TCPS

TURNKEY CYBERSECURITY
& PRIVACY SOLUTIONS

White Paper

August 3, 2022

Secrets of Hiring and Firing Virtual CISOs

By Ray Hutchins, Mitch Tanenbaum, and Andrews Tallon

Synopsis: Cybersecurity professionals share their hard-won experience and knowledge about hiring, managing, and firing one of your company's most sensitive leadership positions– the virtual Chief Information Security Officer (vCISO).

NOTE: While comprehensive, this white paper is not intended to be a complete discussion of this subject matter. Instead, it is an overview of issues which must be considered by management in order to reduce risk, save money, and decrease internal brain damage.

Table of Contents

Introduction

People who read this white paper typically have already reached the conclusion that they need a CISO, but realize that ***they don't need a FULL-TIME CISO***. And they believe that this position, if managed correctly, can be handled by a remote, *virtual, part-time* CISO.

But whether it is full-time or part-time, most companies are ill-prepared to screen, hire and manage this type of senior-level technical talent. Most companies and HR departments have a difficult time even correctly defining the *requirements* for this critical position.

Demand for senior CISOs exceeds supply, therefore it has become prohibitively expensive and problematic for most companies to hire and retain this type of talent.

Please refer to: ***Why Choose Us as YOUR vCISO Partner***

Your Two vCISO Options:

1. Hire your own CISO or vCISO. If this is your path, you will find much useful info here to support your efforts.

2. ***Engage our vCISO services***. In this case you will off-load much of the work associated with this process and you will get access to our vCISO team. Please refer to **Why Our vCISO Team Approach is Better.**

Benefits and Services Provided by a Qualified vCISO

Here are just a few of the ways an experienced vCISO can help your company:

- Helps you save money on all IT and cybersecurity decisions
- Helps you make the right technical security decisions
- Ensures that your security program meets all compliance requirements
- Provides your IT team and/or MSP with cybersecurity support
- Review and monitor the security profile of your MSP if you use one. This is likely your single highest risk vendor since they have admin access to all of your systems and networks. Also, make sure that your MSP agreement covers all of the needed security and privacy tasks.
- Participates in security and other risk assessments as required (internal CISO does not meet the third party requirement)
- Helps vet potential IT hires and 3rd party technical products
- Reduces risk for the organization while increasing its valuation
- Helps management and the board understand cybersecurity and privacy risks and solutions
- Provides required cybersecurity training required by regulations for board members
- Evaluates cybersecurity insurance coverage
- Helps the company signal its commitment to strong cybersecurity
- Leads incident response and forensic analysis activities
- …and more–please contact us for details

Defining vCISO Requirements

The bottom line is that you require a vCISO who is a seasoned IT and cybersecurity professional and who is experienced at providing strategy guidance to management and the folks executing management decisions. Sadly, there are many folks representing themselves as CISOs or vCISOs and they are counting on your inability to properly define and vette such a position. By the time you figure out they are inadequate to the task, you will have wasted much valuable time and money.

If you are going to hire a CISO directly or a vCISO as a service (vCaaS), here are some of the questions to ask candidates:

1. What qualifies you for a vCISO position?
2. How many companies have you provided vCISO services for? (Check these out)
3. Describe the cybersecurity and privacy standards and regulations that you feel you have mastery over. Do you have mastery over *our* regulatory requirements?
4. What support staff will you require as our vCISO?
5. How many hours can you devote to our vCISO needs?
6. …and more.

Note whether the candidate is comfortable communicating with senior management and others in the organization. Do they try to impress with technical jargon that only they understand?

Someone famous once said, *"if you can't explain something in a way that a six year old can understand it, then you don't understand it well enough yourself."* Some technical folks pride themselves on being able to confuse management people with their jargon.

Some preparatory questions for your management staff:

1. Does all of the top management (and board) support the hiring of a vCISO?
2. Do you have a good job description that everyone signs off on?
3. Who will the vCISO report to? Are these individuals prepared to be part of the interview process? Is this person(s) qualified to manage a vCISO? If your answer is the CFO, please keep thinking. This is a technical position and the person managing the vCISO will need to make some (or many) decisions that are inherently technical in nature.
4. How many vCISO support hours does the company require? For the first 90 days? Thereafter? Have you prepared a task list of desired projects? (We can help you with this)
5. Are you prepared to perform background checks and CAREFULLY check all references? Do you plan on asking for copies of IT educational completion certificates and confirming that they are legitimate? (Your background check service can sometimes do this for you).
6. Do you want a trial period to make sure the fit is good and the vCISO works well with your key staff?

Tips for Effective Management of vCISOs
If you have hired the right vCISO, in short order that person's judgment and knowledge will become trusted. The vCISO will start to have significant input and impact on strategic IT, security and privacy planning and execution. Note that we have included privacy here. Privacy has both compliance and technical (security) aspects. Likely your internal IT team or MSP has no experience with this.

But even if that is the case, continuous, methodical management is required. There must be excellent written and verbal communication between the vCISO and all staff. The nature of the work is such that frequent meetings with the vCISO are required. The frequency will be based on exactly what your vCISO is doing for you. Use of project management software to monitor progress on all projects is recommended.

Obviously, there is MUCH more to this topic…but if you hire us, you will automatically solve that problem.

