Get brilliant at the privacy basics: Q&A with Claudette McGowan

FEATURING

Claudette McGowan, CEO, Protexxa

> Read commentary from our lawyers for the latest legal and industry trends in our article "Do Québec's new privacy laws give Québec businesses a competitive advantage?" And for more industry insights, read our in-depth Q&A featuring Talia Abramowitz, Managing Partner, Deloitte Ventures.

Cybersecurity continues to become increasingly more critical for corporations, startups, and customers alike. As someone who has worn all three hats, where do you see the most important opportunity for improvement within this space?

The big thing that concerns me right now is visibility—do people really understand what they have? In the simplest of terms, think about your home. If someone asked for an inventory of what's in your home, you could probably go through each item.

However, when it comes to digital assets, many companies don't have that inventory. This is a problem because if you don't know what you're connecting, then there's very little chance that you're protecting it all. And so, this is an opportunity for people to get brilliant at the basics and to understand all the pieces and parts that make up our digital environment.

So, I would say the improvement opportunity for companies, individuals, not-for-profits, and massive organizations is know what you have and make sure you're protecting it.

What are some of the biggest challenges facing the industry at the moment?

One is, obviously, the threat actors who have very, very deep pockets. They're not constrained necessarily by budgets or have to account for every penny like companies do. A big challenge right now is ransomware. We're seeing many organizations, big and small, being attacked by ransomware gangs.

The second matter is around third parties and interconnectedness. You might have all the controls in place at your company, but who do you work with, and what kind of controls do they have? Do they have the same policies, programs, frameworks, standards, and controls that you have? Because if they don't, you are open to a lot of risk because you're only as strong as your weakest link.

The third thing is critical infrastructure. What do we need to run society, and how are these grids and systems connected? Companies can't run if you don't have critical infrastructure, and when critical infrastructure is under attack, that means everybody's under attack. And so, from a cyber point of view, if you're a company that helps

companies in trouble, how do you prioritize when everybody's in trouble? Who gets help first, and how do you make sure they receive it? Are you taking care of hospitals or banks first? What about schools?

It is important to have a view and understanding of how critical infrastructure plays a role in every company globally.

What advice would you give to founders who are building startups that will integrate and manage a lot of customer data?

The first thing is to have a data management program in place. You can't bolt on security and data literacy. You must make sure these things are built-in and that your team has that kind of mindset and understands what it means to have different classifications of data.

Your people must understand what it means to protect data in different ways. It doesn't necessarily mean that you're encrypting everything at the highest level, but you certainly should know your digital crown jewels and make sure that you're putting all the right provisions around those crown jewels.

Get brilliant at the basics when it comes to data security. Make sure that you have data literacy across all levels of your organization so everyone understands it's not just a file, or a Word document or Excel spreadsheet. These are all actual assets for the organization, and each person should understand what can happen if those assets fall into the wrong hands.

What are some of the most common struggles corporations have in integrating new cybersecurity technologies?

The first thing is price, and how big their cyber budget is. With many corporations, if they don't have incidents, then they don't necessarily think they need to be putting investment into this category. However, corporations should be hiving off the right amount of investment when it comes to data protection. And this protection isn't always software—a lot of times you can get there through process, practice, training, and simulation.

The second thing is to not let fear make your decisions. I spoke to one CEO who told me "I just buy everything so then I know I'm covered", but buying everything doesn't mean you're covered. It just means that you have more complexity and you're wasting money. Instead, look at your budget and evaluate if the level of budget allocated to cybersecurity is commensurate to your entire portfolio. Have budget to run the company, budget to transform the company, and budget to protect the company. In general, protection budget should be anywhere from 5 to 15%.

With Québec's introduction of new privacy laws, some are wondering if this gives Québec-based startups a competitive advantage. What are your thoughts on this?

I think it could be viewed in two different ways. It is great to be clearer about what it means to have the right controls in place, and a key deliverable of that program is having an incident management plan. But there is a tradeoff to that. So, are you trading off speed? Are you trading off agility? Are you trading off functionality? There must be a nice balance.

It is important that companies test their understanding of the law. Businesses need to know what it means for them and what they are mandated to do—and by which date.

As we've seen in California, and with GDPR in the European region, these controls are helpful and can protect customers. They also make sure customers feel like the data is theirs, and they are free to make decisions around it and have a right to be forgotten. These things are important, and we can't lose sight of them.

I like the pilot and scale approach versus it being rolled out on one day and effective immediately.

How have you seen the cybersecurity industry change in recent years?

Things have changed since the pandemic. More people, whether we like it or not, are working from home. So, that means that the perimeter has changed.

Before, organizations just had to make sure that everybody within the four walls of their office was protected—they used desktops that were connected to the main company network, which in turn was connected to a secure data center. Now with people working from home, and the rush to the cloud, there's no longer that data center controlled by the corporation. This has presented a lot of new challenges and opportunities within the industry.

AI is getting a lot of attention. What benefits and risks does it present to privacy?

AI helps us make decisions faster—you get a lot of speed, and you get pattern recognition—but there is a trade-off that we must be thoughtful of as well.

There are concerns about control over the algorithms and biases in the models. AI is being used to find needles in the haystack a lot quicker, but just as much as we're using it on the cyber and protection side, there are threat actors using it to do cyber-attacks and invasion of privacy.

These attackers use AI for malware attacks, to impersonate your voice or to send out phishing, vishing or smishing communications. And so, it is really important to recognize that there we're not the only ones innovating.

What are your thoughts on privacy legislation in the tech ecosystem in Canada?

I think that aspirationally we are trying to do the right thing, and in some instances, there is a focused effort, such as with PIPEDA or these new bills that are coming through, however, at this stage, the legislation doesn't feel fully integrated.

We need to do more to get to businesses and make sure that they are being evaluated for understanding, and helped, where needed. We need to identify who can be the privacy advocates that can go out there and explain what the changes are, why the changes are being made, what value they hold and the benefit they bring. Because, if you're running a corporation, anytime new legislation comes in, you're like, wow, that's more cost. There must be some benefit to it that businesses can see, and the legislators can provide more education and awareness.

What's your 10-year forecast for the industry?

I think we're going to see more artificial intelligence, obviously. We're certainly concerned about quantum computing and making sure that we've got the right controls in place for when encryption is being challenged as we know it today.

We have been talking about things like AR and VR for a long time, but I think, as we saw with generative AI, when it becomes more operational and simpler to use for the everyday person, then we will see its adoption go up quite sharply. I'd like to see proper applications that people of all generations can use and get value out of it.

From an industry perspective, we think about things like the automation of self-driving cars and everyday tasks in life as we know it. How we do things is going to become easier because we're looking at integrating and converging different technologies.

I think the industry will get better at setting policies, enforcing policies, and making sure the value of these policies is shared. But I don't envision any new magical technology. I think we're going to get really smart about how we use the things that we're working on today, which include AI, cloud, quantum—you name it.

Claudette McGowan is a global information technology leader with more than 20 years of success leading digital transformations, optimizing infrastructure and designing new approaches that improve service and cybersecurity experiences. She has worked in the technology industry for several organizations such as Deloitte, Metropolitan Police Services, North York General Hospital, Bank of Montreal, and TD Bank. At BMO, Claudette served as the Chief Information Officer, Enterprise Technology Employee Experience, and at TD she was the Global Executive Officer for Protect Fusion & Cyber Experience. Claudette is currently the Chief Executive Officer for Protexxa, a Canadian-based cybersecurity software and services company.

To discuss these issues, please contact the author(s).