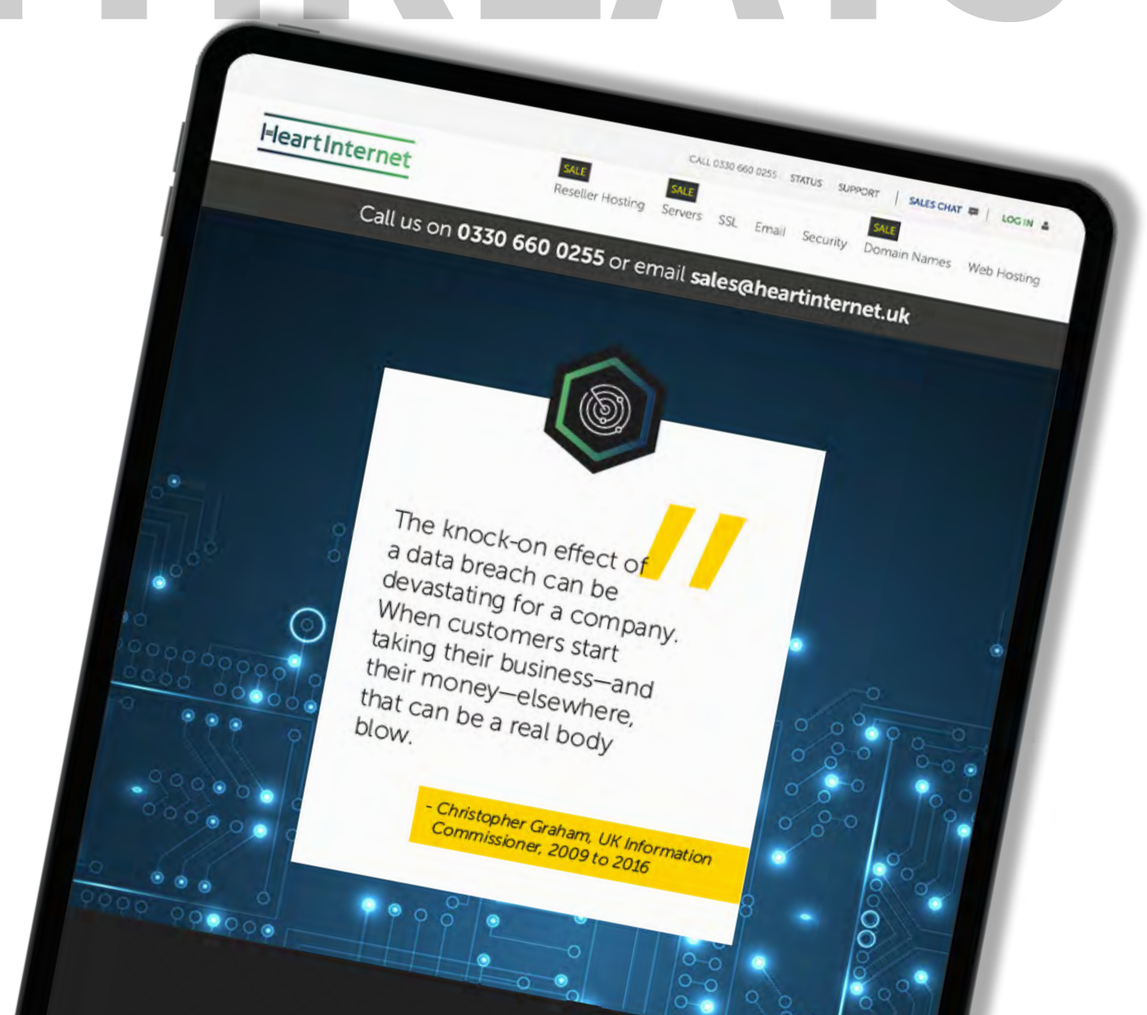
How to

DEFEND YOUR BUSINESS AGAINST A HACK ATTACK

Your guide to website security with:

powered by

HACK AWAY AT **SECURITY** THREATS



There's no way around it – the web is not a safe place. There's a hack attack every 39 seconds, and 65% of these attacks are aimed at small and medium-sized businesses. Website security is one of the most important aspects of doing business online, but for many, it's an issue that isn't thought about until something goes wrong.

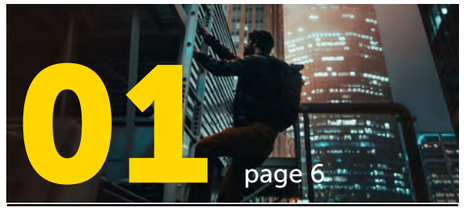
Heart Internet and Sucuri offer a website security & protection platform that delivers peace of mind. Stop worrying about website security threats and get back to building your online brand.

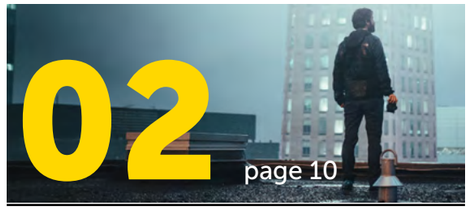
HeartInternet

powered by SUCURI
Real People. Real Security.

