WHITEPAPER

RICOH
imagine. change.

Protecting the Hybrid Workforce

Key security considerations for an ever-expanding work world

In 2021, research firm Forrester reported that 70% of companies are pivoting to a hybrid work model post-pandemic[1]. By now, most companies have implemented some form of remote work capabilities and have invested in the necessary technologies and processes to support it. However, as Canadian organizations pivot from a primarily remote workforce to a more complex hybrid model, security professionals face new challenges in protecting data and systems.

In the hybrid workplace, security leaders are tasked with safeguarding the company's data and systems within a borderless world of work. As employees access network and applications in any location, on any device, attack surfaces multiply while threats such as ransomware are on the rise. Even the smallest crack in a network's defences can bring serious consequences for the business.

In this article, we present 4 key considerations for securing your hybrid workforce:

1. Align IT to your business needs

A key priority for the hybrid workforce is maintaining a highly available, secure network that delivers a consistent and equitable work experience for all users, whether remote or in the office.

As the virtual workspace becomes a permanent part of how we work, new infrastructure and processes must be implemented. Key systems and tools are distributed, hosted in multiple locations be it onsite, in a private or public cloud, co-located in a data centre or through various web applications.

With fewer employees working from the office, many organizations are transforming their physical space to facilitate productive hybrid work. As employees drop in and out of the office, they expect instant access to their files and applications, while maintaining a work experience that is consistent with their remote work experience. To achieve this, organizations are implementing new infrastructure such as videoconferencing and 'hoteling', bringing the physical office space into the virtual network.

In a hybrid workplace, the physical security perimeter of the office no longer exists; the boundaries that once defined what was inside and outside of the network have been blurred, introducing new vulnerabilities, and making security management ever more complex.

2. Assess the business risk

Consider which threats pose the greatest risk to your organization. Hybrid organizations especially need to get a handle on their full risk profile, which is best achieved with an outsourced risk assessment.

Security assessments are critical, however, they don't provide all the information you need to understand the risks to your business. We recommend starting with a holistic view of the organizational and IT infrastructure risk profile before delving into your security posture.

For example, a data breach that obtains the financial and personal information of your entire customer base would be much more impactful than an attempt to steal plans for a new product. A risk assessment allows organizations to classify their information – both critical and not. It should include a quantitative analysis of this data, which places a value on each type of information and what would happen if that data were breached.

Assessing risk first enables organizations to tailor their security strategies to their unique requirements, protecting the business without spending more than they need.

3. Identify & close security gaps

Now that you understand where your organization might be vulnerable and what information is most valuable, you're able to choose security solutions that suit your risk profile.

Managing a hybrid network is incredibly complex, with high demands on IT teams. Blind spots can easily form, which is why getting an outside perspective from professionals who regularly assess different types of networks is an invaluable exercise.

Security consultants provide a range of different assessments, from vulnerability scans to penetration testing to remediation to backup and recovery. Start with a good baseline test that provides data-driven insights to guide your overall cyber security strategy. The assessment should review security policies, device configuration, critical business applications, business continuity, cloud configuration, compliance and best practices at the very least.

It's also important to take stock of where your assets are - and how employees are using them.

Watch out for well-intentioned "shadow IT" where users adopt unvetted tools they perceive as smart and cool new solutions but could be dangerous to your data security and become the source of a breach.

Most breaches originate from employee behaviour, which is why cyber security awareness training is a critical element of a robust security strategy.

4. Strengthen your hybrid security

Managing technology in a hybrid world of work requires a strategic approach that enables employees to access systems and data across multiple locations, securely and seamlessly. As organizations transform the way they work, security leaders must also transform the way they are protected.

The zero trust security model has been around for some time, but its effectiveness in securing the hybrid workplace has made it the prevalent model coming out of the pandemic. Zero trust security assumes no user or device is safe, requiring authentication and authorization every time someone connects to the network. This enables security teams to reinforce BYOD policies, reduce likelihood of devices being vectors for malware, and mitigate credential theft and brute force attacks.

Best practices include implementing multi-factor authentication; endpoint security; mobile device management; continuous system and endpoint monitoring and response; as well as maintaining a robust, multi-layered backup infrastructure.

Organizations should also pay special consideration to the growing threat of ransomware: according to the Canadian Centre for Cyber Security, **attacks increased by 151%** in just the first half of 2021, and newer strains are growing faster[2], stealthier and able to evade endpoint defences.

In the face of this significant threat, we recommend including both prevention and remediation in your ransomware defence. Automated containment solutions like RansomCare immediately stop ransomware attacks at the source, preventing further spread and harm to the business.

CONCLUSION

There's no putting remote work back in the box – Canadian organizations recognize that hybrid work is here to stay.

If you're transitioning from a fully remote work model to hybrid, consider enlisting the help of an experienced security partner that can take you through best practices and provide valuable insights to build a strong, data-driven security strategy.

---

[1] Forrester: Only 30% Of Companies Will Embrace A Full Return-To-Office Model Post-Pandemic

[2] Cyber threat bulletin: The ransomware threat in 2021

Ricoh can help. Our team of security experts will help ensure that your company's critical data protection is innovative enough to stay ahead of the threat environment. **Contact** a Ricoh IT Solutions representative or **click here** to learn more about our comprehensive security assessments.

RICOH
imagine. change.

Ricoh Canada Inc., 100-5560 Explorer Drive, Mississauga, ON L4W 5M3, 1-888-742-6417