BULLETPROOF

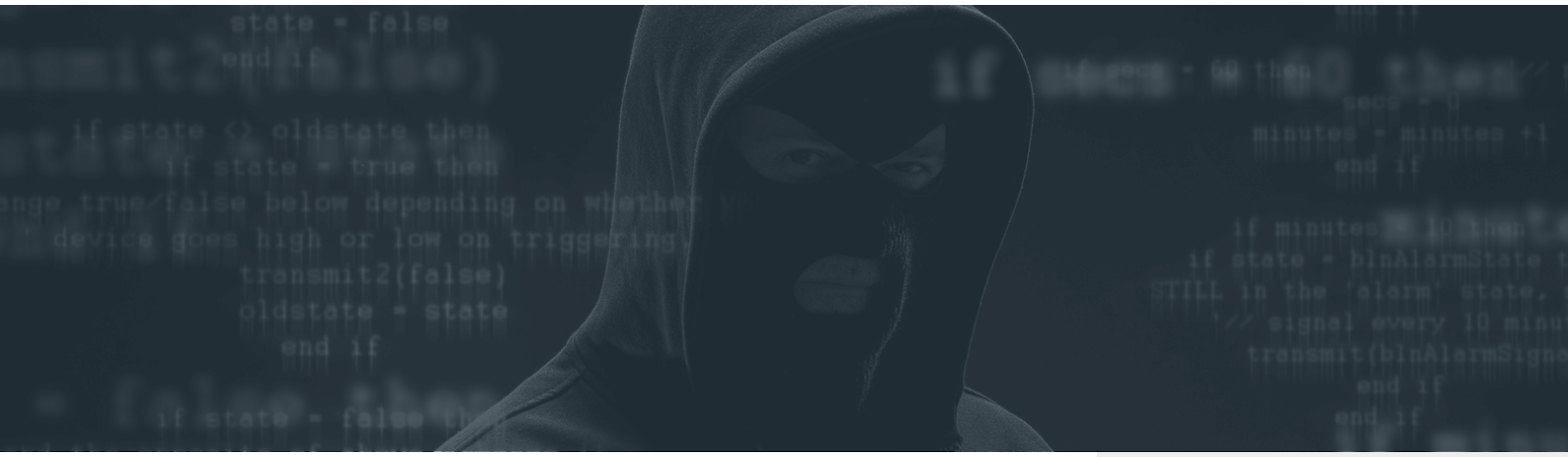
WHITE PAPER

Understanding Virtual CISOs

DECEMBER 2024

CONTENTS

INTRODUCTION



Let's start with a sobering statistic. According to the World Economic Forum , the estimated global cost of cyber crime in 2023 was £8.4 billion. To put that another way, cyber crime cost about £280,000 every single second – which means in the time it took you to read that, over £1 million was lost to scams, ransomware and data breaches.

What's more, it's only getting worse, with the cost of cyber crime expected to reach over £18 billion by 2027.

With businesses being prime targets, information security is now as essential to a company's operational health as anything else you care to mention. Given the rapid advances in cyber crime techniques, however, simply installing antivirus software isn't going to keep your business safe anymore.

Companies increasingly need a dedicated Chief Information Security Officer (CISO) — a senior executive responsible for managing and safeguarding an organisation's information and technology assets.

The problem here is that not every company can afford a CISO. This gap has given rise to the virtual CISO (vCISO), who delivers expert-level security guidance without the financial burden of being a full-time employee.

In this white paper, we'll explore the role of a vCISO, the benefits they bring and why businesses of all sizes should consider adding one to their team.

£8.4B

GLOBAL COST OF CYBER CRIME 2023

£280K

CYBER CRIME COST PER SECOND

£18B+

GLOBAL COST OF CYBER CRIME 2027

SAY HELLO TO THE VCISO

A Virtual Chief Information Security Officer is a security expert who provides leadership, strategy and oversight for an organisation's information security efforts — but unlike a traditional CISO, operates on a part-time, contract or consultancy basis.

As a result, even smaller businesses can gain state-of-the-art information security expertise without it breaking the bank.

Typically, vCISOs are seasoned professionals with extensive experience across numerous industries, with both a deep understanding of security threats and the sector-specific regulatory requirements that go with it.

