October 2018

http://www.ctsioutsourcing.com
229-446-9641

235 Cedric Street Leesburg, GA 31763

How Losing a Mobile Device Puts Your Entire Business at Risk

Losing a mobile phone or laptop is an experience that everyone dreads. The expense and inconvenience of buying a new device is unpleasant, but only represents a fraction of the damage done when a device is misplaced. The cost of data contained within every device can add up to many times more than the total value of the device itself.

Chances are, you already use automatic login on a large variety of online services. Each of these services are vulnerable to an attacker having possession of your device.

Usernames and passwords - An obvious place for an attacker to start is the likely long list of usernames and passwords saved for future use by your browser. This is often done to save time when logging into sites that you visit often. Almost universally, people opt to save login information so that they don't have to attempt to remember it every time they return.

In only a short amount of time, a browser is trained to log in to your Facebook, cloud storage, and bank details just by visiting the page using your regular device. These details, called up by the browser, are saved in a single list accessible to anyone with access to the device. For an unscrupulous stranger with a found device, this list represents a goldmine of information. Simply by finding a phone misplaced in public they may gain access to a huge array of services.

The problem can be made many times worse where a single password or a combination of similar passwords have been used across several accounts. In some instances, an attacker need only gain access to a single one and reuse the same stolen credentials across many sites and services.

Email - Email accounts are a key target for attackers looking for access to your personal information. It is a service that many take for granted, logging in once the first time they set up the device and using automatic login every time after. It is a service that also unlocks a great deal more than just private messages. Of course, an attacker having free access to read your personal emails is bad news, but with email access a malicious user can gain access to many of the most commonly used web services online.

Using the "forgotten password" button on many sites triggers a response that emails a password reset link to the email address registered on file. An attacker may use this feature to reset account passwords to one of their choosing. Doing this both grants themselves access to your account and denies you access to rescue it.

Contacts - One of the best features of instant messaging is that your contacts know the messages come from you. When a message is sent from your device to someone you know it displays along with your name, details, and likely a photograph too. This can lead to identity theft, one of the biggest concerns of a lost or stolen device.

With contact information already programmed in an attacker has an opportunity to impersonate you when speaking to anyone in your contacts list. Using your identity, an attacker may attempt to steal yet more details about you and your contacts.

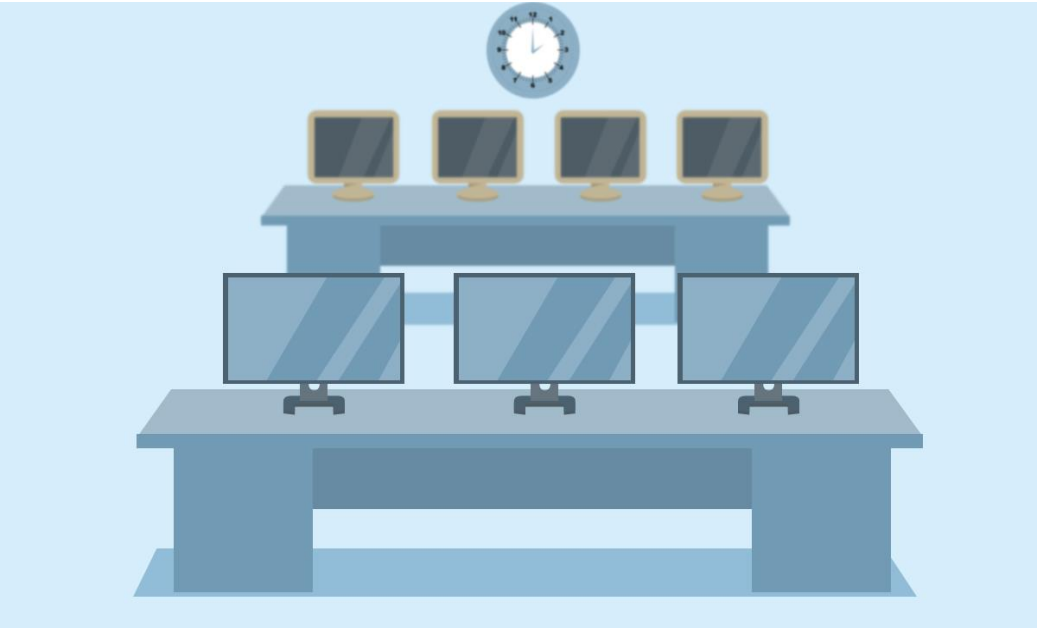
Social Media - Your social media accounts are often the face of your brand. They can be a primary way to reach out and contact customers. They are almost always the first point of contact a client has with your business. They are also extremely vulnerable to being hijacked from a stolen device.

