phishing are still very successful, and until we can educate the whole community, they will not stop.

CISOs must balance the need to continue protecting the existing estate with the requirement to defend against newer threat vectors such as ransomware, supply chain attacks, and state-backed actors. The scope of the role continues to grow, as new risks are added to older vulnerabilities.

Inevitably, security success stories attract less attention than failures. But businesses can boost their protection by being more proactive and ensuring systems are secure by default and stay that way.

Simple steps, such as keeping up with patching or improving machine deployment so that security is baked in, show how basic security can be cost effective and help protect the business when the

worst happens. This approach is neither particularly new nor especially innovative. However, it is proven and, in most cases, highly effective.

Above all, though, the CISO needs to link what they are going back to the strategic goals of the organization. Those goals might mean accepting more risk—the key is ensuring that boards can make an informed choice.

Section 4: Conclusions: The CISO in the Changing World

Bridging the gaps between business units, and stakeholder management

For the CISO, engaging with other areas of the business that traditionally were kept separate from IT means the CISO office needs to consider its alliances and expand its thinking to include more areas of the organization.

The chief information security officer is a common job title. But in practice, no two roles are the same. For today's CISO, it the role is less about technical skills and more about understanding how to put the right resources in place.

This is an inevitable consequence of the CISO's ever broader responsibilities. And it reflects the way that digitization has brought new threats, as well as new opportunities, as cybercrime and malicious hacking has risen. But it also brings opportunities. The CISO is well placed to anticipate those threats, and to respond. In turn, that makes the CISO one of an organization's key advisers on risk.

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook

WPRCRCISO1a 2108