Terminating Your CISO/vCISO with Minimal Risk (Hope for the Best; Plan for the Worst)

A full time CISO has the keys to your IT kingdom. They have passwords to many or all of your systems and they know the architecture and operating systems that make up your company's IT infrastructure. If the CISO ever becomes your adversary, then you could be exposed to serious risk. Typically, a vCISO directs your employees to make changes and as a result, does not have keys to your systems. He or she does have a lot of knowledge about the security of your systems. This significantly reduces your risk, unless you give them more access and power..

Tips for reducing risk during termination and/or separation:

1. Implementation of a strong hiring process.
2. Provide a professionally created employment contract that includes the following:
    - Establishment of the chain-of-command.
    - The CISO/vCISO written acceptance of responsibility for protecting company data and systems.
    - Acknowledgement and acceptance of all company operational, cybersecurity, and privacy policies.
    - Termination/separation procedures including the disengagement process with IT systems and data.
    - CISO/vCISO written acceptance of termination/separation procedures.
3. Provision of strong management that includes formal documentation of the vCISO workflows and activities.
4. Perform regular, documented performance reviews (quarterly?)
5. Have a professional personnel policy that governs separations and terminations and protection and return of all company data and property.
6. Segment company data and control who has access to what. Why would a CISO/vCISO need access to employee non-public information? Or financial data? It is complex to

create access control rules, but it is more expensive not to. It blows our minds how few companies think this through and/or do anything about it.

7. Ensure complete understanding of all company operational and cybersecurity policies.
8. Make sure executive management retains super admin rights to all systems and master passwords. THIS INCLUDES CLOUD SYSTEMS AND NETWORKS.
9. Consider purchasing an employee Surety Bond on this person.
10. Purchase cyber liability insurance that covers risks associated with your CISO/vCISO (we review cyber liability insurance policies as part of our vCISO services)
11. Listen to your CISO/vCISO. Respect them and their work. It is much easier to separate on amicable terms if this is the case.
12. Monitor network activity so you know what is going on. We sell very cost effective tools that management can understand and which give you insights into what is going on. See our white paper written for executive management personnel: ***Monitoring Your IT Systems-The Best Tools That Meet Compliance Requirements and Which are Affordable for SMEs (Small to Medium Enterprises)***
13. If you have an acrimonious separation situation, plan things carefully in advance.
14. There is more related to this subject. But you are getting the picture.

> Some companies establish a separation bonus for such high positions. This bonus is designed to be paid out in six months if there is a smooth transition and the person leaving cooperates fully and returns all company property.

Why Choose Us as YOUR vCISO Partner?

THIS IS OUR BUSINESS AND WE ARE GOOD AT IT

We are a full-service, U.S.-based cybersecurity company that has been approved to work with DoD contractors and U.S. government agencies. No matter where in the world you are located, we are positioned to help you build the best cybersecurity program possible. Please see our websites below for more information about us.

OUR CISOs ARE FULLY VETTED, U.S. CITIZENS

We understand how to vet and check out CISO candidate's qualifications and experience. We have made the decision to only hire CISOs who are U.S. citizens. This is the only way to fully comply with cybersecurity requirements associated with protecting your sensitive information.

ACCESS TO EXCLUSIVE CYBERSECURITY AND PRIVACY PROGRAMS

Turnkey Cyber has developed the country's only TURNKEY cybersecurity and privacy programs that meet NIST and DoD requirements. These programs reduce the expense and brain damage of implementing cybersecurity and privacy across the enterprise.

OUR CISO SYSTEMS SUPPORT YOUR CIO/EXECUTIVE MANAGEMENT

In most companies top management struggles to hire and manage Chief Information Security Officers. This can result in lost productivity, increased risk, increased expense, and potential staff conflict. Our vCISO experience is such that we can cut to the chase and make sure company objectives are being met.

YOU ARE MAKING NO LONG TERM COMMITMENTS TO ANYONE

Hiring, onboarding, and managing a CISO is a slow, tedious process and untangling such relationships can be problematic and even dangerous. Your relationship is with us. We handle any disengagements. Your risk with respect to this issue is minimized.

ACCESS TO VETTED TECHNICAL TOOLS

A cybersecurity program consists of people, processes, and technical tools. There are many potential tools. We have spent years vetting tools to get the best value for our clients. This knowledge is at your vCISO's fingertips and can prevent purchasing blunders.

See more at our vCISO web page here: https://www.your-vciso.com/

WHY OUR vCISO TEAM APPROACH IS BETTER

More heads are better than one. Your company will be assigned a primary vCISO, but this vCISO is backed up by our lead vCISO, specialist vCISOs (DoD, compliance, privacy, etc.) and our technical and business teams. All vCISO strategic advice and project work is reviewed by our lead vCISO. If your vCISO has any cybersecurity or compliance questions, he or she can get support immediately. We are able to recruit principled, seasoned, experienced vCISOs because they prefer to work in our virtual, supported environment as opposed to traditional, geo-restricted office environments. Since we are not limited to any particular geography, we can recruit the best U.S.-based vCISOs.

Want to meet our lead vCISO? Please watch the video on this page:
https://www.cybercecurity.com/virtual-ciso-services/

Or contact Mitch directly at:
Mitch Tanenbaum
720-890-1663
mitch@cybercecurity.com