Fraudulent social media access can allow attackers to harvest both client and business data. Even without profiting directly, posting privileges can be used to cause irreversible damage to a business.

Protecting your business - Services, accounts, and entire businesses can be put in great danger by something as simple as misplacing an unsecured mobile phone or laptop computer.

We can help you to stay secure and remain in control even in the face of losing a device. Give us a call at 229-446-9641 and let us help secure your business.

Stay Ahead of the Curve with an IT Lifecycle Plan



All appliances have an effective lifespan. Computers are no different. In some cases, parts physically fail after years of service, in others they simply become too slow and too ineffective to keep doing the job. Hardware failures and IT issues can cost big in productivity losses, urgent fixes, and unintended downtime.

Improving productivity and lowering costs are the primary driving factors in why many modern businesses choose to adopt IT life cycles.

IT Life Cycle

The IT life cycle aims to make IT budgets predictable, manageable, and reduce costs across the department.

This process starts with a thorough plan outlining the demands of the business. By looking at how and where equipment is deployed we can make the most out of the resources throughout the business. The first step is to reduce equipment duplicated and underused within the firm.

With a big picture approach, equipment can be scheduled for upgrade or replacement at predictable intervals based on use. With a plan in place, the focus of the life cycle can shift to resource procurement. As equipment approaches the end of its effective lifespan it can be brought in for replacement, repair, and recycling. Old hardware and components are often reused and recycled in new roles as they are decommissioned from their primary role.

By maintaining as many usable parts as possible we help lower costs of keeping efficient hardware in the front line business environment. This approach helps a huge number of businesses keep modern, up to date hardware in crucial roles where it can serve the biggest impact for the business.

Making the most of resources

Computers in a busy business environment will always need eventual replacement over time. It is important to plan and prepare for this end of service life to limit unplanned downtime, increasing costs and losses in productivity. Doing so helps to plan a regular, predictable IT budget, less prone to sudden financial spikes.

The IT life cycle additionally allows the business to stay on top of software licenses, upgrades and Operating System changes. By cycling old and out of date systems from the network, security vulnerabilities are dramatically reduced and easier to patch.

Additional financial security comes from manufacturer warranties for businesses that adopt the life cycle. As new equipment is purchased into the firm, manufacturer warranties provide guarantees about the handling of defects and hardware issues. This warranty may cover all, or most of the duration of the equipment's intended life cycle.

The extra coverage provides an extra layer of financial protection from unpredictable IT issues.

In control with information

Tracking the life cycle of your own firm provides invaluable metrics about how equipment use and deployment within your own production environment. Armed with this unique knowledge, better purchasing decisions can be made to equip your business with the tools needed to succeed.

Budgets can be put to better use, getting the important high-value resources to the places in the businesses that need it most. The ones where they will generate the most value for the firm.

A key factor in getting the most from your firms IT is making sure the resources put into the company don't sit idly on a shelf after purchase. The insight gained from metrics related to the life cycle ensure that management stay fully informed.

A complete picture puts your business back in control of its IT by allowing you to choose the best, most efficient, and most cost-effective time to replace critical IT. Firms can plan replacements and servicing outside of busy periods so they can operate without interruption and know their IT is fully serviced when they need it most.

Planning for the future

With a fully planned, fully prepared life cycle, IT budgets can be planned in detail for years to come. Everything from printers to operating systems can be prepared on a tightly controlled schedule.

