OT group

The Complete Tech Guide to Managing Your Remote Team

+ How to Design an IT Strategy for a Remote Workforce

CONTENTS

INTRODUCTION

If you are like the vast majority of businesses in Canada, then 2020 has probably seen your organization transition to a work-from-home model in which your workforce is largely operating remotely.

In fact, Statistics Canada found that 4 million Canadians who don't normally work from home started in response to the COVID-19 pandemic, and that's from data recorded back in March - it's likely these numbers have only gone up since.

Once the research added in all of the workers who normally work from home, the stay-at-home workforce in Canada earlier this year rose to 6.8 million - that's nearly 40 percent of Canada's entire workforce.

Unsurprisingly, a survey of 2,000 working professionals and 1,000 hiring managers by LinkedIn, found that 82 percent of workers want to work from home at least one day per week, and 57 percent want to work from home at least three days per week. Remote work is here to stay.

There's a number of good reasons why small businesses are transitioning to remote work as a long-term strategy. According to Owl Labs, 83 percent of workers (either remote or on-site) say that a remote work opportunity would make them feel happier at their job. OwlLabs also found that those who work remotely at least once per month are 24 percent more likely to be happy and productive in their roles than those who can't or don't work remotely, and that remote workers say they are happy in their jobs 29 percent more than on-site workers.

If your organization is considering using a remote workforce long into the future, there are a few basic things that you will need to consider to ensure that they are successful in their role - and technology plays a key role in that.

1

WHAT TECHNOLOGIES DO YOUR EMPLOYEES NEED TO EFFICIENTLY WORK FROM HOME?

To get the most out of your remote team, and to ensure they are producing the high-quality work that they would be when working from an office, it's crucial that you provide them with the technologies required for a long-term work-from-home strategy.

When in the office, your team will have access to a wide range of tools, technologies and IT infrastructure. While these technologies can't all be taken home by your employees, there are a number of technologies you can invest in to significantly improve how productive they are when working remotely. Here s a list:

Desktop and laptop computers

The most important technology for your employees to get their job done from home is either a desktop or a laptop. While desktop computers are more powerful and comfortable to use, laptops offer the versatility and flexibility of being easy to transport.

While it's possible that you can ask employees to work from their own personal desktop or laptops, we strongly encourage your business to allow employees to take their work device home. This will not only ensure your business retains its security measures, it will also ensure all documents are being saved on the same devices as they would be in the office. This prevents important company information from being scattered across multiple networks and multiple devices.

Printers and scanners

If you work in a document-heavy industry, it's possible that some of your employees will need access to a local printer and scanner when working from home. If they don't have access to a printer at home, your company will need to invest in one if it's crucial to their job.

When choosing a printer or scanner, look for a cost-effective option. If printing is crucial for your company's product offering, make sure the printer that you end up purchasing doesn't lower your standard of work.

Communication tools

Communication is fundamental to any successful remote business. That's why it's important that your company ensures its employees have access to videoconferencing and communication tools when working remotely.

This could include anything from Zoom, Google Chat, Slack, Microsoft Team or organization tools such as Trello or Teamwork. All these technologies ensure that your team is able to stay in frequent communication.

There are two other important technologies that can improve your employee's productivity at work. The first is a webcam so that your team is still able to conduct deeper and more meaningful face-to-face connections. The second is noise-canceling headphones, which help your employees stay focused if they live in a busy house.

2

WHY YOU SHOULD CONSIDER USING CLOUD-BASED TECHNOLOGIES FOR REMOTE TEAMS

Does your company rely entirely on physical hardware and software? If so, this will make it difficult for employees to access the tools they need when working remotely, and potentially increase downtime for your organization.

If your employees rely on physical hardware and software to complete their jobs, this will be challenging for remote teams. Accessing, managing and fixing issues on local hardware becomes a nightmare for IT teams when employees are based at home.

That's not even taking into account the amount of wasted time employees spend trying to get their hardware or software working, or their computer to speed up.

The use of cloud computing, however, can power your remote team.

What is cloud computing?

Cloud computing refers to the range of computer system resources that are accessed by users through the internet (the cloud).

As opposed to being stored locally on physical hardware, cloud-based software stores your data on remote servers - saving space on your company's computer systems and allowing them to work more efficiently. Best of all, cloud providers are entirely responsible for managing errors and resolving downtime.