They bring the same strategic oversight as an in-house CISO but are more affordable and flexible. While some organisations will need a dedicated CISO, most businesses may not necessarily need one five days a week.

The role of a vCISO varies depending on an organisation's needs. For smaller businesses, a vCISO might focus on establishing a basic information security framework, conducting risk assessments or maintaining compliance with regulatory requirements like GDPR, PCI DSS, or ISO 27001.

For larger organisations, a vCISO can provide more targeted, high-level advisory services, helping to develop long-term security strategies, manage ongoing risks and respond to security incidents.

VCISO ROLES AND RESPONSIBILITIES

Whatever the size of your business, vCISOs bring several key strengths to the table.

STRATEGIC LEADERSHIP AND SECURITY OVERSIGHT

One of the main roles of a vCISO is to steer a company's wider information security strategy. This includes assessing an organisation's current security environment, identifying weaknesses and developing comprehensive procedures to address them.

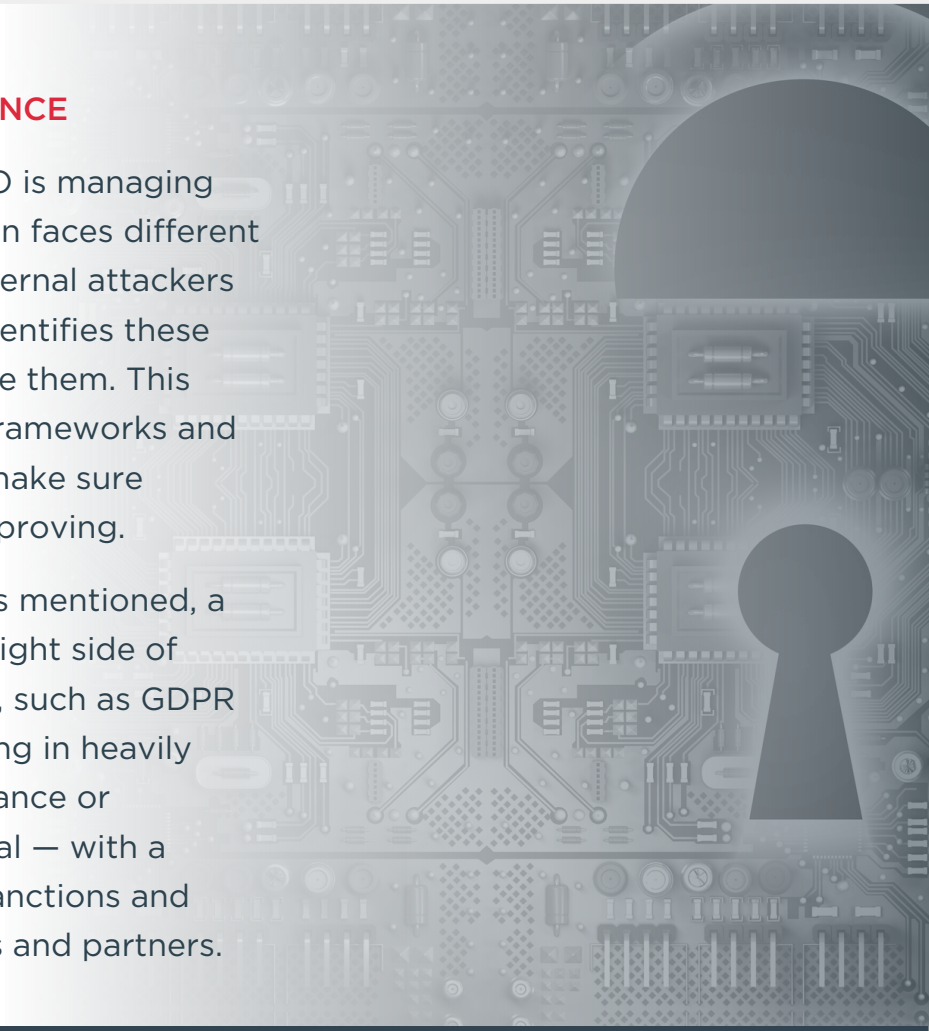
A vCISO also ensures that security policies and procedures are established, documented and followed across an entire organisation. There's little point in creating an overarching security strategy if your remote staff, for example, either don't know about it or aren't paying attention. Virtual CISOs oversee the creation and enforcement of security policies, which can include everything from access controls to incident management protocols.

