Technology and the New Normal

Important questions when the new normal is working from anywhere

Question 1: How can you maintain control of everything if the PC's and laptops are not all in one building anymore?

If people are going to continue to have the ability to work remotely there should be some central control because your PC's and laptops could be anywhere and this is critical to maintaining management and security on them.

Question 2: Is everything secure with patches & updates on computers that may not be connected to the main network anymore?

Good cyber security is all about layers and how we protect against the bad guys has changed over the last year. Security solutions now need to be focused on the computer/endpoint itself and not just the corporate network. You can't just protect the network with a firewall and put basic anti-virus software on each PC anymore. The networks that people are connecting to are potentially dangerous now so most of the security solutions need to be on the PC itself. Even a home network can be dangerous because they don't typically use a business grade firewall.

Question 3: What happens if someone tricks you into giving up your password?

The most common way someone gets compromised is because someone obtains their password. It can be stolen and found on the Darkweb or you can be tricked into entering it through a link you clicked. Having multi factor authentication turned on will keep you safe because a hacker will still be blocked even if they get your password. With multi factor authentication you are sent a code or need to do something on your phone in addition to entering the password. Unless a hacker has your phone he still can't get in.

Question 4: Should you put everything in the cloud and get rid of your local servers?

Many companies are already operating in a hybrid mode where some people are in the office and some are remote. Most companies are not ready to just put everything in the cloud. The technology to do it is available, but there is a learning curve depending on the software your company uses. When we have a client that wants everything moved to the cloud, we work with them to come up with a plan over 6 months to a year and make it a slower transition. This way users don't have a massive change all at one time. If the move to the cloud doesn't have users doing things differently, then it may not be the best long term solution. This is a much larger discussion though. For some companies moving everything to cloud many not even be an option. This requires an IT professional that is familiar with your software and the cloud to guide you.

Question 5: Do you know if the password you are using is available on the Darkweb for anyone to see?

So many people never change their password, it gets published on the Darkweb through one of the many large companies that have been hacked. This makes it very easy for a hacker to get into your accounts. Best practice is to never use the same password anywhere twice and to change it at least a few times a year. Many people never do that, so having a Darkweb password monitoring service is a good thing to have. At least you know the passwords that should never be used.

Question 6: Do you know how to protect yourself from the most common forms of cyber attacks?

Do your users have basic training on cyber security awareness. Knowing just a little bit can keep people from clicking on that dangerous link in the first place. Many scams could be more obvious with a little training. A good awareness plan should have training and testing. Training is how you learn what to look for and simulated phishing testing checks to see if you learned anything.

Question 7: Is cyber security something that everyone takes seriously, or do they think it won't happen to them?

Many times the company culture is what can make all the difference. Just like physical safety in many industries has worked its way into the company culture, cyber safety culture needs to do the same. Everyone needs to have a heightened sense security awareness. If people think it won't happen to them, they are wrong. There are lots of things out there to protect yourself, but people need to care and want to protect themselves and the company first.