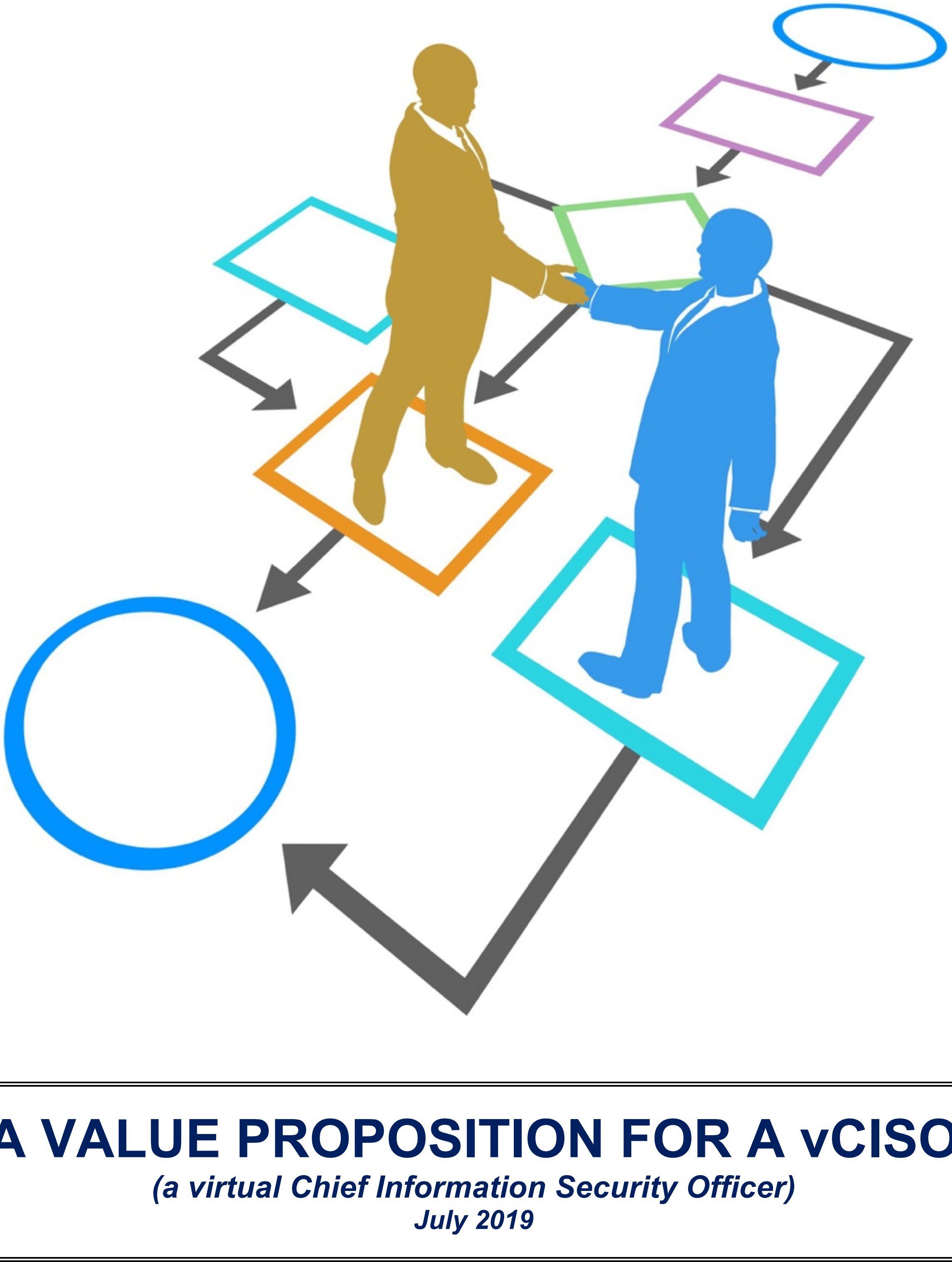
CISO ToGo

Technology Risk Consulting



A VALUE PROPOSITION FOR A vCISO

(a virtual Chief Information Security Officer)

July 2019

INTRODUCTION

If you follow ANY news these days, you can't help but become aware of more and more data, privacy, and/or security breaches, along with how customers of those businesses impacted are also affected by them.

