# Q&A WITH MALCOLM HARKINS

GLOBAL CISO, CYLANCE

> Most of the security industry is focused on profiting from the insecurity of computing - which means they profit at the expense of their customers because they are left reacting to issues and trying to minimize damage.

As Global CISO of Cylance, Malcolm Harkins oversees all aspects of information security and risk, security/privacy policy, and peer outreach to drive improvement across the world to understand cyber risks and best practices to manage and mitigate those risks. A true industry leader, visionary, and driving force behind advancement, Harkins instills his passion with the Cylance team to deliver cutting-edge malware prevention.

Cylance focuses on preventing malware with high efficacy to lower risk in a way that lowers cost and improves the user experience. Harkin's book, *Managing Risk & Information Security*, is subtitled "Protect to Enable," one of the core values of Cylance. "Most of the security industry is focused on profiting from the insecurity of computing - which means they profit at the expense of their customers because they are left reacting to issues and trying to minimize damage. Our core business is focused on preventing issues and truly protecting computing, and if we do that, we make money," said Harkins in a recent interview with Kevin West, CEO of K logix.

The Cylance user experience ties back to three things Harkin's believes are important parts of any security solution:

1. Lowering the risks to people, data, and business
2. Lowering the cost of controls
3. Lowering friction and improving experience and velocity towards business goals

Harkins says, "When I speak with CISOs about how you make a business case for security solutions, you must look at all three of these things. One of them might be good enough to buy a product, but when you achieve all three, it's a 'wow' moment."

Kevin spoke with Malcolm Harkins about leadership, taking action, and experience.

Kevin: We have spent a lot of time focusing on educating CISOs to have executive conversations with CEOs and CFOs. We now believe it is the year of action for CISOs, so what do CEOs and CFOs need to bring to table to make it relevant for the CISO?

Malcolm: It all comes back to understanding the risk by considering what the biggest potential current and future systemic risk issues are. There are three lenses through which people must do this:

1. Risk to the business
2. Risk to the customer
3. Potential risk to society

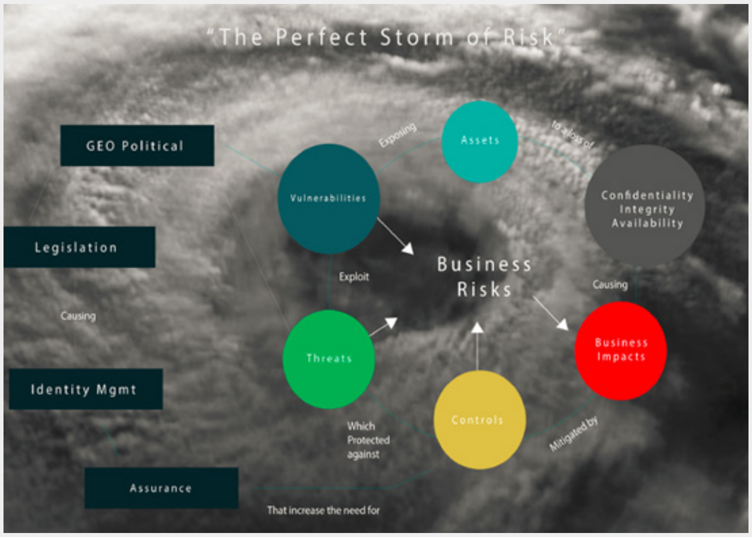
You cannot stay focused on only the risk to the business; you must get to the core and twist the risk issues on these three lenses. Security professionals need to get out of just looking at it from the point of view of a typical IT infrastructure and recognize that even if you are in a brick-and-mortar company, you will eventually become a technology company, or else you will become irrelevant.

Security professionals cannot only focus on specific internally-focused systems, because those may not be part of the technology evolution from a revenue-generation perspective. CISOs need to expand their views and have a very strategic discussion within the context of their organization. This is also something the boards needs to start thinking about from the infrastructure side, product and service side, privacy angle, and link to physical security. They must understand the threading on that Rubik's cube of risk around the information, technology, and how it manifests those risks, as well as the opportunities new technology creates.

Kevin: You spoke at our recent CISO Leadership Summit and shared how CISOs can become great leaders. What is your leadership style and how can others learn from you?

Malcolm: I spent the first decade of my career working in various business roles, from managing credit risk as a call center agent, to running

> “One success measure I am proud of is my ability to move the needle on looking to the future for information security. In 2002, I drew “The Perfect Storm of Risk.”
>
> At the time, people thought it was a few-year effort to upgrade security solutions and insert controls. If I look at what I realized when I drew this, I saw an emerging perfect storm of risk and the elements of security, privacy, business continuity, and disaster recovery. I was able to move my company into recognizing what was coming and how to stay on top of it, but I also galvanized what was coming for the security industry. I spoke about these things in business conferences long before many security conferences even existed.
>
> The success factor that really matters the most relates to the people I have touched who have worked for me or indirectly worked for me. Being able to gain their trust and respect, to me, is the biggest success factor. I still speak with many former employees and maintain their trust. I have always pushed myself to align my beliefs with the work I am doing, something that has helped enable my success. This is also my biggest challenge because there are so many dynamics and pressures that swivel, sometimes from externalities and sometimes from people you work with. You must assimilate their values and views, but also make sure you are clear on your own, and I think this is a struggle for most information security professionals.”



a customer service team. I was able to experience a wide-range of communication and business challenges that built acumen. I got my technical acumen from working at technology companies in procurement and finance, as well as working in some new business ventures at Intel and more recently as Intel’s Chief Security and Privacy Officer prior to joining Cylance.

I have always had a strong sense of mission and fell in love with the people, issues, and challenges aspects of my work. Because I have done such a wide variety of things, my way of approaching leadership is i hope a bit unique; I am more open to different approaches and a diversity of thinking that helps me lead in my own way. **I believe in the three laws of leadership:**

**1. If you don’t believe in the messenger, you won’t believe the message.**
**2. You can’t believe in the messenger if you don’t know what the messenger believes.**
**3. You can’t be the messenger until you’re clear about what you believe.**

To go along with these three laws, Colin Powell once wrote, “You have achieved excellence as a leader when people will follow you anywhere if only out of curiosity.” This stuck with me a long time ago because the power of curiosity is not positional or authoritative power, it creates a different kind of leverage.

A quote I believe to be the best definition of leadership is, “Leadership is the art of motivating others to want to struggle for shared aspirations” (Kouzes & Posner, *The Leadership Challenge*). I believe it is important to recognize there is a strength that comes through struggle.

Another aspect of leadership is trust. In order to create trust, you must also be vulnerable and transparent on who you are, what you believe, and why you believe it. In sum, **trust is a function of two factors:**

**1. Competence – Competencies are not only skills. You must have skills and knowledge, but you also have to do something with them to demonstrate competence.**

**2. Character – You must show how you have integrity, values, and principles.**

When you add all of these up, the leaders who have the most influence are the leaders who are closest to us.

## FIVE THINGS TO REMEMBER ABOUT LEADERSHIP

1. Leadership is a relationship
2. The best leaders are the best learners
3. Leadership development takes deliberate practice
4. Leadership is an aspiration and a choice
5. Leaders make a difference

*The Leadership Challenge (Kouzes & Posner)