ACTIVE CYPHER™

Microsoft Silver Partner

Cybersecurity For Remote Workers

A data-centric approach to securing data in the era of accelerated remote work.

Reference Guide

Version 1.5, March 2020

Introduction

Since being discovered in late 2019, the novel coronavirus (known as COVID-19) has sadly killed thousands and disrupted much of the world economy. Travel bans are spreading, major world events are cancelled, and a slew of companies are increasingly telling their employees to "stay home".

Yet as more workers operate remotely, IT departments are struggling to ensure the same levels of cybersecurity the office usually provides. It is becoming clear that the economic ramifications of COVID-19 may also appear on a secondary front as hackers take advantage of the increased utilization of personal devices, lack of secure Wi-Fi, amongst other blaring vulnerabilities.

We hope this document can help guide your decisions as you and your firm face the prospect of prolongated remote work and its effects on data security.

1. Understanding new cyberthreats

“What already was a monumental task just became 10x harder…,” *Mike Quinn*

Chief Strategy Officer, Active Cypher

Prompted by the rise of the novel coronavirus (COVID-19), government entities, educational institutions, and corporations alike are shifting quickly to the remote workplace. While the creation and adoption of cloud computing has enabled the remote workplace to scale rapidly from a technical point of view, cybersecurity infrastructures remain porous to intrusion, misuse, and data loss.

The stresses on IT departments as large portions of their firm suddenly go remote, will also contribute to security lapses as attention is diverted from the monitoring and prevention of threats to the setting up of loaner laptops, connecting new machines to home printers, resolving longstanding Wi-Fi issues, and painstakingly dealing with the technologically challenged. In effect, the sudden jump in remote work has opened a Pandora’s box for IT professionals, as every employee’s home network, becomes a potential support ticket nightmare and an unknown vulnerability.

In order to prepare their companies for remote work, IT leaders must quickly take steps to secure their data end-to-end. VPNs, if not already utilized, should be immediately deployed along with password managers. Perhaps more importantly, data should be secured at the file level as both a first and last line of defense. “Securing all home offices and ensuring employees maintain compliance with security practices will undoubtedly be difficult. What already was a monumental task just became 10x harder,” Mike Quinn, Chief Strategy Officer of Active Cypher, explains. “We formed Active Cypher with the strong belief that data security is a social right. Obviously, the exposure of data created by remote work greatly perturbs us.”

Discover More

Securing Data & Unknown Endpoints

From securing various Wi-Fi connections to encrypting data, IT departments need to rapidly discover, evaluate, and secure their remote workers’ endpoints.

Training For The Remote

Tensions are high. Minds are on other things. Unfortunately, remote workers will continue to make mistakes (if not even more). A good first step is ensuring all work files stay on work computers.

Compliance in the Distributed Workforce Era

Your colleagues may be in their PJs, but consumer privacy data laws still remain in full force. Remote work won’t be an excuse for lax data security.

2. Securing Remote Wi-Fi

IT departments worldwide should immediately focus on providing comprehensive data security from day 1.

One of the first considerations is checking if a teleworker's connections to the internet is secure. An obvious difficulty is that IT professionals are unable to physically check what routers (and other hardware) are in place and whether or not remoter workers follow security protocols.

Avoid Public Wi-Fi

Public Wi-Fi networks pose a massive risk as convenience is traded for security. Remote workers need to be reminded of the dangers of public Wi-Fi where malicious actors can easily prey on open networks. When connected to a public Wi-Fi network, traffic between the negligent user and their coworkers, clients, etc. can be monitored by hackers.

Secure Home Networks

Remote workers should be advised to secure their home Wi-Fi by ensuring their network is password-protected (some people surprisingly still don't employ this simple way of protecting their networks). Passwords should be complex, with a minimum of 12-14 characters in length and include $ymbol$, CAPS, lowercase, and numb3rs. Words found in a dictionary should be avoided along with substitutions (like p4ssw0rd). Brute force attacks can easily prey on weak passwords. A complex password is a strict minimum.

