Telecommuting and Cyber Risk (webcast script)

Speaker 1 (Scott Naugle)	Hello and welcome to the BXS Insurance webcast this May 22, 2020. I'm Aimee Kilpatrick, SVP and Director of Sales Development & Operations, BXS Insurance, and I'm joined today by Louis Fey, Vice President of Risk Management, BXS Insurance. BXS Insurance is Right Where You Are during these challenging times. We're here with you, helping to advocate and provide guidance, so you can be there for what matters most. Remember, our world changes fast so things might have changed by the time you hear this. The rise of telecommuting is leading to new cyber risks. Today, we're talking about how businesses can shield themselves from cyberattacks and what insurance coverage gaps they should watch out for. Lou, businesses have a lot to think about right now. Why should cyber risks be a priority?
Speaker 2 (Lou Fey)	Hello, Aimee. Yes, you're right—businesses are dealing with a lot right now. But cyber risks cannot be ignored. Cyberattacks have been on the rise, and a single incident can lead to millions of dollars in losses, lawsuits, and fines, as well as reputational damage. Now that COVID-19 has forced many businesses to switch to remote work arrangements, there are new risks, and some of them might not be covered under many cyber insurance policies.
Speaker 1	How does remote work lead to new cyber risks?
Speaker 2	There are a few different ways. One of the most obvious is the potential decline in security standards. We normally expect a company to maintain a high level of security standards, and the same standards might not exist in a person's private home.
Speaker 1	What kind of security issues are likely?

Speaker 2	The Wi-Fi network might not be secure. In an extreme scenario, a worker might be using their neighbor's Wi-Fi, maybe without permission. Or they might have their own network, but they don't have a password, or it's one that's easy to guess. Cybercriminals could exploit these weaknesses.
Speaker 1	What about the devices used?
Speaker 2	That's a risk, too. The devices might be using old software that's not supported anymore, or the workers might not have installed the latest updates. This means they may be working without important security patches. They might not have any anti-virus software, either.
Speaker 1	So how can businesses stay safe?
Speaker 2	Managers should work with employees to make sure their systems are secure. This includes using encryption, strong passwords, two-factor authentication, updated software, reliable antivirus software and firewalls. It's also important to keep secure backups in case data is lost to ransomware or other malware.
Speaker 1	That makes sense. What about the various programs businesses are using to manage remote work? The video conferencing apps and so on. Are these applications secure?
Speaker 2	Unfortunately, no, they're not always secure. The FBI has warned that malicious cyber actors may exploit the increased use of virtual environments. For example, someone could hijack a video teleconference meeting and interrupt it with really hateful or lewd images or messages. And that's not just hypothetical—there have been widespread reports of that sort of thing happening.
Speaker 1	Yes, I think I've heard about that.
Speaker 2	It's been in the news a lot. But there may be some cases we don't know about, too, where the hijackers have eavesdropped on the meetings without making their presence obvious. Hackers could also exploit remote desktop sharing to gain access to sensitive information.

Speaker 1	How can companies protect their information?
Speaker 2	They need to pick their technology and software carefully. Don't just go with the cheapest option. In fact, the FBI has warned that cybercriminals may offer free or cheap remote work software as a way to gain access to sensitive files. So, don't just accept the offers emailed to you, even if they look good.
Speaker 1	Maybe especially if they look really good. If it seems too good to be true, it probably is, right?
Speaker 2	Right. Vet your program options. And when you pick a software program, understand its vulnerabilities and what security steps need to be taken to make it as safe as possible.
Speaker 1	What kind of steps might need to be taken?
Speaker 2	It will depend on the software, but you may need to adjust the settings and options with an emphasis on security. For example, you might have an option of making a meeting public or private. To make it secure, you'll want to make sure it's private. And if you have a link or password that team members need to access video conference meetings or remote desktop sharing, you want to make sure that information doesn't get into the wrong hands. You can't just post it on social media and assume that no one else will notice.
Speaker 1	So, it's not just about the tech. It's about the people, too.
Speaker 2	Oh, absolutely. In fact, your own people are probably the biggest cyber security risk you face. Inadvertent actions have large consequences. People can be manipulated by social engineering, which is tricking people into transfering funds or data, or allowing criminals to access the system.
Speaker 1	Can you give me an example?

Speaker 2	Business email compromise. In this scheme, the scammer will contact someone, usually a specific employee at a company, and pose as a legitimate client, vendor, senior officer of the company, or other party. The goal is to trick the employee into making a wire transfer. Or sometimes they'll try to get information, not money.
Speaker 1	How is this related to COVID-19 or remote work?
Speaker 2	It's not necessarily, but scammers are taking advantage of the confusion right now. The FBI has identified a rise in business email compromise schemes related to COVID-19.
Speaker 1	Oh, really? How did those work?
Speaker 2	In one, the scammer posed as a client in China and requested that invoice payments go to a new bank account due to "coronavirus audits." But that's just one example. Right now, there's a lot of upheaval. Processes are changing, so people might not think twice when they get a request to change account information or payment dates.
Speaker 1	But they should think twice.
Speaker 2	Yes. They should look out for warning signs, like urgent requests and last-minute changes. Never be pressured into making a change without having time to vet the request. Also put procedures in place to verify requests, like calling or video conferencing. If the requester is only willing to communicate via email, consider it a major red flag. Any communications or transactions involving the transfer of data or money must be verified.
Speaker 1	What other schemes are possible?
Speaker 2	Payroll fraud is a growing concern. The scammers pose as an employee and trick HR into changing the direct deposit information for payroll. It's easy to see how this could be easier when HR can't talk to employees face to face. Phishing and spear phishing attacks related to COVID-19 are

