SECURE YOUR BUSINESS FOR THE FUTURE OF REMOTE WORKING

WITH STACEY ROBINSON

Why is it important to partner with a firm with strong data security programs?

Every day you see in the headlines another firm has been hacked and breached and your data is out there. And once your data is out in the wild, it could lead to identity theft and lots of other issues. So, of course, we take the protection of our client data, which is really shareholder data, very seriously. And I think everybody would want to know if they're going to partner with somebody that that data is truly protected, and they do not have to risk an exposure. And, of course, it's not just the damage that's done to the shareholders, but the damage to the company's reputation, the costs associated with a breach. There are so many challenges that come with having a breach. So, I believe everybody in the industry wants to make sure that whoever they partner with has robust cybersecurity in place and is doing everything they possibly can to protect the data.

How has the pandemic affected data security? Are there now greater risks associated with the increase in remote access and what can issuers do to mitigate this?

Certainly, the pandemic has had an impact on cybersecurity and data security. We have more employees working from home than ever before. Remote access was always possible and done, but at this stage now in the pandemic, it has increased exponentially how many employees are working from home. Home environments, they're not protected or known environments. Oftentimes home environments don't have the latest networking or patches or security. They also have non-employees, other family members, that work from home that aren't employees of the company. And so clearly there is increased risk.

Most public companies should approach this from a zero-trust perspective, similar to salespeople that travel with a laptop and might have to work out of a hotel, where they don't know the network and they don't know the security. So, putting increased controls on remote access, making sure there's robust multifactor and identity controls in place, ensuring that the mobile devices that people travel with are secured appropriately and have the correct controls. Encryption is obviously a key thing in case these mobile devices are lost. So, these are practices that have always been around, but they become increasingly important as the workforce becomes more and more remote and working out of untrusted environments.