Users typically pay through monthly subscription-based and cost-effective models, allowing your business to lower day-to-day costs, improve operational efficiencies (since there's no need to manage physical software or hardware) and scale seamlessly.

How does cloud computing benefit your remote workforce?

By implementing cloud computing into your IT strategy, however, you can remove the inefficiencies of physical hardware and enjoy a number of benefits, such as:

1 - Greater mobility and flexibility

Cloud software allows your employees to access the software, documents and tools they need to do their job, no matter where in the world they are. Whether they are working from home, working at a coffee shop, visiting a client's office or on a business trip, your employees will be able to access their work on any device that has an internet connection. Through the use of cloud computing, you can build a highly flexible and mobile workforce.

2 - It boosts your disaster recovery plan

Data loss is a huge concern for businesses. In fact, your organization has probably suffered from a local hardware crash, or a worker error, where you lost important information. Around 31 percent of PC users have lost all of their files due to events beyond their control, according to the Boston Computing Network, and 60 percent of companies that lose their data will shut down within six months. Cloud computing can be a great part of an effective disaster recovery plan. Since data is stored at a remote data center when you use cloud computing rather than local hardware, data loss from faulty equipment or theft is minimal.

3 - Better collaboration and sharing

When working remotely it can be easy for employees to fall into silos and not connect with each other. Cloud solutions are a great way to facilitate collaboration between your team. When all documents are saved to the cloud, employees can access, edit and share documents with each other in real-time. This encourages employees to solve issues creatively as a team.

4 - Complete scalability for growing businesses

Small and medium-sized companies are constantly growing. Investing in hardware and software for new employees is not only expensive, but it can also impact your future cash flow when these technologies become outdated or not needed. Cloud computing, and its pay-as-you-go pricing model, allows you to accommodate large increases (or declines) in your remote workforce very quickly.

5 - Improved cybersecurity

While your company should still have its own security measures, cloud providers actually have their own security practices in place to protect the data that you have stored on the cloud. Cloud providers use passwords, two-factor authentication, file encryption and a wide range of security procedures to protect your data at no extra cost. Not only that, but cloud providers invest large sums of money to ensure they are constantly updating their security measures.

.

3

HOW TO PROTECT YOUR REMOTE BUSINESS FROM CYBERCRIME

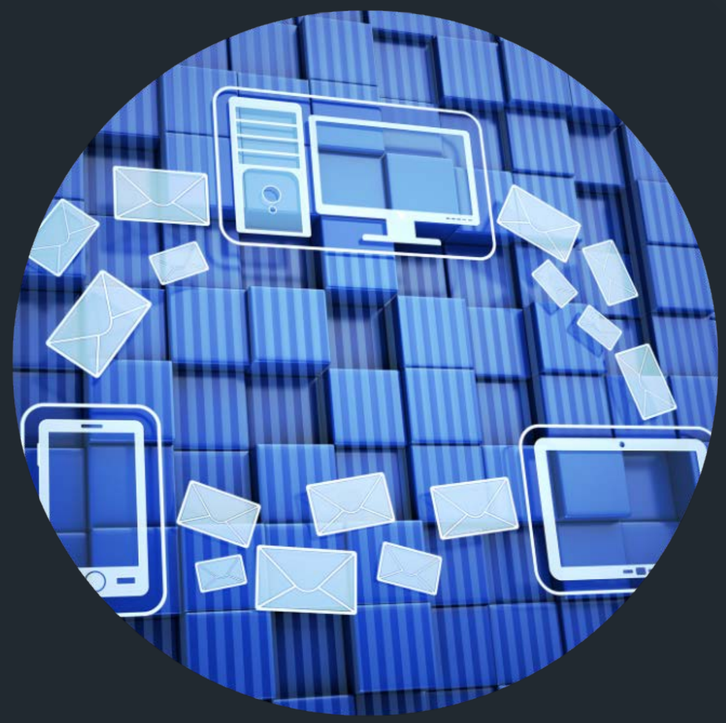
The huge increase in remote work has meant the office of the future has arrived early, according to a new whitepaper from New York-based IT firm Electric, yet small to medium-sized businesses need to do more to prevent cybercrime. Remote teams are at particular risk to cybercrime with some of the most common threats involving:

1 - Phishing scams: Phishing is a type of scam in which hackers send legitimate looking, deceptive emails to your employees. These emails contain malicious links and attachments that, once opened, give hackers access to an employees device or your company's network. Phishing scams are the top cause of data breaches, and result in huge amounts of lost money and operational issues for those companies that fall foul of them.

