THE PATENT BARON™

LET THE PATENT BARON BE YOUR IP COPILOT
Main: 202-570-7380
Direct: 202-897-4747
Cell: 248-697-7635
PATENTBARON.COM

May 2020

How to Protect Your Company's Intellectual Property when No One is Working in Your Offices!

Are you worried that your valuable ideas and sensitive information is threatened by hackers and careless workers?

Table of Contents

Abstract

In this period of unprecedented upheaval, the concept of the traditional office has been shattered. Until recently, working from home was an isolated situation or the domain of gig workers. Now working from home is the norm and the traditional office may never be the same. However, the layers of security present in the traditional office are missing from nearly all home work settings.

Why is this important?

Because now your company's valuable ideas (Intellectual Property, or IP) as well as other sensitive information (SSN, HIPAA) is more vulnerable to hackers and careless workers than it has been in years, if ever. This white paper will provide you with numerous solutions and also cause you to ask yourself difficult questions about the state of your company's security.

The 10,000 Ft View

This white paper will discuss numerous concerns that your company needs to address in order to secure its valuable IP and other sensitive data. Among these concerns are the following:

- Separation of workers and worker devices from the company
- Return and processing of company devices by workers
- New workers and new devices
- Forensic and monitoring software on devices
- Lockdown of USB connections to company devices
- Secure Internet connections for worker use
- Dedicated and secure working space at home
- Bluetooth® security concerns
- Public wi-fi no-no
- Third Party Stories - Ransomware migrating from worker device to company network; Malware on worker device re-routing company data to third parties
- Video conferencing security

- Paper shredding and document disposal
- The Email string and “Reply All”
- Virtual Machines
- Company VPN

Methodology

In preparing this white paper, I researched numerous articles pertaining to working from home security issues, including but not limited to articles posted on Bloomberg.com, CNN.com, ZDNet.com, and PCMag.com. I also reviewed my previous experience working in the automotive industry and in the law to compile best practices and areas for improvement given the current state of technology. I also interviewed Mr. Jon Isenberg of Elijah Information Technology, LLC via video conference in researching this white paper.

Separation of Workers and Worker Devices from the Company

Most Workers Aren’t Happy When They Willingly Leave

Workers leaving a company often aren’t very happy. Whether they are leaving to make more money or to advance their career, at some point they decide they are leaving the company. The problem is that those workers often decide they are leaving weeks before they give notice, giving them ample time to access company information and take it with them – often to a competitor!

Many workers use their own devices for company work – laptop computers, tablets, and mobile phones. All of these devices are capable of storing vast amounts of company information and are very portable.

How can a company then securely separate workers and their devices, particularly when the workers may not actually report to a company office, but work from home? Even more worrying is the fact that

some workers may be located in other city, state, or even country – how can a company protect their information?

In the case of workers using their own devices to conduct company business, it is recommended that all worker devices include software to monitor activity and also include a remote-erase feature. For example, mobile devices can be remotely "wiped" and similarly laptops and tablets can also be remotely erased to secure company information. (Workers are likely to object to their devices having this software installed, which can then steer the issue toward company-provided devices).

An additional concern is the use of backup devices or cloud-based services by workers for their devices. It is of little use to wipe a laptop when the worker has a complete backup stored on a flash drive or a cloud service. Therefore, the use of USB ports and cloud-based services should be blocked by monitoring software installed on worker devices as a condition of their employment.

Departing Workers Often Fail to Follow Company Rules

Let's face it – workers leaving the company willingly are likely to have little concern for continuing to follow company security policies. Often when workers are preparing to leave the company (before they have even given notice), they begin removing data from their devices in anticipation of action by the company once notice has been given.

For example, workers often remove their own personal photos but also contact lists, special projects or reports they have been involved in with the company as they consider those documents "their" work and may use them in the future (for a competitor) or as evidence of their experience at their previous position.

This process of "data extraction" can continue for weeks and often there is little that a company's IT (Information Technology) department can do at the time or even after the worker departs. And at that point, how much can be done? The best approach is to stop the data extraction from occurring.

