

Technology Gadgets Bring Increased Risk



We love our gadgets. From Androids and iPhones to iPads and more, we're a country of gadget lovers. And while the pleasures are many, today's technology can create major headaches for business.

It's common practice for today's workers to bring personal technology into the workplace, whether smartphone or laptop. And why not? Gadgets make us more accessible, more productive, more proactive than ever before.

But...

Smart handhelds may be small in size, but they represent a significant threat to your business. They're loaded with confidential data, from sensitive emails and proprietary PowerPoint presentations to Excel spreadsheets packed with client data, pricing and customer lists.

And letting viruses and data stealing Trojans access your corporate network through our gadgets may be even more dangerous than letting sensitive data out. Most organizations focus technology defenses on the perimeter of the corporation, so a breach of defenses can wreak unfettered havoc with inside systems.

Companies must prepare for such risks, and saying no isn't an option. This consumer-led revolution has produced gadgets so pervasive, powerful and easy-to-use that employees demand them – there's no turning back.

Expect increasing numbers of credit card number thefts and "fake apps" that solicit corporate or personal information and passwords from the unwary. Viruses and malware are cropping up, and hacker attention is growing. Phone thieves incur massive bills, or tap into location-tracking services – making them a stalker's dream.

There will be loss of devices – they're easy to forget in a hotel or coffee shop. They're great targets for theft. So the main security threat is the sensitive information they contain or can access, and how it can be abused.

So while road warriors embrace iPad as a way to finish reports on the road, and at-home associates download spreadsheets on iPhones to work on after the kids go to bed, put a plan in place to protect your organization and deal with the devices you'll see employees using for years to come.

Here are some suggestions:

• **Be Proactive:** Decide what corporate resources devices can tap into.

Even email can still access sensitive attachments, so assess risks and decide how to control usage. Technologies exist that ensure only authorized users gain access to company resources.

• **Be Prepared:** Loss and theft of devices is a certainty, so be sure that all smart gadgets that access corporate resources use data encryption and password protection. Be sure your IT staff can remotely monitor employee devices to wipe data off if lost or stolen.

• **Plan Ahead:** Plan methodically for the kind of mobile security you want. Called "secure by design," decide on the levels of security you'll need as use of gadgets grow. Decide what resources to make available through mobile devices, and build plans from the ground up, creating policies and installing technology defenses – rather than scrambling when a problem inevitably occurs.

Gadgets are fun, make us more productive, and can enhance business performance. Just make sure to develop your plan on how to safely manage this brave, new world of connected consumer devices.



Since 1999, CEO Charles Johnson and EDTS have been providing networking, security and managed services support solutions to Southeastern businesses. The firm provides Experience, Dedication, Technology and Solutions (EDTS) to increase productivity and reduce cost associated with IT.

In the Upstate, call 864.250.9112 or visit us at www.EDTSolutions.com