

September 20, 2018

# Cybersecurity: Do You Need a Virtual CISO?

Businesses concerned with increasing cybersecurity risks and regulations may want to turn to virtual chief information security officers for strategic guidance.

Rodika Tollefson  
Freelance writer and journalist



Compelled by mounting [cybersecurity threats](#) and growing regulatory pressure, businesses of all sizes are taking a more strategic approach to their cybersecurity. Part of this approach is to hire a chief information security officer (CISO) to provide a business-risk perspective.

As they face a cybersecurity talent shortage and a lack of resources to hire a full-time CISO, small and midsize organizations are embracing a new option: a virtual CISO.

"A virtual CISO is an awesome alternative for those organizations that want to take their security up a notch and move it to the next level, but they know that they don't have the bandwidth to do it all on their own," says Inga Goddijn, executive vice president at [Risk Based Security](#), which provides security intelligence and analytics.

Risk Based Security has been offering an on-demand service called YourCISO since 2012. Goddijn says that while at first they felt like "the lone cricket in the field," the concept is now taking off.

Like any consultant, virtual CISOs, or vCISOs, can be hired by project or on a long-term basis, whether it's for a specific need like compliance—as some regulations require a designated CISO—or for a broader role like creating a cybersecurity program or evaluating the company's [cybersecurity risks](#) and recommending a security strategy. A vCISO may also bring other resources when specialized expertise is needed, such as compliance with a specific legislation.

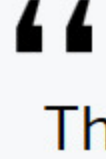
ADVERTISEMENT

Product Solution

## Keep better tabs on cash flow

We help simplify money management. American Express has the solutions to keep you on top of your spending.

[Learn More](#)



Those smaller to medium-size businesses can benefit from having some level of security DNA injected into their organization, even if they don't have the resources to bring in a full-time CISO.

—Brian Contos, CISO, Verodin

Similar to an in-house CISO, a contracted one plays a strategic role in a company's cybersecurity. Organizations can contract directly with an individual, or, more typically, work with a vendor that may offer various cybersecurity solutions, and have an assigned individual. In the case of Risk Based Security, YourCISO has both a self-service online portal and a key contact the client selects as the vCISO and builds a rapport with.

"[The growing interest] may be a function of better awareness of security issues," Goddijn says. "But there's also the dynamic of key partners coming to the organizations wanting to know what their security posture is."

## Changing Landscape Drives Demand

The growing number and magnitude of data-breach incidents is one of the drivers of increased cybersecurity awareness. According to data from the [Privacy Rights Clearinghouse](#), 2017 had 843 publicly disclosed breaches, with a total of more than 2 billion records exposed (based on August 2018 data). By comparison, only close to 319 million records were exposed in 547 breaches in 2015.

"We are more cognizant of security incidents and the cost of recovering from incidents from the technical and reputation perspective," says Justine Bone, former CISO for Dow Jones and Bloomberg and the founder and CEO of [MedSec](#), a cybersecurity services provider to hospitals and medical device manufacturers. "At the same time, we see regulators picking up steam and starting to pay attention to security incidents and the implications to companies and their customers."

Those are regulators like the New York State Department of Financial Services, whose 2017 landmark regulation requires a comprehensive cybersecurity program. Applicable not only to its regulated entities such as banks and insurers doing business in the state but also to their vendors, the regulations' requirements include a designated CISO, whether an in-house role or an outside consultant.

"If you're a small or midsize organization, you have the same security concerns as bigger companies but you don't have the same resources," says Todd Weller, chief strategy officer for threat-intelligence-protection company [Bandura Systems](#). "So you have to look to third parties to help you because you're under the same regulations, and cybercriminals don't discriminate based on size."

## Virtual CISOs Fill a Strategic Role

An in-house CISO role may be hard to fill due to the severe shortage of cybersecurity talent across the board. It may also be challenging for smaller businesses to justify a full-time position, even if they have big risk of exposure due to the [quantity of data they collect](#).

"CISOs are not an incredibly cheap resource to bring on board if you're a small company," says Brian Contos, CISO for [Verodin](#), which provides a security instrumentation platform. "Those smaller to medium-size businesses can benefit from having some level of security DNA injected into their organization, even if they don't have the resources to bring in a full-time CISO."

Sign up to receive the latest [business insights](#)



By providing your e-mail address, you agree to receive the business insights newsletter from American Express. For more information about how we protect your privacy, please read our [Privacy Statement](#).

Businesses with a small budget may be looking at vCISO to both strategize and implement; however, this "on-demand" executive should not be viewed as a "practitioner," or someone who is called upon to deploy technology or provide IT services.

"The idea of people, process and technology that we talk about in cybersecurity is something a virtual CISO can help with in terms of being very prescriptive," Contos says. "They can help you prioritize and lay out the path to being successful and having the fundamentals."

He adds that now that cybersecurity is measured like other business functions—in terms of key performance indicators and other metrics—the vCISO can help rationalize the investment in cybersecurity and how to get the best value from it.

The vCISO is an excellent resource for someone who understands that cybersecurity is a business risk and wants to address it, but doesn't know how to get started, Goddijn says.

"The perfect time to bring in a virtual CISO is the point when you're trying to wrap your head around, as an organization, what security means to you and what you need to do," she says. "The virtual CISO can walk through what goes into a security program and how to prioritize it."

## What to Look for in a Virtual CISO

One of the advantages of a vCISO is a broader and more up-to-date knowledge of technologies, trends and strategies that's acquired from working with multiple clients, Bone says. At the same time, this person acts more like a member of the team than an outsider, likely engaging with departments and leaders across the company.

"This is a leader, business liaison and communicator who oversees the larger program... and must understand the business, the priority of the business and the primary and secondary business assets," she says.

There's an influx of security consulting firms and managed security services providers (MSSPs) now offering vCISOs. Goddijn recommends asking providers if their vCISO program includes additional support and tools. Additionally, check the background of the specific individual who'll be your designated CISO.

"You want to decide, is this someone you can work with over time and have some rapport? Trust is a big thing in security," she says.

One of the first criteria is whether that person has worked in the same vertical as well as company size, Contos says.

"You want to make sure the background of the individual overlaps with your company and is on the cutting edge of what you need," he advises.

Above all, Weller cautions that organizations should not be looking to hire a practitioner for the vCISO role.

"If you're looking for someone from a strategy perspective, you want somebody who's been in that seat and has experience as a CISO," he says. "It's a discussion about what you have to do from a cybersecurity strategy and compliance perspective, to make sure you're doing it right—if you're just looking for someone to implement something, that's not what the CISO is about."

Photo: Getty Images

Want to Dig Deeper?

- [Building Your Team](#)
- [Digital Tools](#)
- [Recruiting](#)
- [Hiring & HR](#)
- [Cybersecurity](#)
- [Getting Customers](#)



About the Author

**Rodika Tollefson**  
Freelance writer and journalist