

Why MSP's NEED Management & Security On Customers Mobile Devices

How one compelling event with a mobile device can cause a catastrophic data breach for a customer of an MSP who had all but one endpoint managed and secured.

The MSP

MacCo is an MSP based in the suburbs of Fort Lauderdale, Florida. MacCo has 6 employees and has revenues around \$1.2 million. They have been partnered with TMT for 5 years, and have consistent MRR. MacCo specializes in 3 verticals, legal, construction, and finance.

MacCo has a goal to protect their clients with the best and most well known security software solutions on the market.

They include Galactic Advisors, Brightguage, Coro, PasswordBoss, Duo, Threatlocker, Web Titan, RMM, N-able, Wattbox, Auvik, and ID Agent. They dabble with Intune and other MDM's, but do not use it for their customers due to its difficult nature.

The Customer

Kathy is the owner of a Medical Malpractice law firm called MedLaw, L.P. on the outskirts of Fort Lauderdale, Florida. Her firm has 10 employees and they are doing exceptionally well.

MedLaw has been a customer of MacCo for 6 years and they have a great working relationship together. MacCo has all their security products installed on MedLaw's computers and have the firewall locked down. MedLaw's internal systems contain financial, health, and personal records of current and previous clients.

The Issue

Kathy had been pushing herself to the brink. It had been five long years since her last vacation, and her coworkers were eager to see her relax.

Kathy's team had reassured her they could handle the operations, so Kathy began her holiday with her family to Europe.

While at the airport, between the security checkpoint and the boarding gate, the unthinkable happened. Kathy left left her phone at the TSA checkpoint.

Her phone contained her business email, bank account information, applications, and CRM system with her client data. Worse yet, she

had no passcode on her phone. It was unprotected and anyone could've had access to her data.

Panic set in as Kathy rushed back to retrieve her phone. She was relieved when TSA handed it back, but the worst was yet to come.

After her family settled down at a nearby Starbucks, her youngest child started to get antsy. He asked to play on her phone to pass the time. Kathy hesitantly handed over the device, thinking it might help keep him entertained.

Her son quickly connected to the free Starbucks Wi-Fi for a faster connection, and in no time, he stumbled upon a website promoting an enticing game. Without understanding the risks, he downloaded the game from an unfamiliar website linked to a foreign country.

The innocent act of trying out a game turned into a security nightmare. The game prompted her son for an in-app purchase, claiming it would enhance his experience. In his eagerness, he used the debit card associated with Kathy's business bank account linked to her Apple Pay.

Unaware of the potential danger, Kathy's husband took their kids to board the flight, while Kathy stayed behind to grab some coffee.

She noticed her phone was running low on battery and spotted a convenient charging kiosk right across from Starbucks while she waited for her order.

Desperate to ensure her phone had enough charge, she plugged her USB cable into the charging kiosk.



As she boarded her flight, Kathy's phone started to behave strangely, prompting her with unfamiliar messages and errors. She had never seen anything like it before.

In a matter of minutes, Kathy had fallen victim to a cybersecurity breach.

Kathy's personal & client data for her medical law practice is now at risk. Along with her reputation.

The Solution

MacCo, as a forward-thinking Managed Service Provider, could have made Kathy's life significantly easier and her vacation far more relaxed.

By implementing a robust mobile security strategy that includes Mobile Device Management (MDM) and a Mobile Threat Defense (MTD) solution, they could have ensured the safety of Kathy's sensitive business data.

The MDM can enforce passcode policies on Kathy's mobile device around specific data like her email and CRM, adding an essential layer of security. Ensuring her client's data was protected.

Furthermore, with MTD, Kathy could have enjoyed the peace of mind knowing her device was equipped to detect and respond to cyber threats in real-time.

This would have alerted her to rogue Wi-Fi networks, untrusted applications, and phishing links, giving her the ability to avoid risky situations. Leading her to trust her son with the device.

In the end, a strategic approach to mobile security provided by MacCo could have spared Kathy the nightmare of a security breach and preserved the reputation of her medical law practice.

About MMS For MSP's

As an MSP, you've mastered network management and endpoint security, but what about your clients' mobile devices? They can not be forgotten.

Troy Mobility's MMS (Managed Mobility Services) For MSP's is your comprehensive solution to address this critical gap in security.

MMS equips you to manage corporate data securely, with features to wipe or lock devices, manage app distribution, and enforce security requirement to ensure complete visibility and device inventory management.

Plus, our Mobile Threat Defense (MTD) safeguards against rogue Wi-Fi, applications, and phishing/smishing attacks in real-time.

With monthly billing, you can select our Standard or Enhanced mobile security package to complement your existing packages. Each Tier is backed by our expert implementation services and Tier 1 support.

If you choose to not manage the UEM & MTD console on your own, Troy Mobility's Managed Mobility Services support team can handle complete support services of your console and devices under management.

Contact Troy Mobility.
To Get Started Today.



Troy Mobility Calendar Link



About Troy Mobility

Troy Mobility has been a mobile security consulting leader for over 15+ years & has a portfolio of 10+ industry leading mobile security solutions. Troy Mobility supports, secures, and manages mobile devices with our MMS (Managed Mobility Services) for every industry and use-case; including MSP's, financial services, healthcare, law, construction, manufacturing, and more.

To this day, Troy Mobility upholds a culture that puts customers at the forefront of everything we do. With zero plans to change that, our service and support are paramount to the success of our customers and their business. Start a conversation with Troy Mobility to explore options and expert advice to best fit your security roadmap.

Have Troy Mobility Help You Add MMS For MSP's To Your Stack



www.TroyMobility.com



(857) 264-5000



Info@troymobility.com



Or Scan To The Right



Troy Mobility Calendar Link