FEELING SECURE MEANS FEELING CONTENT...

Security:
it's time to start a new chapter.





CHAPTER 1

YOUR BUSINESS IS NOT SAFE FROM CYBERCRIME

> Cybercrime is the greatest threat to every profession, every industry, every company in the world.
>
> *- Ginni Rometty, CEO of IBM*

THE MALEVOLENT SEVEN

Cyber security has never been more important. These are the 7 stats you need to know about YOUR business's security.

69% of cyber attacks come from outsiders[5]

65% of cyber attacks are aimed at SMBs[3]

146 Days
The average length of time an attacker spends within a network before being detected.

230,000
new malwares are produced every day[2]

£4.6 trillion/year
How much cyber attacks will cost business, worldwide, by 2021[4]

60% Of SMBs hit by a cyber attack never reopen[4]

There's a hacker attack every **39 seconds**[1]

Heart Internet

www.heartinternet.uk

CHAPTER 2

HOW TO STOP CYBER CRIMINALS GETTING INTO YOUR WEBSITE

> Passwords are like underwear. You should change them often.
>
> *- Eric Griffin, PC Mag Online*

ARE YOU WORRIED ABOUT THE CYBER SECURITY OF YOUR BUSINESS?

You should be!

What are the dangers to my business?

Compromised data.

Businesses store a lot of information about their customers, including market research, website analytics data, account details and personal information. This is exactly the sort of information that hackers are looking for. Once they have captured your customers' information - such as financial information, intellectual property, employee records, passwords, etc - they can either use that information themselves, or sell it on to criminal organisations that will use it.

Damaged reputation.

If a business has been the victim of a data breach, it has been guilty of not showing due care and attention of the data you store. There was a bond of trust that has been broken. This can generate bad publicity if the press gets hold of the information (and it's a slow news day) but, more importantly, customers who no longer trust that business will be taking their custom elsewhere. And who can blame them?

Financial repercussions.

The damage caused by a cyber attack cuts both ways - it impacts on the customers and may cause them problems, but it also costs the business reputation, custom and revenue. Then there are the longer-term repercussions which can include massive GDPR penalties and lawsuits. Many businesses never recover.

Gone phishing: have hackers got me on the hook?

A phishing scam is when you get an unsolicited email with dodgy links to click or attachments to download - but some of these phish have teeth - so just don't, ever! Malware contracted from an innocent-looking email can infect an entire system - so you need to be vigilant. Thing is, now that AI (artificial intelligence) and NLP (natural language processing) is improving, these computer-generated emails are sounding ever-more genuine and convincing. How do you spot them?

Check if you have an account with them

If you receive an email from ReallyBigBank and you don't have an account with them, then it's almost certainly a phishing scam. If you do have an account, but you're suspicious of the message, contact them independently and check whether it's legit. If it isn't, they'll be grateful to you for the phishing scam information.

Check to see if it is asking for personal info

No reputable organisation will send an email asking you to re-enter your password or your login details through an email link; nor will they ask for your NI number, your PIN number, etc. If they do, treat them with suspicion.

Check the 'From' address

Hover your mouse over the address, a drop-down should appear with the return email address. If it isn't EXACTLY right (for example '@your-bank' instead of '@ yourbank') or the address ends differently from the address you might expect (ending .com when you would expect .co.uk, for example) treat it with suspicion.

Check the greeting

Does the email address you by name and is that name correctly formatted? If it doesn't greet you by name, or it uses your full email address instead of your name, treat it with suspicion.

Check the spelling, grammar and punctuation

The software is getting better at this, but it isn't always perfect. So, if the email reads like it's written by a computer, or by someone who isn't a native English speaker, treat it with suspicion.

Check the urgency

If the message offers an incentive for you to fill in the information by a certain time, or threatens that you'll miss something, or be punished if you fail to do so, treat it with suspicion.

Is the Internet of Things watching me?

As more devices become "smart", there are more opportunities for hackers to get into your business. Forbes Magazine isn't pulling any punches when it says "hackers can now gain access to anyone's networks through either a thermostat, digital locks, refrigerators, baby monitors, light bulbs, smart meters and so much more. It is a no-brainer that securing the IoT is fundamental to the well-being, privacy, data security, personal safety, and security of everyone and everything".[10]

So, if you're installing any smart objects in your business, or workflow - do your due diligence. Check out the security features these devices have and investigate the security implications they might bring to your business.

Are hackers putting the brakes on my supply chain?

As larger businesses develop better security, predators will move down the food chain, looking for small businesses without the resources for better security. Don't be the weak link in someone else's supply chain, and ensure that your suppliers aren't the weak link in yours!

