AXA XL Insurance

Cyber risk alert

Cyber security in the time of coronavirus

Changing working patterns

With the ongoing spread of coronavirus, government guidance is changing rapidly. In many countries, healthy individuals are being asked for the first time to avoid unnecessary public exposure, for example at large gatherings, on public transport … and in the workplace.

As a result, many businesses around the world are now either planning for or actively implementing a business model involving far more remote workers than they had ever anticipated. IT and management teams are hard at work on the infrastructure and organization to facilitate this. In the rush to keep businesses working, there is a significant risk that **security** will not be properly thought through.

Good business cyber security practices, under any circumstances, should consider the following:

- Is the **technology and infrastructure** deployed secured against malicious actors, outside and inside the organization?
- Do all company employees, subcontractors and relevant third parties have **clear instructions and guidance** on how to conduct their work in a secure manner?
- Do any of the security measures in place **block** employees from conducting their work efficiently?

If the right level of security is in place, your business will be well-placed to fend off cyber security threats. Too little, and you are vulnerable. Too much security, applied in the wrong ways, and your employees will feel stifled and start finding workarounds, ultimately still leaving the business vulnerable.

Key security advice when building remote capacity

In this spirit, S-RM has listed below some key areas to consider when planning or deploying remote working capabilities.

Securing devices

One key consideration for remote workers is that they have laptops, mobile phones, tablets or other devices to work from. Many companies are now issuing additional equipment to their workers, to allow them to remain fully effective outside the office. But please be aware of the following:

Make sure you have effective **asset management** in place. Know what devices have access to your network and data, plan for any changes, and block or remove obsolete equipment from your network before it becomes a weak point in your security.

All company devices, especially any device taken outside the office, should be **encrypted**, protecting data if they are lost or stolen.

- Use BitLocker or a suitable third party solution for Windows devices
- Make sure encryption is active on Apple devices (it normally is!)
- Make sure appropriate encryption is in place on other mobile devices

Continued ➲

Individuals and businesses worldwide are now being targeted by phishing campaigns designed to play on fear of the virus and of the lack of reliable information on the outbreak.

If you allow employees to use their **personal devices**, consider whether your corporate data is appropriately secured. Mobile Device Management solutions may allow you to secure data on these devices, or you may need to restrict what employees are allowed to access in the first place.

Don't forget about the equipment that is still in the office! With employees working from home, is there sufficient **physical security** at your sites to protect servers, desktops, and other parts of your network from malicious actors?

As you move devices, employees and user accounts around, don't forget the other parts of day-to-day security preparation – strong passwords, secured and appropriate local administrator accounts, and control over the applications and services on your network are just as important as ever, to name a few.

Securing your networks

If your endpoints and your servers are both appropriately secured, it's important to make sure the two can connect! Access to your network should be easy for legitimate users, but blocked (or at least very difficult) for everyone else. Consider the following:

- **Method of connection.** Well-configured VPN clients on all employee devices allow secure access to the network through a private tunnel. Other secure access solutions will be available for particular use cases. If you need employees to achieve access from the open internet, are they connecting to a particular external firewall, or a well-managed cloud service like Office 365? When planning user access, try to limit as far as possible the exposure of additional areas of your network to the internet and its many threats.

- **Restricting access.** Many types of connections can be configured to further secure them against malicious actors. If you are using a cloud service like Office 365, consider restricting access where possible to particular devices, particular IP ranges, or to particular types of connections. Firewalls and other services will offer many similar options for carefully managing access rules. Consider restrictions inside your network too; preventing connections or user accounts from going beyond certain areas will reduce the risk from one unsecure employee or unforeseen vulnerability.

- **Strong authentication.** The next step in securing any access is to ensure that strong password policies and multi-factor authentication are enforced. Enforced strong password policies are a must for all services, not just those that are meant to be publicly accessible. Multi-factor authentication should be used as much as is practical for your business. Remember that there are many types of authentication; while text messages might seem like the path of least resistance, if you have time to set up an authentication app your business will be much more secure, while device-based authentication might be appropriate in places to reduce frustration for employees.

- **Think of everything.** To secure a network, you have to consider all the different ways it can be accessed. How are your employees accessing their mailboxes from their mobile devices? Do employees need to connect to operational technology such as factory equipment (and is it safe to let them)? How is remote desktop access into your network structured? If you fail to secure these, you create vulnerabilities; if you fail to facilitate them, you prevent employees from working.

Securing employee connections

The network may be thoroughly secured at your end, but that data has to come from somewhere. As employees are based outside your secure environment, it is often up to them to make sure they are acting appropriately. You can help by providing them with suitable guidance (as discussed further below) on topics like:

- **Setting up home wifi.** Ordinary home users often neglect basic security when setting up their home environments. You can help your employees with simple advice backed by senior leadership. Basics like changing network name and access and administrator credentials are key, and employees should also ensure appropriate network encryption is in place, remote access is disabled, and that the software is kept up-to-date.

- **Accessing other networks.** You may want to consider providing guidance to your employees about (not) using public wifi, about how network names can be spoofed, and how man-in-the-middle attacks can be launched on public wifi networks. A lot of the guidance on using public wifi for business purposes is now very similar, but by specifically setting out your own rules and guidelines you can make sure your employees have a clear understanding of best practice. Don't forget to mention the other risks of working in public places, relating for example to Bluetooth connections and to simple over-the-shoulder spying.

