Remote Working Security Lessons to Take into 2021

As 2020 draws to a close, we're probably not the only ones looking forward to kissing this year goodbye. As your organisation looks to the future, make sure you factor security into your plans for 2021.

Although lockdown began 10 months ago, sometimes it feels as though it's been 10 years. We began our lockdown podcast series imagining it would only last a month – how wrong were we? Despite vaccine rollouts now appearing on the horizon, we're not out of the woods yet.

Chances are that lockdown could continue well into Spring, so it's important to prepare your business for that possibility. That, of course, means an ongoing period of remote working, at least for the next few months, but let's take advantage of the lessons that 2020 taught us, and step into 2021 with security in mind.

Rein in Your Risk Appetite

When the pandemic first hit, organisations had no choice but to adapt to lockdown restrictions as quickly as possible. As a cybersecurity company, we always preach a security-first approach, but it's understandable that in times of duress, a business's first priority is business continuity.

In order to sustain the business, organisations had to accept some risks in order to allow their office-based teams to work from home. This led to major changes, like issuing laptops at speed without proper protections or precautions, building devices ad hoc without using golden images, changes to your VPN, moving services to the cloud, etc. These sacrifices made sense in March, but now we're in December, so it's worth revisiting them to ensure your systems are secure.

In risk management, it's common to see issues added to the risk register and then never taken off again, but now's the perfect time to go through that list, revisit things now if you can, or set a deadline for when the risk will be re-addressed. Lots of decisions were made in less than ideal circumstances this year, but don't accept those risks going into 2021. Ask yourself: if not now, then when?

Re-think Your Remote Working

You may have had robust security for your corporate perimeter when it was office-based, but with the majority of your employees now working from home, do you even have a perimeter anymore? Remote working has obvious benefits, but it also expands your threat landscape and gives malicious actors more opportunity to attack your business from many different angles.

Maybe your organisation didn’t have the resources to send every employee a company laptop and phone, so you’ve had to embrace BYOD – but that presents a major risk if there’s no device security policy in place. How can you protect corporate data on your employees’ personal devices? What networks are they using and how are they connecting to them? When everyone works from home, there’s no one size fits all.

Have you considered the physical access risks that come with working from home as much as the technical ones? After all, not everyone’s remote working environment is the same; some employees don’t have a dedicated private workspace, so how can they take confidential calls if in that situation?

Staff will be working remotely for a little while longer at least, so looking at how secure your employees’ new work environments are, updating documentation, and revisiting decisions will prepare you for the next couple of quarters.

Stay Vigilant Against Cyberthreats

Your staff members may have settled into working from home, but now’s not the time to get complacent. Cybercriminals still pose a huge threat to your organisation, and they’re taking advantage of lockdown confusion in order to do it.

Phishing hasn’t gone away, it’s developing. If all your staff know about phishing emails is to “not click on any links in a suspicious email,” you might need to update your security awareness training. Scammers aren’t just targeting your staff via emails, they’re also targeting mobile devices in order to crack your 2FA. Phishing is now more sophisticated, with bad actors creating Deepfakes (AI generated fake audio or video content) to trick targets into handing over data and funds. If you haven’t already, revising your security awareness training to include changes to the threat landscape should be high up on your 2021 to-do list.

Just because your staff are remote, that hasn’t made ransomware less of a risk, so don’t neglect your internal office architecture. Network security tests may have been moved to later in the year while the main focus was business continuity, but your network infrastructure still needs attention, so get it pentested. You may think this is a job for an on-site tester, but that’s not the case; penetration tests can be done remotely, thanks to VPNs.

The Future’s Bright

If you’re thinking about implementing remote working going forward, now’s a great time to plan how that architectural change will impact your business. Don’t catch your IT team off guard with a sudden office shut down, that’ll only lead to more emergency changes without planning in place. If flexible working is your future plan, think about turning off the WiFi while no-one's in the office, shutting some of your office infrastructure down, or looking at behaviour analysis, etc.

If you're going to build a new way of working, make sure you do it right. Build security into your new working culture from the ground up. Consider how this year's changes have impacted your company's culture; for example, if you've furloughed staff, those employees' responsibilities haven't disappeared. It's likely that other members of your team are taking on that responsibility, but do they understand the security implications of that role? Without the proper security awareness training, these employees could be an inadvertent risk to your business.

It's safe to say it's been a hell of a year for businesses, employees, and security experts this year. Lockdowns, changing government restrictions, public safety concerns, demand fluctuations, and business uncertainty have certainly created a wild ride for decision makers in business. The dust is finally starting to settle and we have a clear view of what the next six months is going to look like, so now is the time to plan ahead. By moving cybersecurity up the list of your organisation's priorities, you can ensure a secure and successful 2021.

If you'd like to know more about how we work with organisations to protect them against real world cybersecurity threats, get in touch with one of our experts.