2 - Insecure home WiFi security: Businesses spend a lot of time and money to ensure their network security is up to scratch. Strong network protocols make it almost impossible for hackers to gain access to your network and steal your information. Your remote employees will not have the same level of WiFi security, and public WiFi connections will be even worse.

3 - The use of personal devices to access your company's network: In 2014 Cisco research, 46 percent of employees admitted to transferring files between work and personal computers when working from home. Unfortunately, allowing employees to access your company network on personal devices opens your company up to a range of cybersecurity threats.

4 - Insecure passwords: Poor passwords are one of the most common ways that hackers gain entry to a network or account. In fact, simple passwords are incredibly easy for hackers to crack. Data from the 2016 Verizon Data Breach Investigations Report shows that 63 percent of all confirmed data breaches involve weak, default or stolen passwords. If your employees are using the same insecure passwords across several platforms, then hackers will be able to gain unauthorized access to multiple accounts in a short period of time.



OT Group uses AI security such as **Covalence,** DarkTrace, **and** Cisco Umbrella, **along with Multi-Factor Authentication tools and EDR anti-virus products, to improve client's security** measures.

Thankfully, there are a few technologies, processes and softwares that your business can implement to ensure that your remote team is secure from the threat of cybercrime.

1 - Make sure your employees are all using a secure WiFi connection

Most WiFi systems at home are correctly secured these days. However, it's possible that they aren't secured probably if employees are working off an older WiFi installation. Insecure connections will allow people in the vicinity of your WiFi to access it and see what you are doing. If you are in doubt about your, or your employees', internet connections then you can use a virtual private network (VPN) to secure it. A VPN will secure an internet connection by encrypting your information from outside eyes.

2 - Ask employees to change their router login and password details

The default login and password required to access a WiFi connection are widely known and easy to access. Cybercriminals can easily gain entry to your company's data by hacking into a remote workers' WiFi network or software accounts. Thankfully, avoiding this is an easy fix. Simply encourage your employees that are working from home to change their router login details and other passwords on a regular basis.

3 - Download antivirus software

In the office, your company probably has powerful antivirus software installed on each system to ensure your devices are protected from cybercrime. It's unlikely that your remote workers will have this software installed on their personal desktops or laptops. Any device that handles corporate data should have antivirus software installed on it.

4 - Provide employees with a password manager

Password managers, which are powerfully encrypted applications that generate and store unique passwords for each website an employee visits, are a fantastic way to offer your company greater security and convenience. LastPass, for example, is a widely regarded secure platform that manages login credentials across your organization while improving your security measures at the same time.