Consider Carefully Allowing Worker Devices for Company Use

As I have illustrated, workers using their own devices for company use is fraught with dangers. There are numerous situations where data can be compromised and the extent of the breach of security may never be fully known – but can be felt in the success of your competitors as they bring on board your former workers.

At some point it was decided that it was affordable for companies to piggy-back on worker devices, rather than provide dedicated company devices – laptops, mobile phones, etc. While there is cost savings up-front, the lack of ability to control the devices (and the data stored therein) should cause companies to reconsider. Companies may find that the perceived benefits of using worker devices are diminished by the damage that security breaches can cause.

Return and Processing of Company Devices

What Happens When Company Devices Are Returned?

So, you've managed to avoid issues with worker devices by issuing company devices. But what happens when the departing (and likely disgruntled) worker returns those devices?

A typical situation is that the device (a laptop, for example) is given to a human resource (HR) person and then the laptop is sent to the company's IT department. There it will sit until it is needed for a new worker. The IT department will then wipe the laptop and reinstall all the relevant software, making the laptop "squeaky-clean" for the new worker.

However, that situation is far from ideal. What should occur is the following: the company should immediately examine the laptop using forensic software to determine the data activity of the laptop. Ideally, the laptop should have previously included monitoring software to track data accessed by the worker on the laptop. But the forensic software used after the laptop is returned can still provide the company with the necessary information.

Forensic Software Can Reveal Extent of Data Extraction

Specialized forensic software installed on all company devices can quickly reveal the volume of data that the recently-departed worker accessed, copied, printed, or otherwise removed from the company's servers.

Without forensic software, it is very difficult, if not impossible, for typical IT departments to determine the data that the laptop accessed recently or even over the entirety of its use by the worker. Even if an IT department were able to determine that data had been removed by the worker, without forensic software that information may not be useful in any legal proceeding against the recently-departed worker.

Forensic Software Can Be a Deterrent to Data Extraction

While the use of forensic software on company devices is a good idea, it is still an after-the-fact situation. However, the knowledge of its presence by company workers can be a useful deterrent in avoiding data breaches in the first place.

The importance of securing company data and preventing the extraction of data on all types of company devices (laptops, tablets, and mobile phones) should be considered particularly in the current work from home environment.

New Workers and New Devices

How Can the Company Protect Data Going Forward?

Bringing on new workers gives the company the opportunity to start with a clean slate. Change is often difficult for existing workers, while new workers are more open to change as it is central to starting a new position. The company should make use of that openness to roll out more security for their data.

New workers can be trained and made aware of data protection systems in place from their orientation, while existing workers can be retrained on those same systems. Over time, the awareness of both sets of workers to the concern held by the company for its data will affect worker compliance with data protection.

New Devices can be Selected with Data Protection in Mind

Often a company chooses devices based on cost, compatibility with existing systems, or other biases or perceptions. While these attributes can still be considered when selecting new devices, data protection should be at the forefront.

As will be discussed below, new devices can be chosen that have or omit certain features that can boost the level of data protection for the company. The new devices should be evaluated against forensic and monitoring software compatibility, for example. It may be prudent to choose one computer provider and one mobile phone provider to facilitate use of that software and the ability of the company's IT department to implement and operate the software on the company's network.

Consider Requiring a Separate Work and Home Computer

It is far more secure for the company to provide a laptop, mobile phone, tablet with security software, forensic software, and other software (such as a VPN or Virtual Machine) to existing and new workers than it is to allow workers to use their own devices.

Often workers are tempted to use devices for home and office work and without protocols in place to prevent this, security breaches can occur. For example, many social media sites are commonly the source of security breaches (as well as drains on productivity). Additionally, many gaming sites and software also can allow for security breaches and are easier to prevent on a company device that locks out gaming, social media, and other unwanted websites.

Finally, standardizing devices company-wide provides benefits to the company's IT department. They don't have to deal with particular issues relating to one brand or kind of device that a percentage of

workers are using. All software can be chosen for compatibility with one type for device (e.g., laptop). Additionally, automatic lockouts on USB, public wi-fi, and other undesired activity can be built-in from the start.

Is an IT Audit a Good Idea to Protect IP?

