Grant Thornton

Internal Audit & Quantum Computing Risks: Preparing for the Future

Teaser Video Transcript

Cybersecurity Risks

Cybersecurity risks are going to stay and they're probably going to increase in terms of scope and risks. So as we pair innovation with AI models, more data is developed and stored in our environment. So if we do have the risk of quantum computers being able to make current cryptography unsafe, we really need to understand what that means for our current asset inventory, our data inventory and making sure that we are resilient in terms of cyber practices. Also in terms of Business Innovation. access to quantum computing is going to really shorten the time to resolutions and innovations, scientific discoveries, medical breakthroughs.

There was a plan with the Cleveland Clinic to be able to use quantum computers for biomedical research, to be able to drive performance of computing and models to get to discoveries quicker. And then also as all landscapes change, the regulations will change. So looking to governments, regulatory bodies, really understanding how laws will change or they will be upgraded or updated to understand the impact on data and data protection. So with that, we're going to understand some of the impacts. So as we talked through the trends, what does it really mean for organizations for you all?

So as we talked about cryptography vulnerabilities is really going to be center stage as we talk more about quantum computing over the next three to five years. So traditional encryption methods will be vulnerable. We'll talk through Q Day and when that is in a couple of slides, but it is going to render this type of encryption vulnerable and really we have to understand how to protect our sensitive data and also online communications. This is traditional encryption is how the majority of software and communication channels are protected today. So we need to understand what that impact looks like at our organizations.

Like I mentioned earlier, cyber security threats, it's just going to increase. The threats and the pervasiveness of the threats of managing that risk and understanding what this could mean for our industries and our organizations. As you noticed on the side, the average cost of a breach in 24 was just under 5 million. So this will only increase as we go into the realm of more advanced computers and powerful computers, and especially as we are being made a bit more vulnerable in terms of cryptography. As with all new innovations in terms of tech, there is ethical concerns that we do need to make sure we understand.

So as we're creating more data with AI, what's the ethical dilemma behind that? If we are storing more data, having more models, more information in our environment, how do we make sure that we protect it and that we understand the data privacy implementations around it and make sure that we develop a strategy for that? And then economic disruption and geopolitical risks. So as organizations need to develop and enhance their security tools, they may face challenges in order to do that, especially adapting to the quickly changing quantum advancements. So, you know, disruptions in the economy, understanding of geopolitical risks, they're all something that is in the near future that that might impact our organizations.