Security Resilience in the Face of COVID-19

Gallagher

Insurance | Risk Management | Consulting

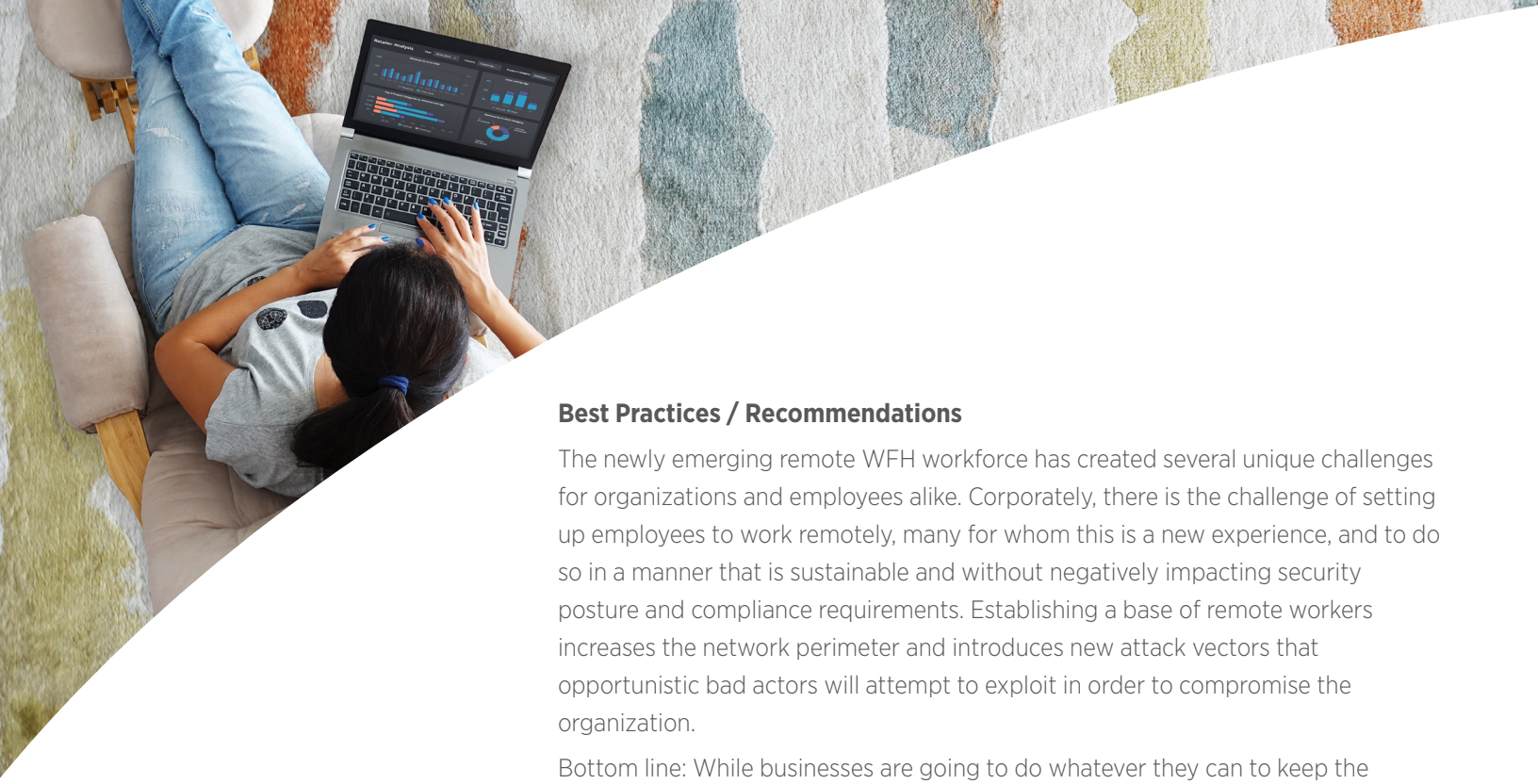
As the COVID-19 outbreak continues to navigate unchartered territory, businesses globally are being forced to engage Business Continuity Plans (BCP) and address this rapidly evolving exposure from an operational, regulatory and business continuity perspective head-on.

While cyber-security should be front-of-mind at all times, this statement cannot be more true as many organizations look to implement work-from-home (WFH) strategies. For many, WFH practices may form part of the organization's BCP, however in many cases businesses have not practiced or tested their BCP with regular frequency, if at all. Aside from concerns surrounding efficiencies, the concern surrounding cyber-security hygiene ought to be on the forefront as well.

It has been well publicized over the past several years that cybercriminals thrive at instilling fear into the economy – even more so when operational resilience is being tested by external events. COVID-19 is not an exception. The Canadian Centre for Cyber Security has recently documented that there has been an increase in reports of cybercriminals using Coronavirus in phishing campaigns and malware scans[1], with Kaspersky's threat detection technology documenting malicious content disguised as Coronavirus related information all the way back to January[2]. As the pandemic and fear continues to span the globe, the attacks will only become more complex and sophisticated.

New or perhaps overlooked vulnerabilities exist and are at risk of being exploited with new WFH processes being implemented. While employees work remotely, it is vital that the same cyber-security hygiene exercised in an office environment is adhered to in the WFH environment. The reality is that this expectation would be challenging to both enforce and monitor.