Has your company ever conducted an audit of your worker's devices? If so, when was it last conducted? Are you aware of the vulnerabilities of some devices that your workers are using for company business?

You should consider an audit of all of your worker's devices – those that are used for company business. You may be surprised to find out that many workers don't secure their devices sufficiently using anti-virus/malware software, for example. Many may not have kept up with automatic updates to operating systems (e.g., Windows 10, MS Office). An IT audit is a good first step toward improving security for your company's information.

END PART 1

Forensic Software on Devices

Install Forensic Software on Company Devices

Workers may chafe at the idea of forensic software at the c on company devices, but the installation could be conditional on continued or new employment by the company.

The forensic software can be used by the company, both inside and outside the office, to determine the data accessed by the worker's devices. In the ordinary course of business, this should be of little concern. But if the volume increases or particular information is accessed then additional action can be taken by the company.

For example, the forensic software could be integrated with or work alongside a virtual private network (VPN) to monitor, in real-time, data accessed by the worker. A log can be generated for review by the company's IT and/or HR department.

Forensic Software on Company Devices

The forensic software, as discussed previously, can prevent data extraction by its mere presence and also be useful after-the-fact to determine the extent of data extraction. Monitoring software can be useful in insuring that workers are using company devices appropriately and only for company purposes.

Companies may be familiar with software or firewalls to prevent workers from accessing Facebook®, gambling sites, or other unwanted Internet destinations, but monitoring software can extend much farther and deeper than that. Monitoring software can track and report on worker activities including time using the computer for work.

How Do Companies Keep Workers Working During Work Hours?

A big concern with the extent of working for home is: How much actual work is being done?

It's an all-too common sight now, workers in their pajamas, on the couch, "working". Whereas previously workers had to be at their desks working at a set time for a working day, now workers are often not doing work when they should be. Why is this a security concern?

Because a lack of professionalism and distractions while working from home leads to a disregard for security! Quite simply, if workers know they are being monitored for work activity during work hours, they will be more aware of security of company information.

I understand that many workers are doing their assigned work during work hours, but it is human nature to relax when not in a setting where there is supervision – the company office. It should be approached from this perspective – workers can get their work done and then have time for other activities "after work hours".

Lockdown USB connections on Devices

USB Connections are Company Enemy Number One

It should be no surprise that USB connections (as well as other data ports) on devices are a quick and easy way to extract company data. Flash drives (and portable hard drives/disks) are ubiquitous and workers are well aware of their capabilities. A worker can easily extract gigabytes of data in minutes and walk out of the company doors (or in today's environment in the safety of their own homes) with tremendous amounts of company data.

When acquiring new devices, the company should consider those without USB or other easily-used data ports as they are developed. For example, some new laptops do not include USB ports at all. The company can source laptops that have these ports internally deactivated by the manufacturer or the company's IT department as an alternative.

USB scanning stations

The use of centralized USB scanning stations can limit the ability of workers to extract data using flash drives. As discussed above, if laptops are not capable of locally accessing flash drives, then USB stations provide more secure method for handling flash drives.

For example, a customer may provide the company with a flash drive containing important information. The scanning station can securely check the flash drive for malware or other inappropriate data while not exposing a local laptop or the network to any risk. After the scan is complete, the flash drive can be downloaded to the network for the worker to access rather than the actual flash drive. Similarly, data that is approved for extraction by the company must be uploaded via a central scanning station.

Lockout USB Ports

For existing devices, the company's IT department can lockout USB (and other data ports) using software or hardware by physically blocking the ports. Alternatively, USB ports can be reconfigured for use that excludes data transfer so that other devices can still use the USB ports – keyboards, mice, and other peripherals not involving data.

Require Written Approval for Flash Drive Access

Another approach toward USB flash drive control is requiring written approval from the company's IT department to use a flash drive with a company computer.

For example, if access to a flash drive is required, a worker must submit a written request to the company's IT department. The written approval is recorded and then granted if the access meets company requirements. Only then is the flash drive accessed, scanned, and placed in a location on the company network where the worker can access the downloaded data. The reports may be submitted electronically as well, but a written log can be useful in future investigations.

