Women Leaders

Cyber Risk: Who Says Women and STEM don't mix?

An Interview with
Emily Mossburg, Principal; Mary Galligan, Director; Bethany Larson, Partner; and Deborah Golden, Principal;
Deloitte Advisory Cyber Risk Services


Emily Mossburg


Mary Galligan


Bethany Larson


Deborah Golden

EDITORS' NOTE *Emily Mossburg leads Deloitte Advisory's Cyber Risk Services Resilient practice, where she helps organizations, public and private, to prepare for, respond to, and remediate after cyber incidents. She works with executives and boards overseeing cybersecurity to help them translate technical risk to business risk and understand the business impact when a threat is realized. Mossburg regularly contributes as a speaker at various events and conferences, and with media on the topic of cybersecurity and incident response.*

Mary Galligan retired as the Special Agent in Charge of Cyber and Special Operations for the New York Office of the FBI. She spent over 25 years in the FBI leading cyber and terrorism investigations. She works with boards and executives on cyber risk awareness and cyber wargaming. She received her master's in Psychology from The New School of Social Research and her bachelor's in communications from Fordham University.

Bethany Larson leads the enterprise application integrity practice (Cyber Risk related to transformation of business processes) for Deloitte Advisory's Cyber Risk Services, with over 30 years of security, privacy, and internal control experience. She received her M.B.A. in Accounting & Finance from University of St. Thomas.

Deborah Golden has over 20 years of information technology, security, and privacy experience encompassing various industries, with a specialization in Cyber Risk Services, as well as within the Federal, Life Sciences & Healthcare, and Financial Services industries.

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. Working 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 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.

INTRODUCTION *Recent reports tracking the percentage of women in information technology and cybersecurity fields show an alarming trend: the number is declining. Debunking the trend is Deloitte LLP, the world's largest professional services firm. In 2015, the company appointed the first-ever female CEO of a U.S. consulting firm and ranks consistently among the best places to work for women. So maybe it's no surprise that we discovered that within Deloitte's Cyber Risk Services practice, there are more than 700 female professionals advising the nation's biggest organizations, public and private, on their cyber risk strategy, planning, response, and recovery. Who says women and STEM don't mix? LEADERS' President, David Schner, spoke with four of the firm's partners on their roles, responsibilities, and the cyber challenges on the horizon.*

Would you touch on the value of cyber risk and cybersecurity in today's world?

Emily: Cyber risk and cybersecurity are now hot topics among executives. Executives are now asking a lot of questions; they are realizing they need to focus on cyber risk and the associated impacts as the landscape is evolving, and threats are becoming more pervasive and real to the organizations they lead. They realize they need to communicate about these topics with the board. This has not always been the case, and we are in a period of change.

Executives need to be able to speak about cyber risk in clear business terms and to explain the true business implications using the type of terminology that the C-suite is accustomed to in describing other enterprise risks. This changes, to some degree, the profile of what is needed when it comes to a Chief Information Security Officer.

This has interesting implications for women because we're starting to see a role that is focused on bridging the technical and business areas. These aren't easy skill sets or capabilities to acquire but these are roles that are interesting to women. We're at a point where we could start to see a real swing in the number of women interested in this space.

As you talk to those trying to get ahead of this curve, what steps should they take?

Emily: The first and most foundational thing is understanding what the organization really needs to protect. What do they have that is not only important to their business but would also be interesting for the adversary to gain access? Once you understand your data assets, you can start to identify the true business impact if those assets are exploited, inappropriately accessed, or destroyed, and determine the approach to secure those assets and best minimize risk. Securing your assets is not enough. Ongoing monitoring is important to understand if the security solutions and processes in place are working. Monitoring is critical in recognizing targeted attacks and, if attacks are effective, an organization must be ready to respond. They need to be sure that the right people across the organization understand the response plan and their role in that plan. This should include the escalation path for response, technical investigation protocol, business operations impact management, decision making governance, communications plan, and customer management.

How far along is the industry in really understanding this risk and in their preparedness?

Emily: There are some industries that are more in front of this issue. These are typically industries that have been in a more highly regulated space, as well as those having more to lose in a typical cyber smash-and-grab scenario.

This includes industries like financial services, as well as the U.S. defense and intelligence agencies. Increasingly, we're seeing an evolution in healthcare from the plan and provider sides because the issue is escalating with additional attacks and disclosure of data breaches.

Those industries that are more mature are generally becoming more secure and more able to recognize and remediate when under attack. We're seeing that organizations are still working on the culture shift associated with cyber risk and integration into the innovation lifecycle. Cyber risk is embedded in everything we do from an innovation standpoint. We have moved so rapidly into an integrated, connected world and have been very focused on the efficiencies and insights we've gained, and in some cases our cool new devices, that we haven't been focused on the risk those innovations have introduced. As we continue to innovate, we need to think about not only how cool and advanced what we're innovating may be, but also what new risks we are introducing. When we think about the risk after the fact, it's much harder to understand and manage.