"There's little point in creating an overarching security strategy if your remote staff, for example, either don't know about it or aren't paying attention."

RISK MANAGEMENT AND COMPLIANCE

Another key responsibility of a vCISO is managing your security risks. Every organisation faces different threats, whether they come from external attackers or internal vulnerabilities. A vCISO identifies these risks and designs strategies to reduce them. This involves creating risk management frameworks and conducting regular assessments to make sure security measures are continually improving.

Compliance is another major area. As mentioned, a vCISO helps businesses stay on the right side of industry-specific standards and laws, such as GDPR and PCI DSS. For companies operating in heavily regulated sectors like healthcare, finance or government, this guidance is essential — with a vCISO reducing the risk of fines or sanctions and helping to build trust with customers and partners.



INCIDENT RESPONSE AND CRISIS MANAGEMENT

In the event of a security breach, a vCISO plays a key role in coordinating an organisation's response. They develop incident response plans that detail the steps to be taken during a breach — from identifying the threat to mitigating damage and recovering from the incident. Regular simulations or drills are conducted under the vCISO's leadership to keep businesses prepared and able to respond quickly and effectively should an attack occur.

A key part of why a vCISO is so valuable is that they can get your business prepared for an incident without the preparation taking too much time or resources away from your business as usual. Beyond immediate incident response, a vCISO is also responsible for long-term crisis management, helping the company to minimise damage and maintain business continuity. This might include coordinating with legal teams, liaising with affected clients and making sure that any regulatory reporting obligations are met.

TRAINING AND AWARENESS

The role also helps nurture a security-conscious culture within an organisation. A virtual CISO will develop and deliver training programmes designed to educate employees on cyber security best practices, such as recognising phishing attacks, using strong passwords, and maintaining proper data handling procedures. With human error often being the weak link in security, vCISOs focus on education and awareness to help reduce the risks associated with people just being people.

"With human error often being the weak link in security, vCISOs focus on education and awareness to help reduce the risks associated with people just being people."

COMMUNICATION WITH STAKEHOLDERS

Finally, a vCISO acts as a bridge between the technical and business sides of an organisation. They communicate security risks, strategies and progress to C-level executives, board members and other key stakeholders clearly and concisely.

In this way, they ensure that security remains a priority at the highest levels of an organisation and that all departments are on the same page. Part of their job is to engage the business leadership and make sure information security is on the agenda, and on the budget. Again, the vCISO can co-ordinate, play a key role, and serve as a trusted advisor, but ultimate responsibility lies with the leadership of the business

THE BENEFITS: WHY THE VCISO HAS BECOME SO POPULAR

The short answer is: they're affordable. Hiring a full-time, in-house CISO is prohibitively expensive for most companies, especially SMEs and mid-market organisations. With a traditional CISO costing an average of around £155,000 a year, they're not cheap to employ by any means. A vCISO, on the other hand, delivers a more flexible and affordable alternative, allowing businesses to access high-level security expertise on an as-needed basis, without the overhead costs of a permanent employee.

This flexibility is particularly appealing to companies that may not require a full-time security executive but still need expert guidance. A vCISO can be brought in for specific projects such as risk assessments, compliance audits or developing security policies, allowing organisations to address security issues according to their immediate needs.

"With a traditional CISO costing an average of around £155,000 a year, they're not cheap to employ by any means."

UP-TO-DATE EXPERTISE

Cyber security is a continuously and rapidly changing arena, and keeping up with the latest threats, regulations and technologies requires specialist knowledge.

No matter how technically-minded you may be as a business owner, you're unlikely to have the same insight and understanding as a dedicated professional. You wouldn't check your own teeth to keep them healthy, and you shouldn't rely on your own security assessments to keep your business healthy either.

MULTIFACETED EXPERIENCE

Most importantly, a vCISO brings a wealth of experience gained from working with different organisations, industries and technologies.

This diverse background equips them with deep insight into information security and the specific issues that individual sectors and businesses face.

What's more, as the nature of cyber security threats has grown in sophistication and frequency, the demand for security leadership has intensified.