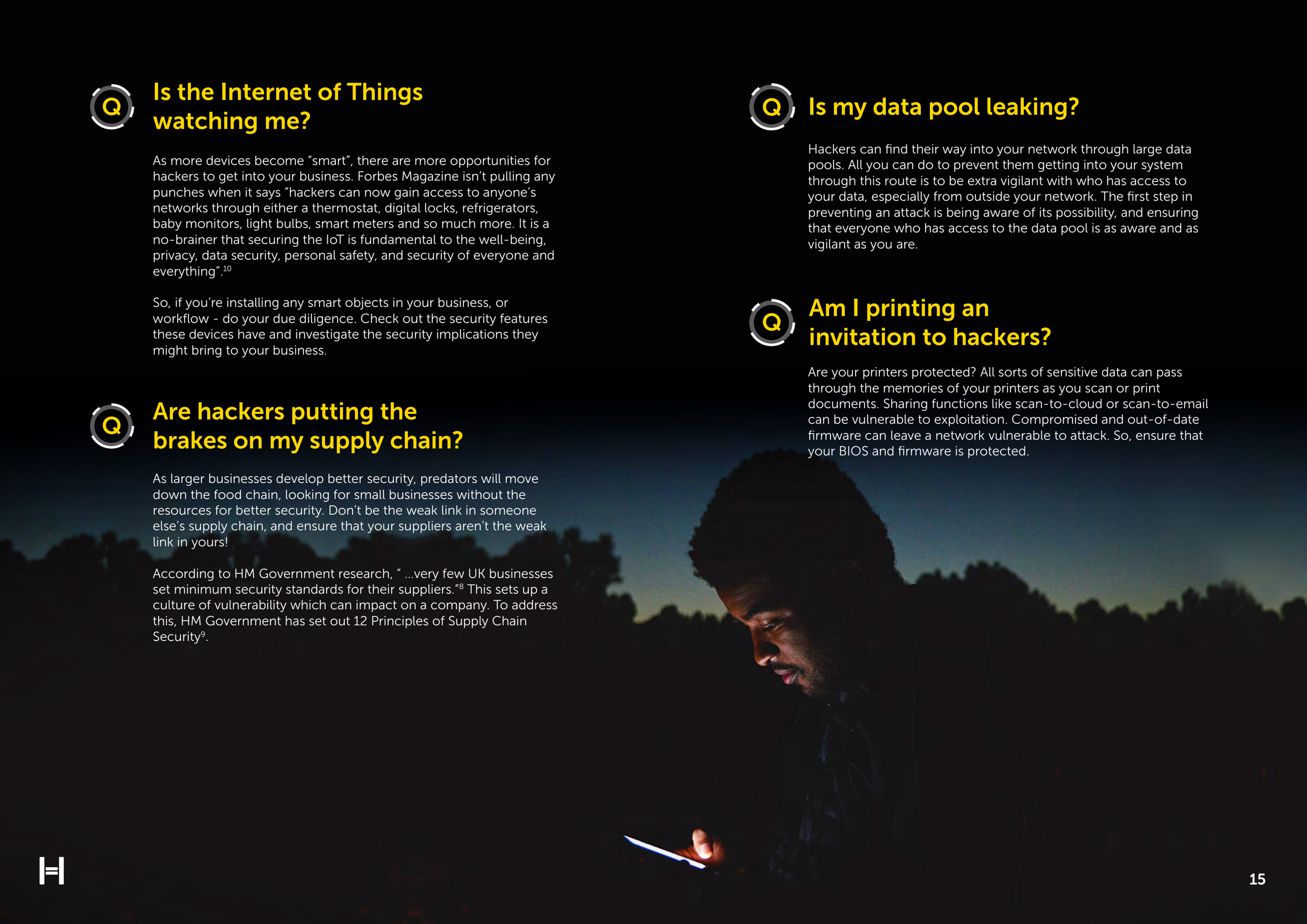
According to HM Government research, " ...very few UK businesses set minimum security standards for their suppliers."[8] This sets up a culture of vulnerability which can impact on a company. To address this, HM Government has set out 12 Principles of Supply Chain Security[9].

Is my data pool leaking?

Hackers can find their way into your network through large data pools. All you can do to prevent them getting into your system through this route is to be extra vigilant with who has access to your data, especially from outside your network. The first step in preventing an attack is being aware of its possibility, and ensuring that everyone who has access to the data pool is as aware and as vigilant as you are.

Am I printing an invitation to hackers?

Are your printers protected? All sorts of sensitive data can pass through the memories of your printers as you scan or print documents. Sharing functions like scan-to-cloud or scan-to-email can be vulnerable to exploitation. Compromised and out-of-date firmware can leave a network vulnerable to attack. So, ensure that your BIOS and firmware is protected.



BE VIGILANT, NOT A VICTIM

But, how do you defend yourself against burglars who are invisible and who break in through your wires and software?

You can implement simple protection protocols throughout your workflow, each of which will make it harder for cyber criminals to breach your security.

Passwords.

Best practice is to use a complex and different password for each account - something that a hacker can't guess, or an algorithm can't work out. Of course, remembering each of those passwords can be a task in itself, but there are various tools you can use to help keep these passwords safe and available. Also, don't forget to use passwords or PIN numbers on your mobile devices.