	possible, too, particularly messages from scammers posing as the CDC or WHO.
Speaker 1	OK, we've seen that a lot can go wrong, and companies need to be on guard against cyberattacks. But if something happens, what next? Can they file a claim with their insurer?
Speaker 2	If a cyberattack occurs, companies need to act fast to mitigate the damage. Depending on the type of attack, regulations must be followed regarding the notification of consumers who may have been impacted. Companies should immediately notify their insurance company, assuming they have Cyber Insurance protection.
Speaker 1	Not everyone has cyber insurance, right?
Speaker 2	Right. More and more companies are realizing they need cyber insurance, but there are still some companies without this vital insurance protection. Even then, some Cyber policies may not provide full coverage for all exposures, especially exposures unique to remote work environments.
Speaker 1	Is this because cyber insurance policies often contain exclusions?
Speaker 2	Exactly. And some of those exclusions can be directly relevant when remote work arrangements are in play.
Speaker 1	Can you give me an example?
Speaker 2	Sure. Some cyber policies only cover company devices. These exclusions may have been written with bring your own device, or BYOD, arrangements in mind, but they can apply to work-from-home situations, too. Other policies might require devices to meet certain security standards in order to be covered. For example, policies may exclude devices that aren't encrypted. If an employee's personal device doesn't meet the policy's requirements, it wouldn't be covered.
Speaker 1	So, what happens if there's a claim?

Speaker 2	That's a good question. The claim might not be covered. For example, if there's a data breach that's traced to an employee's personal device, and if personal devices are excluded from coverage, the insurance company could deny the claim. Then the business would be solely responsible for the entire cost of any breach response and any liabilities associated with the breach, which can be exorbitant.
Speaker 1	And what about the devices themselves?
Speaker 2	They might not be covered, either. If an employee's device is damaged, the insurer may not cover the repair or replacement cost. It depends on the policy. Most cyber policies do not cover damage to the physical hardware, or the computer itself.
Speaker 1	That could be really bad.
Speaker 2	It gets worse. An insurer could even argue that a policy should be cancelled on the grounds that a company isn't adhering to the security standards it described in its insurance application.
Speaker 1	But then what are companies supposed to do? In many states, we have executive orders that require workers to telecommute. It's not like companies have a choice in this.
Speaker 2	Right. When the cyber insurance policies were put in place, nobody could have known that so many people would be forced to work from home to stop the spread of a virus. That's the point – many of these policies weren't written with the current situation in mind.
Speaker 1	So, what should companies do?
Speaker 2	They should obviously talk to their insurance agent and secure the proper coverage,however it needs to be kept in mind that this world-wide Pandemic was completely unexpected and therefore, many businesses were unprepared and should seek the assistance of IT security professionals to evaluate system security for these remote work

	arrangements. The key is to discuss potential problems sooner rather than later – before a cyber incident occurs.
Speaker 1	*If* a cyber incident occurs.
Speaker 2	The question is not if a business will be attacked, but when. Purchasing Cyber insurance is just as vital to a business today as General Liability coverage, possibly even more so now because of expanded remote workforces. Just the cost to properly respond to a breach makes this relatively inexpensive coverage a no brainer. Just ask yourself; Is my business equipped to comply with up to 50 different Cyber security laws? If breached, how will I determine what data was compromised, what laws apply, who we are required to notify, and what is the required form and content of that notification? Just these issues alone make the coverage a must-have, and quite frankly, a bargain.
Speaker 1	And this may be going on for a long time.
Speaker 2	Yes. Some states are starting to reopen their economies, but that could change if infection rates increase. And businesses are still being encouraged to use telework options if they can. Some workers may prefer remote work, too. Now that they've proven that they can do their jobs from home, they might fight to make this a permanent option.
Speaker 1	That could be an extremely attractive benefit.
Speaker 2	Definitely. Employees want flexible work arrangements, and remote work can be a big part of that. Allowing remote work could help end the pandemic – that's the immediate goal – but it could also help companies attract and retain talent, and reduce expenses by way of downsizing office space. But the cyber security issues will obviously need to be addressed.
Speaker 1	We've covered a lot today. Would you give us a quick recap?

Speaker 2	Yes. Remote work is increasing cyber risks. Employers need to help their teams secure their networks and devices and seek IT security advice from qualified professionals if needed. Employers need to train all employees with regard to phishing, social engineering, and other cyber threats. They also need to pick secure telework software options. But even with all these measures in place, a cyberattack is likely to happen at some point in time.. It is therefore very important to have robust cyber insurance in place, to review your cyber policy for exclusions related to remote work, and to work with your insurance agent to make sure you're covered for these risks.
Speaker 1	That's great. Thank you for sharing your insight today. I'm sure this information can help a lot of companies.
Speaker 2	I hope so. And thank you.
Speaker 1	Remember, our world changes fast so things might have changed by the time you hear this. Thank you for listening to our webcast.