Encourage Personal Hotspots

Vulnerabilties will still exist, particularly between the user's hotspot and destination, but the risk of being hacked by another user on the same open public Wi-Fi network is remediated. 4G and 5G internet speeds are typically almost as fast as regular home networks.

A Good VPN is Worth Every Penny

Virtual private networks (VPN) provide remote workers with a safe internet experience by obfuscating IP addresses, increasing privacy, and encrypting internet activity. While the majority of Fortune 500 companies already utilize VPNs, remote workers will need to use them on ALL devices being used for business affairs.

Secure the Actual Data

Regardless of a network's security, attacks will happen and firewalls will be breached. Data should be tracked and encrypted at the file level. Disk encryption is not effective enough as remote data around too many different endpoints (including likely unsecure personal computers and phones for printing/ease).

ACTIVE CYPHER™

Now that data is everywhere. How are you securing it?

3. Securing Remote Data

Remote Data Protection Checklist

- [ ] IS YOUR DATA STORED / BACKED UP IN THE CLOUD?
- [ ] ARE YOU ENCRYPTING ALL YOUR DATA?
- [ ] IS THIS ENCRYPTION PROCESS AUTOMATIC? (NO USER INTERACTION)
- [ ] IS DATA ACCESS PERMISSIONED VIA ACTIVE DIRECTORY?
- [ ] DO YOU HAVE THE ABILITY TO TRACK YOUR DATA?
- [ ] DO YOU HAVE AUDITABLE TOOLS TO MAINTAIN COMPLIANCE (GDPR, CCPA, HIPAA, PCI)?

Zero Trust: the New Standard

The remote workforce and cloud applications have fundamentally redefined the security perimeter. Important files are frequently shared with external agents such as partners, consultants, vendors, and other outsiders, creating a serious risk to the company. Implementing a zero-trust security model has never been more important.

Lifehack: Encrypt all the data

IT Leaders must realize that notwithstanding the best cybersecurity training and strongest firewalls, remote security infrastructures will have unique vulnerabilities and data breaches will occur. Data therefore should be made to fight and defend itself. Data encryption is the answer.

A Solution to Consider: Active Cypher File Fortress

Active Cypher File Fortress uniquely provides end-to-end file encryption permissioned by Active Directory. Active Cypher utilizes a combination of cypher-block and bit-shifting, permutation algorithms to create quantum-resilient encryption which automatically encrypts data at the file level. This identity-centric file encryption prevents unauthorized access to files no matter where they are stored or moved in the remote environment.

Create a Secure Private Cloud

Leveraging deep integration with Azure and Active Directory, File Fortress deploys your own secure private cloud, synchronizing with Office 365 and Azure Active Directory cloud services. File Fortress requires no additional management, nor the knowledge and exchange of keys, certificates, passwords, or secrets.

Zero Trust Just Got Real

Never trust; always verify. Do you really trust the entire workforce to comply with security protocols now that they are not physically in the office? Identity-centric attributes obtained from Azure Active Directory metadata are constantly evaluated by Active Cypher File Fortress with risk-based escalations. Artificial Intelligence (AI) driven threat protection and incident response prevents the spread of breaches inside any data center and cloud.

4. Training For Remote

Responsibility for Company Data

- Beyond the confines of an organization's walls, with its nearby IT support and tech-savvy colleagues to help, the frustration of some employees may lead to major gaps in security.
- Companies should, unfortunately, expect an increase of non-compliant activities, including the use of personal devices and lapses in the proper classification of sensitive data. "When the cat's away, the mice will play (and not follow security protocols)," says Active Cypher's President, Greg Morrell.
- IT leaders should emphasize to their coworkers that everyone has a shared responsibility when protecting company data. Data security isn't something for the "back office" to handle.