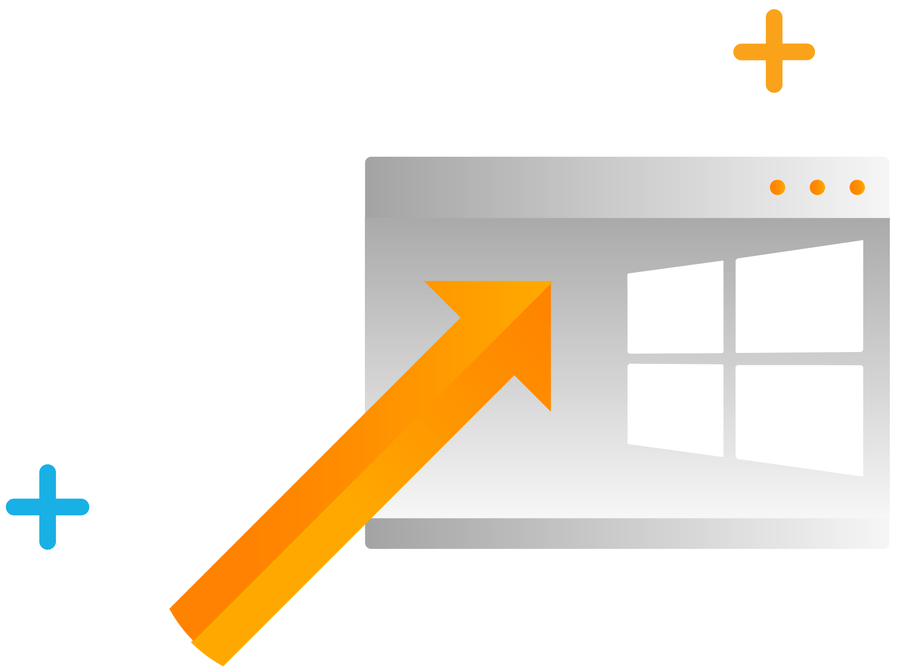
4

DESIGN A DATA BACKUP AND RECOVERY STRATEGY TO PROTECT YOUR WORK

According to Cisco, more than 20 percent of businesses that experience data loss or suffer a cyber-attack lose customers as well. Shockingly, 40 percent of those companies lose more than 20 percent of their customers.

If you've followed our advice above then you will have significantly reduced the likelihood that cybercrime will impact your business. But it's better to be safe than sorry, and that's why we recommend companies with remote teams to also implement a data backup and recovery strategy.

Data backup and recovery is the simple process of backing up data so that your organization is able to recover that data in the event of a loss. By creating processes in which your company stores multiple copies of its important data, you will ensure that you'll still be able access that data in the event of data deletion, corruption or cybercrime.



Why is data backup and recovery important?

Data backup and recovery is important for all companies, but it's perhaps more important for remote workforces where the employer and IT departments have less control over the workflow of employees. While cybercrime is the most common cause of data loss among businesses, there are a range of threats that make data backup and recovery important for your organization.

Hackers, viruses and ransomware: Cybersecurity Ventures predicts that cybercrime will cost the world more than $6 trillion last year, and that's because data is now the most expensive commodity on earth. Through viruses, phishing scams and ransomware, hackers can steal a company's data and then blackmail them for money. Nullify these crimes by properly backing up your organization's data.

Natural disasters: A fire, flood, tornado and other natural disasters could completely wipe out all of the data you store in a specific location. If this happens, you have absolutely no way of recovering that data if the hardware is destroyed. Even the physical theft of your not-backed-up data will result in the permanent loss of that data.

Technology fails and employee hiccups: By storing data on just one piece of hardware, you're leaving your organization open to a plethora of ways that data can be lost. If that piece of equipment fails, or your employee accidentally deletes it from the device, then you have absolutely no way of recovering that information.

How can I backup my company's data for a remote workforce?

There are a number of easy ways to create backups of your data, and many office-based businesses simply use local and network backups to protect their data. That means using devices such as hard drives, storage devices and physical hardware to create multiple data storage locations.

This becomes more complex when your company is decentralized through remote work. Thankfully online backups and cloud backup solutions are a fantastic answer to backing up work-from-home data.

Cloud backups allow you to move your important data to an offsite, secure location where copies of your documents are stored on remote servers and accessed through an internet connection.

CONCLUSION

Many of the challenges that come with managing remote teams have straightforward solutions if you know what technologies to use and which vendors to select. Unfortunately, however, most organizations realize they don't have the right levels of technical expertise in-house to implement IT strategies that drive productivity among their remote teams.

That's why your business should look to leverage the expertise of an outsourced IT partner, based right here in Ontario.

OT Group can provide you with the IT infrastructure, cloud technology, cybersecurity and data backup solutions that ensure your organization can efficiently manage a productive and effective remote team.

CONTACT OT GROUP

Founded in 1988, OT Group is a leading provider of integrated business solutions. Whether you want to communicate between offices, update your infrastructure, take advantage of the cloud or update your disaster plan, OT Group offers complete IT solutions from design and installation to training and support.

The company is now one of the largest independently-owned office technology suppliers in Canada. This growth is directly attributable to OT Group's laser-sharp focus on providing exceptional customer service, industry-leading technology products, and substantial financial value.

OT group

175 Lahr Drive, Belleville, Ontario K8N 5S2

Phone: 1-800-267-5594 | Email: info@otgroup.ca | **www.otgroup.ca**