Cybriant
strategic. adaptive. resilient.

Here's How We Are Securing Our Remote Workers.

How to Keep Corporate Data and Remote Workers' Data Safe During the COVID-19 Global Pandemic.

WELCOME

ANDREW HAMILTON

CTO, CYBRIANT

Andrew Hamilton is a member of the executive management team of Cybriant, a leader in the cybersecurity services industry. As CTO he is responsible for the technical vision and the delivery of services at Cybriant. Since its founding in 2015, Andrew has led the selection, evaluation, and adoption of all security technology and tools utilized by Cybriant in the delivery of its managed security services.

Cybriant

strategic. adaptive. resilient.

2020: AN UNPRECEDENTED TIME

In a unique time in our lives, more and more workers are being asked to work from home because of COVID-19 or the Coronavirus.

It's important for everyone to take an abundance of precautions during this time. However, if your corporate cybersecurity policy is not in place, this could cause security concerns that could be detrimental to your business.

Here are the steps Cybriant recommends to secure your business. And this is how we are securing ours.

PERSONAL DEVICES

Nation-State hackers may not be targeting your employees' home networks.

Then again, they may be.

It's safer for your employees to assume their accounts and devices could be targeted and compromised. **Therefore, remote workers need to be prepared to play defense**. There's no need to panic, but instead proceed in a methodical manner.

The following steps are not ultimately exhaustive, and there could be situations for which I haven't accounted.

However, these steps are the things I would personally do as a security professional were I suspicious of being compromised.

DEVICE RECOMMENDATIONS

/01 Disable any browser extensions.

There are instructions for how to do this for Firefox, Chrome, and Internet Explorer. Another option would be to simply download a different browser. Always used Internet Explorer? Download Chrome or Firefox for the following steps.

/02 Check your personal email account for devices you don't recognize.

- If you have Gmail, you can do that by following the information in the following link: https://support.google.com/mail/answer/45938?hl=en
- Log out any unrecognized devices.
- If you don't recognize any of them be sure to log all of them out.

/03 Enable multifactor factor authentication on your email address.

Perform Step 2 again. **Here's why:** This time you should only see your current device as the only device logged in. If there are any other devices logged in, it means that someone else logged into your account while you were enabling multifactor authentication.

/04 Sign Up for a password manager (we like LastPass).

- Create a complex password.
- Memorize it.
- Put it in a safe. DON'T LOSE IT!!! **Here's why:** If you lose your password manager password you lose ALL of your stored passwords.
- By the same token, if you're still trying to memorize passwords for the websites you visit, I can guarantee you're reusing passwords. So, when your favorite website is cracked, the hacker now has access to any other site you used that password on (and yes, this is true if you use variations like adding a "1" at the end of your password.)

DEVICE RECOMMENDATIONS

/05 **Change your email password using the password manager to generate the password for you. It should be complex.**

It's always good to have a backup email account where a recovery password can be sent.

/06 **Be sure that you can log back into your email account with the new password with no problems.**

/07 **Enable multifactor authentication on your password manager.**

/08 **Sign up for email monitoring (free service) at https://haveibeenpwned.com/**

/09 **Go through every account that has been shown to be compromised on https://haveibeenpwned.com.**

Immediately change the password with a password from your password manager.

/10 **Go through all of your other sites and update your passwords using passwords generated from the password manager.**

Yes, this will take a while. I suggest grabbing a beer and putting on some Netflix in the background to make the time pass faster.

/11 **Ask your company if there is a version of the corporate next-generation antivirus that you may use on your personal device.**

If your company doesn't offer this, suggest that they start a program to do so. Personal antivirus solutions typically use old signature-based detection, and they're simply not effective.

DEVICES THAT CONNECT TO CORPORATE RESOURCES

With the age of bring your own device, work from home, and ‘any system/kiosk/etc. can connect in to get my email’ many corporations have unwittingly opened themselves to attack vectors that had previously been uncommon.

