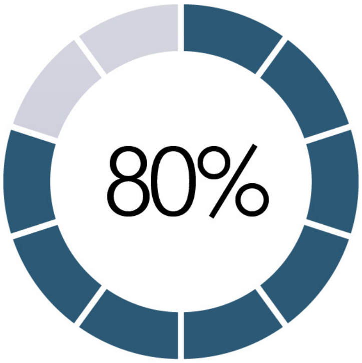
Acapella

ENTER 2020:
THE AGE OF MOBILITY

Have you harnessed the strategic advantages offered by mobile technology? Mobile devices have made it easier and easier to get work done while on the go. Laptops, tablets, and smartphones are a simple way to share and review documents, stay in touch with employees, and more while on the road.



Did you know that 80% of the workforce operates at least in part from outside the office?

That’s thanks to a combination of the cloud and the mobile devices that each and every person you work with carries around in their pocket. By 2020, the number of smartphone users world-wide is expected to reach 2.87 billion.

Mobility has delivered a number of advantages to organizations that are willing to embrace new technology, including:

Cost-Effect

Having your staff use their own personal devices for work means that you don’t have to pay for the technology they’d be using otherwise. Depending on the size of your practice, that could mean potential savings of thousands of dollars that would have been necessary to pay for tablets and work phones.

Convenience & User Experience

Allowing your staff to use their technology also means there’s no pesky learning curve to overcome with new devices. Instead of having to ensure your staff knows how to use the hardware at work, they can simply use the phone, tablet and/or laptop they’re already familiar with.

Productivity

Being able to use a mobile device, managing and executing tasks using the devices they’re familiar with can greatly boost productivity – in some cases, up to 53%.

It's no surprise that mobile devices are continuing to become a central and necessary part of the business world. What might be surprising is how unprepared some businesses are for that reality.

The Need For Mobile Security In 2020

No matter what kind of cybersecurity you have in place at the office, it won't extend to the mobile devices that have access to your data.

This is a critical limitation of your cybersecurity software, and it's obvious when you think about it – if your firewall is only installed on your work devices, but you let employees use personal devices and home workstations to access business data, then obviously you won't be totally secure, and you'll be left open to critical vulnerabilities that will only be more common in the coming years:

- Lost or stolen devices can do major damage to you, leading to compromised data and lost work.

- Unsecured Wi-Fi hotspots and other vulnerabilities allow intruders inside your private network.

- Mobile devices are becoming bigger targets for cyber criminals, who use malware and other methods to attack smartphones and tablets.

Are There Apps To Help Keep You Secure?

Virtual Private Network
One of the most proven techniques to make sure your data is safe is to use a virtual private network (VPN), which will give you back control over how you're identified online.

A VPN creates a secure tunnel for your data to transit the Internet, using a network of private servers.

When you use a VPN, your data is encrypted, or hidden, as it moves from your device to the VPN and then continues onto the Internet through what's called an exit node. A VPN creates the appearance that your data is coming from the VPN server, not from your device.

That makes it harder for an attacker to identify you as the source of the data – no matter whether you're on your mobile device's data connection, or using an unsecured retail Wi-Fi network while you're in line for coffee. Even if attackers can intercept your data, the encryption means the attackers can't understand your data or use it to their advantage.

When you put your data out to the VPN server, it exits back out to the public internet. If the site you're visiting has HTTPS to keep the connection safe, you are still secure.

Find My Phone
Whether you left your phone on the train, or suspect it was stolen intentionally, Find My Phone is the app you need.

These types of apps allow you to remotely turn on your phone's GPS to determine where it is. Furthermore, some of the more security-focused versions of these apps allow you to execute additional actions in order to eliminate security risks".

The right monitoring software for mobile devices will protect you from a number of dangerous scenarios, including:

- Jailbreaking and rooting company devices
- Unauthorized access to company data
- Lost or stolen devices that need to be remotely wiped

Password Managers
These programs store all of your passwords in one place, which is sometimes called a vault. Some programs can even make strong passwords for you and keep track of them all in one location, so then the only password or passphrase you have to remember is the one for your vault.

Multi-Factor Authentication
Multi-Factor Authentication is a great way to add an extra layer of protection to the existing system and account logins. 45% of polled businesses began using MFA in 2018, compared to 25% the year prior.

By requiring a second piece of information like a randomly-generated numerical code sent by text message, you're better able to make sure that the person using your employee's login credentials is actually who they say they are. Biometrics like fingerprints, voice, or even iris scans are also options, as are physical objects like keycards.

Implement A Mobile Device Management Policy

This type of comprehensive policy dictates how your employees can use their personal devices for work purposes, dictating which security apps should be installed, and what best practices need to be followed.

An effective MDM policy should also instill safe and secure practices for employees that use personal devices for business purposes. Key considerations include:

1. Decide when and how mobile devices will be used.
Integrated into your internal network, these devices can be used to access, store, transmit, and receive business data.

You'll need to have policies in place to regulate how employees use their devices to interact with sensitive data. Take the time to consider the risks associated with mobile device use, such as the potential for devices containing business data to be lost or stolen, infected with malware, or the potential for accidental disclosure of confidential information through sharing a device with a family member or connecting to an unsecured wireless network.

2. Consider how mobile device use can pose risks to your data.
A risk analysis will help you identify vulnerabilities in your security infrastructure, and help you determine the safeguards, policies, and procedures you'll need to have in place. Whether the devices in question are personal devices, or provided by your Fort Lauderdale IT company, you will still need to have a clear idea of how they're being used to communicate with your internal network and systems.

Assessments should be conducted periodically, especially after a new device is granted access, a device is lost or stolen, or a security breach is suspected.

3. Develop, document, and implement mobile device usage policies and procedures.
Policies that are designed for mobile devices will help you manage risks and vulnerabilities specific to these devices.

These policies should include processes for identifying all devices being used to access business data, routinely checking that all devices have the correct security and configuration settings in place, whether or not staff can use mobile devices to access internal systems, whether staff can take work devices home with them, and how you will go about deactivating or revoking the access of staff members who are no longer employed.

4. Implement practices for controlling which apps are permitted for business use.
Maintaining mobile security isn't just about having the right apps – it means following the right protocols, to eliminate unknown variables and maintain security redundancies:

a. Review installed apps and remove any unused ones on a regular basis.
b. Review app permissions when installing, and when updates are made.
c. Enable Auto Update, so that identified security risks are eliminated as quickly as possible.
d. Keep data backed up to the cloud or a secondary device (or both).

5. Train your staff.
Everyone on your staff should be educated on how best to use mobile devices to avoid costly security errors. Your safeguards can't protect you or your clients if your staff doesn't understand your policies and procedures, and lacks a basic grasp of security best practices.

Your entire team should be taught how to secure their devices, how to protect business data, what the risks are, and how to avoid common security mistakes.

In 2020, and beyond, technology can be more than just a way to keep your business running, secure from cybercrime and backed up in the event of a disaster. Truly optimal IT should help you transform your business and your customers' businesses for the better – but that will only happen if you embrace new opportunities, like those offered by mobile technology.