Are you Ransomware Ready?

4% of organisations say they are “very confident” of their ability to protect themselves against ransomware attacks.

By deduction, **96%** are not quite so confident.

Where does your business fit in?

StorageCraft.

What is **Ransomware?**

Ransomware is a type of malware that prevents you from accessing your data until you pay a ransom.

The number of ransomware attacks have been growing rapidly since 2015. In 2016, the occurrence of ransomware attacks nearly doubled, showing a 172% increase in the first half of 2016 compared to the whole of 2015.

This growth is being fueled by the rise of “Ransomware as a service”. This is a type of ransomware designed to be used by anyone with little or no technical knowledge.

These agents simply download the virus either for free or for a nominal fee, set a ransom and payment deadline, and attempt to trick someone into infecting his or her computer. If the victim pays up, the original author gets a cut - approx. 5% to 20% - and the rest goes to the “script kiddie” who deployed the attack.

The FBI estimates ransomware to be a $1-billion-dollar source of income for cyber criminals in 2016

Considering the amount of income it generates, it’s safe to say that this won’t go away anytime soon.

For the safety and health of your business, you need to be aware of the risks and take the necessary appropriate steps.

Ransomware
The facts

54%

Percentage of UK companies that have been hit by Ransomware

60%

of attacks demand ransoms of over $1,000

20%

of attacks asked for more than $10,000

1%

of attacks asked for over $150,000

58%

58% of UK companies pay up

32%

32% of UK companies lost files after refusing to pay

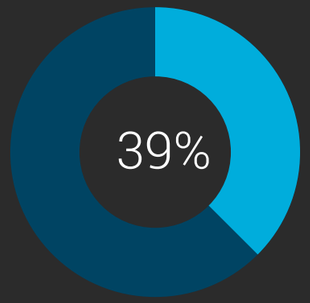
63%

63% experienced severe downtime

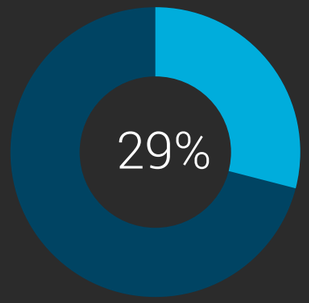
34%

34% lost revenue as a result of the attack

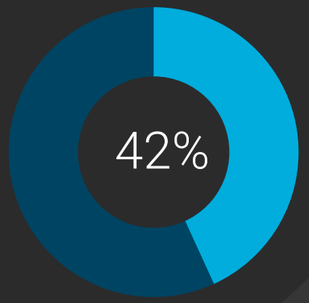
Ransomware exploits a company's weakest link: **their employees**



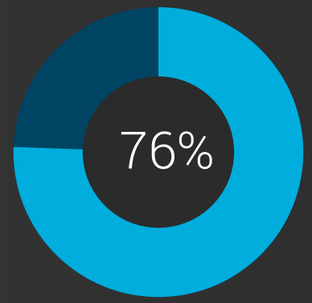
39% of organisations hit by ransomware said it came through an email



29% of companies said that the attack hit lower-level staff



42% hit mid-level managers



76% of UK adults don't know what ransomware is

Make Ransomware defense **everyone's** responsibility.