Businesses worldwide have adopted IT life cycles as a way to eliminate unwanted surprises, lessen productivity losses, and make the most out of IT budgets. Implementing or redesigning your own IT life cycle can greatly improve the way your business operates.

Talk to us about how you currently do IT today and we'll see if we can't make the life cycle work for you. Give us a call at 229-446-9641.

The Top 5 IT Security Problems for Businesses

"Each of these common issues have simple solutions to secure against IT failure."

Companies that suffer security breaches nearly always have one of these IT security problems. Is your company guilty of any of them?

No Backups

A shocking number of businesses are not backing up their data properly. According to market research company Clutch, 60 percent of businesses who suffer a data loss shut down within six months.

Not only should every business be fully backing up their data, but their backups should be regularly tested to work too. It's a step that businesses miss surprisingly often. Many businesses don't find out that their backup can't be used until it's already too late.

Reactive and not proactive

The world is constantly changing. The IT world doubly so. Attackers are always figuring out new ways to break into businesses, hardware evolves faster than most can keep up, and old systems fail due to wear and tear far quicker than we would like. A huge number of businesses wait until these issues impact them directly before they respond. The result is higher costs, longer downtime, and harder hitting impacts.

By responding to hardware warnings before it fails, fixing security holes before they're exploited, and upgrading systems before they are out of date: IT can be done the right way. Being proactive about your IT needs means systems don't have to break or compromised before they are fixed. The result for your business is less downtime, fewer losses, and lower IT costs.

Weak Passwords

A surprising number of people will use the password "password" to secure some of their most important accounts. Even more still will write their own password on a post-it note next to their computer. In some cases, many will even use no password at all. Strong passwords act, not only as a barrier to prevent unwanted entry, but as a vital accountability tool too. When system changes are made it's often essential that the account that made changes is secured to the right person.

With an insecure password or worse; none at all, tracking the individual responsible for reports or accountability becomes impossible. This can result in both auditing disasters on top of technical ones.

Insufficient Staff Training

Humans in the system are commonly the weakest point in IT security. Great IT security can be a bit like having state-of-the-art locks on a door propped open with a milk crate. If staff aren't trained to use the lock, it's worth nothing at all.

Often times businesses can justify spending big on security for the latest and greatest IT defenses. The very same firms may exceed their budget and spend almost zero on training staff to use them. In this instance, a little goes a long way. Security training can help staff to identify a threat where it takes place, avoiding and mitigating damage, often completely.

Weak Data Controls

Some companies can take an ad-hoc, fast and loose approach to storing professional data. Often crucial parts can be spread across many devices, copied needlessly, and sometimes even left unsecured. Client data can be found regularly on employee laptops, mobile phones, and tablet devices. These are famously prone to being misplaced or stolen out in the field along with vital client and security data.

It can be easy for both employees and firms to focus on the costs of devices and hardware purchased for the business. The reality is that the data held on devices is almost always worth many times more than the device that holds it. For many firms, their approach to data hasn't been changed since the firm was first founded. Critical data is often held on single machines that haven't been updated precisely because they hold critical data. Such machines are clearly vulnerable, outdated, and prone to failure.

Common problems with simple solutions

Each of these common issues have simple solutions to secure against IT failure. With a professional eye and expertise in the field, every business should be defended against IT issues that risk the firm.

If you need help securing your IT to protect your business, give us a call at 229-446-9641.

Storage Struggles? How to Keep Up with the Data Explosion

Many businesses have already embraced the benefits of going fully digital. It has allowed us to do more than ever before; saving us both time and money iterating over work drafts and emails. It has saved us a ton of space too, eliminating the need for stacks of file cabinets in every office.

The digital boom presents us with brand new problems too. By moving all our files into a digital space, the amount of storage we need to maintain has grown larger and larger just to keep up.

As digital technology has improved, the resolution, clarity, and size of the digital files we create has exploded. Items such as Xrays, which used to be printed on film are now digital files transferred by computer. As a result of the increase in both the number of digital files we use and their ever-growing size, the size of the data we need to store has exploded exponentially.