Secure URLs.

Only visit websites which are secure. Most web-browsers, these days, will tell you if you are visiting a website which isn't secure. You can also check for yourself - look at the URL bar, if the address begins 'https://' - that letter 's' tells you the site has an up-to-date security certificate. There should also be a little lock icon next to the address. Although, don't rely on this entirely - cunning cyber criminals can fake the lock icon. So, even if the URL says it's secure, if the site doesn't look right, leave!

Back it up.

It's always a good idea to make backups of your data, whether you use your computer for fun, for social, or you run a multinational corporation. Backups are a vital part of any business. They protect you against everything from cyber attacks, to server failures and natural disasters. They even come in useful if you accidentally delete that thing you didn't want to delete. Also, most hosting packages and website builders will include an option for automatic backups.

Don't be too social.

Social media is a great place for cyber criminals to find out personal information about you - including birthdays, the names of friends and family, addresses, even favourite films and books - all the kind of information that you use when creating an online account. Never share anything like this, and make sure that your social media Privacy settings ensure only your Friends see what you do share.

So, make use of the technology that exists to keep you secure!

CHAPTER 3

HOW TO EVICT CYBER CRIMINALS FROM YOUR WEBSITE

> It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it
>
> *- Stéphane Nappo, Global Chief Information Security Officer of the year, 2018*

SO, YOU THINK YOUR WEBSITE HAS BEEN HACKED?

What do you do: First thing's first - don't panic. All is not necessarily lost. Look at this picture of a cute and cuddly kitten and take a breath.

OKAY? CALM NOW? GOOD.

Right, you need to know that help is out there.

HELP, I THINK I'VE BEEN HACKED

Give Google a go

Google's Web Fundamentals reference guide offers really useful advice on what you need to do if you think your website has been hacked[11]

Step 1: Verify that you own the site.

The road to recovery starts with verifying ownership in the Search Console. Sign into the Search Console[12], click "Add a Site", enter in your site's URL and then continue through the process.

Step 2: Inform your web host.

Once you have verified your site with Google, you need to let your web host (hopefully, that'll be us at Heart Internet) know that your site has been hacked. This allows us to take measures to protect you from further harm, and we can also help you find out how your site was compromised in the first place.

Step 3: Take your site offline.

This prevents hackers from causing further damage and also prevents visitors from seeing a malware alert when they visit your site.

Step 4: Review and clean all accounts.

Once your site is offline, review user accounts, especially the newest ones. Anything that looks suspicious, delete. And change all the passwords for all site users, accounts, FTP, database access, system administrators, CMS, and anything else that requires a password. All of 'em. No exceptions. You may never know which account was compromised, so assume they all were.

Step 5: Determine how you were hacked.

Check the messages in your Search Console to see if you received any information on what your site was used for. Was it serving spamming pages or links? Phishing? Distributing malware? You can also go to Security Issues to get more information.

Step 6: Disinfect.

Remove anything that was added by the hacker – content, links, images, users, whatever. Do a clean install of your software and program updates and eliminate the third-party widgets you rarely use. If you have access to the root of your server, do a clean installation from the ground up. And if you have any backups, make sure you only upload the files you know are clean.

Step 7: Ask Google to review your site.

Once you've verified ownership, cleaned up your site and put it back online, it's time for a Google review. This is important as it should result in all the warnings being removed.

