SECURANCE CONSULTING

the advantage of insight

The Emergence of the Virtual CISO

www.securanceconsulting.com

LEADERSHIP IN A TIME OF CYBER CRIME

The explosive growth of cyber crime forces businesses of all sizes to dedicate more resources to IT security and compliance. While large organizations and small and medium-sized businesses (SMBs) face similar risks, large companies have the financial resources to hire and retain highly skilled security experts. As they expand their IT security efforts, the market salary for qualified IT security executives rises, pricing SMBs out of the hiring market.

Even if cost is no object, companies and governments are faced with a global shortage of skilled cybersecurity experts, creating a demand for innovative solutions. Enter the Virtual Chief Information Security Officer (vCISO), an executive that provides cybersecurity leadership to multiple companies, minimizing costs and maximizing ROI. In the same way that cloud services allow smaller organizations to access technology solutions that would be too costly to build in-house, vCISOs provide leadership and guidance at an executive level that would be too costly to hire in house.

This paper discusses the risks that skyrocketing IT security salaries and rising levels of cyber crime pose to SMBs and how working with a vCISO can enhance security and regulatory compliance.

> 2019 saw **4 trillion** intrusion attempts across the globe.[1]

THE HIGH COST OF HIGH SECURITY

SMBs have three things hackers want— information, access to larger companies, and money— but it's their lack of cybersecurity expertise that makes SMBs such appealing targets. Many try to meet their security needs by distributing security, risk, and compliance duties across their existing staff or reassigning someone to become the "expert." These methods are ill-suited to handling the threats posed by organized criminals and government-sponsored cyber spies, who have endless resources at their disposal.

Too Many Hats

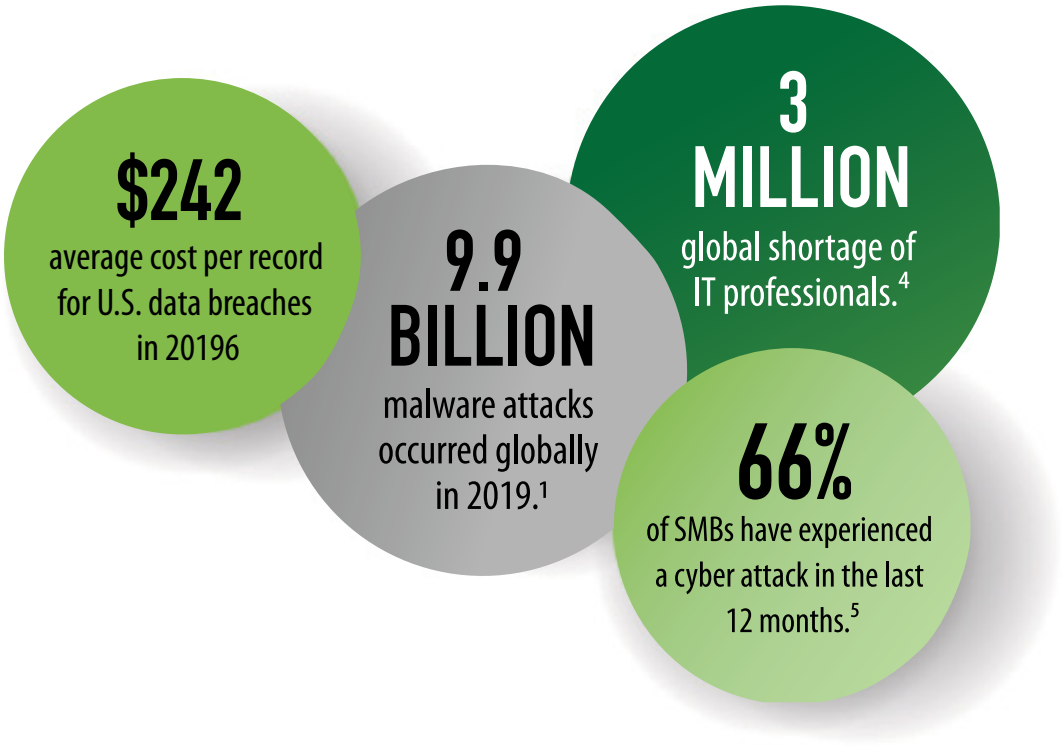
Large corporations hire teams of experts to manage each component of their sprawling IT infrastructures. SMBs employ smaller teams, requiring individuals to have diverse experience and wear many hats within the organization. The diversified skills approach to staffing works well for traditional IT software and systems management, but it doesn't work well for cybersecurity.

