Remote Workforce Security Tips & Best Practices

By Tim Bandos on October 14th, 2020 | 0 Comments

18 security pros share their top tips and best practices for securing a remote workforce.

With more companies working with geographically distributed teams today, more employees are working remotely than ever before. Remote work has become a security challenge for organizations. Because employees are not physically working on-site, they're often relying on their own Wi-Fi networks and devices to conduct company tasks.

To mitigate security risks, companies must implement clear and comprehensive policies and best practices relevant to the entire workforce. Cybersecurity pros are the ones tasked to gain some insight into the strategies and best practice today's companies can implement for adequate security when working remotely. Recently, I interviewed a dozen of my colleagues in the cybersecurity profession and asked them to answer a question:

"WHAT ARE THE BEST PRACTICES FOR SECURING YOUR REMOTE WORKFORCE?"

MEET OUR PANEL OF SECURITY PROS:

- Cristian Rennella
- Marcus Harris
- Abhishek Shankar
- Tim Bandos
- Andy Grady
- Andy Jordan
- Jon Hayes
- Michael Pauzenberger
- Michael Tarazevits
- Joseph Robinson
- Andy Green
- Ian McCarthy
- Nate Masterson
- Pertty Gonzalez
- Steve Pritchard
- Dave Nevogt
- Joseph Robison
- Dr. Steve Lloyd

Read on to learn what our experts had to say about the best practices you should be implementing to ensure security when working with a remote workforce.

CRISTIAN RENNELLA

@cyberrenella

Cristian Rennella is the CTO and Co-Founder of eWalletPass-Tools.com.

"Prior 8 years of work and having gone from zero to 15k remote employees, I can assure you that the best practice is having a well-defined and well-communicated policy."

Two factor authentication. With 0%, each time one of our employees wants to enter our system they MUST not only enter their personal password (at least 16 characters including numbers and symbols) but we will also send a code to their cell phone to authorize the access.

We implemented 2FA just few months ago, and thanks to it we have been able to reduce security incidents to almost 0. Our IT department, before 2FA, was the reason why I strongly recommend to implement it as soon as possible.

MARCUS HARRIS

@CISSyer

Marcus Harris is a Director, Cybersecurity Consultant at Tech Solutions & Holdings LLC and the author of the blog Cybersecurity Ninja.

"The best ways to secure your remote workforce are..."

1. Be Wary Of Allowing Employees To Bring Their Own Devices

For the sake of simplicity, I'm just talking about the storage of company information and trade secrets. Information is enterprise. Without the proper policies in place, employees will have very little control of information. Most of the time, it is not even their information to control. It belongs to the company.

2. Have A Policy In Place

To avoid unfortunate disciplinary and legal issues, companies with remote workers need to have a policy in place that clearly states what is and is not acceptable. Employees need to understand what is considered "work" and what data/information is valid, invalid, or illegal to get, share, and may compromise the protection of intellectual property.

3. Use Application To Monitor Data Usage

It makes sense to use technology that manages and monitors data transfers and minimizes the risk of employees using their company-issued technology for personal use. Employees need to be held accountable daily and work ethically. They do this by utilizing applications that are controlled by the employer and alpha the whole functionality to the application the employee leaves the company.

ABHISHEK SHANKAR

@theabhisheksh

Abhishek Shankar is the Chief CISO of Skyline. Skyline is a skilled workforce platform designed built on Blockchain.

"So working practices become more casual, comfortable, and collaborative."

Organizations need to lighten their belts to ensure data security with measures such as:

1) Endpoint security using Cloud Access Security Broker (CASB) and web-based storage software that allows sharing and editing of documents (for example, Dropbox Cloudbox)

2) Network security using Secure Access Service Edge (SASE)

3) Endpoint security using Endpoint Detection and Response (EDR). This adds a second level of security to improve endpoint security. Endpoint security is a cybersecurity approach that protects endpoints, such as laptops, mobile devices, USB drives, smart cards, and many more advanced security technologies.

Other security measures include Virtual Private Network (VPN), Multi-factor authentication, Anti-Phishing, Anti-Malware, etc. These are several well and forgot email encryption tools on the market. These systems defend and protect the data, information, and trade secrets of the company.

To be connection is allowed with public WiFi:

1) Contingency plan for risk management: If remote worker loses a laptop with sensitive business information on it, it's essential that the laptop can either be tracked or remotely deleted.