Given the volume of these incidents, it would be understandable for small and mid-sized businesses to simply give up and believe that if larger enterprises are defenseless against them, then they must certainly be as well! A common misunderstanding of small to mid-sized business is to believe that they simply aren't worth the hacker's time and effort, leading to even more haphazard cybersecurity practices. Quite the opposite is true, however, as hackers often have an even greater understanding of the value of the data they are stealing from small to mid-sized businesses than the organization being compromised!

This sort of mistaken thinking can be very harmful to your business and leave your private data (and that of your customers) even more vulnerable. In fact, the growing number of disclosed incidents means that cybersecurity measures need to be taken even more seriously. Appropriately implemented, these measures can effectively minimize your risk of a breach and will help to instill customer confidence.

MYTHS FOR SMALL AND MID-SIZED BUSINESSES

The following are three cybersecurity myths that your business should simply NOT believe!

Myth #1: We're Too Small To Be Hacked

As mentioned above, a significant miscalculation made by small and mid-sized businesses is that they believe they are too small to be the target of hackers. This error in judgement can lead businesses to believe that they don't have to invest in their cybersecurity. However, the opposite is quite true. Hackers target small businesses because they are easier to attack. Since these organizations have a lot of valuable data but often little protection, it is actually easier for hackers to successful gain access to the information they want.

Myth #2: Cybersecurity Is A Technology Problem

It's easy to push the problem to be the responsibility of the IT department (if you are fortunate enough to even HAVE an IT department!), but that thinking doesn't solve anything. The security of an organization's data is not an IT problem, but rather a concern for the business as a whole to ensure it is addressed. Granted, the IT department (again, if there is one) needs to protect the data and understand what is important, but the business must also understand why the data is important, and how it can be appropriately secured, backed up and restored if it was to ever be compromised.

Myth #3: We Have An Antivirus Solution, So We Must Be Covered

Having a decent antivirus program is important and a good start … but it is simply NOT enough. Antivirus programs can protect you from certain attacks but won't be able to protect you from others. That's why it is crucial to have a multi-layered approach to security … thereby ensuring that you have other ways to cover your security needs. For instance, no antivirus program will ever be able to address human error due to phishing emails or other mistakes (this would require established cybersecurity guidelines for employees to follow).

THE VALUE OF A CYBERSECURITY PROFESSIONAL

Cybersecurity has become a household word, and while we hear about data breaches and phishing scams on a daily basis, what does it all mean to your organization? Well, it could mean the very survival of your business! Below are **SIX SOLID FACTS** that demonstrate the critical and urgent need for trained, experienced cybersecurity professionals.

Fact #1: The Cost of Cybercrimes Is Increasing

By 2021, cybercrimes will cost $6 trillion per year worldwide. The cost of cybercrimes has almost doubled over the last five years, up from $3 trillion in 2015, according to a report published by Cybersecurity Ventures. This includes not only stolen money and ransom, but also the value of lost productivity and intellectual property, data theft, business disruption, reputational harm, and more. Experienced cybersecurity professionals can help reduce this cost for their organizations by putting protections into place, firming up security policies and identifying vulnerabilities before attacks happen.

Fact #2: Ransomware Attacks Are Everywhere

Businesses experience ransomware attacks every 40 seconds. According to Kaspersky Lab, between January and September 2016, businesses experienced ransomware attacks once every 40 seconds, up from the previous rate of once every 2 minutes. Also, in 2016, the number of daily ransomware attacks jumped 300%, from 1,000 per day in 2015 to 4,000 per day in 2016, and nearly one-fifth of hacking attacks included ransomware. As the threat of ransomware continues to increase, it's important for organizations to have a response plan in place when (not if) it happens to them.

Fact #3: Malicious Emails

1 in 131 emails is malicious. More than half of all emails are spam, according to Symantec's 2018 Internet Security Threat Report, and the amount of spam containing malware continues to increase. Today, malware has gone pro, with authors outsourcing spam campaigns to specialists, and the scale of these operations indicates profitability, which means they will likely continue, according to Symantec. Training staff to use caution with unknown emails can be the first line of defense in cybersecurity.