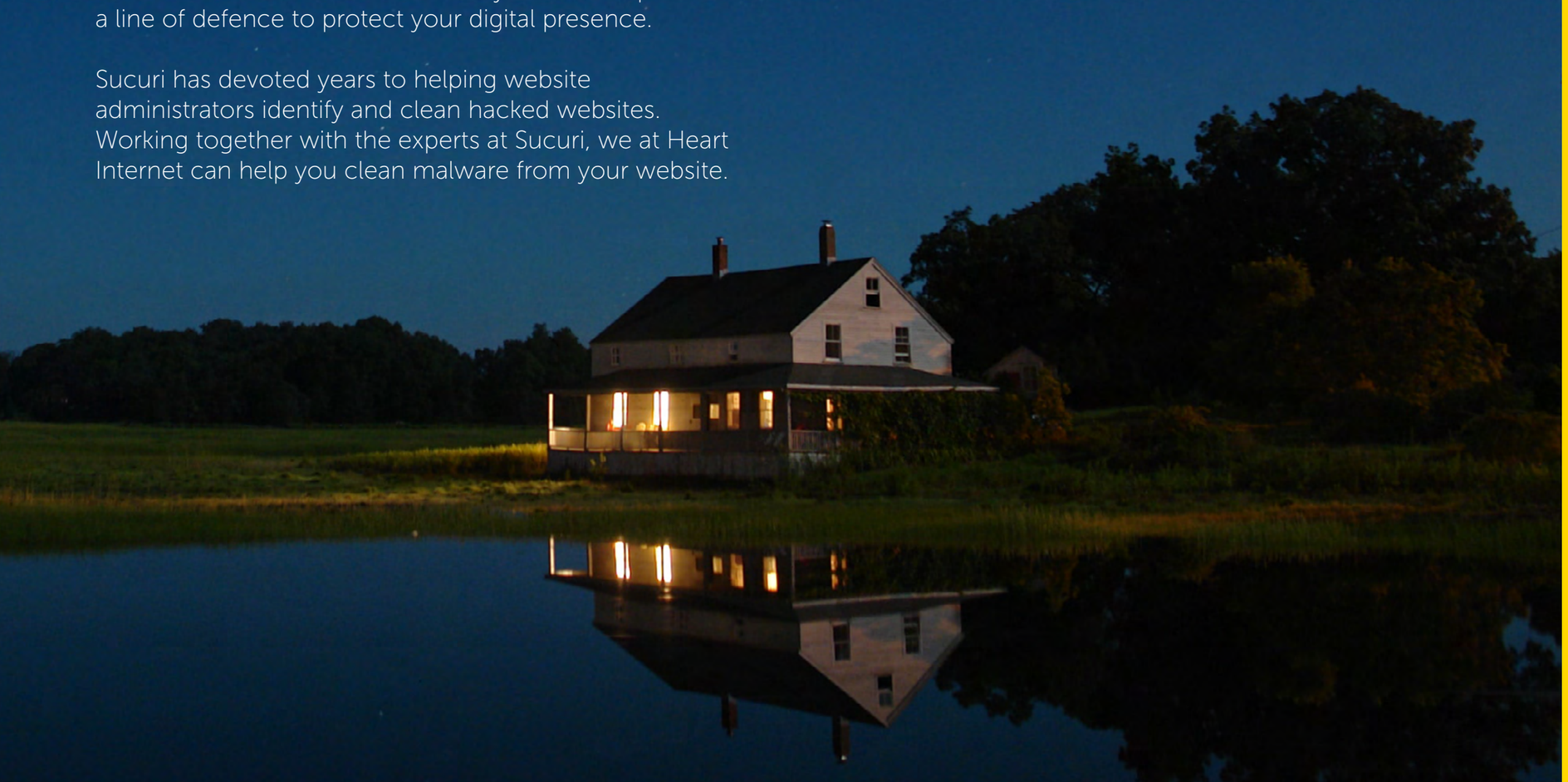
Just request a review[13] and follow Google's instructions. If you've followed all the steps properly, they'll find that your site is clean and remove the "this website is not safe" warning. Then you'll be good to go again!

PROTECT YOUR ONLINE HOME

BY BEING SUCURI SECURE

If you're busy running your business, finding time to safeguard your website can be tricky. And, given that evicting hackers is so critical, having backup from web security specialists can be pretty reassuring. That's what we do at Heart Internet. Powered by Sucuri, we provide a line of defence to protect your digital presence.

Sucuri has devoted years to helping website administrators identify and clean hacked websites. Working together with the experts at Sucuri, we at Heart Internet can help you clean malware from your website.



This process includes (but isn't limited to)

- Scanning your site down to the server
- Checking core file integrity
- Checking recently modified files
- Checking diagnostic pages
- Checking PCI DSS (Payment Card Industry Data Security Standard) compliance

We can then

- Clean hacked files
- Clean hacked databases
- Secure user accounts
- Remove backdoors
- Remove malware warnings