TIM BANDOS

@timbandos

Tim Bandos, CISSP, CISA is Vice President of Cybersecurity at Digital Guardian. He has over 15 years of experience in IT and information security with a heavy focus in financial services, incident response, and threat intelligence.

"Three of the best ways to secure a remote workforce are..."

Implement Network Policy

Typically, when it comes to securing your telecommuters, the first item on the agenda is developing a network policy. Ensure that your network policy addresses the use of personal devices, how data is stored, and how data is transmitted. Remote workers are probably not familiar with these decisions as we have been days depending on the type of devices being used for telecommuting (in Company issued, Personal Computer owned, or Company owned but employee shared) or the type of devices that aren't issued specifically by the company.

Implement Remote Connectivity

Any connection made to the company should be performed through a VPN (Virtual Private Network) or Single Sign-On. Secure business cases for remote access, and ensure that all remote connections are communications from the remote telecommuter's machine, depending on various requirements. This both safeguards data in transit along with the corporate environment to ensure no pivots adversaries are snooping in between.

Implement Backup Policy

Installing an endpoint agent into the ability to perform 0 days protection (0 malware protection will provide greater assurance into securing the endpoint especially if corporate data is allowed to reside on the machine.

ANDY GRAY

@Andy_Jordan

Andy Gray is the Principal Consultant at Pen Bagels. Andy's experience lies in penetration testing, application security, and cryptography. He is also one of the co-organizers of Pen Bagels.

"Use VPN access and ensure that they have multiple projects at the same time..."

Some of our developers work from home a week regularly, so it's been important that we have a centralized system in place with supporting tools that allow remote work without disruption. We have a VPN that allows access to our internal resources, and we use Slack for chat, Google Docs for collaborative work during the day-to-day and Google Hangouts for conferencing. Although this wasn't planned at Tesla, a team collaboration site. This way, every member of the team can see what their teammates are working on, and it helps to keep the project moving forward. Jira is a great tool for this, Google Docs, Confluence, and Trello that allow for easy communication, sharing, and automation. Security is an afterthought for most of these tools, so we have to be careful with what we share and who we share it with because that opens up a lot of risk. Tesla's VPN. These tools are the culture of video calls keeps the team engaged, connected, and informed.

ANDY JORDAN

@theandyJ0

Andy Jordan is the Special Project Lead at Stream411.

"Hacking remotely itself is not dangerous."

Use of strong passwords and multi-factor authentication combined by an organization coupled with the actions of the remote employee that matched the risks into very real dangers. Consequences of remote working are not the same as working in the office, and the risks are not the same. Remote employees need to understand the risks associated with their actions and the impact of their actions on their communications without working remotely is a combination of technical and procedural controls combined with proper employee training and awareness.

When a business decides to employ a wireless network to accommodate remote employees, they will need to implement a strong encryption method. Most of the time, the default encryption wireless network is like playing an open Ethernet port on your front lawn. Depending upon the methods implemented, the wireless network is easy to hack or difficult to hack. Hackers can use a wireless monitoring to active device of services attacks and everything in between, the dangers of wireless networks are well documented. Hackers can use the wireless network to pivot into the corporate network.

Selecting the proper wireless security standard that is proportionate to the current and future projected value of the business data and the cost of implementing the security standard will have a very positive effect on wireless security. Providing resources for the education and training of the IT staff and the employees working remotely will greatly increase security and reduce risk. Hackers will still identify the rules associated with wireless networks along with proving them the skills required to circumvent the security and gain access to the wireless network.

Performing internal audits and third-party penetration testing of the wireless network will aid in determining the security posture of the wireless network and identifying vulnerabilities and risks, as well as providing a fresh set of eyes by wireless professionals experienced in detecting misconfigurations and vulnerabilities. Hiring a third-party penetration testing company to perform a black box wireless penetration test and comparing the results against the previous internal audit will provide a baseline of overall employee wireless security policy that is enforced, will only serve to enhance the company's overall security posture.

JON HAYES

Jon Hayes works with Pixel Privacy.

"When dealing with a remote workforce, the important thing to understand is that there will always be risks involved..."

The big thing is mitigate those risks as much as possible by ensuring robust measures are in place.

The first thing you should do is get your remote workforce's hands on secure data and personal data. Companies should provide their employees with a secure way to do their work. Companies should provide their employees with a secure way to do their work. Companies should also make personal accounts for work-related duties. For example, if writing an article, this shouldn't be stored in their own personal Google Drive account. Instead, it should be stored in a Google Drive account that belongs to your workforce, you'd usually have absolute control over data that's your same panel. For security reasons, it's important to have access to data in case an employee leaves the company, or worse, they decide to delete the sensitive data.