Fact #4: Network Vulnerability Is Pervasive

Attackers reside within a network for an average of 146 days before being detected. Although this number has dropped from a prior 200-day average, the fact that hackers can dwell undetected for almost five months should raise red flags. Experienced cybersecurity professionals can not only identify and analyze anomalies on the network, they can manage vulnerabilities before an attack occurs.

Fact #5: Need Outpaces Availability In The Cybersecurity Profession

Apart from the reality that cybersecurity is everyone's responsibility, from the help desk to the CIO and even non-IT employees, unfilled professional cybersecurity roles will reach 3.5 million by 2021. In fact, the number of jobs specifically in the field of cybersecurity will increase exponentially in the next five years. And Cybersecurity Ventures estimates that by 2021 every large company globally will have a chief information security officer (CISO) in seat, compared to the 65 percent that have one now and the 50 percent that did in 2016.

Fact #6: IoT Devices Create New Vulnerabilities

An IoT device can be attacked in less than 2 minutes. By the end of 2017, the world had 8.4 billion connected devices, up 31 percent from 2016, according to a Gartner study. While consumers are driving the adoption of IoT devices, companies will spend an estimated $964 billion on IoT hardware this year. Cisco estimates that the number of IoT devices will be three times as high as the global population by 2021! But what do connected devices have to do with cybersecurity? Not all IoT devices are created equal when it comes to security – some are put on the market so quickly that they have vulnerabilities, and the consumers using these devices may not set them up securely when they bring their own devices to work, exposing their employer to cyber-threats. IT pros need to apply behavioral analytics to IoT devices in the same way they do to computers, servers and the network. Anything could be vulnerable.

What Is A vCISO, And How Can Your Organization Benefit?

A vCISO (virtual Chief Information Security Officer) helps organizations to protect their infrastructure, data, people and customers. A vCISO is a top security expert that builds the client organization's cybersecurity program. The vCISO works with the existing management and technical teams to help you determine if your organization needs a vCISO.

How an organization uses its vCISO depends on the business itself. The organization's structure, products and services, markets and IT context all factor in. Some companies are content to just sit and wait for problems – but that kind of apathy can be damaging. In most cases, waiting around is a very poor strategy ... a vCISO helps a firm to be proactive when initiative counts most!

When a company is struggling to implement security, comply with industry regulations, and outpace competitors, a vCISO can help. A vCISOs provides guidance and measures the effectiveness of the client's cybersecurity program.

Reading this, you may be wondering if your organization needs a vCISO. Here are some of the things that these experienced professionals can do to help your company toward success and security.

A Virtual CISO Helps Protect Your Organization ...

Managing cybersecurity in today's world is almost indescribably tough. Many organization's leadership teams either don't quite feel up to the challenge, or they understand that outside firepower can enhance their security model.

Most mid-sized firms have some IT personnel or contractors that handle most of the technical needs of security. But who is looking at the big picture of cybersecurity for the organization? Often this is a CIO, CTO, Chief Compliance Officer or another executive that has a full plate of responsibilities. This executive, however, might not have the time or detailed knowledge to cover their enterprise's cybersecurity program. That gap leads to unnecessary risk!

Other organizations may choose to put a mid-level technical manager in charge of security. They also have a full-time job, but they may not have the executive presence to influence senior management. They need buy-in for key security programs – especially when there's a time-sensitive project. Often, it's not that the people in these roles aren't working hard enough to implement best practices – but rather that the company hasn't invested in the right areas to ensure their success.

A Chief Information Security Officer (CISO) is a senior-level team member. The CISO establishes and maintains an enterprise's security vision, strategy, and programs. The role ensures information assets and technologies are appropriately protected. Most large organizations have a full-time CISO to handle their cybersecurity needs. Mid-sized companies and smaller may not have such a role … but having a non-security expert in charge of security is a recipe for trouble!

A vCISO provides expert security guidance through:

- Understanding the organization's strategy and business environment
- Providing threat analysis and strategy updates in real-time
- Anticipating future security and compliance challenges
- Overseeing mid-level and analyst/engineering teams
- Discovery, triage, remediation and evaluation of threats

The vCISO Can "Fill The Void", And Serve As An Interim CISO ...

There are many cases where a larger organization's CISO departs due to a new role, termination, illness, or retirement. In these cases, the organization needs a qualified person to immediately step in to manage its cybersecurity program and needs. The mandate to "handle security in real-time" means the CISO's chair should not ever be empty: if an interim presence is needed, a vCISO is an invaluable solution.