[1] https://cyber.gc.ca/en/guidance/cyber-hygiene-covid-19
[2] https://usa.kaspersky.com/blog/coronavirus-used-to-spread-malware-online/20213/



Best Practices / Recommendations

The newly emerging remote WFH workforce has created several unique challenges for organizations and employees alike. Corporately, there is the challenge of setting up employees to work remotely, many for whom this is a new experience, and to do so in a manner that is sustainable and without negatively impacting security posture and compliance requirements. Establishing a base of remote workers increases the network perimeter and introduces new attack vectors that opportunistic bad actors will attempt to exploit in order to compromise the organization.

Bottom line: While businesses are going to do whatever they can to keep the business going, they should also take into account adequately addressing the risk associated with the New Perimeter, the proliferation of heterogeneous and decentralized computing devices, and at times the make-them-up-as-we-go-along procedures to accommodate this new world.

For the remote employee, there are quite a few things to do in order to secure your WFH environment. Whether you are using a company provided laptop/workstation or using your own devices, there are several factors to be considered:

- Make sure that you are familiar with existing remote computing policies/ procedures as well as acceptable use policies
- Install antivirus/anti-malware software and make sure it configured to provide automatic updates
- Install/enable personal firewall software on the system
- Make sure the operating system is current on its patching, and make sure that it is configured for automatic updates.
- There are several things to consider for home WiFi network users:
  - Ensure that you have a strong password for your home WiFi (should be at least 15 characters).
  - Ensure that you are using a secure wireless protocol such as WPA2 (do not use WEP)
  - For those whose equipment support it – create a separate wireless network for non-work devices (i.e. kids' computers, IOT home devices, etc.)
- Enable 2-factor authentication (sometimes referred to as multi-factor authentication) on all of your work and personal accounts (your company should provide what you need for any work accounts)

Now is a good time for companies to provide a fresh round of security awareness training.

- Be extra vigilant about opening emails or attachments, and/or clicking on links as attackers are focusing even more on phishing campaigns targeting a generally nervous and concerned public. Now is a good time for companies to provide a fresh round of security awareness training.
- Be paranoid about your working environment – if you work with any sensitive data, you should either purchase a privacy screen for your computer or make sure that eavesdroppers can't peek through your windows (there are many inexpensive high power binoculars/telescopes).

Another thing to consider is how WFH users are connecting to corporate networks. For some organizations, much of the network infrastructure is cloud-based and therefore may more lend itself to seamless connectivity. For others, virtual private network (VPN) connectivity is used to connect remote users to the corporate network. Considerations for VPN connectivity include:

- Ensure that the remote users are using company-approved VPN software and that it is current.
- Ensure that there is a strong authentication mechanism in place for remote users – multi-factor authentication is expected here.
- Make sure that VPN client is configured to NOT allow for split tunneling – this would potentially allow for outside connections to access the endpoint during a VPN session.
- For companies that must allow unmanaged devices to connect to their networks, it is advisable to configure some sort of gatekeeper to ensure that the remote device is currently patched, has anti-malware software etc. prior to allowing it to connect to corporate networks.

Regardless of whether you can setup a separate work LAN in your home, you should be aware of all of the devices in your home that have Internet connectivity, what are commonly referred to as "Internet of Things" (IoT) devices. These could be the ones you know about, (i.e. Alexa), but also major appliances (i.e. home security systems, televisions, or even lightbulbs & switches). Every one of these devices is a potential attack vector that could be used by an attacker to gain access to your home environment, and in turn, potentially your employer. While these devices have become part of just about everyone's life, it is important to:

- Change any default passwords on these devices
- Make sure that you regularly check for firmware updates for these devices

Never worked from home before? Apart from the security considerations that need to be addressed by new WFH employees, there is the need for some practical advice for creating the most productive work environment possible.

Here are some suggestions from a long-time remote worker:

https://info.obsglobal.com/blog/when-life-gives-you-limes

Any challenge.
Any risk.

Anywhere in
the world.

The Applicability of Insurance

The combination of a potential weakened state of security as the result of employees working remotely in their home environment, and the heightened exposure of phishing schemes targeting employees in a moment of anxiety and distress may put businesses in a precarious situation.

While insurance related questions continue to revolve around the availability of business interruption coverage, liability concerns, travel and health insurance, the applicability of cyber insurance is also a consideration during these unsettling times. A stand-alone cyber form provides the broadest form of coverage for protection against network events that may impact your business.

Stand-alone cyber insurance policy forms have continued to broaden over the past several years and exist to respond to attacks or situations arising from these scenarios. The most comprehensive coverage addresses items such as non-attack related system failure or the voluntary shutdown of your network to mitigate an attack, in addition to the more commonplace provisions of coverage related to ransomware/extortion, business income loss, network restoration and third party and regulatory concerns surrounding the breach of privacy and corresponding litigation. As standardization does not exist from one carrier to the next, it is important to conduct a review of your coverage form to understand the coverage available to you and how it may apply. It should be cautioned that the cyber coverage often included as an extension of property and liability policies does not address many of the true exposures faced in today's cyber landscape.

Gallagher

Insurance | Risk Management | Consulting

For more information:

Brian Dagg
Account Executive
t: 204.925.8862
brian_dagg@ajg.com

ajgcanada.com

online business systems

For more information:

Steve Levinson
VP – Risk, Security & Privacy
t: 800.668.7722
rsp@obsglobal.com

info.obsglobal.com