Secure Vigilant Resilient

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

Ed Powers

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.*

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.*

With more than 2,500 professionals, Deloitte's Cyber Risk Services (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.*

Would you talk about the growth Deloitte has seen in the cyber risk area and the talent you have been able to bring in to meet the need?

It's obvious that cyber risk is receiving growing attention at all levels within today's organizations – from the board through executive management down through line-of-business leadership, and through various functional business areas.

The growth of our cyber risk practice reflects this increased attention and concern. We are widely regarded as the largest cyber consulting business in the market according to key analysts. Our team grew by 37 percent last year.

Cyber risk is much more multifaceted than many people understand it to be. To achieve that growth, we've utilized many different sources to acquire talent with a wide variety of skill sets. We aren't just looking for those with engineering and computer science skills, which are obviously very important, but also for those with business, government, and liberal arts backgrounds.

Do you find that young talent has an understanding that this kind of work is being done in professional services firms today?

Yes, but we also spend a great deal of time on campus trying to educate students about what we're doing.

Cyber risk plays to the sense of purpose that this generation is looking for. In the generation we're recruiting now, that sense of purpose is really important. When I talk to students on campus, I tell them about my having come up in the age of the *promise* of the Internet – how exciting that was in the 1990s, and about how they are now coming up in the age of the *peril* of the Internet. In the realm of cyber threats, we are actually dealing with one of the biggest societal problems of our era. It's not just about us protecting credit cards on behalf of banks, but rather how we're protecting the infrastructure we all use every day through virtually all aspects of our lives. I've found that talking about why this is such a crucial issue is one of the most effective ways to engage young talent.

Is the view of cyber risk now shifting from just being a technology issue to more of a business issue?

Over the past year, in the U.S. alone, we have served over 500 clients in this space and close to 1,000 globally.

We consistently hear that organizations are spending more money than they've ever spent on cybersecurity, and paying more attention to cyber threats than they ever have, yet the issue persists. Board members and executive leaders are used to resolving issues – but cyber is less a problem to be solved than a risk to be managed. Like any other top-level business risk, organizations can improve their ability to manage cyber risk, but some measure of risk is always present.

We stepped back to look more deeply at the nature of the problem. When we think about what is being said in the media and what the various experts and pundits talk about, when we think about what most consulting firms focus on and where they try to take their clients on this issue, much of the dialogue is focused on the adversary. We always hear about very sophisticated, rapidly evolving, highly motivated, very well-resourced adversaries who may be connected to organized crime or rogue nation states. There is a notion that this adversary is very formidable and, therefore, why this is such a difficult problem.

This is important and much of that is true, but it doesn't account entirely for why this is such a difficult issue. When we started to really examine the problem, we realized that everybody talks about the adversary, but very few organizations are talking about what they, themselves, are doing to magnify the risk or actually create it.

Organizations can improve their ability to manage cyber risk, but some measure of risk is always present.

In the final analysis, it comes down to three very common issues that make this such a difficult problem. One is that over the past 15 years or so, we've systematically connected our economy and our society in some really powerful, compelling ways, but we've done this using technologies that were largely designed for sharing information and making it available – not for protecting that information. While it's possible – and necessary -- to protect information and infrastructure in this connected world, it's costly to do so, and in most cases, impossible to do it perfectly.

The second issue is the notion that no matter what business a client is in and no matter where they're operating, they have to trust people every day to handle sensitive information, to operate the business, and to access critical infrastructure. People, quite simply, don't always do the right thing. Most often it's because they're ill-informed, unaware, or complacent. In some cases, people behave maliciously. However, organizations can't stop trusting people and, as long as they have people, they are going to have some degree of this risk.

The third piece is that there is a very intimate connection between the things that organizations do to innovate and drive performance on the one hand, and the things that actually create cyber risk on the other hand. What I mean is when we look at the strategic agenda of any organization, whether it includes things like globalization, mergers and acquisitions, extension of third-party networks and relationships, outsourcing, adoption of new technologies, movement to the cloud, or mobility – all of these are initiatives that organizations undertake in order to drive performance and execute on their business strategies. However, these are also things that create cyber risk.

This part of the equation is one that our clients have some control over, but it's also one that creates a paradox for them. In some aspects of life, or in some parts of business, if we identify something that creates a lot of risk, we can opt to stop doing the things that create the risk. But businesses today must grow and innovate to improve performance; they are actually looking to do more of the things that create cyber risk.