Why Do Companies Hire a Virtual CISO?

Many companies are getting aggressive about getting a CISO on board for a number of reasons. One is the range of new cybersecurity regulatory and compliance requirements that companies have to wrestle with. Industry standards like PCI and HIPAA are now joined by bold new privacy and security rules that change how we view the company's responsibility to safeguard data. Perhaps the best recent example is the European General Data Protection Regulation (GDPR) that's having a profound impact not just in the EU, but around the globalized business community. Then there are the cautionary examples: data breaches splashed across the front page, chilling tales of pilfered data, identity theft, and commercial loss.

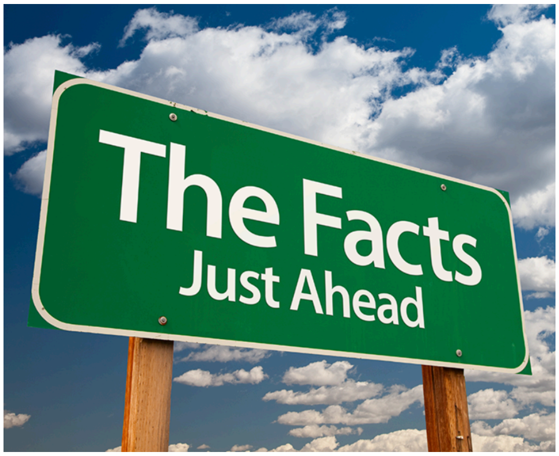
More Benefits of Hiring a Virtual CISO ...

The key benefit of hiring a vCISO is that you get the same expertise and capability as a full-time CISO. But you don't have the associated level of overhead, benefits, and training. This allows any organization to achieve its security goals related to prioritization, risk evaluation and training.

THE FACTS CAN'T BE DENIED ...

A vCISO IS A GREAT OPTION FOR SMALL TO MID-SIZED ORGANIZATIONS

Organizations continue to face modern cyber-attacks such as ransomware threats and data breach incidents. In the wake of a non-stop onslaught from advanced hackers, it seems that no matter what defensive measures organizations put in place, cyber adversaries and malware authors are able to circumvent them.



But cybercriminals are not only motivated to target high-profile enterprises; in fact, they actually tend to look at smaller and emerging businesses MORE, because they are assumed to be vulnerable targets. Most small and mid-sized organizations face a double-whammy when it comes to protecting corporate networks and having the foresight for tackling increasingly difficult mandates in governance, risk management and compliance (GRC) for long-term success. First, they struggle to commit larger budgets to finance evolved security fixes. Secondly, even if they are prepared to invest in modern defenses, they either suffer from a lack of in-house expertise or find it extremely difficult to source the right talent, as there is a serious shortage of qualified/experienced professionals.

Findings from Verizon's latest Data Breach Investigation Report support this, as the research shows that 43% of all breaches occur at small businesses. The same report also highlights that as high as 56% of data breaches take months or longer to become known, as this is largely due to the absence of the right kind of expertise.

Turning To A vCISO Is A Pragmatic And GREAT Option ...

At a time when regulatory guidelines are becoming more stringent than ever, with some recommending appointing a CISO, organizations must find a way to respond to modern cyber threats that are growing in scope and cost.

The first daunting challenge lies in being able to manage and control all the potential weak points in the corporate IT network and end-user devices. Next, and this is where the real difficulty lies, is being able to do it with limited financial resources and in-house expertise — or even with hired guns, that can be difficult to find and retain. There is a pressing need to up the ante in cybersecurity to proactively combat a dangerous combination of mounting malware threats of increasing sophistication and a widening gap in the skills required to identify and combat them.

The time to consider useful alternatives such a hiring a vCISO is now, for it not only helps restore the confidence in an organization's IT security while correcting its risk posture, but it also would provide immense help to CIOs or IT managers in delivering a more streamlined and secure rollout of IT policies. Companies with stretched financial resources and/or inadequate security expertise can discover a very meaningful use case in appointing a virtual chief information security officer (vCISO).