Beth and Mary, within Cyber Risk Services, what are your various areas of focus?

Beth: My team is focused on serving clients who are running an ERP backbone for business process transaction processing. For example, these would be clients that have a large SAP or Oracle back office (on premise or in the cloud).

The practice has evolved over the past few years. It used to focus on building security and internal controls in those environments, but as the system's landscape has evolved, there isn't a clear perimeter anymore. Many systems now connect with each other and users are accessing data via handhelds, and systems are on premise and in the cloud. In addition, many of our clients have an increasing number of users touching their systems, which increases the risk platform. Now our practice focuses more on strategy and architecture design, and addressing broad cyber risk business implications.

Our professionals have a deep understanding of cyber risk for industries. Deloitte has 24 industry sectors within seven focus industries, which we specifically focus on, and this is important because the types of cyber threats faced in each of these sectors are very different. The transaction processing component of this is very important to the financial statements, and the protection of intellectual property, PII, customer data, etc. and the potential for error can be quite large in some of these environments. Today, we aren't focused just on the traditional financial statement risk but, in addition, compliance, regulatory, and risks associated with data privacy and sensitive information that is housed in and flows through these systems.

Deloitte is different because we have such an industry focus. Our professionals choose an industry they're going to focus on early in their careers. They don't have to stay there forever but a lot of professionals get enjoyment from doing that. It gives them a deep understanding of how the business operates and why their clients do what they do to be competitive. We address not just the security landscape but more so protection of the key business data and processes.

"As I talk with government leaders and CEOs, cyber threats are top of mind for them. Those threats today are only increasing in breadth, sophistication, and impact. Our clients recognize that cybersecurity is no longer just an IT problem – it's the intersection of strategy, operations, and technology. Leaders with foresight are weaving that recognition through the fabric of their organizations and taking action to be prepared. I'm proud that Deloitte is helping to address our clients' most critical concerns in this area, and that we are leading the way with our more than 700 female professionals in our cyber risk practice."

- Catherine Engelbert, Chief Executive Officer, Deloitte LLP

Almost 60 percent of the Partners, Principals, and Directors in my group are women, and we have quite a few women professionals at all levels doing this kind of cyber work. We spend a long time working with the same clients so our professionals have strong relationships with them, which provides value to clients and career satisfaction for our team members.

Mary: I've been at Deloitte for the past two years after spending 25 years in the FBI. I concentrate on talking to the C-suite and the board about cyber risk. There is a large and increasing demand from boards for guidance on how they should be looking at cyber risk to ensure they're fulfilling their fiduciary responsibilities and incorporating cyber risk principles across what they do.

I also do cyber war games along with other partners for our clients. It's another area in the cyber risk arena based on increasing regulations and the desire for companies to test their level of cyber preparedness, and see how well they are positioned at responding to an incident.

Also, having been in the FBI, oftentimes our clients will have questions and concerns after an incident has occurred about what type of information they should share with the government. I walk them through the kinds of information the FBI and Secret Service want and how to best provide it.

What separates Deloitte from other cybersecurity firms is the willingness and forward-thinking in hiring people, like myself, who can bring to our corporate clients knowledge on what the government is doing in this area. Cyber risk and cybersecurity is probably one of the few areas that intelligence agencies do better than business.

What are the major difficulties in helping to protect your clients around these concerns and does it require an understanding that it's more about when than if?

Mary: When we look at the fact that only 5 to 10 percent of breaches become public, it's definitely a matter of when. With organizations having so many employees spread over vast geographic areas, business is dependent on technology, the Internet, and the sharing of information securely. We will often hear people say cyber is an overwhelming area for executives to address. It actually comes down to the risks that are specific to a particular company and industry. While businesses need to have the right technical controls in place to protect the integrity of their organizations, their employees, partners, and customers, they also need leadership from the board through the executive suite to recognize that cybersecurity is now and forever going to be a strategic business priority that no section of the business can avoid.

How far along are large companies in understanding that this is not only a business concern but that the actions are necessary to keep the companies moving in the right direction?

Beth: We believe it's critical for our clients to continue to innovate and do the things that give them a competitive edge. They need to implement and transform their technology environments to be more efficient, and at the same time, they have to share data (i.e., leverage the Internet), and trust large groups of third parties, vendors, employees, etc. accessing their systems. All of this is critical to their overall business strategy and success, but they inherently do create cyber risk.

We caution our clients to understand that cyber risk is a reality and each client needs to have a risk-based, pragmatic approach to address it. They need to be secure, vigilant, and resilient. Each of those pillars matters.

