RAM COMMUNICATIONS INC.

GREEN PAPER

Mobile Expense Management Best Practices

Keeping Your Mobile Data Safe on Employee Mobile Devices

Today, nearly 50% of U.S workers are performing their jobs remotely. *So, who's keeping track of your organization's data on all those mobile devices?*

The RISKS

If your organization uses 100 or more mobile devices you need to consider the potential security exposure. Remember, if your company-related apps (O365, Salesforce, other CRMs) are installed on mobile devices then there's potential for hacking attempts.

Even if your business doesn't have to meet specific security compliance standards there's a bigger issue at play: a security compromise can cause financial damage your company may not be able to overcome. You don't have to take our word for it. There are numerous government and private resources who provide data on the devastating business impact of security compromises. (For your reference, we've listed a few resources at the end of this document.)

Some Wireless Expense Management organizations offer specific security tools designed for protecting mobile devices and wireless infrastructure. There are also cyber security companies with the tools to effectively secure and monitor your wireless assets. In both scenarios, RAM Communications can help. We can bring you complimentary or exhaustive levels of security tools and resources for your company's needs.

ESSENTIAL TOOLS

Here are some recommended security items you should ask for from your security experts.

Multi-factor Authentication

At minimum you should receive multi-factor authentication or MFA tools for your end users. Login controls are an absolute must. MFA helps defend your data from easy hacking opportunities.

BEST PRACTICES

Threat Detection Management System

You want a solution that uses a combination of automation and personal management (eyes on glass). Why? Because too many times the 'automated only' systems are used with the expectation that everything is secure. However, software is only a tool. The tool can't completely replace people. You need people to analyze the data and consider the risk to your organization. Despite all its analytical capabilities, threat management software may not be able to anticipate all the tricks of a sophisticated hacker. Therefore, the best solution requires a mix of people and software.

Periodic Security Reviews

A good security team will also check in with your team on a regular basis. Quarterly reviews are used to cover updates and changes in your organization. If you think about it changes in end users, devices and policies can and do affect the security. So, it only makes sense the security system should be updated to keep pace with those changes. Otherwise, there's potential for hackers to find new holes in your system.

Ultimately, people need to do analysis, ask the right questions and monitor the cost and the technology and the security pieces that are relevant to your organization. People have to work the security tools accordingly in order to meet the security objectives of your company.

Here are some additional security resources to check out for more information:

https://www.knowbe4.com/security-awareness-training

www.cisa.gov/ransomware

If your organization is serious about shoring up its corporate mobile services program consider contacting RAM for help. We are a trusted advisor for our clients because we've saved them substantial money and time using our WEM resources. If your firm has over 100 devices then we fully expect to save you upwards of 30% on your monthly costs. Contact RAM Communications today and let us help you find the right solution for your organization.

RAM COMMUNICATIONS INC.

2720 S. River Road
Suite 152
Des Plaines, IL 60018
847.358.0917
info@ramcomminc.com
www.ramcomminc.com

Arlington Heights Park District · Mather · Park Ridge Park District · Scott Harris Hospitality · ECC Engineered Components Company · RUSH Rush Copley Medical Group · Testa Produce, Inc. Green by Nature... Greener by Choice