CTO/CISO BUSINESS PARTNERSHIP

As businesses become increasingly reliant on technology, it has become more important than ever for business leaders to establish strong partnerships with the CTO (Chief Technology Officer) and CISO (Chief Information Security Officer) within the organization. We spoke with Etienne Castiaux, Founding Partner and CTO of Motive Labs, and Sean Dobson, CTO of Wafra, to hear their insights on how to establish firm alliances and business partnerships.

How important is it for a CTO or CISO to establish a firm alliance and business partnership within the organization? What are the key responsibilities and priorities?

Etienne Castiaux: The CTO and CISO roles have evolved over the last five years. I would argue if you look back five years ago, they were very much inward facing, making sure that the policies are in place, that the security tests run, that IT teams take appropriate measures to protect the systems, awareness programs, activities like that. And what you see more and more is that the responsibilities are increasingly more outward facing.

A CISO's job is to evaluate the risks and work with the business to build a framework for effectively managing those risks

For example, if your company wants to prove that it took the appropriate measures to avoid data leaks, it needs to prove compliance with standards like ISO27001.[1] Typically, the CISO of a payment solution provider to banks for example will have to negotiate with the clients' risk and compliance officers which policies to prioritize, because the one thing you want to avoid is to have to implement every single policy. You really need to have a risk-based approach where you evaluate the risk as low, medium or high, and also the impact of these risks occurring. You might end up implementing 130 out of the 200 ISO27000 policies, and so it's basically transforming into a role where they've got more external communication and more

[1] There are more than a dozen standards in the ISO 27000 family, which enables organizations to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties.

homework to do. As a result, more and more companies are purchasing CISO as a Service from external companies to be able to focus on the more important matters. Clearly a very interesting area to invest in based on the growth in this industry.

What are some best practices or ideas on how CTOs and CISOs can effectively communicate to business leaders on the cybersecurity program?

Sean Dobson: The first thing you need to do is really get buy-in from management. I like the idea of creating a security committee, bringing in folks from various areas in the firm, and that allows you to spread your culture of vigilance around the firm. Starting with policies is also a good idea, because I think people can understand policies and those drive your program. But as Etienne said, you really must focus on risk. You can't focus on the technology. A CISO's job is to evaluate the risks and work with the business to build a framework for effectively managing those risks.

You need to think about how you're going to communicate to your community, to the ecosystem, to your partnership and other companies

From a metrics perspective, some important ones are phishing statistics, incidence statistics like dwell time, which is how long it took you to detect an incident or how long did it takes you to fix it. Patching statistics are always good, as well as vulnerability statistics. What's really important is that cybersecurity needs to be thought of as a value-added area. This is my current lifelong goal. If we're going to take on a new fund or a new client, cybersecurity helps make that possible.

What are some best practices for portfolio companies and how do you recommend communicating with key stakeholders?

Etienne Castiaux: You have the internal communication to senior management which requires automatically generated KPIs (key performance indicators) which have become more and more important in operation management remuneration. I think the statistic is very important. You also need to think about how you're going to communicate to your community, to the ecosystem, to your partnership and other companies.

So, this is an opportunity to play the card of basically tracking and logging, continuously, every single access that has been granted, and every single access that's been used. We have been seeing more and more demand.

But I think it's going to be a common theme in the future where the CTO's role is to communicate the solutions, prove where the leak came from, and prove you have the right measures, and have the tools and process in place to take action.

Sean Dobson: I think the bottom line is that the cybersecurity program needs to be measured for its effectiveness and these metrics need to be communicated to senior management in a way that can be understood. The best way to do this is to focus on the risk to the firm and when possible, the financial impact of these risks should be quantified so management understands them and can ensure there is a focus on putting in controls around these high impact risks. Having a shared understanding of cybersecurity risks between IT and the business ensures that there is a shared focus on the most impactful and likely risks that the firm faces.

This discussion was adapted from a longer panel discussion and has been edited for brevity.
The views and opinions expressed are those of the panelists and do not necessarily reflect those of Capital Constellation or Wafra Inc.