"Secure" refers to the foundational things that lock down the environment. However, in addition to security and controls, they have to be "Vigilant" to monitor what is happening in the risk environment around them. For example, sensing new risks in the industry, and using intelligence analytics to help assess threats and recognize what abnormal looks like to their organizations.

The third pillar, being"Resilient," means being prepared to respond and recover to a cyber incident. It's important that organizations understand who is responsible for what during the duration of a cyber incident, the impact of which can last for months and years. Preparation and response plan testing are critical to organizational resilience.

Twenty women partners, principals, and directors in Deloitte Advisory Cyber Risk Services are blazing trails in information technology and cybersecurity, while other U.S. businesses struggle to attract top female talent in STEM fields. Back: Jamie Fox, Sharon Chand, Sonia Powell Powell, Julie Ho, Elvia Novak, Taryn Aguas, Mary Galligan, Rene Waslo, Anne Litke, Beth Larson. Front(L to R): Tania Webb, Fiona Williams, Johanne Pollock, Deborah Golden, Nancy Albinson, Julie Bernard, Emily Mossburg, Lynne Challender. Not pictured: Allison Eng-Perez and Carey Miller.

Deborah, would you touch on your focus in the firm?

Deborah: I lead Deloitte Advisory's federal cyber risk services practice. I also do quite a bit around client engagement delivery focused predominantly on Federal Health agencies.

What is the impact of legislation today?

Deborah: Legislation brings up an interesting challenge when it comes to level of potential impact across a myriad of organizations. As cyber legislation continues to advance in areas such as information sharing and privacy, we see the impact on not only our public sector clients but the private sector clients as well. While the approach to achieving heightened cybersecurity awareness may be varied, one commonality has been the need to share information, specifically those facets associated with cyber threat intelligence, both within the public and private sector.

Our clients continue to familiarize themselves with these types of legislative activities, recognizing the potential bearing of such efforts on both public and private organizations. It's not just about the basic parameters of the legislation, but more so the ability for each impacted entity to establish and/or update policies, processes, and technologies, including legalities and disclosures, to address the mechanics of the proposed legislation.

Mary: The FED, SEC and others are all talking about addressing cybersecurity and attacking it based on the standards that came out in February 2014 from the National Institute of Standards and Technology (NIST).

This is a problem that can be addressed in a systematic way in terms of how to identify, analyze, protect, respond, and recover. Each of these five areas need to be addressed.

It's clear we can't protect everything, so the question is, what data or controls will have the most significant negative impact to a company if lost or disrupted? Have they done an asset assessment of the most important things to the company and aligned security resources to them?

Anything is possible when it comes to cyber threats, but it is important to narrow it down with a focus on what makes that organization a target, what is "probable" in their company, and then building plans, procedures, and technologies to best defend the organization while advancing the company's mission.

How close is the coordination among you and the leaders within cyber risk?

Deborah: Coordination within our teams, our clients, regulators, law enforcement, and third parties is critical to the way we go to market. A key differentiator for Deloitte is our ability to leverage both our private and public sector experiences, which allows us to leverage leaders and practitioners from across the organization to help us understand potential synergies across various marketplaces. For example, many of our private sector financial services clients are interested in the trends associated with those activities occurring in the Federal National Security sector, and vice versa.

Anything is possible when it comes to cyber threats, but it is important to narrow it down with a focus on what makes that organization a target.

It behooves us to look at our clients and their challenges, and collaborate among ourselves so that we can bring our cumulative knowledge to the marketplace. We have a great ability to do so and it enables us to solve our client's most complex problems.

Mary: I have seen firsthand that there is incredible coordination. I would not be as happy as I am at Deloitte or be able to add as much value as I hopefully do without the coordination that exists in our practice.

When you look at the next generation coming into the industry, is it well understood how much Deloitte can offer?

Mary: Deloitte's reputation is stellar. We are well recognized as a cutting-edge professional services firm. We are known to be very ethical, which is extremely important to me, and we are constantly rated among the best professional services firms in the world.

Beth: One of the roles I play involves leading our learning programs for the 10,000 professionals we have in Deloitte's Advisory practice, which includes Cyber Risk Services. Understanding the broad learning requirements and how we continue to evolve our talent across that many people is a rewarding challenge. The diverse skills of professionals we're bringing in makes this really interesting. We have every kind of professional one can imagine in that group of 10,000 (nurses, pilots, accountants, veterans, etc.) with many of our team members having other careers before they joined the firm. It's fascinating to see how these specialists come together to serve clients, and we're constantly thinking about how to help them collaborate to bring more value to our clients. I'm proud of the strong tapestry of tightly woven, deep, and unique specializations we have across the firm. ●