USB Read-Only

If flash drives are deemed to be required for use by a worker, the company may limit the ability of the flash drive to read-only (and not add data). The one-way data path will prevent company data from being saved on the flash drive. However, the flash drive should still be scanned for security risks by the company's IT department before it is used locally on a worker's laptop.

Endpoint Security Protection Plan

All of the company's devices should include an endpoint security protection plan. The plan includes software that automatically scans any device connected to any company device. The software prevents the reading of any data on the device until the scan is complete. This scan can include non-data peripherals as well as they may contain malware or other unwanted software that can find its way onto the company's devices.

Secure Internet for Home Use

Is Your Worker's Home Internet as Safe as the Company's?

In all likelihood – NO.

Typically, a company's network includes a physical firewall device. The firewall prevents unwanted access to the network including unknown sources – only allowing approved sources to pass to the company's network. Nearly all home Internet connections do not include a physical firewall device.

Workers' Internet Connection Should Mirror the Company

What is the point of having a secure computer network within the company's offices when there are so many weak points in worker's home Internet connections? The answer is unfortunate but the company

needs to address the issue by raising the workers' Internet connection to the same level. Hackers are now realizing that the easiest way to

Hackers are Using Workers' Internet Connection as Backdoor to the Company

It is only natural that hackers are using workers' Internet connection to backdoor into the company's network. Many workers have little or no computer experience and therefore rely on their Internet provider to set up their connection. As a result, the level of security for home Internet is levels below that of most companies. However, with many workers accessing the company network from home, it is much easier for hackers to bypass what little security is present via the home connection to extract data or cause other problems (such as ransomware) for the company.

Conduct an Internet Audit of Workers' Connection

The company's IT department should conduct an audit of each worker's Internet connection to determine the level of security present and what is required to bring it to the same level as the company's Internet connection.

Once the audit is complete, corrective action to address the deficiencies must be made. For example, this may include a physical firewall. The wi-fi password may be changed from "password" to a more secure password. An approved anti-virus/malware software package may be installed and/or updated if not present already.

It may not be a low-cost solution to address these issues, but the alternative could be a ransomware attack, computer virus, or other malware infecting the company's network via its own workers' devices.

END PART 2

Dedicated and Secure Home Workspace

Most companies have door locks and security systems. Some have security guards as well. As a result, it is usually not easy to enter a company facility. There are security cameras, visitor log books, even stickers to cover phone cameras. How easy is it for someone to break into a workers' home, vehicle, or other personal space?

Many Workers have Sensitive Information at Home

With so many people working from home, the amount of sensitive, private, secure, and confidential information at workers' home is frightening.

It can be fairly easy to find out a worker's company and position via a simple Google® search or using LinkedIn®. After that it is only another search that can typically provide the worker's home address. It is entirely plausible that someone seeking particular information contained on a worker's laptop (or other physical information such as prototypes, drawings, etc.) could target that worker's house for a burglary.

While this could have occurred before the current situation, it is exponentially more likely now with so many people working from home now and into the future. How often do you hear of cars being broken into and laptops being stolen? Is it possible that that the laptop wasn't stolen for a quick buck but to access the information contained within?

It may be necessary for sensitive information to remain at the office and not be allowed to be brought home, for security reasons. The company should evaluate which information is at a critical level that it must remain on the company premises.

Security Systems for Workers' Homes?

The company should consider providing security systems to safeguard those workers that it deems appropriate to protect (and the information that they have at home). For example, a company vice-

president may have sensitive information at home that is simply necessary for the job and therefore that information should be protected.

It is unfortunate that it has come to this, but providing a security system can be considered a benefit to those workers. If there is an emergency at the worker's home, the company can act as a backup to sending first responders to safeguard the worker and the sensitive information.

There is a Lock on the Company Office – What About the Home Office?

I am sure we have all experienced workers on the job all over the house, poolside, etc. None of these locations appear to be very secure to say the least!

The company should consider requiring a dedicated room in the home to be the office, and that access should be restricted (e.g., a lock on the door). A dedicated office allows for privacy (from the worker's family and guests) and also provides a better work environment.

While this may seem over-reaching, is it really? Is it too much to ask that company business not be conducted in the presence of people who would not be allowed into the company's offices?

