Aug 31, 2021, 09:00am EDT | 4 views

Why Small Businesses Need To Know About A VCISO For Cyber Risk Management

Jim Goldman Forbes Councils Member
Forbes Technology Council COUNCIL POST | Membership (fee-based)
Innovation

Jim Goldman, Co-founder and CEO, Trava Security, Inc.

GETTY

It is certainly not news that cyber threats are on the rise globally. Every day there are multiple headlines, social media posts and commentaries about companies falling victim to an attack. The statistics are alarming. As *Forbes* reported, "the year 2020 broke all records when it came to data lost in

breaches and sheer numbers of cyber attacks on companies, government and individuals."

Cyber risk is a growing threat to *all* companies, even small- and medium-sized businesses. So much so, that the White House recently published a plea for all businesses to take urgent security measures to protect against ransomware attacks.

The fact is online criminals can as readily attack a small business as a large one. But while Chief Information Security Officers (CISOs) are imperative for enterprise companies to manage their cyber risk, the salary range for such professionals is likely prohibitive for small-, even medium-sized, businesses. Depending on the size of the business or where it is in funding rounds, it also may not be a standalone full-time position. This is one reason virtual Chief Information Security Officers (vCISOs) have become a popular option for a large number of companies, allowing them the option of obtaining the services of a highly qualified CISO at a fraction of the typical CISO salary.

There are other reasons to consider a vCISO. These specialized professionals can help you:

Win Business

If you are a growth-oriented company, you know how important it is to close enterprise-scale customers. Most, if not all, will likely ask you to fill out a standard vendor security questionnaire. In the cases of SaaS (software-as-a-service) companies, what the company will be looking for, as one example, is

evidence that your company has implemented a legitimate Secure Software Development Life Cycle (SDLC) program. This will tell them that you have proactively and effectively built in security — as opposed to waiting until the software is written and fixing bugs at the end — to help discover and reduce vulnerabilities early.

Develop an Effective Cyber Risk Management Program

Putting an effective cybersecurity strategy in place can be overwhelming. And with a tight budget, how do you prioritize efforts when it comes to investing in a cyber risk management solution?

A highly experienced vCISO can:

• Perform a vulnerability risk assessment on your organization's infrastructure.

• Analyze the key risk drivers and help you prioritize what to do in response.

• Highlight what level of risk reduction can be expected from a given level of investment in risk mitigation.

• Help you implement and evolve your cyber strategy over time to match up with the appropriate needs for each stage in the company's life cycle.

Prepare for SOC2 and ISO 27001 Certification

For security-conscious companies that are doing business with SaaS providers, SOC2 compliance is a minimal requirement. ISO 27001 is designed to function as a framework for an organization's information security management system (ISMS), including all policies and processes relevant to how data is controlled and used.

Larger customers typically insist that vendors adhere to these recognized standards and provide objective third-party evidence of the achievement of those certifications.

A vCISO can help you:

• Achieve SOC2 and/or ISO 27001 certification.

• Discuss the differences and relative merits of SOC2 versus ISO 27001.

• Get you properly prepared for a certification audit by third-party auditors.

Choosing the Right vCISO

A vCISO is a critical member of your leadership team, and you want them to be the right fit. First, clearly align internally on why you think you need one and what pain points you need to address. Seek referrals from your professional networks. Talk about your specific issues with vCISO candidates. And start with one project.

Your vCISO should be able to grow with your company as it scales and fill this critical role until you are at the point when you are ready to fill a full-time CISO role. There is typically not a lot of pushback from your internal teams because, particularly in small businesses, everyone is stretched thin, trying to make big things happen and get the company on a growth trajectory. External service providers like vCISOs will supplement your team, not replace anyone's job.

How To Engage A vCISO

There are two common ways to engage with a vCISO:

• Statement of Work: A SOW is best for project-based work with specific objectives, deliverables and timeframes. This also offers an opportunity to vet a vCISO to make sure they are a good fit for your cybersecurity goals.

• Retainer Agreement: For ongoing or ad hoc work or when a company wants to have access to a vCISO's expertise on an as-needed basis without writing a detailed statement of work in advance, a retainer agreement is often the best option. One positive outcome in this type of engagement is

that it gives investors and customers the confidence that you have a dedicated person working towards cybersecurity and data protection.

Even with the most comprehensive cyber risk management plans in place, a cyber event might still occur. Make sure you have an SLA in place so that you both have expectations set for how they will respond if a crisis occurs. But before that, create a crisis management plan — complete with messaging templates — and practice it. This way, you can react swiftly and your vCISO will assist.

Many companies start working with a vCISO for a project with an SOW. If it goes well, they move to an ongoing retainer agreement.

A vCISO should start with a risk assessment to identify cybersecurity gaps. Expect this process to take two to four weeks.

Conclusion

There are many ways that a vCISO can help small and medium-sized businesses develop and maintain a comprehensive cyber risk management program and prepare you for information security compliance audits. It can be a cost-effective way to approach your cybersecurity initiatives while having the peace of mind that a cyber risk management professional is helping you take a complete approach, leaving nothing to guesswork or chance.

Follow me on Twitter or LinkedIn. Check out my website.

Jim Goldman

Jim Goldman, Co-founder and CEO, Trava Security, Inc. Read Jim Goldman's full executive profile here.... **Read More**

Reprints & Permissions