Finally, we can restore your wesite and

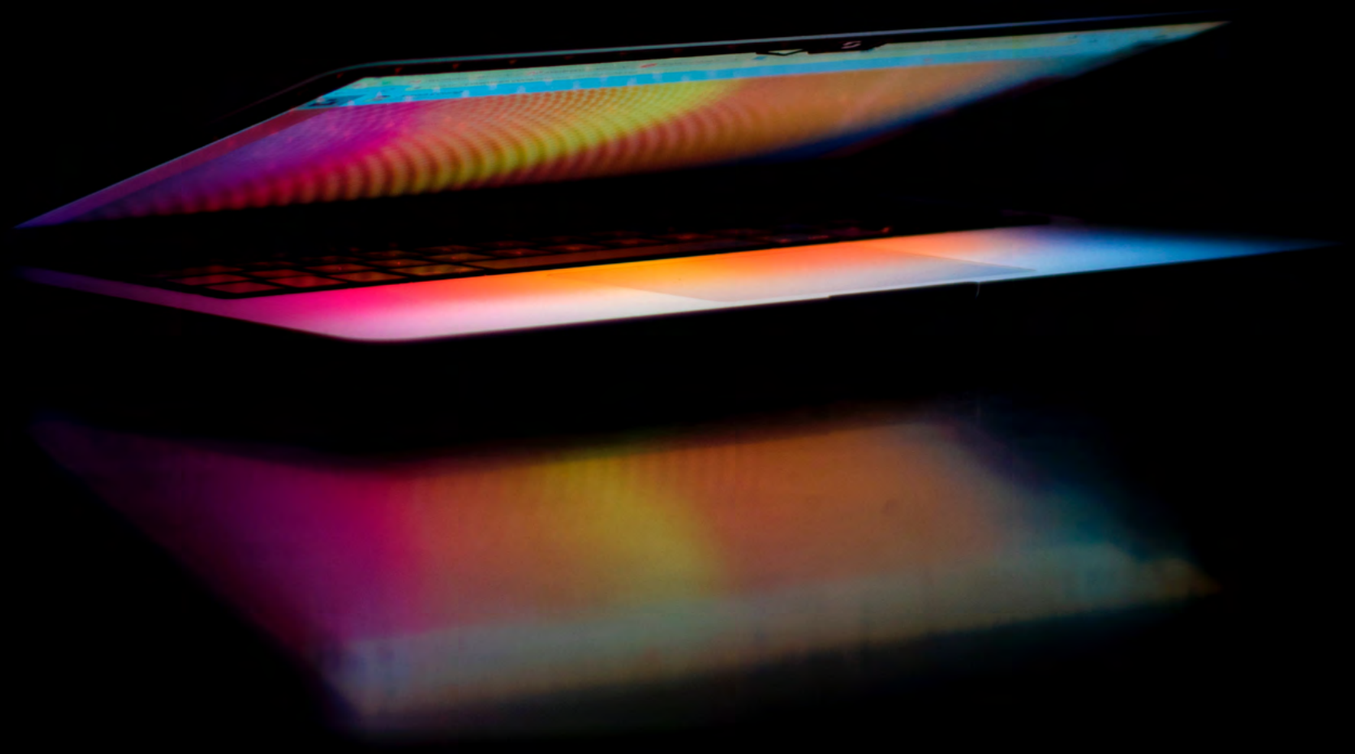
- Reset configuration settings
- Reset passwords
- Harden your server
- Set backups
- Scan your computer
- Create a firewall

Heart Internet

powered by Sucuri
Real People. Real Security.

CHAPTER 4

HOW TO MAKE YOUR BUSINESS DISASTER-PROOF



> Try to turn every disaster into an opportunity.
>
> *- John D. Rockefeller*

74%

OF SMBs HAVE NO DISASTER RECOVERY PLAN[14]

Whether you call it a ‘Disaster Recovery Plan’ or the slightly less apocalyptic-sounding ‘Business Continuity Plan’, it prepares your business for the same thing: zombies!

Okay, so disaster doesn’t have to be zombies (much as you might like it to be), it can strike in many forms - it could be a fire, flood or phishing scam - they all have the capacity to wreck your business.

As well as investing in a backup generator or some form of uninterruptible power supply, and having the right insurance, you could spend a moment familiarising yourself with the British Red Cross’ advice on how to prepare for emergencies[15].

You also need to make provision to recover your data if disaster strikes.

Because a business disaster doesn’t even have to be an event that affects people outside your company; it can be as simple as a hard-drive failing at the wrong moment, or a power-cut, or an employee accidentally overwriting a line of code.

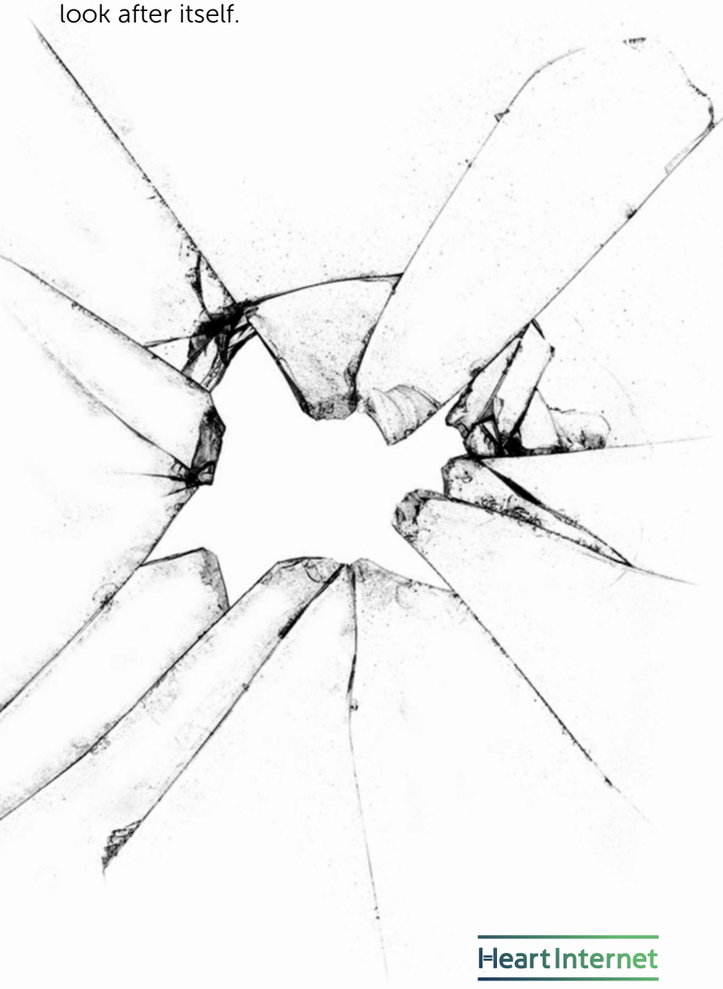
IF YOU FAIL TO PLAN, YOU’RE PLANNING TO FAIL[16]

Without a Business Continuity Plan, these tiny problems can quickly spiral into the end of the world for your business. So, how do you plan to not fail?