It may be difficult for some workers to find such a space given their living arrangements, but it should be encouraged and considered when bringing on new workers.

Bluetooth® Security Concerns

Bluetooth® Devices Not Well Protected

Bluetooth® is a wireless communication system that allows for devices such as keyboards and mice (but also headphones) to send and receive data. Depending upon the situation, that communication of data can be intercepted.

For example, using Bluetooth® headphones in the company's office is a fairly well protected activity because of the company's firewall. However, using the same headphones in a coffee shop is not nearly as well protected an activity because of a lack of a firewall and the proximity to other devices that could intercept the data (voice conversation, etc.) using Bluetooth®.

The use of Bluetooth® devices outside of the company or home office (with firewall) should be carefully considered due to the risk of interception of data. Mobile phones and other devices used outside of the office setting do not have firewall protection and so are vulnerable to hackers.

Public Wi-Fi a No-No

Public Wi-Fi should be avoided at all costs

It may come as no surprise, but public wi-fi is not secure! Typically, a company's wi-fi includes a firewall that prevents unauthorized access of devices. Public wi-fi cannot be counted on to have the same level of security. In fact, it should be assumed that public wi-fi is compromised, and workers should be instructed to never use it.

Public wi-fi can include malware that is then unknowingly deposited onto a worker's device (e.g., laptop). The worker then connects to the company's network and the malware can be spread company-wide. This situation would not have developed if the worker were using wi-fi within the company network.

Public wi-fi can enable hackers to intercept data being sent and received by your worker's laptop without your worker's knowledge. This type of electronic eavesdropping is commonly called a man-in-the-middle attack.

False Positives - Spoofing Authentic Wi-Fi

Another situation is fake public wi-fi. A hacker sets up a wi-fi device and assigns it a name that is similar to or appears to be the public wi-fi of a location. A worker, thinking the wi-fi to be authentic, connects to it and the hacker is provided access to that device and the data that travels between it and the company network. To make matters worse, the hacker can then access the entirety of the worker's laptop with the worker having no idea this activity is occurring. In a matter of moments, the hacker can mirror or completely copy the entire hard drive of the worker's laptop.

The best way to avoid this situation is not to use public wi-fi, ever.

Use Mobile Device as Hotspot Instead

It is now easier than ever to use a mobile device (phone) as a wi-fi hotspot. A worker can avoid the multitude of dangers of using public wi-fi by simply configuring the phone to be a wi-fi hotspot.

Workers should be trained to use their phones as wi-fi hotspots, even at the possible higher cost of data plans for phones. The security benefits that the cellular phone network provides versus public wi-fi make the use of hotspots a much more secure choice.

Third Party Story

Home Worker with No Firewall or Security Software

The following is an example of what could happen to your company if one of your workers does not have a secure home Internet connection.

A home worker, using her own Internet connection, had been processing data for her company. The Internet connection was unprotected by a firewall and the worker's computer did not have any security software to protect it against malware, virus, and other attacks.

The worker received a communication from her company stating that she was terminated, effective immediately. She asked why she was being terminated and she was told she had leaked confidential company information over the Internet. She replied that

Video Conference Security

Is Video Conferencing Safe, or is it the Next Security Breach?

Now more than ever, video conferencing is becoming the default way of doing business when workers are at home. It appears that the for the foreseeable future, a great deal of business will still be conducted outside the office and many workers and companies are migrating to video conferencing software. But is it safe?

There have been concerns raised by those in the IT community that video conferencing services are not safe. There are a number of services currently available, and not wanting to single out a particular one, it is best to use these services sparingly and not for confidential discussions or sharing of information (screen shots).

There have been reports of individuals “crashing” video conferences with the host unable to kick out the intruder. If there are a large number of people in the video conference, can you say that everyone who is there - should be there? This actually happened to me recently. I joined a scheduled conference with the host-provided link. I joined early as is my custom and discovered someone was already there. The other person had no name, only a phone number listed (phone numbers can be spoofed as well). I asked the person who they were and if they were here for the conference call – but received no answer. I tried chatting to reach the person to no effect. I could hear various noises in the background which led me to think that the person had logged in to the video conference and may have stayed connected. In any event, as mentioned above, the host was unable to kick the person out and so had to end the video conference.