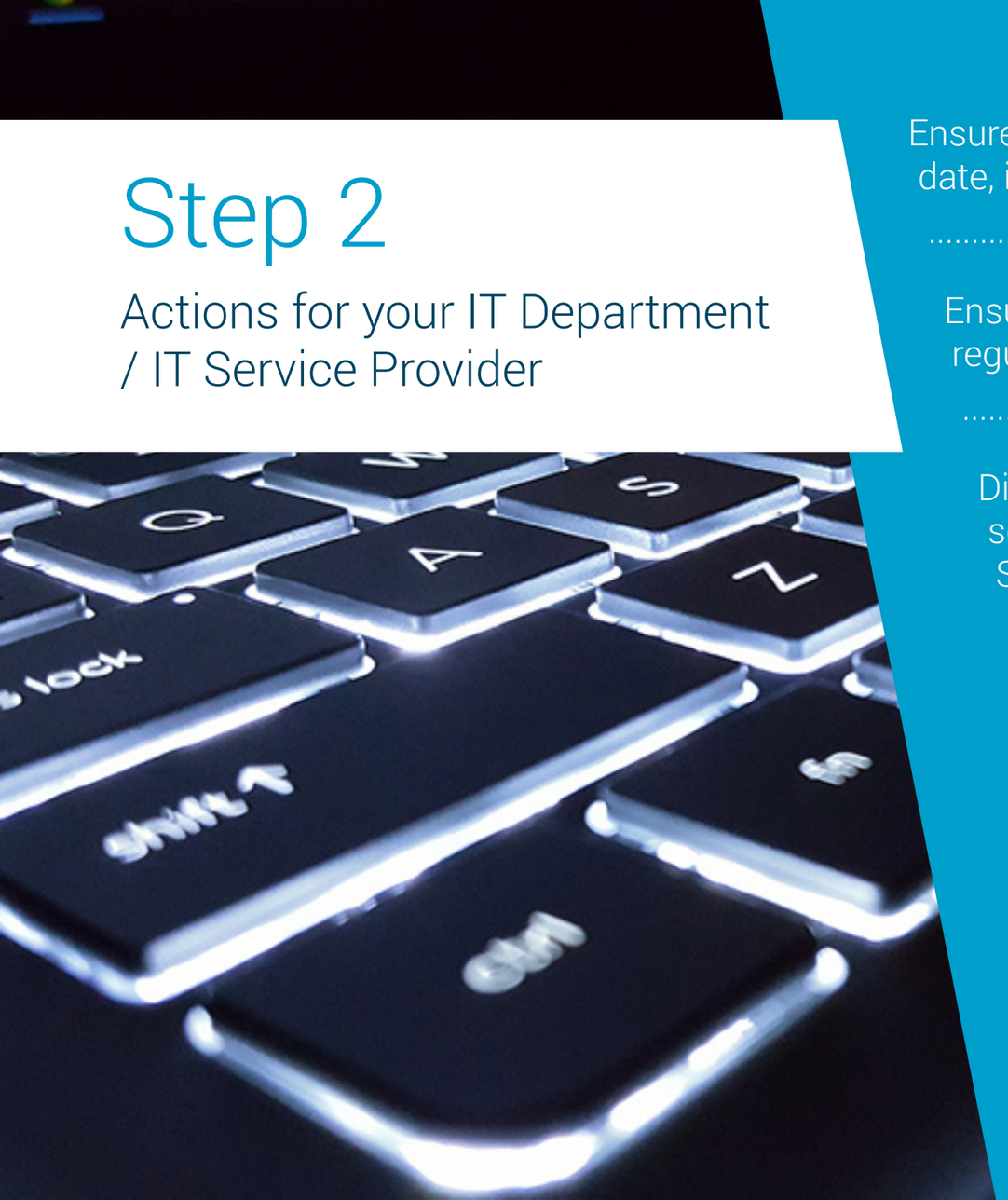
Step 1
Educate your employees

Best practices should include:

Scrutinizing links contained in emails and do not open attachments included in unsolicited e-mails.

Only download software - especially free software - from sites you know and trust. When possible, verify the integrity of the software through a digital signature prior to execution.

Invest in training for staff so that they are aware of how ransomware works (including Phishing).



Step 2

Actions for your IT Department / IT Service Provider

Ensure application patches for the operating system, software and firmware are up to date, including Adobe Flash, Java, web browsers, etc.

Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.

Disable macro scripts from files transmitted via e-mail. Consider using Office Viewer software to open Microsoft Office files transmitted via e-mail instead of full Office Suite applications.

Implement software restrictions or other controls to prevent the execution of programs in common ransomware locations, such as temporary folders supporting popular Internet browsers, or compression/decompression programs, including those located in the AppData/LocalAppData folder.

No users should be assigned administrative access unless absolutely needed. Those with a need for administrator accounts should only use them when necessary; they should operate with standard user accounts at all other times.

Step 2 continued...

Actions for your IT Department / IT Service Provider

Patch all endpoint device operating systems, software, and firmware as vulnerabilities are discovered. This precaution can be made easier through a centralized patch management system.

Configure access controls with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories or shares.

Use virtualized environments to execute operating system environments or specific programs.