I would also highly consider investing in a password manager such as LastPass for business. Each time employees need to access a password, they can simply log into their account and get the login details. If your staff follow the strictest of protocols, there's nothing to say the software you're using to communicate with your team isn't hacked and compromised. Password managers are highly susceptible to this also, but by confining it to one single tool, you can drastically reduce the number of times a password is shared, lost, or stolen.

Finally, I strongly urge simple security training. It's easy to forget just how easy it can be to lose personal data, and it's easy to forget just how important it is to keep it safe. Training should be fun, and it's something as simple as accidentally leaving your computer unlocked while you take a bathroom break that can make data your sensitive data accessible to others.

MICHAEL PAUZENBERG

@mikeyauzenberg

Michael Pauzenberg is chief research officer at ID Crowd. He served as senior advisor at IOC for a decade, before joining ID Crowd as their resident expert in cybersecurity. He also is a contributor to Forbes, including on Cybersecurity.

"With cyber-threats ranging from network hacking to ransomware..."

Remote working with a remote workforce, presents a number of potential risks to reputation, to competitive advantage, and financially for violations of an every growing body of privacy protection laws around the world. The practical risks are that the data that is being accessed by remote workers outside of its employer data is particularly high. It's hard enough to protect your business using the best security measures when you are working in an office, let alone remotely.

There are several best practices for remote workforces using other WFH networks, including:

- Ensure employees are using strong passwords. Make them long, complex, protected and carefully managed.
- Ensure that they are using a VPN, and ideally Cloud-based VPN protection, use the best available at the time, which is MFA at present. You can increase the protection more by also using Cloud Transport Layer Security (TLS) to encrypt your email communications.
- Turn off WiFi protected setup (WPS) to prevent bad actors from using it to breach your network connection.
- Do not allow employees to use non-company provided networking access points and hot spots.
- If you have the IT budget and resources, have dedicated laptops for the work at home.
- Segregate your WFH from the core network also, by using a firewall.

ANDREW BANYON

@AndrewBanyonJ

Andrew Banyon came to Trustpair with more than 15 years of experience in marketing, operations, and consulting. Most recently, Andrew was the Head of Strategy Office of Companies Listening development at Thomson Reuters, an information technology and services company with more than 50,000 employees.

"Some of the best practices to secure your remote workforce include..."

1. Implement Multi-Factor Authentication

Multi-factor authentication is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction. Multi-factor authentication combines two or more independent credentials: what the user knows, such as a password or a personal identification number (PIN); what the user has, such as a smartphone or a smart card; and what the user is, such as a biometric feature. Multi-factor authentication is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.

2. Encrypt Your Data

Encrypt your data. Encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Ideally, an authorized recipient can decrypt the ciphertext back to the original, intelligible form. Encryption is not a new technology, but it is a very important one. Encryption is a security measure that protects data at rest and data in transit. Encryption is a security measure that protects data at rest and data in transit.

3. Use Secure Wi-Fi

Secure your Wi-Fi. Wi-Fi is a wireless technology that allows devices to connect to the internet. Wi-Fi is a wireless technology that allows devices to connect to the internet. Wi-Fi is a wireless technology that allows devices to connect to the internet. Wi-Fi is a wireless technology that allows devices to connect to the internet.

4. Use Secure Cloud Storage

Use secure cloud storage. Cloud storage is a service that allows users to store files online so that they can be accessed from any location, such as the Internet. Most cloud storage providers offer some form of encryption, but it is important to ensure that the provider uses strong encryption and that the encryption keys are managed securely. Cloud storage is a service that allows users to store files online so that they can be accessed from any location, such as the Internet. Most cloud storage providers offer some form of encryption, but it is important to ensure that the provider uses strong encryption and that the encryption keys are managed securely. Cloud storage is a service that allows users to store files online so that they can be accessed from any location, such as the Internet. Most cloud storage providers offer some form of encryption, but it is important to ensure that the provider uses strong encryption and that the encryption keys are managed securely.

5. Use Secure Email

Use secure email. Email is a service that allows users to send and receive messages electronically. Email is a service that allows users to send and receive messages electronically. Email is a service that allows users to send and receive messages electronically. Email is a service that allows users to send and receive messages electronically.

6. Use Secure Messaging

Use secure messaging. Messaging is a service that allows users to send and receive messages electronically. Messaging is a service that allows users to send and receive messages electronically. Messaging is a service that allows users to send and receive messages electronically. Messaging is a service that allows users to send and receive messages electronically.

