accenture

TOMORROW, TODAY 4: ON HIGH ALERT: GETTING SECURITY RIGHT

VIDEO TRANSCRIPT

Oli Barrett
Cybersecurity is a constant threat, but not always a boardroom issue. Now, world events have set us all on high alert. So, what should boards and senior management be considering to protect themselves? I'm here with Accenture's Giovanni Cozzolino and Saba Ahmed to find out. Welcome back to Tomorrow, Today.
Gio, Saba, thank you for joining us.

Giovanni Cozzolino
Thanks for having us Oli.

Saba Ahmed
Thank you.

Oli Barrett
Gio, let's start with you. Cybersecurity here in the UK, any sense as to whether we're more vulnerable, more prone to being attacked than other countries? But also give us a flavour of how seriously we take this as a nation.

Giovanni Cozzolino
As a country, I think we are as susceptible as any other country out there. And probably looking at some of the geopolitical events that we see in the world at the moment, you would probably argue that the UK is maybe even just a little bit more of a target out there. The UK has been relatively on the forefront of bringing in regulation about guiding businesses, and we're only going to see further regulation in the UK to actually guide those businesses in a little bit more in preparation for cybersecurity.

Oli Barrett
So I get that sense Saba of a rising threat, any extent to which an organisation can dial up and down their security?

Saba Ahmed
Absolutely. For organisations, they always need to stay a step ahead of attackers and that itself is a constant challenge. For them, it is about dialling up security and to do that they need to combine two factors, one is to understand the threat landscape.

Oli Barrett
Yeah.

Saba Ahmed
The second part to it is to understand your assets and their value.

Oli Barrett
What about the human element? How do we all play a role in this? How do you see it playing out?

Saba Ahmed
So, humans are the weakest link in any organisation. Your staff, your employees potentially could be the weakest link if they don't have the right training in terms of security. But there's another aspect as well, in terms of cybersecurity skills, which is a shortage. It is high in demand and short in supply. So, for organisations to bring in innovative ways to retain talent and to upskill talent is a critical one.

Oli Barrett
So Gio, that reminds me of the sort of conversations that an organisation might have around health and safety. I mean, is that pushing it too far?

Giovanni Cozzolino
No, I think the organisations that we see leading the pack are actually moving away from just the standard education that they would do once or twice a year, or the passive education, to those organisations that are really pushing cybersecurity to be part of their culture. So as you pointed out, health and safety, why not include security as part of that?

Oli Barrett
That's a fascinating shift, Saba this is such a huge topic. But I do want to get a glimpse of the types of attack that you've seen on the rise, anything that's more prevalent today than it would have been a few years ago. Just give us a quick snapshot.

Saba Ahmed
The trends that we are seeing in terms of attacks are the top three I would say are, cloud attacks, cloud infrastructure attacks, ransomware attacks and supply chain attacks. Oli Barrett Gio, on supply chain, this goes back to the threat analysis, because it's not just your own organisation that you need to be thinking about. Tell us more.

Giovanni Cozzolino
Yeah I mean, supply chain attacks are extremely complex because even when an organisation has full trust in their supplier, in the way that they operate, in their own sort of security controls, what's not to say that that supplier's suppliers, doesn't have the same kind of standards? As Saba said, we've seen a massive increase in supply chain attacks. We saw the colonial pipeline last year, which was a major attack. We've also seen quite an increase in vulnerabilities that have been notified.

For example, Log4j and SolarWinds, where organisations are just scrambling to understand where these sources of codes are so they can actually remediate those vulnerabilities.

Oli Barrett
Log4j, this is a particular piece of code which became very vulnerable, caused a huge outbreak of attacks.

Giovanni Cozzolino
Yeah, that's exactly right.

Oli Barrett
So, Saba, give us a practical tip on this supply chain point. How do we shore those up? Because as Gio is telling us, the network effects mean that this is incredibly complex.

Saba Ahmed
There are a couple of things that organisations can do. One is audit. So, integrate audit into your DevOps. Ensure that security is embedded not just into DevOps, but also into your application onboarding with things like automated code scanning.

Oli Barrett
And what's another way of saying DevOps in that context?

Saba Ahmed
Your operations team that develops applications. The other thing that organisations can do is to threat model, threat model suppliers, threat model third party organisations that they work with, threat model value chains and supply chains, which means that understand who has access to what, at what level they have that access. Understand the security practises of the organisations that you're working with.

These things together, as well as being prepared in case a cyber attack or a supply chain attack does impact you, then how are you going to deal with it? How well prepared are you?

Oli Barrett
And on threat modelling, presumably Gio, not all suppliers are equal. I mean, otherwise this

whole process could be completely time constricting for the organisation.

Giovanni Cozzolino
No I mean, I think there's a big difference between a bank and what they need to protect, say for example, to a small manufacturing. But the risks, although, are very relevant for both organisations in the sense that a very small organisation that does manufacturing of a product, they can be attacked and that organisation could cease to exist.

Oli Barrett
Right. Saba, let me put to you another challenge which I know plays on the mind of many viewers. Cloud transformation and cyber threats associated. Where do we start?

Saba Ahmed
We know that most of organisations started their cloud migration journeys very early on, but with the pandemic, they accelerated cloud adoption. With that acceleration came the challenges around security and compliance requirements and meeting those at a faster pace.

There are two parts to this again with cloud transformation and the cloud journeys. Security not always has been at the onset of that transformation; it's always been an afterthought. The other thing is that, for organisations cloud skill set and cloud security skill set is gold dust. Finding and retaining that talent is a challenge. The other side to this is that for the same reasons why organisations are adopting cloud, attackers are also leveraging cloud to scale and make their command-and-control infrastructure more reliable.

Oli Barrett
Which means the impact of their attack is all the greater.

Saba Ahmed
Exactly, it’s much stronger and faster and quicker as well.

Oli Barrett
So why don't we finish, Gio, with some practical thoughts for someone watching today that is conscious not only of protection but also responding in the wake of an attack.

Giovanni Cozzolino
Yeah, I mean, I think I would advise any client to first of all, get their cybersecurity basics in place. And then there's the other area which is around having that level of preparation and so that's all about getting their resiliency plans in place, their incident response plans in place.

Oli Barrett
And mapping out Saba, how that could look in the eventuality that it did actually get triggered. What about a final practical thought?

Saba Ahmed
This is more like a recommendation for CISO’s to engage and collaborate with the wider executives within the firm, rather than working in the traditional very security focused siloed way of working. For them to collaborate with the wider leadership, would help define that security strategy which is much more aligned with business priorities and risks which benefits the organisation overall.

Oli Barrett
And involves demystification.

Saba Ahmed
Absolutely.

Oli Barrett
And back to the communication point. Thank you for doing just that today Saba, Gio. Great to see you.

Giovanni Cozzolino
Thank you very much.
Thanks a lot, thank you.