Who Operates Video Conference Services?

Regardless of the particular video conference service you may be using, it is a good question to ask. One video conference company may be based overseas, another may be searching the content of the video conference for advertising data, or another may have ties to a government agency. Which one would you prefer have a copy of your last video conference stored forever?

It is naïve to think that any video conference is totally secure and that any information shared is entirely confidential. It is entirely feasible that one or more video conference service has been compromised (knowingly or unknowingly by the service itself) by bad actors, including government intelligence services. It would be wise to consider then, the types of information discussed and presented using video conference services.

Hackers are Probing and Testing Video Conferencing Services

Video conferencing is still a relatively new technology insofar as the companies providing the service and security of their mainframe and cloud computing platforms. Hackers are seeking to probe their weaknesses and exploit those to obtain all sorts of confidential information.

Just as hackers have used email to trick users into clicking and installing malware, viruses, or ransomware on users' computers, the next frontier is video conferencing. Already I have seen reports of fake or spoofed links to video conferences being sent using email to unwitting recipients. People are seeing a link in an email that is formatted in the particular style of a video conference service and they reflexively click on the link (which is not to the video conference site) and bad things happen!

Workers should be cautioned to always verify that a video conference link is authentic. A follow-up email to the host is a simple double-check on the authenticity of the video conference link. Alternatively, an old-fashioned phone call or text to confirm are both good approaches to avoiding spoof video conference links.

END PART 3

Home Document Printing and Shredding

What Happens to All Those Printed Pages?

With so many people working from home, it is natural that they are printing documents in the course of their work. However, there is one big difference from printing at the office and printing at home – secure document destruction.

Many companies already have a system for deposing of documents. Often each desk has a shred bin, or even better, locked community shredding bins that are regularly serviced by a contractor. Workers are by now (hopefully) aware of the need not to simply toss documents in the trash – though common news stores seem to dispel that notion!

What is different in working from home is the need for secure document destruction. Workers need to have a shredding device that is capable of destroying documents at a level comparable to the company office.

Do All of Your Workers Have a Secure Shredder?

While workers may have a shredder, often it is an out-of-date device that generates shreds that can be easily reassembled. In other more frightening cases, workers may not have a shredder at all!

It is very important for the company to stress to its workers that they have a secure, state-of-the-art shredder to use for shredding company documents at home. Company documents no longer needed for work should be immediately destroyed to prevent the accumulation of company documents at a worker's home. This is particularly concerning when or if the worker decides to leave the company, or the company decides to separate from the worker. Which leads to…

Is it Really Necessary to Print Everything?

I've been hearing for years that we are going to a paperless society, but from what I've seen that is far off! Perhaps this situation will accelerate that change.

The company should encourage (or limit, using company devices) a very limited printing of company documents. Editing, comments, and revisions should be made within the document and not on a printed version that then needs to be dealt with securely (destroyed).

While it can be frustrating not having a physical copy of a document, drawing, schematic, or photo in one's hand, any time something is printed is yet another possible security breach that can be more easily avoided – by not enabling it to be printed in the first place!

Email Strings and Reply All

Consider Protocols for Email

Email has been around a long time. You would think that by now people would know the difference between "Reply" and "Reply All" – but they often don't or are too careless to notice! I still get emails with replies that were clearly not for "All" but only for the sender. This is not only embarrassing but also is a possible security risk.

It is certainly possible for email systems to have restrictions put in place to limit Reply All actions, or at least add a dialog box asking the sender to confirm Reply All. Additionally, a company can put controls that can limit recipients to those within the company, or to select customers or other approved recipients.

Another issue I am seeing lately is auto-fill. Many email programs attempt to auto-fill a recipient to an email, and the sender may think that the correct recipient has been selected but in reality, another

recipient with a similar name actually receives the email. Again, a dialog box with a confirmation query to the sender can ensure that only the correct recipient gets the email and any attachments.