As uncomfortable as it may seem, you have to do an honest audit of your business and list all of the people, services, technology and supplies you are dependent upon; then think about what would happen if each of them was taken away. Just think about things that directly affect your business - things that you can control.

You don’t need to work out a detailed strategy for every eventuality. After all, if aliens invade or Godzilla stomps through your city, you’ll really have more pressing matters to concern yourself with than making sure your work is backed-up!

That said, having a written-down plan for what to do if a hard drive fails, will also cover you in case Cthulhu monsters rise up out of the sea and invade the land. So, take care of the little picture (your business) and the big picture (the rest of the world) will look after itself.



WHAT SHOULD AN IT RECOVERY PLAN INCLUDE?

- A log of all your IP addresses.
- A schedule of regular off-site backups.
- Contact details of people in the company you need to reach in case of a problem - in order of importance.
- Designated people to make these calls, in case managers are away or incapacitated.
- A detailed list of vendors who can service, restore or replace your technology quickly - including any passwords or customer reference numbers needed to access that support.
- The location of important documents relating to your tech, such as device serial numbers, and other important details (including an archive of necessary passwords and profiles).
- A clear indication of where your data backups are located and how to retrieve them.
- Ensure all staff are aware of this plan and understand what to do in case of a problem.

The TechTarget network has compiled an essential guide to business continuity recovery[17]; this includes a free IT Disaster Recovery Plan, which you can download and adapt to your own business's needs.

Backups

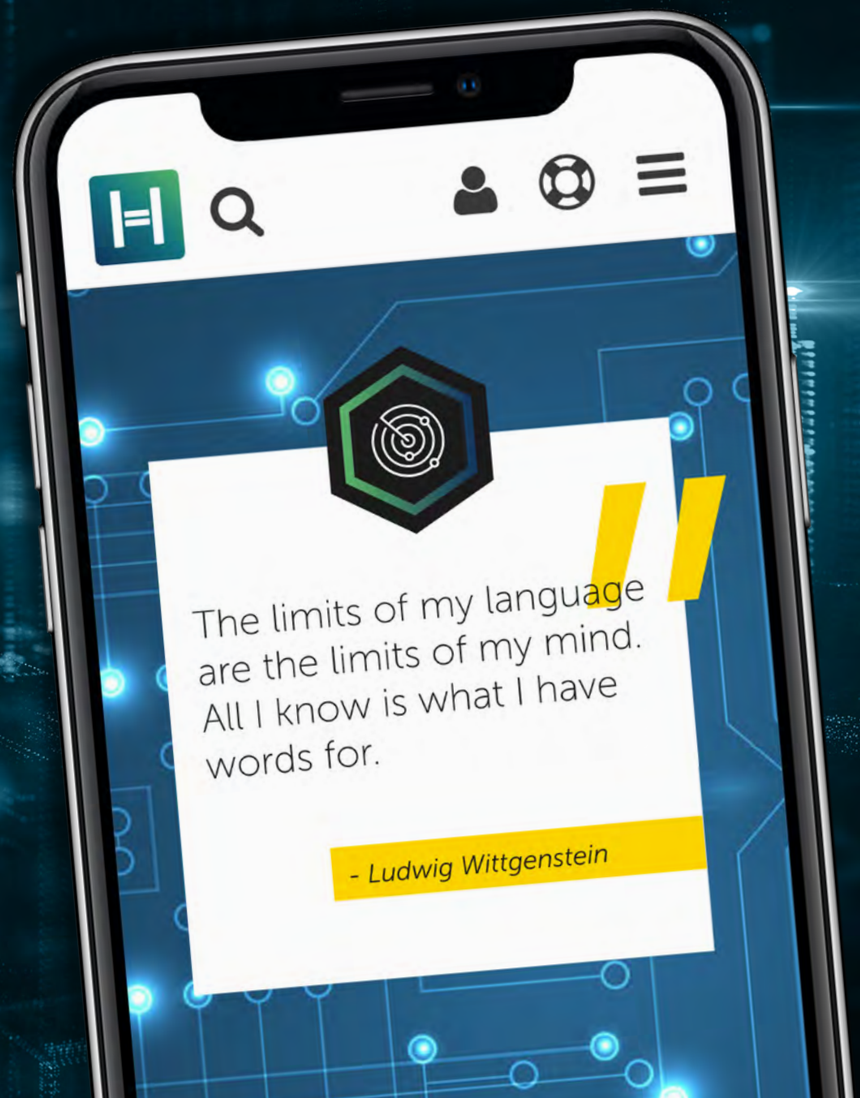
You should have a plan to securely and regularly backup the data from every single piece of technology you have on hand – from your company mobile, to your web server, to that dusty printer in the corner, the one under the boxes.

