Federated Insurance

BRING YOUR OWN DEVICE

Protecting yourself when employees use their own devices for business

Bring Your Own Device:
The new approach to employee mobility

In business today, the value put on the timeliness of access to data is high. Having the right information at the right time is useful in some cases and essential in others. If you're like most Canadian business owners, using mobile phones is part of your day-to-day business.

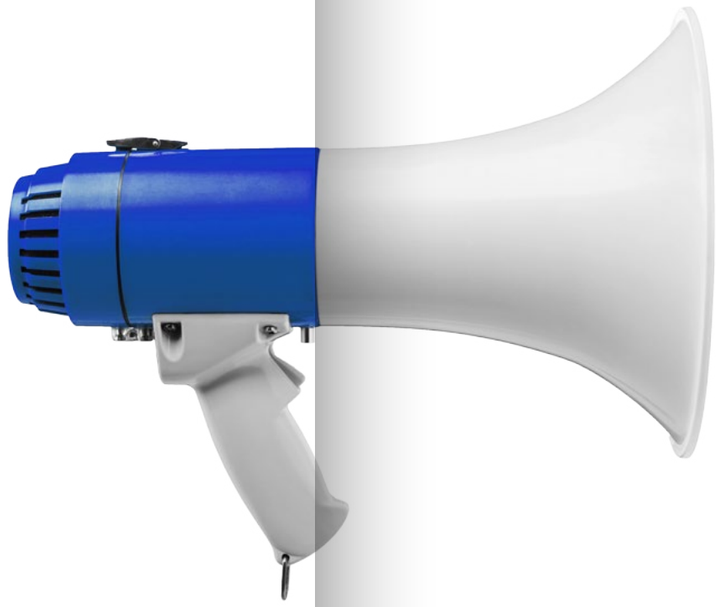
If you're a business owner, there's an undeniable attractiveness to pushing the costs of the initial cellular phone and plan to your employees. The current trend to Bring Your Own Device allows your employees the benefit of using a device they feel comfortable with and chose to use, and you get to communicate with the employee via that device for 'free.' And while this approach is most certainly cost effective, it's not without risk especially when it comes to sending potentially sensitive information about schedules, business plans, or clients to the employees' devices that is untrusted and perhaps already compromised.

But that's not to say it can't be done. You just need to be aware of the risks and know how to protect yourself against them.

The low cost of convenience vs. the high cost of a damaged reputation.

It's the potential loss of sensitive data that can be most damaging to the reputation of your business. Word-of-mouth advertising works both ways: if you're successful in protecting clients' data people will want to work with you. If you have a breach of their data, they'll never come back and will be sure to let others know their data isn't safe with you. Worse still, if you're the cause of an information security breach for your larger partners or clients (as we saw with the Target and Home Depot breaches in 2014), your brand could be irreparably damaged.

So what's a business owner to do? Risk sending sensitive client data to employees' personal devices? Or take on the burden and cost of issuing mobile devices to employees that don't want to carry and use another device anyway? There is another option–a Mobile Device Management (MDM) solution that allows you to have the benefit of easy communication with employees while protecting the data sent to them.



Be aware of the type of sensitive information you send using your device.

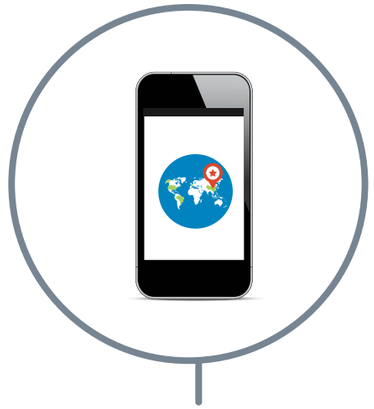
Mobile Device Management:
Easy communication meets data protection

An MDM solution is a service you can either subscribe to or purchase as a software package and install on your own.

The MDM allows you to:

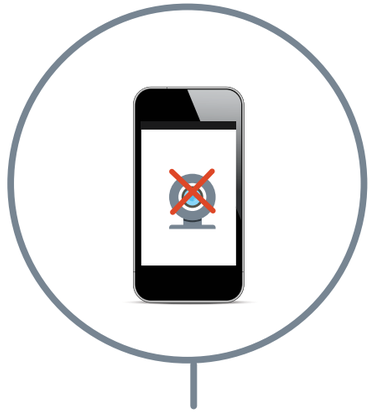
- Ensure users have a password to access their devices
- Find a lost or stolen device on a map of the world.
- Remotely destroy the data on a device anywhere that is connected to the Internet. Either all the information on the device or just the company information leaving the personal contacts, mail and photos intact.
- Disable the use of the device camera in certain locations. For instance, you may not want employees taking pictures of customer information on company computer screens. You can disable that camera while they're at work by time or geography.