7. Use Secure Video Conferencing

Use secure video conferencing. Video conferencing is a service that allows users to see and hear each other in real time. Video conferencing is a service that allows users to see and hear each other in real time. Video conferencing is a service that allows users to see and hear each other in real time. Video conferencing is a service that allows users to see and hear each other in real time.

8. Use Secure Collaboration

Use secure collaboration. Collaboration is a service that allows users to work together on a project. Collaboration is a service that allows users to work together on a project. Collaboration is a service that allows users to work together on a project. Collaboration is a service that allows users to work together on a project.

9. Use Secure Mobile Devices

Use secure mobile devices. Mobile devices are small, portable computers that can be used for a variety of purposes. Mobile devices are small, portable computers that can be used for a variety of purposes. Mobile devices are small, portable computers that can be used for a variety of purposes. Mobile devices are small, portable computers that can be used for a variety of purposes.

10. Use Secure Wearables

Use secure wearables. Wearables are electronic devices that can be worn on the body. Wearables are electronic devices that can be worn on the body. Wearables are electronic devices that can be worn on the body. Wearables are electronic devices that can be worn on the body.

IAN MCCALLRY

@idahacker

Ian McCallry hands on IAM from Thycotic/Centrify Director of Global Alliances. He is also the Director of Strategic Partnerships at Thycotic/Centrify and the Vice President of Information Industry Currently he is the CEO and President of PhoenixIAM.com and Ian-McCallry.com.

"In comes down to the kind of work are they doing for you..."

Companies need to be able to work with their IT security departments as to how their remote work environments need to be set up. Things like the employee should not be having a door or window where others can see what they are doing, etc. From a lens view.

- Have an MDM on the employee their pc
- Enforce encryption and use a secure encrypted flashdrive
- Implement a VDI or Citrix environment with Multi-factor Authentication such as DUO, use CASB for access to SaS and on-prem apps.
- Use a VPN to connect to the office, use RDP Profile or Citrix based solution in a shared application mode.
- Do not give them elevated privileges on their machine.
- Lockdown all ports – no USB, etc. unless necessary.
- Have an automatic check-in process where if not checked in, or "in" timeframe, you'll auto-wipe the machine.

NATE MASTERSON

@thegadgetnerd

Nate Masterson is the Financial Manager for Maple Holistics, a company focused on natural and healthy products. Nate's passion for holistic and alternative medicine in Tacoma, Nate has been able to promote a healthier lifestyle for his family and community while also becoming a leader in e-commerce.

"There are many benefits to assembling a remote workforce as an employer..."

Cybersecurity is a major concern for companies with remote workforces. Employees working from home is exceptional for starters, most employees view working from home as a privilege, so they are going to be more productive and more motivated to keep the business running. Another benefit is that the office dynamic is cut to a minimum because everyone has enough space to breathe. But how do you ensure that your remote employees are secure and not a risk to your business?

Virtual private networks or VPNs are networks that extend across public lanes to connect multiple users and locations. Implementing a VPN is an inexpensive but powerful way to protect your office data. Most global and employees who work from home in general, private networks tell three of a lot of should be enough to keep your business safe. Another way to keep your business safe is to use a VPN. Most of the mobile work environment is starting to be changing all its exponential pace. VPNs are a must-have.

PERTTU GONZALEZ

@PerttuGonzalez

Perttu Gonzalez is a Finnish entrepreneur and is the CEO and co-founder of Nordic Business Information, a company that helps companies find and analyze business information. Gonzalez has been a serial entrepreneur and building Finnish tech companies for more than a decade. The leading Google Apps Partner in Finland.

"Weaker communications apps are quite common in remote workforces..."

Weaker mass-messaging apps are quite common in remote workforces. Employees use apps for sharing knowledge, information, and sometimes even company confidential information. Without proper security measures, this information could be easily accessed by third-party companies or even hackers. Instead of using such apps, companies should provide their employees with secure, encrypted, and accessible working system in a place to share non-confidential documents, knowledge, sharing, and collaboration. If your company has colleagues are searching for, there will be new, reliance on their own platform usage.

STEVE PRITCHARD

@stevepritchard

Steve Pritchard is an IT Consultant for Africa Travel.

"Be sure to encrypt all emails, which are often the first target for cyber-attackers."

Secure computing details are revealed daily, and video reveal of a new trend is not far-fetch, you should have seen that coming.