Categorize data based on organizational value and implement physical/logical separation of networks and data for different organizational units. For example, sensitive research or business data should not reside on the same server and/or network segment as an organization's e-mail environment.

Require user interaction for end user applications communicating with websites uncategorized by the network proxy or firewall. Examples include requiring users to type in information or enter a password when the system communicates with an uncategorized website.

Implement application whitelisting. Only allow systems to execute programs known and permitted by security policy.

Step 3

Put a Disaster Recovery Plan in Place

In spite of all of the preventative measures you take - you need to plan for the possibility that you will get hit.

> “We were hit and not because we were careless. In the face of a targeted attack your preventative measures can (and often will) fall short. When this happens you need to have a DR plan in place.”

Jonathan Anstee - Scott Aerospace

Scott Aerospace successfully combatted a targeted Ransomware attack using StorageCraft Technology as part of their Disaster Recovery plan.

A Disaster Recovery plan is your last line of defense.

StorageCraft Technology has been the bedrock of Disaster Recovery solutions for over 10 years across 4 continents.

Drawing on our extensive experience here is what a good Disaster Recovery plan should have:

1. Back up

All backups are not the same. Here is what to look for in a backup.

A Image based snap shot technology is best of breed
Important note - There are still a lot of companies backing up to tape - this is hugely unreliable. Tapes get corrupted and wiped very easily. We hear horror stories all of the time of companies failing to restore from tape. Be warned!

B You need to be able to backup as often as appropriate (every 15 minutes for critical data)

C Being able to easily verify that your backups work

D You need to make sure that your whole environment / workforce are being backed up - including your remote workers and any SaaS applications you are using (e.g. Office 365 / G Suite)

E Ensure that your backups are not connected to the networks that they are backing up

Here is what a good Disaster Recovery plan should have (continued):

2. Offsite Replication

It is essential that you replicate your backups off site to ensure business continuity in the event of a site issue.

Backing up locally just might not be enough should a more destructive ransomware attack shared folders on your NAS boxes by accessing file services on your PCs. The best way to prevent this is to have uninfected backup versions stored in an offsite location.

A good Disaster Recovery solution will replicate your data to a location of your choice (maybe that's a second site within the company; or maybe a private or public cloud) and replicate to a schedule that suits you.

3. Testing

You **MUST** be able to test your Disaster Recovery plan. Do not let a disaster be your first test.

A good Disaster Recovery plan will be easy to test (and test often).

This is the only way that you can validate that your recovery time objectives can be met.

4. Recovery

It may seem obvious but sadly this is where a lot of so called "Disaster Recovery solutions" fail. Your Disaster Recovery must be able to recover your data every time and on time.

When a disaster like Ransomware hits, you want to be 100% confident that you can recover your data and get on with the job!

StorageCraft.

Conclusion

There is no silver bullet in dealing with Ransomware. The best approach is a multilayered one, incorporating educating staff; keeping your anti-virus software up-to-date; regularly software patching and most importantly having a robust and tested Disaster Recovery plan in place.

StorageCraft Technology is an award winning developer of Business Continuity and Disaster Recovery solutions. We work with a global partner network of managed service providers (MSPs) and value-added resellers (VARs) who deliver the StorageCraft Recovery Solution to end users around the world.

Business continuity starts here.

StorageCraft.

Sources

https://blog.barkly.com/ransomware-statistics-2016

http://www.computerweekly.com/news/450303068/UK-organisations-still-not-taking-ransomware-seriously

https://sentinelone.com/article/freedom-information-requests-reveal-6-10-universities-ransomware-victims-almost-23-targets-hit-multiple-times/

https://success.trendmicro.com/solution/1112223-ransomware-solutions-best-practice-configuration-and-prevention-using-trend-micro-products

http://www.cbronline.com/news/mobility/security/10-shocking-ransomware-stats-54-of-uk-companies-hit-by-ransomware-attacks-4970214/

http://www.itgovernance.co.uk/blog/ransomware-attacks-strike-hard-54-of-businesses-in-the-uk-hit/

http://uk.businessinsider.com/ransomware-as-a-service-is-the-next-big-cyber-crime-2015-12?r=US&IR=T

StorageCraft.