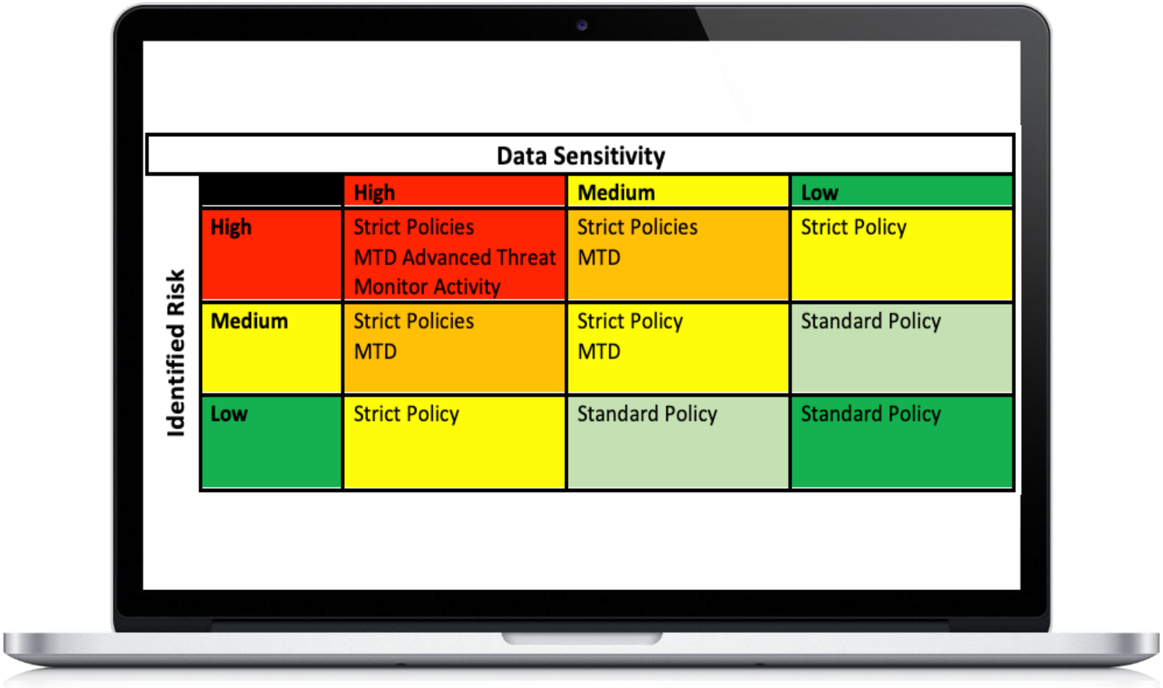
Office365, Gmail, and other cloud services are great, but now anyone can sign into them from *any* compromised device if proper controls aren’t in place.

The number of organizations Cybriant employees have seen implement proper cloud controls has been in the single digits.

LAPTOPS

We recommend creating a risk matrix for resources.

We use this one for both Mobile Devices such as iOS and Android devices as well as laptops. Here is an example:



		Data Sensitivity		
Identified Risk		High	Medium	Low
	High	Strict Policies MTD Advanced Threat Monitor Activity	Strict Policies MTD	Strict Policy
	Medium	Strict Policies MTD	Strict Policy MTD	Standard Policy
	Low	Strict Policy	Standard Policy	Standard Policy

By understanding your data sensitivity, you can start prioritizing the scrutiny of your security controls.

For example, let's say that we have highly sensitive data that by policy is *only* allowed to be accessed while in the corporate workplace.

During a time such as the Coronapocalypse, the policy isn't tenable.

HIGHLY SENSITIVE DATA

For laptops with access to highly sensitive data, a work from home policy could potentially include the following requirements:

1. Create a Terminal Services portal with no cut & paste allowed.

2. Whitelist home IP addresses to access the portal.

3. Ensure that all connections are directory authenticated (to Azure AD, Active Directory, or whatever else is your identity management technology).

4. Require all home systems to be MDM connected to prove compliance, and for home systems require the following:
   - Corporate patch management
   - Corporate EDR/MDR and endpoint protection technology

     You must be careful with this. Many EDR technologies can see URLs and domains that are visited by the employee. This can obviously be very private information, and so often the URL tracking is disabled for personal devices.
   - Encryption (Bit locker for Windows and File Vault for Mac)
   - Login password

5. Utilize Conditional Access polices for access to privileged data and documents as well as SharePoint sites.

NON-SENSITIVE DATA

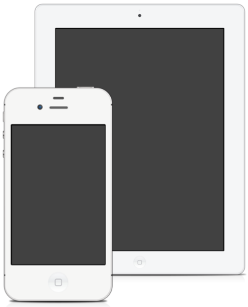
For laptops with access to medium and low sensitive data only, a work from home policy could potentially include the following requirements:

1. At a minimum I'd suggest requiring the corporate EDR/MDR & EPP be required to access corporate data.

   Same caveat applies: You must be careful with this. Many EDR technologies can see URLs and domains that are visited by the employee. This can obviously be very private information, and so often the URL tracking is disabled for personal devices.

2. Invest in a webcam cover. Videoing in video conferencing software is often set to automatically start. Sometimes you *really* don't want it to. .

BYOD MOBILE



Corporate infrastructures have been venturing into the BYOD (Bring Your Own Device) world for years often without knowing it.