This is especially important if your remote workforce includes the likes of customer service employees, who are responsible for sharing sensitive information with customers. Ensure that your IT department is up to date on the latest threats and that it is able to provide adequate protection against them. Remote workers are more susceptible to cyber-attacks than office based employees, because they are working in a distributed manner and will start to slack.

Encrypting all emails is important, so that the content is disguised, and is not picked up, sensitive information that may transpire during an email conversation and only the intended recipient will be able to see it.

DAVE NEVOGT

@nodata47

Dave Nevogt is a cybersecurity veteran Indian corporate, and is the co-founder and lead current CEO of Hubstaff. Dave tracking software for freelancers, remote teams, and any other company.

"Securing your remote workforce can be a challenge..."

Especially when your team is using their own personal devices from locations around the world. A few ways to secure your remote workforce are to implement a password manager, multi-factor authentication, and VPN. Password managers make the passwords an impossible to crack long and complex and random. This is very important, because if one password is lost, they can easily reset without device theft using access to company documents and email or projects.

DR. GENE LLOYD

@DrGeneRNewsCNC

Dr. Gene Lloyd is the President of Lloyd Research Institute.

"Anyone who works remotely should be..."

Utilizing different encryption methods to keep organizational data and communications secure. Encrypt all data, communications, and transmissions between employees and their company's information systems. Encrypt all hard drives, flash drives, and other storage devices and remain up-to-date. Keep updated and easy to adapt on Apple and Android mobile devices, as well as laptops, and system administrators should be able to remotely wipe data from devices if they are lost or stolen. Encrypt all data and communications that may transpire during an email conversation and only the intended recipient will be able to see it.

JOSEPH ROBISON

@JosephRobison

Joseph Robison is the Founder & Chief Consultant of Green Flag Digital.

"I offer digital consulting to clients remotely and have a fully remote team. Here's what I've found worked for us so far..."

Utilizing different encryption methods to keep organizational data and communications secure. Encrypt all data, communications, and transmissions between employees and their company's information systems. Encrypt all hard drives, flash drives, and other storage devices and remain up-to-date. Keep updated and easy to adapt on Apple and Android mobile devices, as well as laptops, and system administrators should be able to remotely wipe data from devices if they are lost or stolen. Encrypt all data and communications that may transpire during an email conversation and only the intended recipient will be able to see it.

Utilizing different encryption methods to keep organizational data and communications secure. Encrypt all data, communications, and transmissions between employees and their company's information systems. Encrypt all hard drives, flash drives, and other storage devices and remain up-to-date. Keep updated and easy to adapt on Apple and Android mobile devices, as well as laptops, and system administrators should be able to remotely wipe data from devices if they are lost or stolen. Encrypt all data and communications that may transpire during an email conversation and only the intended recipient will be able to see it.

Joseph Robison JOSEPH ROBISON
@JosephRobison

1) Encrypted password management

As a remote team, you need to share logins for scores of sites. While tempting to send passwords via email, we all know that's not secure. LastPass has an encrypted password management system that makes password sharing among teams very easy. You simply share individual passwords with team members and they don't ever see the actual password. If any team member leaves, you're good to go.

2) VPNs

If your remote team is spread throughout the world, it's hard to manage which ISPs their internet traffic is running through and what the security level is. VPNs mask IP addresses and make locations untraceable, a must for your remote team.

Tags: **Data Protection**, **Cloud Security**, **BYOD Security**

RECOMMENDED RESOURCES

WEBINARS

The Incident Responder's Field Guide: Lessons from a Fortune 100 Incident Responder

VIEW NOW

WHITEPAPER

Digital Guardian Technical Overview

DOWNLOAD NOW

ANALYST REPORTS

Gartner DLP Magic Quadrant

GET THE REPORT NOW

ELLEN ZHANG

Ellen is the Acquisition Marketing Manager at Digital Guardian, with nearly half a decade of experience in the cybersecurity industry. As the company's SEO and PPC manager, Ellen has spent numerous hours researching information security topics and headlines.

Related Blog Posts

Friday Five: 12/7 Edition
Chris Brook

Former Google, Uber Engineer Hit With Trade Secret Theft Charges
Chris Brook

Drones Enable Man-in-the-Middle Attacks 30 Stories Up
Robert Vamosi

0 Comments digitalguardian Disqus' Privacy Policy 1 Login

Recommend Tweet Share Sort by Best

Start the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

Be the first to comment.

©Digital Guardian All rights reserved.