Among many of its obvious benefits include being able to move swiftly in the right direction to become compliant with emerging regulatory guidelines and plugging leaking holes to prevent data loss. What's more, contracting a vCISO isn't cost or time prohibitive like recruiting a full-time security expert. A vCISO comes with all the advantages that a full-time, seasoned CISO offers with their breadth of knowledge and security expertise. Further, a vCISO can help you conduct a quick assessment of existing IT programs and policies, ensuring your organization is able to make all the required changes to strengthen the security posture as demanded by the evolving cyberthreat landscape and regulatory climate.

vCISO REQUIREMENTS

It's important for a vCISO to have a sufficient background in security, to ensure an understanding of the security landscape. The vCISO has to keep up to date with the latest in the security industry. But how can you make sure that a prospective vCISO is a security expert?

Cybersecurity credentials can help, but certifications only speak to part of the proof of capability for a CISO. While the vCISO needs to be able to talk intelligently about systems and compliance, and translate that knowledge to teams, the role also needs to have "people skills" as well as "tech skills" and expertise in the multiple industries. This crucial combination helps companies to safeguard their systems and re-organize for the business world of the future.

Selecting A vCISO Goes Way Beyond A Makeshift Arrangement ...

For small to mid-size organizations looking to bring on a vCISO in a consulting capacity, here are some noteworthy traits to consider before hiring:

- A vCISO must be able to articulate the inherent risks, educate management and explain available options in appropriate business terms terms that are jargon-free.
- Taking a page from former Intel CEO Andrew Grove's bestselling book, "Only the Paranoid Survive," the vCISO can never rest or rest assured. They should never be complacent but remain diligent (and maybe slightly paranoid).
- A vCISO must have a solid grasp on the fundamentals of IT security, ensuring daily tasks (like server security, patching, backups, and coding skills) are executed properly and consistently.
- A vCISO must have good working relations with local law enforcement due to the inevitability of needing to report breach incidents (vCISOs need to respond urgently).

A vCISO From CISO ToGo ...

With a vCISO from CISO ToGo, each engagement is a little different. In every case, the vCISO will quickly understand your business environment, culture and objectives. A typical engagement involves being on-site for one to two weeks of the first eight weeks of the process *[note: for more details on CISO ToGo's offerings, review our services from our website].* On-site participation varies based on customer preference and the requirements of the engagement.

The vCISO will then work on any/all of the following:

- Assess the current cybersecurity maturity, and the overall "risk appetite", of the organization
- Establish the organization's cybersecurity strategy
- Build a cybersecurity plan and program
- Build a Governance, Risk and Compliance (GRC) program
- Maintain core security operations
- Focus on people – including managing personnel, contractors and/or vendors
- Build and execute a company training and awareness strategy

CISO ToGo's virtual CISO service imperatives include:

- Understanding the business environment and matching a management style that resonates with the client
- Building trusted relationships with key personnel, resulting in a more successful cybersecurity program
- Meeting customer requirements with a flexible vCISO program
- Delivering great templates and systems to maximize ongoing leverage

Unique qualities of a vCISO from CISO ToGo's include:

- Our vCISO's have the talent to introduce creative approaches – especially at smaller organizations pinched by limited budgets. Focusing on employee training and ensuring two-factor authentication should be top of mind.
- A vCISO should possess good communication and collaboration skills to help win upper management buy-in to ensure that security remains a priority. Applying security protocols to existing products may boost sales while offering a competitive advantage.

THE BOTTOM LINE

Organizations that aim to seize emerging opportunities in digital transformation such as cloud, mobility, blockchain, the internet of things (IoT) and more — but fear legacy IT or poorly configured IT security environments as major bottlenecks — can think of vCISOs as strategists who are adaptive to their clients' needs and capable to help customers learn quickly to embrace disruptive technology with confidence and a well-planned road map.

Having trained and experienced cybersecurity professionals on staff can reduce an organization's risk to cyber-crimes exponentially. And when, not if, the organization does get attacked, an experienced cybersecurity pro can mitigate the problem and help to get the business back up and running quickly and efficiently ... **this is where CISO ToGo can help**!

To find out more information, check out our services listed on our website at **www.CISO-ToGo.com**, or call us at **1-401-264-0880** to begin the discussion on how we can help!

CISO ToGo, LLC ...
because security is everyone's concern,
but it's OUR business!