Users require a password to access their devices



Users can locate a lost/stolen device on a world map

Users can remotely destroy data via Internet connection

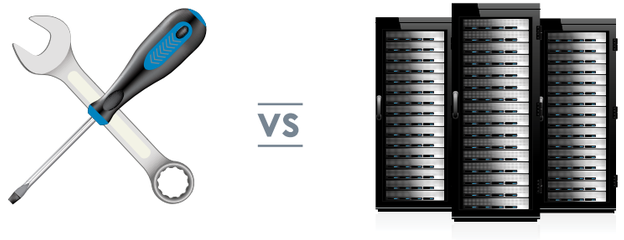


Camera use disabled in certain locations by time or geography

DIY vs. Using a service provider

The amount of time and effort needed to implement an MDM solution depends on whether you choose to buy the software and build it yourself or sign up with a service provider to manage the devices.

If you go with a service provider, you don't have to worry about additional networking, new servers, new training and operational headaches. But even if you go the service provider route, you're still accountable if something goes wrong – just because you outsource something does not mean you transfer the liability. The service provider is helping you manage those risks, not taking on the responsibility of them.



Here are a few things you should be looking for in an MDM solution:

FEATURE	BENEFIT
Containerization	Containers on phones allow for the separation of different types of information, by source or by type
Password enabled	Ensures that access to the company data requires a secret password or PIN
Encryption	Encryption renders the data unreadable unless the correct key is used, perhaps from the user entering the correct password
Auditing	An audit trail ensures that there is a record of the use and access of the company information. Excellent for troubleshooting problems as well as understanding who has accessed the data
Updated AV and anomaly detection	Mobile malware is a growing trend. Keeping the mobile devices that hold your company's data clean may require installation of anti-virus software much the same as the AV software on your computers
Integration with existing authentication sources such as AD	To reduce costs and easy deployment, using the existing Active Directory in the company will allow faster implementation and easier user experience and thus adoption
Cross platform support for key devices	It is important the MDM solution you choose supports all the most common mobile devices at the time so that your employees devices are all equally protected

Don’t forget about cyber insurance

Implementing an MDM strategy is one way to protect yourself against the risks. Another way is to add cyber coverage to your insurance policy (you might also see it referred to as data protection insurance).

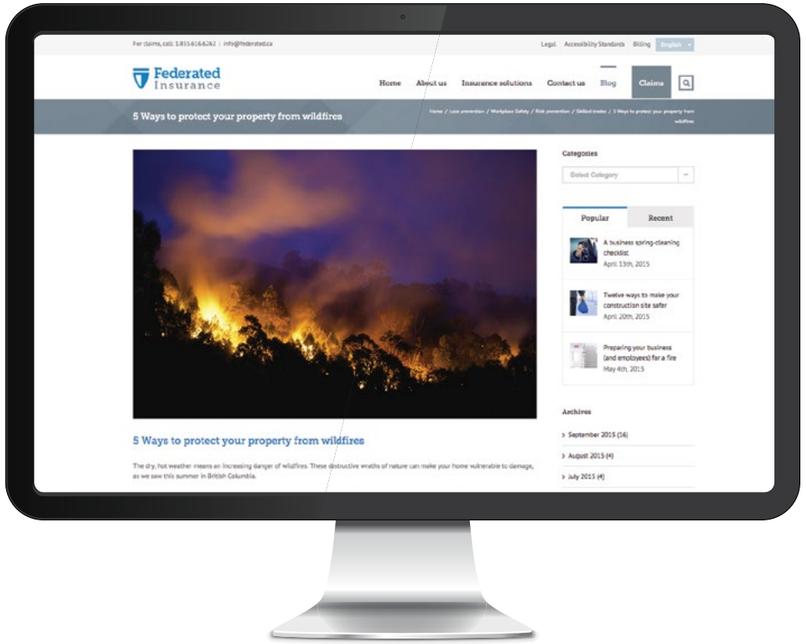
When you’re choosing a cyber insurance solution, make sure it includes coverage for laptops, tablets, smartphones, USB keys/flash drives and similar portable devices.

A good cyber insurance policy will not only cover your business’ liability in the event of a covered data breach or a downloaded virus, it will also cover certain “offline” events where a physical file or document ends up in the wrong hands.

One last thing... don't forget about the employee part of the MDM equation.

MDM solutions, are without a doubt, extremely powerful and put a great amount of power into your hands as an employer. Just as important as that control is the trust of your employees that you're not using it to secretly track their movements and activities. All use of an MDM should be performed with full knowledge and full consent of the end user. If they don't want to opt-in then they shouldn't have to.

It's also important to ensure that your employees are aware of the risks associated with using their own devices and that they're made aware of the steps they can take on their end to ensure your company information is kept safe.



Want to know more about protecting your business?

Visit us at **www.federated.ca**


Federated
Insurance