CISO ToGo
Technology Risk Consulting

In the past few years Managed Security Service Providers (MSSPs), Managed Service Providers (MSPs), and Cyber Insurance Providers have increasingly added virtual Chief Information Security Officer (vCISO) services to their portfolios. Anecdotally, based upon informal daily browsing of LinkedIn posts and direct feedback from some of my clients, it seems that the past six months have seen enormous growth in this space.

On one hand, it makes sense, because certainly a vCISO line of business can be lucrative for MSSPs, MSPs, and Cyber Insurance providers. But on the other hand, this is not without very real concerns of conflict of interests. Therefore, fully vetting a vCISO service is important so that your small or midsized business (SMB) receives correct consulting and is not given bad advice which can actually put your SMB in a worse security posture than before the engagement.

So, just what is a SMB to do? First, the SMB must understand the Three Lines of Defense (3LoD) model. Basically, it breaks down in this way:

- The **FIRST line of defense** is operational IT security management, such as maintaining firewalls, SIEMs, and patching. It is highly focused on the configuration of technical controls.

- The **SECOND line of defense** is risk management, and is concerned with all information security controls, not just cyber (technical) ones. One example is the information security policy suite. The second line of defense ensures risks are properly evaluated and that proper controls are implemented to reduce those risks to be in line with the organization's risk tolerance level. In large organizations, this is where the CISO operates. Similarly, for SMBs, the vCISO should be proficient in the second line of defense.
- The **THIRD line of defense** is audit, which makes sure that first and second line are doing what they claim to do with regards to protecting information and infrastructure and that such protective efforts align with one or more specific frameworks and/or best practices.

But a problem occurs when separation of duties is not maintained. For example ... a firewall administrator should not be the one responsible for reviewing firewall rules; a system administrator should not be responsible for user access reviews; and so on. By not separating these duties appropriately, the opportunity to commit and/or hide fraud exists. That is why **effective security frameworks require separation of duties as a basic practice**. MSSPs, MSPs, and/or Cyber Insurance providers who offer virtual CISO services are mixing both first and second line of defense roles. If they do not carefully and effectively manage that, there is opportunity for fraud.

And it can get worse! I have seen posts on LinkedIn promoting MSSPs, MSPs, and/or Cyber Insurance providers adding vCISO services to their offerings not primarily to increase service to their clients, but rather as an inside sales approach. Let's use an example to see how this might work in practice:

- An SMB contracts with an MSSP for vCISO services.
- The first step a vCISO should undertake when engaging a new client is to determine the "as-is" of the security environment by conducting a gap analysis against an applicable framework (e.g. NIST, CIS CSC, CMMC, HITRUST, etc.). The gap analysis may then be leveraged to uncover gaps.
- Low and behold (and by no coincidence), the MSSP just happens to offer services to resolve the gap.

- In this example, the only way to eliminate this bias is for the MSSP to state up front that they will not offer to resolve any gaps found that require technical services such as managing a SIEM.
- Yet, this is exactly what some are pushing MSSPs to do: add vCISO services as a pathway to ensure additional sales.
- Additionally, since the MSSP is more focused on upselling, the vCISO may downplay other potential gaps that the MSSP does not have services to resolve.
- Engaging a biased vCISO, therefore, can result in bad advice and unknown gaps, in addition to potential costs for technical solutions that may or may not be needed.
- Put plainly, these practices are simply not ethical!

This is not to say that all MSSPs operate in this way ... there are many who do not. Those are the ones who understand the value of unbiased consultants. A simple and recommended check would be to ask for a requirement that any MSSP, MSP, and/or Cyber Insurance provider being considered as your organization's vCISO cannot provide services to resolve any identified gaps in your security posture. If the MSSP balks at such a suggestion, they may be leveraging the vCISO to upsell.

The bottom line is this ... carefully vet any vCISO service that you consider because your businesses' security posture relies on having a trusted partner!

CISO ToGo
Technology Risk Consulting

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

www.CISO-ToGo.com

Email: WRichmond@CISO-ToGo.com

Phone: 401-264-0880