# TECHNOLOGY: SECURE FROM THE START

## AUDIO TRANSCRIPT

**Simon Gooch, Identity & Access Management Lead - Accenture** [00:00:00] Always continue to evolve your strategy. You need to be able to think long and short term and then work out how you would adapt that thinking to the rapidly changing threat landscape.

**Penelope Prett, Chief Information Officer - Accenture** [00:00:16] Hi, I'm Penelope Prett, Accenture's Chief Information Officer, and I'm really glad to be here today with Simon Gooch and Kris Burkhardt, two extraordinary leaders who are helping to protect Accenture's security posture. Our global I.T. team is driving technology and empower, business transformation to support Accenture's businesses. And today with Simon and Kris, we're going to take a closer look on how we approach security at Accenture and share some insights on what we need to be watching for in today's world. Kris, let's start with you. Can you talk just a minute about how you're able to keep such a large global organization as Accenture safe in today's world which is just filled with cyber threats. How are we keeping the technology landscape secure and protected?

**Kris Burkhardt, Executive Director IS Tech & Ops - Accenture** [00:00:59] Hi Penelope. I'm very pleased to be here and I look forward to sharing a few insights. So really, for us, technical hygiene plays a key role. First and foremost, we know and measure our assets. We have a very large footprint, more than five hundred thousand endpoints, sixty thousand infrastructure devices and a couple of million cloud objects. So understanding and tracking where those are and who owns them and what current state of posture they're in is critical for security at Accenture. We do that. We have multiple programs to manage those three areas I just spoke about. Our workstation patching,

for example. We approach ninety nine percent Windows compliance on patching within days of new Microsoft releases. We have automated workstation remediation tooling and we average just a few infected workstations every month, which would clean up quite quickly again through an automated process. On the infrastructure side, we do a significant amount of vulnerability management. Of course, we have advanced endpoint protection and monitoring in place for our infrastructure using modern tooling. And then finally, in the cloud, we have more than 300 controls that we measure - different controls for different types of cloud objects - but those address access, encryption and network posture to keep all of our cloud safe. So, Penelope, it is a full time job for many people to do this. But if you keep good hygiene, you have a lot less problems to chase.

**Penelope Prett, Chief Information Officer - Accenture** [00:02:45] Thanks, Kris. When you and I have talked about all the activity going on, the logistics of what it takes to manage our environment are just staggering. And at the heart of that, there are some capabilities around identity and access management. And Simon, perhaps you can talk a bit about some of those.

**Simon Gooch, Identity & Access Management Lead - Accenture** [00:03:02] Yeah, there are three things, Penelope, I'd like to call out. First of all, we're applying multifactor authentication to all points of access: to our network, our systems and our applications. Then Privileged Access Management Strategy is looking to reduce the risk of compromise to the key or privileged accounts that are used to run our systems and our applications. We have moved to using admin use only accounts, securing application accounts in a secure application vault, and isolating the highest privilege accounts used to run our most critical systems into their own dedicated environment. And then thirdly, we are moving to a role based access model where only those in approved role-specific positions can get access to certain types of data environments, infrastructure and platforms. So hopefully that gives you a sense, Penelope, of what we're looking to do in the access management space.

**Penelope Prett, Chief Information Officer - Accenture** [00:04:05] It does and thanks Simon. Kris, as you turn your eyes to the future, what do you think we at Accenture and everyone in the market needs to be looking at for the next one to two years? What are the biggest risks ahead of us?

**Kris Burkhardt, Executive Director IS Tech & Ops - Accenture** [00:04:19] Well, that's a difficult question. It's a little bit hard to see too far in the future, but I think there are a couple of obvious things that we should be thinking about. Ransomware and remote access should be on everyone's list of concerns. With all of us working from home, really ensuring that your remote access is as secure as possible with Two-Factor Auth and constant monitoring I think is critical. We spend time on that and we're very concerned about potential attacks in that space because that is where hackers are focusing right now. And ransomware, of course, will continue to be a concern. I think it pays well. We read about it all the time. People do, in fact, pay ransoms. And as long as it continues to pay well that's not going to go away. I think a third thing to keep in mind, as long as we're dealing with the pandemic, is we're gonna continue to see, Penelope, social engineering related to work from home and pandemic themes. So I would encourage firms to be on the lookout for those types of schemes.

**Penelope Prett, Chief Information Officer - Accenture** [00:05:30] Yeah Kris, the pandemic and the move of most employees to a remote landscape has definitely broadened the attack surface that most companies have to protect at this point. So, Simon, maybe I can ask you, when you think about that and you think about the time we're in right now, what would you advise companies to look at? What are the two or three key elements they need to be paying careful attention to right now?

**Simon Gooch, Identity & Access Management Lead - Accenture** [00:05:55] Yeah, in answer to your question, Penelope, I'd recommend the following foundational items to focus on. I mean, start with 'stay current' and that means always be on the most up to date versions of your software, your code, etc., and patch everything. And then I've mentioned it earlier on but apply multifactor authentication to everything. Simple. And lastly, always continue to evolve - and Kris talked about security strategy - but always continue to evolve your strategy. You need to be able to think long and short term and then work out how you adapt that thinking to the rapidly changing threat landscape as those threats evolve. And I think if you do those simple things, then you're in a good position to focus on what you need to do for your company.

**Penelope Prett, Chief Information Officer - Accenture** [00:06:45] Well Kris and Simon, thank you so much for the discussion. And, as things are constantly evolving and changing in the space, I look forward to getting together with the two of you for an additional discussion in the not too distant future.

**Kris Burkhardt, Executive Director IS Tech & Ops - Accenture** [00:06:58] Thank you, Penelope.
**Simon Gooch, Identity & Access Management Lead - Accenture** [00:07:00] Thanks, Penelope. Always glad to be part of this great discussion.
**Narrator** [00:07:06] Thank you for joining today's podcast. Be sure to subscribe to the Accenture CIO podcast series on Apple podcasts or Spotify. Find the full CIO 24/7 podcast series and additional ways to subscribe at Accenture dot com slash CIO podcast.