Conditional restrictions often are not in place to prevent access to corporate data such as email, SharePoint, calendaring, corporate contacts, etc.

And even in cases where conditional restrictions may exist, the usage of mobile threat defense software may not be present or utilized on the device.

However, companies will often stringently safeguard their corporate laptops and desktops with MDR solutions, SIEM agents, and vulnerability management solutions.

The duality in approaches to BYOD devices versus corporate managed is perplexing since they often can access the same confidential data albeit without similar safeguards.

With the recent string of major vulnerabilities discovered in both the Android and Apple iOS ecosystems it should be obvious that any device that can access corporate data is a legitimate avenue for attack.

TYPES OF CYBER ATTACKS

App Vulnerabilities

Just like your laptop/desktop computer your mobile (phone or tablet) device runs software that must be updated regularly. This includes apps running on the phone which may have vulnerabilities exploited by potential attackers or phishers (SMS/Email/etc.) to install malware or gain control of the mobile device data.

This problem is compounded when apps request elevates privileges (and are granted by the user) on the phone. For example, “This app would like to have access to your contacts” could be a target for phishers.

User Granted Privileges

This follows App Vulnerabilities namely because most users do not read software EULAs or take time to comprehend the privileges requested by an app. Furthermore, most app developers will request greater privileges than necessary to ensure ease of development, and to avoid needing to require the user to agree to privilege escalation in the future due to an app update. The elevated User Granted Privileges are a ticking timebomb for vulnerable phone operating systems and apps.

TYPES OF CYBER ATTACKS

Sideloaded Applications

Any app that is installed on a mobile device in a manner other than via the official App/Play store for the device is a Sideloaded Application. Sideloaded applications are typically not vetted by the official Apple/Google antivirus measures in their stores. So, users will install the "free" version of an app to avoid paying a fee to Apple/Google.

It is common for the "free" software to have malicious code or device profiles/SSL certificates coupled with the software to harvest user data, banking credentials, personal pictures and messages, or your corporate data. Sideloaded Applications will commonly take advantage of the User Granted Privileges and App Vulnerabilities to gain access to data that was "secured."

Malicious Device Profiles/SSL Certificates

Malicious Devices Profiles and SSL Certificates are commonly utilized to conduct Man in The Middle (MiTM) attacks on any cryptographically secured data leaving the mobile device.

This combined with the fact that it is common for mobile application developers to not implement mobile SSL correctly in their applications is a common way for an attacker to harvest usernames/passwords as well as sensitive data.

TYPES OF CYBER ATTACKS

Rogue Networks

Attackers can set up wireless access points and give them the same name as a legitimate network. For example, an executive of your organization likes to drink coffee and read the news on his phone at Starbucks.

An attacker could set up a wireless access point with the same wireless name SSID as Starbucks.

To make matters worse, they could require the executive (without their understanding) to install a “Starbucks” device profile “to ensure the security and privacy of Starbucks customers.”

At that point, all data could be routed and decrypted via the MiTM attack that occurred on the executive’s phone.

TYPES OF CYBER ATTACKS

There are many more vectors by which an attack could occur on a mobile phone (Man in The Storage, baseband, phishing redirect to malicious IP, Multifactor Authentication harvesting, etc.).

The vectors listed above are some of the most common attack vectors seen by mobile threat defense professionals.

Without protection above and beyond that which is provided by an EMM/MDM solution any organization should assume that data that their users can access via mobile has already been compromised.

Additionally, depending on the method of multifactor authentication an organization allows it is reasonable to assume that standard access to company information (via portal/website/etc.) may have been compromised by a user or users as well.

CYBRIANT RECOMMENDATIONS

Mobile Security Risk Assessment

Our comprehensive mobile security risk assessment will allow you to evaluate risk presented to the organization by mobile phones and tablets, evaluate potential omissions in policies, documentation, and implementation. This assessment will also help evaluate impact of mobile device policy on diverse geographic and economic user groups. Plus, we'll be able to recommend actions to better secure and align mobile devices to business practices

Managed Detection and Remediation (MDR)

With MDR from Cybriant, our security analysts monitor your endpoints 24/7 and filter out false positives. You'll receive the alerts when relevant threats are detected along with advice and insight from our cyber security team to help you mitigate and respond to the threat.

Mobile Threat Defense

With two levels of service, Cybriant's Mobile Threat Defense (MTD) service is an affordable way to protect the majority of your workforce, contractors, and BYOD users. It provides a baseline of protection and assurance that your mobile devices will be secured against common threats and attack vectors.

Cybriant

strategic. adaptive. resilient.

Contact us.

Cybriant.com
844.411.0404
info@cybriant.com