Address New Threats

- Awareness of physical security of laptops, phones, etc. also important. For many, the 2019-2020 COVID-19 outbreak period of remote work will be their first.
- Working with sensitive data in close proximity to neighbors, roommates, and family leave open the door for "wandering eyes". More private home workspaces should be encouraged, whenever possible. Devices should be always logged out or password-locked when not in use.
- Kids want to surf the web with mommy's or daddy's computer? Not acceptable. Malicious software from unknown sources (e.g., a free gaming site) could be accidently downloaded, infecting the network, and leading to ransomware attacks and/or data loss. Corporate-set screensaver lock outs help to ensure the security of work devices.

KEY POINTS

Company Data? Company Computer!

- Perhaps the greatest immediate risk from a rise in remote work is that more personal devices will be used. Whether it's out of ease or negligence, remote workers will undoubtedly use their home computers to conduct corporate affairs. Company guidelines need to be clearly shared.
- Work computers are backed by IT teams who block malicious sites, instalregular security updates, automatically set screensaver lock outs, and run antivirus scans. The introduction of personal computers to a work environment creates a massive weak point – inviting hackers to take advantage of the situation.

Remind & Refresh

- Remote workers should be aware that their digital actions outside the office are even more impactful then when taken in the office. Refresher courses are essential.
- From reminders of social media policies to safe browsing rules, remote employees should understand that such guidelines are not primarily there to increase worker efficiency, but protect the company's network.
- Another responsible email usage course? Yes. That tempting link is still as dangerous. For example, just recently, North Korean hackers have been utilizing the COVID-19 crisis in spearphising attacks.

5. Compliance in the Distributed Workforce Era

Government's around the world have made a clear message: consumer data is private and needs to remain that way. It's up to companies to encrypt and protect data regardless of the vulnerability of their remote workforce.

With consumer privacy laws such as the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), which came into effect January 1, 2020, economic consequences of data loss will be compounded. Last year alone, European data protection authorities enforcing GDPR fined Marriott International $110 million and Google $50 million. While those amounts may be a drop in the bucket for large corporations, they are burdensome for smaller companies. Expect more breaches and fines to come.

Personal Information Protection and Electronic Documents Act (PIPEDA) (2000)

Federal Data Protection Law (2000)

Personal Information Protection Act (PIPA) (2011)

Personal Data Protection Act (PDPA 2012)

The Privacy Protection Act (PPA) (2017)

General Data Protection Regulation (GDPR) (2016)

Australia Privacy Principles (2014)

Protection of Personal Information Act(POPI) (2013)

Personal Data Protection Bill (2018)

Personal Information Security Specification (2018)

California Consumer Privacy Act (CCPA) (2018)

General Data Privacy Law (2019)

6. Remote Work User Case with Active Cypher

*"As this all came out of the blue, we needed an effective solution deployed immediately to all users. Active Cypher's default comprehensive data protection provided us with a path towards business continuity. Frankly, it was a no brainer."- CTO*of Active Cypher Client*

*We respect the sensitive nature of cybersecurity and therefore do not divulge our clients' identities publicly. References are provided on request to verified professionals.

Batten down the hatches!

Faced with its entire worldwide workforce being required to go remote overnight, our client (a publicly traded financial firm) needed a fast-track option to ensure its data was secure.

Turn-key deployment of AIP

Avoiding months of classification, our client was able to deploy and encrypt all their files within an afternoon and begin taking advantage of many of the advanced features of both Microsoft Security and Active Cypher. No additional servers, infrastructure, API's or synchronization tasks were required.

Immediate Compliance

Faced with increasing regulatory demands, our client achieved CCPA and GDPR compliance with Active Cypher. Our security solution's comprehensive approach ensures all important files are automatically encrypted.

Business As Usual

Our client wanted to avoid any disruption to their business. Functionality was to remain the same and zero-latency was a high priority. Active Cypher delivered on all these fronts.

Contact

Address

3188 Airway Ave. Costa Mesa, California, 92626

Phone

+1 (714)–477–1045

Media

operations@ActiveCypher.com

www.ActiveCypher.com

Microsoft Silver Partner