Podcast Episode 2:

Nick 0:07
Hello, everyone, and thank you for tuning in to the HCLTech Trends and Insights weekly podcast, where we'll be discussing the latest key technology stories that are impacting and disrupting business and society. I'm Nick Ismail, the Head of Brand journalism, HCLTech. And today I'm joined by our US reporter, Jordan Smith. Hi, Jordan. How are you?

Jordan 0:31
Hi, Nick. I'm good. How are you?

Nick
Excellent. Thank you. And thank you so much for joining us today for what I'm sure is going to be a really interesting discussion. So today we're going to be covering a significant global topic, cybersecurity, and in particular, how the U.S. is approaching this. And just before we start, I'd like to paint a little bit of a picture of the current cybersecurity landscape. In 2022, the average cost of a ransomware attack was more than $4.5 million globally, and $9.4 million in the US, according to a report from IBM. In addition, the current and numerous geopolitical crises around the world have also impacted the situation. In 2022, state sponsored cyber-attacks targeting users in NATO countries increased by a massive 300% compared to 2020, according to data from Google. This is a global threat. And it calls for a global response and an enhanced and coordinated action. So, Jordan, you've covered this subject in the us quite a bit. Can you please explain in more detail about this new cybersecurity strategy being rolled out by the White House?

Jordan 2:40
Yeah, so first, I do want to emphasize the need for a National Cybersecurity strategy, not just based on the information you laid out here today, but in addition to that, in 2022, according to Mandiant, a leading cybersecurity firm, claims spy agencies working on behalf of the Chinese government have launched an attack on the networks of six different U.S. state government systems. During the Russia Ukraine War, Russia has also targeted Ukrainian infrastructure, including banking, power grids, and internet facilities, while Ukraine set up its own IP army to attack crucial Russian websites, through DDoS attacks, distributed denial of service. There have been numerous reports of significant cyber-attacks in the private sector, as well. And in a nutshell, what the National Cybersecurity strategy here in the U.S. wants to do is provide a guide, it's not going to be enacted law, it's more of if your boss is telling you that you should follow these steps, then you are going to follow these steps. And the administration is most concerned about who is major adversaries are and how it might achieve its goals through legislation or executive action. The framework is an initiative that's focused on protecting critical infrastructure that including hospitals, and clean energy facilities from cyber threats. It also aims to increase collaboration with international coalitions and partnerships to counter threats to the digital ecosystem. This latest 2023 version calls for improved sharing of information between the government and private sector about cyber threats, vulnerabilities

and risks. It also recommends coordinating cyber incident response across the federal government and enhancing regulation.

Nick 6:37
Okay, Jordan, thank you so much for giving that overview of the cybersecurity strategy. It seems that collaboration between private sector and public sector, international coalition's is an important aspect of it. And it's something that we're seeing in every aspect of technology, collaboration is super important for transformation, for improving one's cybersecurity posture for all manner of things. And just in terms of looking at the business impact of this new cybersecurity strategy launched by the U.S., how do you think it's going to impact organizations?

Jordan 7:22
So, the key point I would target here in the national cyber strategy when looking at how it impacts organizations is that it really does aim to reduce the cyber burden on individuals, the customers, and smaller organizations. So, if your company introduces systemic cyber risks to others, the administration now wants companies to be more liable for those risks. Companies that provide IT services to customers, suppliers, employees, or any other stakeholders now have cyber risk as a boardroom concern. Even if they aren't necessarily an IT company, per se, this kind of falls into the line of thinking that all companies are going to start being technology companies. Security is what matters and having encouraged them to share insights with each other. Another key strategic objective is to streamline the notification and escalation process to ensure information sharing and ownership of response actions for those incidents that require federal response. So, making sure that goes much more quicker. The strategy combined with also the upcoming SEC cyber rules, which are supposed to be released this month have far reaching implications for companies in the U.S.

I'm interested to find out your opinion on how organizations themselves can protect their own organizations, their own employees, their own customers, and there's no doubt that cybersecurity has shot up as a boardroom priority. But, you know, we've heard the old adage shot, there is no silver bullet. So my question is, what are the best practices that organizations can put in place to protect themselves from the threats without hampering their growth or innovation ambitions?

Yeah, so a lot of the cybersecurity experts that I've heard, have conversations with or who I've spoken to and interviewed directly. They're really emphasizing taking a holistic approach to cybersecurity. That's having buy in enterprise wide, whether that's from the entry level positions to the boardroom, it's an important element to reducing security risks. The taking a holistic approach also extends to product life cycles and ensuring security is built in from when the security journey is first started. More recently to I would say there's been an incentive for organizations to rescale employees to remediate security risk and provide programs to really shrink the disparity between the number of developers and cybersecurity experts. Right now, there are just way more developers than there are cyber experts, at least in the United States. What this means for the C-Suite is that data is saved, or dollars saved when it comes to a data

breach. So, in 2022, it took an average of 277 days or nine months to identify and contain a breach, which is such a long time when we're talking about security. shortening the time, it takes to identify and contain a data breach to 200 days or less can save so much more money. Another thing that experts emphasize is to not just make an incident response plan, but to test it. Having an incident response plan is really only the first step. But testing that plan regularly can help you proactively identify weaknesses and your cybersecurity and shore up your defenses. Not to mention you can save millions in data breach costs. AI and automation also offer really big savings organizations that fully deployed AI and automation programs, they have been able to identify and contain a breach 20 days faster, faster than those who didn't. Saving about $3 million U.S. dollars, however, is not all or nothing. organizations with partially deployed AI and automation program fared significantly better than those without.

Nick 9:09

Yeah, thank you so much, Jordan. And thanks for providing all these really useful tips. It's certainly something that organizations are considering they must consider it take a holistic approach to cybersecurity, embed AI and automation, test your incident response plan. And, you know, be proactive, aiming to identify breach as soon as possible in order to save costs, save reputational damage, and save potential fines from regulators. So, thank you for all those insights. And just now on to the event round up portion of the podcast. I'd like to highlight that HCLTech has just attended RSA Conference in San Francisco. At this conference, which is touted as the biggest cybersecurity conference in the world, we discussed how enterprises can achieve a future ready security posture by proactively addressing the emerging digital threats, which is a lot of what we've covered in today's conversation. And all the content from this event, including interviews with some leading HCLTech executives that focused on the main trends with identity access management, security vendor consolidation and zero trust will be available on our HCLTech Trends and Insights page, and you can find a link to this in the description below. So Jordan, thank you once again, and hopefully we'll have you on the podcast soon. Thank you for your insights and thank you to the audience for tuning in. Goodbye.