As a result, there's a severe shortage of qualified CISOs, with many companies struggling to fill the role. A vCISO provides an ideal solution to this talent gap, offering immediate access to highly experienced professionals.

COMPLIANCE AND REGULATORY DEMANDS

Compliance isn't always at the forefront of businesses' security concerns (certainly for smaller businesses), but it's an increasingly unforgiving environment that can cost companies dearly if they don't adhere to regulations. Given the ICO issues fines for data protection breaches each and every month, compliance is a central issue that shouldn't be overlooked.

Complicating the issue further is the fact that there's currently no regulatory consensus, with numerous different security regulations existing depending on the sector you operate in as well as your geographic region.

A vCISO helps businesses stay on top of all this, keeping them on the right side of everything from GDPR to HIPAA. By doing so, they not only help businesses avoid fines but also improve a company's reputation by demonstrating a commitment to protecting sensitive data.

FOCUSED SECURITY LEADERSHIP

Unlike IT managers or staff members who often juggle multiple responsibilities (including security), a vCISO delivers dedicated leadership in the field. In many organisations, security is treated as an additional task rather than a primary responsibility which can result in oversights or incomplete security measures. A virtual CISO will ensure your business resources are used efficiently and effectively to make real security improvements.

SCALABILITY

As businesses grow, their security requirements expand as well. A key advantage of a vCISO is their scalability — they can adjust their involvement as the company evolves. For smaller businesses, a vCISO may provide part-time services, focusing on core security needs. However, as the company grows or faces new challenges, a vCISO can increase their level of support, tailoring their security strategies accordingly.

This flexibility means that businesses always have the right level of security oversight, whether they're undergoing rapid growth, a merger, or expanding into new markets. It also allows for cost control, as companies can scale their vCISO services to match their budget and security needs without compromising quality.

OBJECTIVE PERSPECTIVE

As convenient and knowledgeable as internal teams may be, they have a habit of developing blind spots due to being overly accustomed to their environment. A vCISO brings an impartial, third-party perspective to a company's security, identifying vulnerabilities that might go unnoticed by internal staff.

The internal politics within this shouldn't be ignored. Criticisms of security measures made by internal staff can quite easily be seen as an attack on whoever was responsible for the measures (no matter how valid the criticisms may be). A vCISO doesn't suffer from this political tiptoeing and will call things out as they see them.

ADVANTAGES OF A VCISO FOR SMALLER BUSINESSES

It's an unfortunate (and equally unfair) reality that cyber criminals are increasingly targeting smaller businesses, precisely because they don't have the security infrastructure associated with larger companies.

In 2024, 81% of all UK companies that experienced a cyber attack were small to medium-sized businesses.

While smaller businesses may recognise the need for an effective security framework, they simply don't have the money to hire a full-time professional. This is where a vCISO offers the biggest advantage, delivering expert-level security insight at a fraction of the cost.

When you add the 'on-demand' flexibility of vCISOs to the equation, even small businesses can implement the solid cyber security measures needed to keep them safe and compliant.

IN 2024, 81% OF ALL UK COMPANIES THAT EXPERIENCED A CYBER ATTACK WERE SMALL TO MEDIUM-SIZED BUSINESSES

ADVANTAGES OF A VCISO FOR LARGER BUSINESSES

Larger companies operating in numerous territories face complex security challenges. From diverse technological infrastructures to a wide array of regulatory requirements, there are any number of issues that a vCISO is well-positioned to address.

COMPREHENSIVE EXPERTISE

Larger organisations typically require a broad range of security expertise due to the multifaceted nature of their operations. The wealth of varied knowledge and experience that a vCISO brings to the table provides larger organisations with the wide-ranging insight they need, quickly and cost-effectively.

SCALABLE SOLUTIONS FOR GROWTH

As larger businesses expand or enter new markets, their security needs can change dramatically and quickly. A vCISO provides scalable security strategies that rapidly adapt to an organisation's evolving requirements.

Whether it's integrating new technologies, managing increased data flows or navigating the complexities of mergers and acquisitions, a vCISO makes sure a business's security posture moves in tandem with its growth.

