Disaster recovery guide

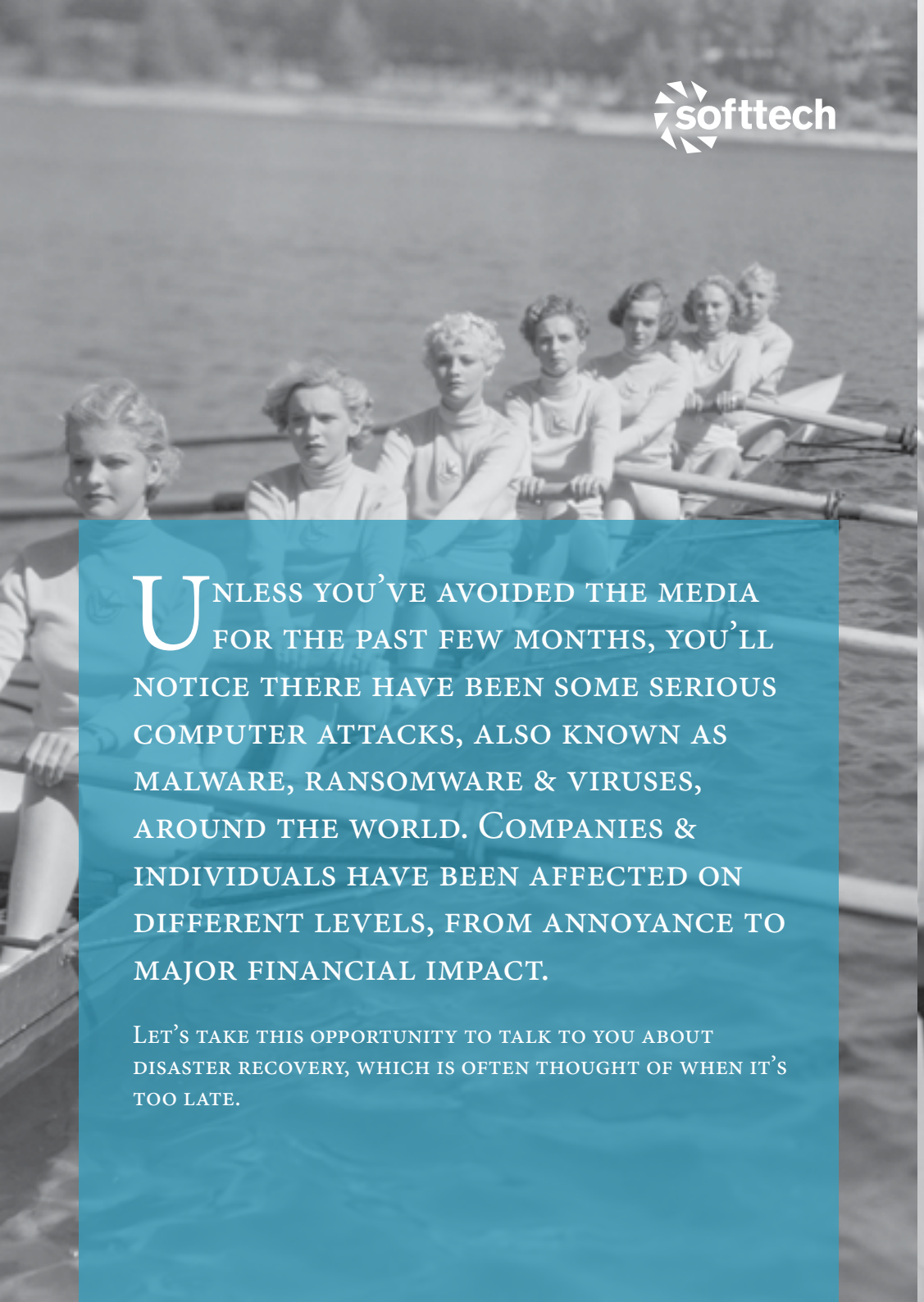
Aliens stole my computers

Rowan Hick
Chief Technology Officer, Soft Tech

July 2017

softtech

info@stgroup.com | stgroup.com



softtech

Unless you've avoided the media for the past few months, you'll notice there have been some serious computer attacks, also known as malware, ransomware & viruses, around the world. Companies & individuals have been affected on different levels, from annoyance to major financial impact.

Let's take this opportunity to talk to you about disaster recovery, which is often thought of when it's too late.

How to avoid an attack

Before we get into disaster recover, here are some tips on how to avoid an attack:

1. Make sure that every computers' operating system is kept current with system updates. Like your phone needs updates, all of your computers do too.
2. Ensure you run anti-virus software and it is also up to date.
3. Engage a professional IT consulting company if you are unsure what to do.

softtech

Wait, where are my computers?

Picture this scenario: it's 2pm, in the middle of production and Aliens swooped in and take all your computers across your entire business. What happens now?

Well Aliens may or may not exist, but the reality of some of these attacks, these mystery bandits can destroy everything on the affected computer, and anything that your computer can talk to, very quickly, without physical access to your building.

The reality is, while the hardware might physically power on after an attack, the whole computer needs to be reinstalled, a costly and time-consuming process. Multiplied by the number of computers in your business, the headache starts growing.

To read more articles about security and malware attacks please Visit Ars Technica or type http://bit.ly/2utCTVx

How to get up and running?

1. Assess your backups and restore strategy

People tend to think about backups when it's too late. There are three major steps to your backup and restore strategy:

1. Discovering what you need to backup.
2. Ensuring it gets backed up.
3. Checking that you can restore from your backups.

Go through everything that is stored on your computers, that is required to run your business, and ensure it is backed-up. Ask yourself when using important software/files 'are these part of my backups?' If not, then add them into your process.

backing up to multiple locations. having an external hard drive attached to your computer is only slightly better than having no backups. If your computer gets attacked by ransomware, there is agood chance that your external hard drive will be affected too. Have multiple locations both onsite and offsite/in the cloud. Think about how often backups run, this about the cost of losing a days' or a weeks' worth of data?

Finally, and most importantly check your backups are actually working. put a calendar reminder in to periodically check the backups are current and you can restore from them. There is nothing quite as frightening to an IT person, as to do a restore and the backup files don't work.

2. How do I get ten computers installed and running?

Here come the less obvious and harder tasks, like 'how do I get ten computers installed and running?' This is going to cost money, and take a lot of time.

It's a very good exercise to pretend everything has disappeared, you just have your phone and a credit card, how are you going to get up and running? Methodically work through a task list, this will help you to uncover holes in your backup strategy.

3. Access critical documents to get back up and running

Part of that "I only have a phone and a credit card" exercise is getting access to your critical documents & information, to recover from disaster and to keep your business running in the meantime.

Ensure you have some independent way of accessing critical data, that doesn't rely on your existing computer network. How will you know what customers were affected, where your insurance & IT company details are, how your payroll will work, where your passwords are stored...

Quite often many of the answers are 'well that's in a document in my blah folder...' wait, it doesn't exist now, which starts really making the headache bigger. The more questions answered in your disaster recovery plan, the better off you will be if you ever have to use it.

Creating your disaster recovery plan

Plan for the worst, hope for the best!

The more plans and checks in place, the more assurance you have in the worst-case scenario. Whether your systems are taken offline through a malware attack, or failed hardware, or theft by unscrupulous aliens, you can sleep easy knowing what to do and in what order to get your business back online again.

While we don't want to scare you, we do hope this guide has provided you some thought provoking tips that will help you safeguard your business going forward.

Need more help?

If you get stuck or want further advice, then we suggest you contact an independent IT consulting company to help you put plans in place. It's insurance for your business!

softtech