Lastly, email strings can be a source of potential security breaches. An email string can extend over many emails and to a widely varied number of recipients, including those whom may not necessarily need to receive all of the information in previous emails. As a result, email strings should be discouraged and if possible, limited within the company's email program.

Virtual Machines

Consider Virtual Machines to Protect Information

A virtual machine (VM) is essentially a program that behaves like a computer. This can be useful in today's environment by putting the security of a company' information back into the company's IT department and not relying as much on the worker's local Internet security.

One way to protect the company's confidential information from hackers and bad actors is to require workers to connect to the company's IT system using VMs. Once connected, the company has more control over the security of the work being conducted (including internal video conferences) and information being exchanged.

In many ways, workers logged into VMs at home are very nearly in the same situation as if they were in the office physically connected to the company's IT systems. Additionally, damage can be limited within the VM if it occurs rather than infecting the entire computer's operating system. By connecting to the company's VM, all users' activity is supervised by the company's IT department (not strictly the case with all VMs, such as those run privately).

To VPN or Not to VPN

Advise Workers to Use Proven VPN

A Virtual Private Network (VPN) protects information by shielding it from interception by hackers and Internet service providers (ISPs). When a worker connects to a VPN, the connection bypasses the ISP's servers and connects directly with the VPN's servers, masks the worker's identity, and through operation of the VPN, makes it much more difficult for hackers and bad actors to intercept that information.

A company would do well do advise workers to use VPNs not only for connecting to the Internet via their computers, but also their other mobile devices – phone and tablets, for example. Using a VPN should be a 24/7 activity to provide the maximum protection for confidential information.

The company IT department should recommend VPNs for workers to use, or work out an arrangement for a particular VPN service to avoid conflicting issues for workers.

A Company VPN Offers Advantages

It is entirely feasible for a company to set up its own VPN, rather than use an outside provider. The company VPN can provide complete encryption of information between the company and its workers, wherever they may be located. This is more important than ever, as companies decide that centralizing workers in one building may not be the most favorable situation going forward. Additionally, a company VPN opens up a secure way to engage workers located in diverse locations that otherwise may not be considered for employment.

A company-specific VPN can allow for the company's IT department to effectively monitor worker activity, such as login and logout time, work conducted, data accessed, websites visited, as well as other information that the company may consider valuable.

Conclusion

There are many potential issues that have become apparent with so many workers conducting business from home. This white paper has attempted to bring many of these issues to light so that they can be addressed by companies and workers to secure their important information, much of it in the form or IP.

While new technology allows for improved accessibility, that accessibility comes with a price – and that is the vulnerability of the new technology to breaches by hackers, bad actors, disgruntled workers, and even through innocent errors by well-meaning workers. It is important for every company, firm, and business to evaluate their particular situation and work with their own IT department or outside IT support provider to make their systems as robust as possible. In many cases, the easier and less-protected targets will be breached first, but high-profile targets will always be in the crosshairs and should be especially vigilant.

It is hope that this white paper causes the reader to pause and consider how to protect their company's valuable IP that may be threatened by the new work-from-home environment that we are currently experiencing and appear to be in for the foreseeable future. Perhaps never before is the world of IP and IT so intertwined than it is at this moment. It is recommended to consult with IP counsel to protect your company's most valuable assets – its ideas.

References

https://www.forbes.com/sites/forbestechcouncil/2018/11/15/what-is-a-business-vpn-and-how-can-it-secure-your-company/#66e3476863a5

https://us.norton.com/internetsecurity-privacy-safe-vpn.html

https://blog.mailfence.com/virtual-machine/

https://www.makeuseof.com/tag/virtual-machine-makeuseof-explains/

https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html

https://www.pcmag.com/news/do-you-need-a-personal-firewall

https://www.zdnet.com/article/working-from-home-cybersecurity-tips-for-remote-workers/

www.bloomberg.com

https://www.consumer.ftc.gov/blog/2020/03/online-security-tips-working-home

https://www.forbes.com/sites/carrierubinstein/2020/04/10/beware-remote-work-involves-these-3-cyber-security-risks/#1ca76a1861c4

https://www.cnn.com/2020/03/20/tech/telework-security/index.html

https://www.entrepreneur.com/article/348346