There are a number of ways in which we can tackle our ever-growing storage problem.

Local server or Network Attached Storage (NAS)

A local server is a machine physically located within your own office or building. These are typically designed to serve many files to multiple clients at one time from locally held storage.

The primary advantage that a local network server has is that all your vital data is available to all users in one central location. This means that employees across the network can access all the resources made available.

These machines can serve files at the speed of the local network, transferring large projects, files, and documents from a central position within the network with ease.

A NAS has many of the same network properties, typically packaged as a smaller profile, low powered computer. A NAS is specifically designed to enable network file sharing in a more compact package. These can be available in units small enough to fit in a cupboard nook and yet still provide staggering storage capacity on only a small amount of power.

Both a local server and NAS device allow for large amounts of storage space to be added to the local network. These units are often expanded with more and more storage over time. As an organization grows over time, so do its data storage requirements.

Cloud Storage

Sometimes the best option for storage is to move your ever-expanding data outside of the business completely. Often, offloading the costs of hardware and IT management can work out to be an intelligent business decision. One that provides freedom and flexibility in your data storage needs. The major advantage of cloud storage comes from the ability to expand and contract your services as needed without the unnecessary overhead of adding and maintaining new hardware.

By moving storage to the cloud, data can be accessed from anywhere in the world. The flexibility provided by cloud storage allows limitless expansion to any number of devices, locations, and offices. Being able to access data from many locations at a single time can often provide a valuable boost to productivity that can help to speed projects along.

Some of the drawbacks of cloud storage come from factors that may be outside of the control of the business. Not all internet connections are found to be up to the task of handling large amounts of data to and from the cloud. In some cases, the infrastructure is quite simply not in place yet to support it.

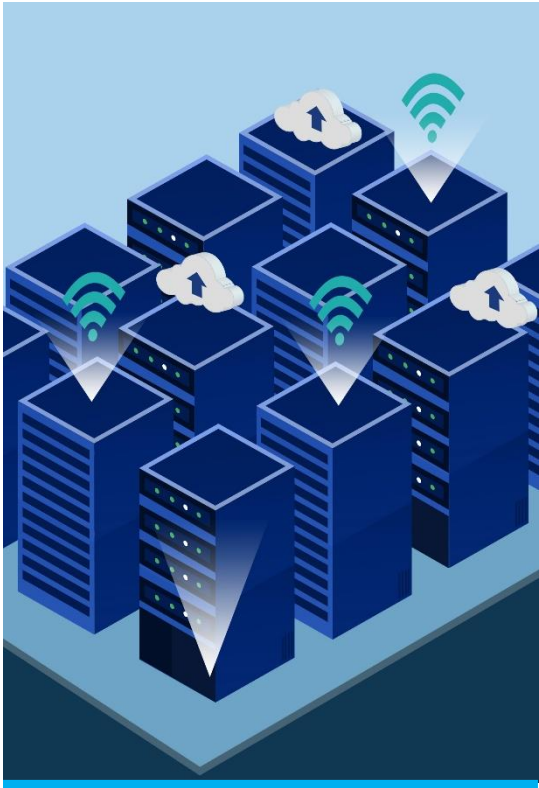
IT security regulations can prove to be a barrier to enabling storage in the cloud too. Some regulations either prohibit the feature entirely or enable only certain specific types for use.

The Right Choice for your data

Both cloud and local storage can provide further benefits to enhance your business. Audit logs, central backups, and version control can all be used to secure the way your firm handles data.

Whatever your situation, whether a small NAS can boost your office productivity, a local server can provide the connectivity missing from your firm, or cloud storage can switch on new resources, we can advise on the best choices for your business.

Give us a call at 229-446-9641 to allow us to use our expertise to make the right chose for your data.



Comnet Technical Solutions, Inc.
CTSI
CTSIoutsourcing.com

229-446-9641

235 Cedric Street
Leesburg, GA

HOURS OPEN
Monday to Friday
8:30am - 5:00pm

CTSI Facebook