By working with us, our clients start to realize that while they can reduce the number of cyber incidents, or the damage they cause, it is infeasible to think that they're going to protect everything. There might even be some cases where an organization would deliberately choose not to protect certain things because to do so would be too stifling to the business agenda.

This is starting to hit home with leadership and with boards. Once they accept that this is a risk problem, the next question is: What do we do about it?

We have built a construct we call *Secure. Vigilant. Resilient™*. The idea behind this is to move beyond cybersecurity as a discipline that focuses on the protection of information and assets to the discipline of cyber risk. This means incorporating *security* where appropriate, but augmenting it with *vigilance* – the ability to see threats better, to understand them better, and to recognize when one is under attack – and with *resilience*, which is the ability to respond quickly and to minimize the business impact of the increasingly likely, and perhaps inevitable, cyber incidents.

Is protection or response the priority?

Historically, it has been protection. Today's approach is becoming more inclusive of building better vigilance, preparing for incidents, and planning responses.

We are also doing work to demonstrate that organizations need to expand their horizons on how they can be impacted by cyber attacks.

We see attention shifting, especially in the boardroom and among senior leadership and executive management, toward becoming better prepared. We're doing a lot of work in the area of cyber war-gaming, which uses scenario-based exercises to help organizations get better at responding when a cyber incident happens. In fact, for organizations that have been underinvested in security, focusing on resilience may be the first thing they should do; given the likelihood of cyber attacks, they are more likely to first need better response skills while, over time, they invest in a stronger set of prevention mechanisms.

How critical is it to address risks across all areas to have the desired impact?

We believe it's essential. This is why we're having so much success in this space. Historically, this is a field that has been treated as a technology field. Today, organizations are beginning to realize they can't "technology this problem away" – they can't install a bunch of tools to resolve this problem.

We approach the problem strategically from a capability perspective by recognizing that this is an issue that exists at the intersection of business risk, regulation, and technology. Those are three core dimensions, and one has to look at the interplay among those when dealing with cyber.

Another reason we're doing so well in the cyber market is that we have great technology chops, but we also have a market-leading risk consultancy at Deloitte, and a market-leading regulatory consultancy.

With the access a firm like ours has to boards and executive management, and the deep industry knowledge our teams have, we bring together all the disciplines needed to help the board, CEO, and C-Suite address cyber risk at a strategic level better than anyone else can.

Does this cover all industries today and how broad has the awareness become?

It's pervasive. Every industry has some degree of cyber risk, but it's really important for each organization to understand the specific risks it faces. Organizations within a specific industry group tend to have the same kind of information, assets, and business processes, and therefore tend to have similar exposures, but risks vary by organization and by industry.

We advise our clients to not just think of the broad swath of things that can potentially happen, but to think about what is likely to happen in their organization given the specific things they're doing from an operational and information perspective, and what assets they have.

Is it challenging to show impact in this area?

The notion of how to show value for cyber risk investment is one that the industry struggles with because success is invisible – it's the absence of a cyber event, or the ability to show that an event had a lesser impact than it might have had. It is difficult to show return on investment for cyber risk programs.

One of the things we've been helping our clients with is developing the ability to demonstrate that the investments they are making are aligned with the actual risks they face. This is an important concern for many organizations right now. They have to ask if they are making the appropriate investments in security, vigilance, and resilience, and whether those decisions are based on a realistic understanding of the specific risks their organization faces – and the magnitude of impact that a cyber attack could have.

We are also doing work to demonstrate that organizations need to expand their horizons on how they can be impacted by cyber attacks. Instances of large-scale data theft capture a lot of media attention, partly because of what organizations are required to disclose. As a result, organizations are fairly familiar with typical costs, such as breach notification programs and regulatory fines. But there is less light shed on other kinds of impacts that are not publicly disclosed, and less understanding of the intangible impacts, such as impact to brand, or the costs associated with drawn-out operational disruption. We have been working with our financial valuation team to actually quantify that full range of business impacts, and will publish a paper on this shortly.

Do you worry that as cyber threats become more prevalent, the need for companies to continue to innovate and take the risks to grow will be stifled?

I don't think we're going to see organizations avoiding innovation or putting the brakes on their strategic agenda because of cyber risk. History tells us that organizations will drive harder around their strategic agendas and innovation initiatives.

However, I think we'll start to see this notion of cyber risk become much more prevalent. Over time, we'll see that the organizations that have a better handle on cyber risk will be the ones that can best reap the return on their investments and innovations; they will outperform the others. ●