Cyber Risk

An Interview with Ed Powers,
U.S. Managing Principal-Cyber Risk Services, Deloitte

EDITORS' NOTE *Ed Powers is the U.S. Leader for Deloitte Advisory Cyber Risk Services and principal at Deloitte & Touche LLP. Under his leadership, Deloitte's team of nearly 2,500 Cyber Risk Services professionals has been recognized by all major analysts as the leader in cyber risk and security consulting. He led the expansion of the practice's vigilance capabilities in threat research, analytics, and advanced monitoring, and strengthened Deloitte's resilience capabilities to help businesses achieve strategic growth objectives in the face of sophisticated cyber threats. Powers has helped many large financial services companies integrate strategic risk, regulatory, and technology program components, and works with industry organizations to help improve the sector's overall cyber risk posture.*

Ed Powers

FIRM BRIEF *Deloitte provides industry-leading audit, consulting, tax, and advisory services to many of the world's most admired brands, including 80 percent of the Fortune 500. They work across more than 20 industry sectors to deliver measurable and lasting results that help reinforce public trust in our capital markets, inspire clients to make their most challenging business decisions with confidence, and help lead the way toward a stronger economy and a healthy society.*

Deloitte was recently ranked number one by Gartner in Security Consulting Services for the fourth consecutive year. It's industry-leading Cyber Risk Services practice (deloitte.com/us/CyberRisk) provides advisory and implementation services, spanning executive and technical functions, to help transform legacy IT security programs into proactive, Secure.Vigilant.Resilient™. programs that better align security investments with business risk priorities, establish improved threat awareness and visibility, and strengthen the ability of organizations to thrive in the face of cyber incidents.

Looking at the growth that Deloitte Cyber Risk Services has achieved, and the critical function this area plays, will you talk about how this division has developed and the expertise of the team that you have assembled?

Cybersecurity, as a field, has been treated largely as a technology discipline over the years. We've done quite well in that business because Deloitte has been in it for 20 years and we have a very large technology consulting practice with advanced capabilities.

Over the past four or five years, this area has evolved from being considered a traditional IT problem to a much more multifaceted, multidimensional problem that we see as sitting at the intersection of business risk, regulation, and technology.

We have since built our cyber risk practice around that multidisciplinary set of constructs. If we think about the hundreds of providers that are competing in this space today, almost all of them are still coming at this primarily with a technology competency. They talk about how they can implement tools to take care of elements such as securing data or analyzing network traffic or blocking attacks.

However, our clients, and the organizations that are dealing with this problem, are dealing with it on all of these different dimensions, which generally coalesce around business risk, regulation, and technology.

We have brought together all of those pieces into a single process at Deloitte to address not just cyber security but cyber risk.

As an interesting data point, we have roughly about 125 partners and managing directors who are the leaders in our practice, which is many times larger than our nearest competitor. These people lead parts of our cyber risk business and lead client engagement. The interesting part about that population is that more than 25 percent of them have degrees in arts and humanities. They are not tech oriented people. Another very large swath has degrees in business or economics.

We have a well-rounded team here that is, just like this issue, multifaceted. We aren't coming at this as just engineers. We come at this with people who have deep knowledge of business risk, regulation, and technology and who are also good problem-solvers.

How broad is the recognition in the C-suite across industry that this is not just a tech issue?

We've moved the needle on that considerably over the past few years. A few years ago, most boards of directors would have said it was a tech issue that they didn't fully understand.

Today, we're seeing more recognition that this issue presents itself with some really important business context, so they're seeing the business risk associated with this through some of the big attacks that have occurred against the big banks or the large retailers, or through some of the other destructive cyber attacks we've seen in the past year.

They recognize the business impact that flows out of this and that when we do have one of these incidents, it manifests itself in a series of business crises. While they're not 100 percent there yet, the mindset is shifting dramatically around the business nature of this issue.

There are so many business implications of cyber risk. From a CEO perspective, what are the key areas they have to focus on and the questions they need to ask within their organizations to understand those implications?

The biggest thing, be it for the CEO or the board, is whether the organization fully understands the specific risks that it faces from a cyber perspective. When a business executive talks to the people who manage cyber within their organization, they often get a discourse on all of the things that one is supposed to do from a standard perspective or a framework perspective, like manage firewalls, intrusion detection, etc. That is the standard laundry list of issues to address.

What they rarely get is a really thoughtful discourse on what the full risks are that their particular organization actually faces. These need to be based on the businesses they're in, the ways they interact with customers and suppliers, and on the geographies in which they operate throughout the world. It also needs to deal with the nature of the operation, the nature and sensitivity of information that is handled, and the critical infrastructure that is managed. All of this needs to be addressed to fully understand the specific risks that this particular organization faces.