POTENTIAL PITFALLS OF OPERATING WITHOUT A VCISO

It's a brave (or foolhardy) business that engages with the modern digital marketplace without a well-thought-through security strategy. Without a vCISO, the responsibility for cyber security will likely fall onto IT managers or staff members who are already juggling multiple roles. This can lead to insufficient focus on security, resulting in overlooked risks, outdated protocols and compliance gaps.

LOSING SIGHT OF THE BIGGER PICTURE

The experience and expertise that a vCISO brings allows companies to tailor security strategies that align with their needs and objectives. What does that mean in practice? It means companies can adopt a proactive approach to security that places them ahead of the curve. Without the guidance of a vCISO, businesses tend to adopt reactive measures instead, leaving them vulnerable to all manner of threats.

CHALLENGES IN RISK ASSESSMENT AND AUDITS

Without a vCISO, organisations may struggle with risk assessments and audits. Regular assessments are essential for identifying vulnerabilities and understanding potential threats. Without these evaluations, businesses can remain blissfully unaware of any existing security gaps, resulting in major financial and reputational damage in the event of a data breach.

"Taking vCISOs out of the security equation leaves companies with the profound challenge of staying current with continually evolving threats."

DIFFICULTY KEEPING UP WITH THE CRIMINALS

Taking vCISOs out of the security equation leaves companies with the profound challenge of staying current with continually evolving threats and compliance requirements. If there's one word that characterises the cyber security arena, it's 'change'. Without dedicated expertise, businesses risk falling behind and becoming prime targets for cybercriminals who view them as an easy target.

WHEN TO CHOOSE A VCISO AS OPPOSED TO A CISO

As should be clear by now, there's little doubt that companies need dedicated cyber security talent as part of their team. The only question is deciding between a traditional in-house CISO and a virtual CISO. The key factors you need to consider are as follows.

THE SIZE OF YOUR BUSINESS

A traditional CISO is typically better suited for larger organisations with complex structures. Although vCISOs offer definite advantages over CISOs to larger companies, such as a wider range of experience, and service continuity during employee time off, for example), CISOs have traditionally tended to be the normal way forward. Conversely, a vCISO is a more practical choice for startups, SMEs and mid-market companies. These businesses often don't require full-time in-house security leadership and benefit more from the flexibility a vCISO offers.

BUDGET CONSTRAINTS

Cost is a key factor, of course. Hiring a full-time CISO comes with substantial financial commitments, including a high salary, benefits, and related expenses. On the other hand, a vCISO provides a more budget-friendly option, with flexible pricing models and no gap in service continuity.

CYBER SECURITY NEEDS

If your organisation operates in a heavily regulated industry or faces constantly changing cyber threats, an expensive in-house CISO may be your first thought. However, a vCISO is ideal for companies with more predictable security needs or those looking to bolster existing security strategies without the need for a dedicated, full-time position.

STRATEGIC GOALS

Long-term security culture building, at enterprise scale, is probably best supported by an in-house CISO, who can align security initiatives with the company's corporate vision. For smaller organisations, a virtual CISO will handle the job of promoting security awareness and education in-line with company mission and values.

STAY SAFE WITH BULLETPROOF'S VCISO SERVICES

Whether you're a small business looking to establish a basic security framework or a large company in need of strategic guidance, our team of expert vCISOs is here to help.

Our vCISO services include:

- **Risk assessments:** We evaluate your current security environment, identify vulnerabilities and provide actionable recommendations to reduce risk.
- **Security strategy development:** Our vCISOs work with you to develop a comprehensive security strategy that aligns with your business goals and industry requirements.
- **Compliance support:** Our experts guide you through the complexities of achieving and maintaining compliance with industry standards such as ISO 27001, PCI DSS, and GDPR.
- **Incident response:** We help you prepare for and manage security incidents, minimising the impact on your business and ensuring a swift recovery.
- **Ongoing Support:** Whether you need ongoing strategic advice or help with specific projects, our vCISOs are available on a flexible basis to meet your needs.

With a vCISO from Bulletproof, you gain the highest-level of security leadership in the most cost-effective way possible. More than keeping your business safe and compliant, we'll keep you from becoming yet another cyber crime statistic.

To find out more about vCISOs and how Bulletproof can keep your company secure without damaging your bottom line, get in touch today.

www.bulletproof.co.uk

contact@bulletproof.co.uk

+44 1438 500 500

BULLETPROOF