Continued ➲

- **Communications channels.** Make sure your employees have a clear understanding of how they should communicate with you, with third parties and with each other. Make clear that work emails should be confined to work accounts, and which messaging services they should use (do you have a specific business solution, or are they on WhatsApp?). If you don't make sure there are clear lines of communication available, before long your employees might well be texting each other passwords or customer names, with all the attendant risks. If you do provide clear solutions, you can effectively monitor them for any potential threats, for inappropriate data movement, and for other business purposes.

- **Watch out for Coronavirus phishing.** As with other major world events, the COVID-19 outbreak represents an opportunity for malicious actors, from simple scammers to government-backed hacker groups. Individuals and businesses worldwide are now being targeted by phishing campaigns designed to play on fear of the virus and of the lack of reliable information on the outbreak. Extra vigilance should be exercised by all regarding any communication, hyperlink, attachment or request for information relating to coronavirus. Warning your employees about this will reduce the threat to them and to you.

Individuals and businesses worldwide are now being targeted by phishing campaigns designed to play on fear of the virus and of the lack of reliable information on the outbreak.

Informing your employees

The points above are all important areas where you can provide guidance to your employees, but in fact clear and effective communication is one of the most important steps you can take in any area. Even if you have a clear plan and a secure infrastructure in place, without clear information employees will make mistakes, or else assume you **don't** have a plan and start taking (potentially unsecure or counterproductive) measures of their own.

Make sure employees are clearly informed, at least a week in advance if practicable, about what devices they can use, what services they can access, and how they should do so. Keep them up to date if this changes. Some employees may not have the access they need; you need to find a solution before they come up with their own! If access isn't in place yet, employees should know when implementation is planned so they can act accordingly, and if at all possible, what alternative solutions are available in the interim.

Make sure employees are clearly informed, at least a week in advance if practicable, about what devices they can use, what services they can access, and how they should do so.

Communications of this type are not just a matter for technical IT or Cyber Security teams. Communication with employees regarding remote access should be overseen by **executive management-level staff**. While the technical teams can provide the appropriate solutions and guidance that employees need, this information needs to be effectively prepared and packaged so it can be delivered in clear and simple language, using an appropriate method, and at an appropriate time. Importantly, the guidance or policy should be clearly backed by the senior leadership of the organization, to ensure that it has the authority and clarity needed to convince employees to follow the advice given.

As much as practicable, make sure you provide sufficient information to **third parties** as well, including any **customers** who need to access your network. They will also need to know how to contact you, how to access relevant services and infrastructure, and what you expect from them in terms of their own security. Make sure your planning and requirements are clearly in place, then let them know clearly and decisively what you want – and, if the situation changes, consider when it will be most effective to update them.

Planning for the worst

Any cyber security professional knows that no one is ever absolutely safe from a malicious attack. Combining the increased exposure from remote working with the confusion and short deadlines of responding to the changing coronavirus situation only increases that risk.

If you have effective **cyber incident response, crisis management** and/or **business recovery plans** in place, it is important to review them in light of your new operating environment. Can you access all the equipment you will need to test or reset? Is your data still being backed up to a secure site? Can your users still effectively report phishing or other indicators of cyber incidents? How are you going to maintain communication between the key crisis managers if all your laptops and mobiles get encrypted with ransomware? If your plan isn't tested yet, now may be the wrong time to start – but at a minimum do all the relevant staff at least have a clear understanding of the plan, and how your current situation has altered it?

Continued ➲

If you **don't** have these plans in place, you likely don't have time to build them right now, but it is important to at least consider the basics. Do you know where your key data is stored? Do you know what services are key to your business survival? Do you have backup communication channels, independent of your network? Do you have similarly separated, and regularly updated, data backups?

Most of all, in your current situation – who will be needed to respond to a crisis? Who else needs to be informed? How are they going to coordinate, and who will replace them when they need to get some sleep?

Evolving

As stated earlier, the global situation, and advice from governments, is changing rapidly. As time passes, businesses may have more time to implement additional measures and better adapt to the new situation; or new events may force them to continue to react. In either position, please bear in mind the following:

- Cyber security should be a part of your IT and business planning, not something added on at the end where it will be ineffective or will get in the way
- Always keep your eye on the prize of your key data, assets and services that need protection
- Always consider your whole network or organization – be careful not to miss gaps in your defenses, or legitimate business needs that you are inadvertently blocking
- Communicate with your employees – use clear and simple messaging, make sure the information provided is well-founded and authoritative, and explain how they should act in order to do their jobs effectively

If you have effective cyber incident response, crisis management and/or business recovery plans in place, it is important to review them in light of your new operating environment.

About the authors

John Coletti is Chief Underwriting Officer & Head of North America Cyber and Technology for AXA XL, a division of AXA. He can be reached at john.coletti@axaxl.com.
Aaron Aanenson is director of cyber security for S-RM. He can be reached at a.aanenson@s-rminform.com.

To learn more, contact your AXA XL Cyber underwriter.

S-RM is a global consultancy that helps clients manage regulatory, reputational and operational risks.

6366_03/2020