Microsoft’s Sarah Armstrong-Smith on cybersecurity, digital transformation and diversity

Sarah Armstrong-Smith is a highly respected cybersecurity, digital transformation and crisis management expert. She was appointed the Chief Security Advisor at Microsoft Europe in 2020, kickstarting her career with the technology company during a historic challenge – the COVID-19 pandemic.

Temps de lecture : minute

25 August 2021

Named one of the Most Influential Women in UK Tech and Most Influential Women in Cybersecurity, Sarah is also a firm supporter of female representation in technology industries. She is regularly booked for corporate conferences and events, to speak from the perspective of a woman in business and highlight the importance of diverse thoughts.

With the support of *The Female Motivational Speakers Agency*, we sat down with Sarah to learn more about digital transformation, cybersecurity and workplace diversity.

You have been the Chief Security Advisor at Microsoft Europe since 2020, what has been your proudest achievement in this role?

For me, I actually joined Microsoft one week after the UK went into lockdown. So I’ve actually spent my entire Microsoft career to date from this very office! It’s been quite interesting for me to be literally in the

middle of a global pandemic, joining a new company, but also seeing the inner workings of Microsoft.

Throughout everything going on, we had to keep Microsoft up as an entity – Microsoft has over 160,000 people worldwide. But they also had to make sure the current customers were supported, and that's all of the global Cloud and the data centres and all of those types of things. Because of the pandemic, we've seen a massive acceleration to the Cloud as well, particularly collaboration sites like Teams, and those types of things.

We almost got a triple whammy, if you like, of all of these things coming together; the capacity that was required, the help and support with all of these things that have been going on. To see that from the inside and sort of seeing how Microsoft rose to the occasion and how they help customers has been phenomenal.

For me, it doesn't really matter how bad things get. We've talked about some of these big, big crisis moments that we've had over the years – I always focus on the opportunities. So, 'what can we learn this?', 'what can we do better?' And that's where I get really excited. I'm really proud to be able to work for such an amazing company."

Having worked on the Millennium Bug, what did you learn from the potential threat?

I think having a background in business continuity has really enabled me to think about the big picture, those worst-case scenarios – 'what's the worst thing that could happen?'.

We need to think wider, we need to think about incidents that are not just relevant to our own company, but issues that go cross-sector and even across the world. That scope and scale are really important, and some of

these major events have also triggered global changes, as well.

So I think back, and I would say 9/11 was a really good example of a major incident, at massive scale, that we probably never seen before, how that was televised and the shock that came with it. It really brought home the impact of terrorism, and again, how important business continuity is at that scale.

> *I bring that forward to what's going on now, the global pandemic and this crisis, it's really brought home just how much we're all connected to each other and how dependent we are.*

That's from small businesses up to those large enterprises as well. So, ultimately, when we're thinking about these threats – it's not just about business continuity but cybersecurity attacks as well – it's really about thinking holistically, thinking much, much, much wider.

It's really about having resilience to all of these types of attacks and types of threats.

As a cybersecurity expert, what is the biggest threat businesses face and what advice do you have for them?

It's very interesting. We think about cybercriminals and the type of attackers, and they're inherently opportunistic – they absolutely love a crisis. And what a crisis we've seen over the last 12 to 18 months! So, they're really taking advantage of this.

We've seen a massive increase with regard to phishing attacks, or really preying on people's fears and emotions. So, they pretend to be your bank, they might pretend to be just offering support. They might pretend to be a charity and those types of things.

It's really trying to fool you into a false sense of security, to try to get you to give up credentials or click on links. We've also seen a massive increase with regards to ransomware, specifically targeting healthcare or other critical infrastructure. I think what's been interesting to us is there's almost no company is out of bounds – they're small, large enterprises, these frontline services.

And even to us, it was quite shocking. You'd think, 'surely in the middle of a pandemic, you wouldn't attack a hospital, you wouldn't attack the emergency services. But they did, particularly when we're talking about ransomware because they feel that they're more likely to pay if they're being backed into a corner.

I think there's a real psychology behind the way that cybercriminals act and the way that they take advantage of the situation. It's important that we're mindful with regards to what's going on and how these changing tactics and techniques are going to continue to evolve.

It really comes back to that kind of business continuity, which means constantly asking questions: 'what if somebody could get access to our systems? What if somebody could disrupt our services? What if someone could get access to our data? If that data is leaked, what's the impact of that? And therefore, where do I put my priorities?'

So, we're no longer just talking about *cybersecurity*. We have to think again and have more of a holistic response, where we're thinking about 'if we have these types of incidents, what's the business doing?' It's very much about thinking much wider."

Considering the pace of digital transformation, how can businesses keep up with such rapid transformation?

I think it’s important to reflect on the fact that security is intrinsic to almost every business, particularly when we’re talking about digital. So, we really need to think much wider, much broader.

As we’ve talked about, really with a global pandemic, many companies are really evaluating their business models, their working practices. They’re asking, ‘what happens next?’ Do we all go back to the office? Do we continue to work remotely? The reality is we’re going to work in this hybrid environment, where people have more choices about where they work from, what type of devices they use.

And that ability to embrace the Cloud is really important because it enables them to try a proof of concepts, new designs, spin up projects very, very quickly, which they might not have been able to do previously because of the time it takes to procure servers and storage and spin up projects and all of these types of things.

So it really comes down to speed and scale, and that’s really one of the benefits of the Cloud. It’s really about taking advantage of all of these different things that are available and just really explore.

I think that’s the bit I love, really. We’re talking a lot about being agile, which is the ‘fail fast, fail often’ philosophy, which is if you want to try something new, if you want to have these innovative projects, try it out, get some insight, run some analytics, and it doesn’t work? Close it down.

I think that’s where the agility and the flexibility of this kind of digital transformation is, it enables companies and even individuals to experiment a lot more.”

With a passion for women in business, what more needs to be done to improve gender inclusion in the workplace?

I think it sometimes sounds like a bit of a cliche, but we really need people who can think outside of the box, who can think and act differently. And that is why diversity is so important, but it's about the diversity of backgrounds and experiences and culture.

It's not about being a woman, per se, it's about being able to celebrate all of our differences and how we can utilise all of those differences to be our best advantage. I think one of the things that we've been reflecting on is the need to have different perspectives and viewpoints, because if we all have thought the same thing we would come out with the same answer, in essence, and that is not what's going to help us to innovate.

> *I also think it's important that we remove this kind of false barriers and misconception that [technology] is principally a career for men, or that you have to be deeply technical to work in cybersecurity because that's not the case at all.*

It's about encouraging people to remove these false barriers – 'this is a career for men, this is a career for women' – I think that's really key when we're talking about inclusion."

This article was previously published on ParlayMe

Article by Sarah Armstrong-Smith