Consider an IT manager, let's call her Mary, planning a server operating system upgrade. She must research and evaluate everything from costs to hardware compatibility and system downtime, but nobody is working against her while she does it. Contrast this with Jim's attempt to harden cyber defenses, where every door he closes is liable to be pushed and pried at by automated bots or hackers, who may be operating alone or with a team of people with specialized skills and unlimited time.

> The average salary for a CISO is **$172,000.**[3]

Mary can do her research, make a plan, upgrade the server, and move on to the next project. It is unlikely that someone is going to break in and undo her work. Jim can walk away and move onto the next project, but the hackers working against him won't go away.

The more time Jim has to spend working on other projects— like software upgrades, backup systems, router configurations, or one of many other tasks IT teams have to manage and monitor— the less time he has to stay on top of the constantly evolving threats from sophisticated, efficient, and innovative hackers around the world.



Not Enough Experience

Some SMB leaders survey the threat landscape, realize they need someone dedicated to security, and try to promote from within. However, those candidates, coming from an IT background where security was one of many duties, lack the business acumen and subject matter expertise to advise the C-suite on information security, compliance, and risk management.

The competencies required to provide leadership and guidance at an executive level (e.g., CEO, COO, CIO) are not easy to attain. The leadership component requires a candidate with the capacity to persuade and interact with a variety of stakeholders, drive change, integrate security initiatives with business objectives, and provide strategic foresight. The cybersecurity component necessary for a CISO demands knowledge of numerous technology solutions, deep understanding of regulatory issues, experience assessing and managing risk, and strategic foresight.

Another pitfall of promoting an under-qualified candidate from within is the asking salary for someone legitimately qualified to serve as a cybersecurity expert, which, at the executive level, starts around $200,000 and can exceed $1,000,000. Some reports estimate a global shortage of more than 3.5 million cybersecurity professionals by 2021, which means hiring costs will continue to rise. If a smaller company hopes to promote from within and pay for training necessary to fill knowledge gaps, they need to be prepared to lose the promoted employee as soon as his or her resume is strong enough to attract outside attention. Even the most loyal employee would find it hard to turn down a recruiter offering more experience, training, and compensation.

> Appointing a CISO results in an average decrease of **$180,000** in the cost of a data breach, where the average cost is **$3.92 million.**[2]

The convergence of escalating risks and a lack of skilled professionals drives hiring costs up and threatens SMBs with a cybersecurity talent gap. However, SMBs can take advantage of innovative vCISO services that deliver solutions designed to fit their needs and budgets. In this sense, SMBs have an advantage over companies that are larger but still have difficulty paying for the services of a full-time CISO.

Why Invest In Executive Leadership For Cybersecurity?

CISOs bring the level of skill, authority, and accountability delivered by other C-suite executives, such as CFOs, COOs, and CEOS, to information security. Working with other company leaders, they develop a strategic vision for how the business can integrate cybersecurity efforts into normal operations, creating a more secure, more resilient organization that can thrive in an environment plagued by constant threats.

A SCALABLE SOLUTION FOR AN ESCALATING PROBLEM

In a 2019 study of 500 senior decision makers at SMBs, 66 percent said they did not believe a cyber attack was possible at their organization,[7] yet 43 percent of all cyber crime victims are SMBs.[8] Despite the common misconception, the reality is that SMBs face greater risks than they have at any point in the past, and just like large businesses, need to do more to protect data, reputations, and financial accounts.

Investing in qualified cybersecurity leadership is a proven way to reduce the costs and likelihood of a data breach. That is why many cybersecurity experts openly criticized Target for not having a CISO to provide leadership and a vision for security initiatives after their high-profile data breach in 2013. Hiring a CISO works well for large companies with deep pockets, but it just isn't an option for a small business.

The bottom line is that SMBs need to maximize results and minimize costs. Many have flocked to cloud computing solutions for this reason. By distributing the expenses across a large user base, cloud service providers offer services in discreet amounts at a lower cost to many different organizations.