Oftentimes, we find that what the checklist says a company should be doing is important but it doesn't necessarily square up, especially from a priority's perspective, against the risks one's organization actually faces – things like understanding if they're trying to protect sensitive customer information and if so, from whom? Are we a transportation company, like an airline, where we are concerned about things like flight operations and how dependent our operations are on cyber sensitivity and how

Boards should start thinking about cyber as a business risk, just as they think about other business risks, like market, credit, or strategic risk.

vulnerable those may be to potential disruption and attack? It could be an aerospace defense contractor who handles very sensitive intellectual property and trade secrets that they are trying to protect.

When I meet with a CEO or talk to a board, one of the first things I talk about are the people who work for them and handle cyber, and whether they are able to articulate the risks they are managing. Not just the standard checklist, but do they have a broad understanding and work closely with management to understand the risks they're trying to address through their cyber programs?

The usual answer is, they have a lot of work to do there. There are a handful of organizations getting good at this, but many still have a disconnect around the investments they're making in cyber and the priorities that they've established for themselves. They need to be consistent with the actual risks the organization is facing.

Is the thinking more about addressing the problem or about prevention?

It's both, and a bit more. While historically people have treated this as a prevention exercise, to protect information and protect infrastructure, it must evolve beyond that. For a variety of reasons, not only is it not feasible, but it's often not desirable, to lock down all data and infrastructure.

At Deloitte, we developed a construct called "Secure.Vigilant.Resilient." that recognizes a company has to balance their approach and investments and understand there are things one will do to protect information and infrastructure. However, at the same time, they need to be investing in things that are designed to create vigilance such as better visibility to see when assets are at risk. They have to be able to see when they're being attacked and understand how they're vulnerable. They also have to put a robust intelligence and monitoring capability in place to allow them to see when those protection controls are potentially failing.

The resilient piece of it is about how to prepare and respond to the cyber incidents that are increasingly likely and, in some cases, potentially inevitable. That requires evaluating whether they have adequate incident response and crisis management plans in place and whether they exercise those. Do they practice them? Do they know what they're going to do and how they're going to make decisions when faced with a cyber crisis? This includes all of the things associated with recovering from a cyber incident, which is beyond just a technical clean-up. It certainly requires the technical investigation and clean-up of the environment, but it's also about how to manage customers, suppliers, and business partners, as well as regulators and the public.

All of the crisis management activities that one would expect to see in any business crisis are now getting layered into the cyber world as part of that cyber resilience.

When it comes to the approach that needs to be taken, you mentioned the people who manage this. How critical is it that the Chief Security Officer be prominent within organizations and is industry moving toward every company having that role as a given?

Just as important as the role of the CSO, is the person in the role. It's not enough to say that our CSO has a seat at the table or is part of the strategy process.

Who are the people in these roles? How well do they understand the business? How credible are they with the security team and with the technology teams? Are they able to bridge the gap between these two worlds, because one of the biggest failures we see is that there is still a gulf in thinking and in language between executive management on the one hand and the people who manage cyber risk in most organizations on the other hand.

It's really important to find somebody who can operate credibly in both of those roles, and those people are rare. Over time, we're going to see more people who fit that bill just as, over the past decade, we saw an evolution of the role of the CIO in many organizations to more of a technology-minded business executive as opposed to just a tech manager. We will likely see a similar evolution in the role of the CSO and we're already beginning to see where we're going to have a risk and security minded business executive play that role of the CSO in many organizations.

You referred to senior management in the C-suite but you always mention the board. Many members on these boards don't have experience around cyber. Do they know the questions they should be asking, and going forward, is it important that boards start to bring in people who also understand this issue?

The board issue is still evolving. This question gets asked a lot – should we put cyber experts on the board? More important than that is educating the board broadly on what this actually means. We spend a lot of time with the board. I personally spend 25 percent of my time with boards where I used to spend almost all of my time with management.

We try to help them understand that they don't need to know how firewalls work or how network traffic gets routed or how a particular adversary might try to attack a particular organization. These issues perk up people's ears because they're 007-type stuff. As a board member, one needs to understand the business risks to their organization that are created by the things they're doing around cyber.

Great example: When one undertakes a merger or expands into global markets or undertakes a large outsourcing relationship with another firm, or when one undertakes a digital transformation and starts to interact with customers and suppliers in different ways, those are the things embedded in business strategy that actually are creating cyber risk.

We help boards understand how the things that management is doing strategically actually create cyber risk, and how management can articulate to them where these cyber risks are actually created and how significant these risks are.

Boards should start thinking about cyber as a business risk, just as they think about other business risks, like market, credit, or strategic risk. That's the level at which we need boards thinking about cyber. Can they oversee and govern what management is doing from a cyber risk perspective? How have they constructed their program? How are they setting their priorities and what kind of investment are they making in risk protection?

Are there ways to put metrics in place around the cyber efforts for a management team?

From a quantitative perspective, there are few meaningful metrics at the executive management level. When we talk about operations at the operational level, there are all kinds of metrics.

When we talk about things that actually should matter to executive management around metrics, it's less about quantitative data driven metrics that we may see in certain other areas like credit risk, for instance.

What we do see is a much more qualitative approach but a disciplined qualitative approach. ●