Similarly, a cybersecurity expert can deliver executive-level knowledge and accountability to many SMBs simultaneously, so individual companies do not have to incur the cost of a full-time expert's salary and benefits. As with a traditional CISO, the vCISO reports to the CEO or CIO and translates complex IT security issues into meaningful action plans, directing IT security investments, increasing ROI, and strengthening digital defenses. Unlike a full-time CISO, SMBs can scale the amount of time and effort they need from a vCISO to fit their specific business needs.

> There are **498,480** unfilled IT security jobs in the U.S.[4]

While the benefits associated with hiring a vCISO are many, this solution is not a perfect fit for every business. vCISOs are best suited to organizations with fewer than 500 workstations and no more than two data centers. As organizations grow beyond that size, the effort needed to manage security and risk requires a dedicated, full-time CISO.

How CISOs and vCISOs Serve Businesses

- Integrating cybersecurity with business goals
- Providing strategic leadership to executives and users
- Creating a cyber defense program and governance framework
- Promoting a culture of information security
- Mitigating risks and managing incidents

Vetting a vCISO

Virtual CISOs should have the same level of knowledge, expertise, and leadership experience as traditional CISOs. Look for individuals or firms with these qualifications:

WHAT TO EXPECT FROM A vCISO

The relationship between a vCISO and a client is collaborative. Companies need to select the proper level of service for their business needs and integrate the vCISO with other members of the executive team to gain the most value from the service. This sense of continuous collaboration is one of the ways a vCISO is different than a consultant brought in to advise a company on specific projects and initiatives.

The vCISO should have sponsorship from the CEO, CIO, or IT Director and work directly with other executives. As with a traditional CISO, the vCISO should not report to mid-level managers or others who are not authorized to set company-wide policies.

vCISOs should also function like other executives: attending executive meetings, providing strategic planning and budget guidance for their area of responsibility, developing policies and programs, preparing annual reports, and fulfilling other commitments as necessary. The exact menu of services will vary depending on which vCISO firm is hired and how the individual contract is written.

The purpose of vCISO advisory services is to provide strategic leadership to guide the cybersecurity efforts of SMBs. Firms offering these services have a range of pricing levels to suit businesses of varying sizes and their unique needs. Some offer quarterly plans, where price is determined by the level of service required by the client organization. Others offer on-demand services packaged in hourly bundles to be used within a specified period of time.

The high degree of flexibility, combined with subject matter expertise and executive leadership, is what makes vCISO services ideally suited to the needs of SMBs.

> **"Security is a process, not a product.** Products provide some protection, but the only way to effectively do business in an insecure world is to put processes in place that recognize the inherent insecurity in the products. The trick is to reduce your risk of exposure regardless of the products or patches."
>
> —Bruce Schneier, Security Expert & Fellow at the Berkman Center for Internet and Society at Harvard Law School

vCISO: LEADERSHIP THROUGH INNOVATION

The rising costs of hiring cybersecurity experts will force some SMBs to operate without access to the skills and expertise necessary to protect data and reputations. Working with a vCISO allows those businesses to gain the benefit of cybersecurity executive leadership without incurring the cost of hiring a full-time executive. It's a smart solution to a difficult and expensive problem.

Securance has built a reputation helping businesses across a variety of industries manage risk and compliance, enhance information security, and improve operations. To get more information about how our vCISO services can help your organization, **visit our website** or **contact us** today.

ABOUT SECURANCE

Securance has two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.

SOURCES

1) https://www.sonicwall.com/2020-cyber-threat-report/

2) https://databreachcalculator.mybluemix.net/?_ga=2.173355811.1432796061.1584126984-172232738.1584126984&cm_mc_uid=54714355130115841269832&cm_mc_sid_50200000=29735291584126983236&cm_mc_sid_52640000=55146681584126983250

3) https://www.ziprecruiter.com/Salaries/CISO-Salary

4) https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=D087F6468B4991E0BEFFC017BC1ADF59CD5A2EF7

5) https://www.keeper.io/hubfs/PDF/2019_Ponemon_Infographic.pdf

6) https://www.hipaajournal.com/2019-cost-of-a-data-breach-study-healthcare-data-breach-costs/

7) https://www.keepersecurity.com/blog/2019/07/24/cyber-mindset-exposed-keeper-unveils-its-2019-smb-cyberthreat-study/

8) https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

The Emergence of the Virtual Chief Information Security Officer

SECURANCE CONSULTING

the advantage of insight

13904 Monroes Business Park • Tampa, FL 33635 • 877.578.0215

www.securanceconsulting.com