Once upon a time, making backups required a stack of discs, or at least an external hard-drive that you could take off-site. Now, thanks to the cloud, you have no excuse not to schedule regular, automatic backups of every scrap of data your business relies upon.

Hopefully, the time you spend creating a hacker-proof, water-proof, disaster-proof Business Continuity Plan will be time wasted, because you'll never need it. But a plan is a form of insurance and, as with any insurance, it's better to have it and not need it, than need it and not have it!

CHAPTER 5

CYBER SECURITY: KEYWORDS



WHAT'S YOUR SAFE WORD?

As with anything to do with computers, the whole subject of cyber security is littered with impenetrable acronyms and complicated turns of phrase. Hopefully, you'll be able to navigate your way through this guide, and the process of ensuring the health and welfare of your business' computer network, with the terms we define for you, here:

Backup (or Data Backup)

this is when a copy of the data in a computer is made and stored elsewhere, so that it can be used to restore data after a loss event or cyber attack.

Brute force attack

this is an attempt to crack a password or username using software to generate sequential passwords in a trial and error approach, until it eventually stumbles on one that works.

CDN (Content Delivery Network)

this is group of servers which work together to share the load of delivering your website to users, increasing the speed your website loads, and reducing the danger of hack attacks.

Cross-site attack (Cross-site scripting)

this is when an attacker infects a website, allowing them to intercept transactions on that website, or to infect users of that website.

Cyber attack / Cybercrime

this is any illegal attempt to access a computer network, to alter, disable or destroy software or data within that network, for the purpose of stealing the data, depriving the owner of it, gaining secret, unauthorised access to it or making illegal, unauthorised use of it.

Cybercriminal

this is a person who uses computers or software to commit crimes, either alone or as part of an organised crime gang.

Cyber security

this is the process used, or the software employed, to protect computer hardware, software and/or data from corruption, theft or damage and the implications thereof.

Data breach (or Data leak, or Personal data leak)

this is the intentional (or accidental) release of secure or private and confidential information from a secure environment into an insecure or public environment.

Data pool

this is a Gateway to a Synchronised Data Network which allows for standardised transactions between trading partners.

DDoS (Distributed Denial of Service) attack

this is when a cyber criminal makes a service or network unavailable, usually by bombarding it with enough spurious communications to overload (or 'crash') the system and prevent it from completing legitimate transactions.

Firewall

this is a network security system that monitors and controls incoming and outgoing network traffic to your website and/or to your computers, forming a barrier between your internal system and potential threats from outside.

Hacker

this is a person who attempts to intentionally access or harm your computer systems without authorisation (or without sufficient authorisation) by deliberately circumventing or defeating security systems.

Injection attack

this is when an attacker injects code into a program to alter it, or injects malware onto a file to infect it.

IoT (Internet of Things)

this is a system of interconnected computer-controlled devices which do not require human-to-computer interaction. When humans do interact with them, it is usually via devices such as smart phones and smart speakers.

Malware

this is any malicious software, script, or code run on a device that alters its state or function without the owner's informed consent.

Network

this is a group of computers and devices (such as printers) connected together to share data and resources.

Phishing

this is when a cyber criminal contacts you in a personal way (such as 'Dear customer' or 'Hello friend') and asks you to submit your personal information, such as passwords, or to click a link, which will almost certainly download malware onto your computer.

SMB (Small to Medium-Sized Business)

there is no hard and fast definition of what makes a small or medium-sized business; but a business with less than 100 employees would generally be considered small, while one with between 100 and 1,000 employees is considered medium-sized.

Spear Phishing

this is a phishing attack where the cyber criminal pretends to be a bank or other financial organisation. These are harder to spot because they can be addressed to you directly.

Trojan

this is a type of malware that can be hidden within seemingly-safe pieces of software. It takes its namesake after the mythical Trojan Horse which, disguised as a harmless gift, was trotted inside the impenetrable walls of Troy. Of course, as legend has it, the horse was full of soldiers who ransacked and burned down the city.

Zero-day exploit (or Zero-day vulnerability)

this is a flaw in the security of a piece of software which hackers have noticed and for which programmers have not yet created a software patch, to repair the flaw. Zero-day means that the flaw is exploited immediately upon being discovered by the hackers.

References:

1. Source: University of Maryland (https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds)
2. Source: Panda Security (https://www.pandasecurity.com/mediacenter/press-releases/all-recorded-malware-appeared-in-2015/)
3. Source: Kelser Corp (https://www.kelsercorp.com/blog/press-release-kelser-enables-mid-size-companies-to-defend-forward-against-cyber-attacks)
4. Source: Forbes (https://www.forbes.com/sites/ivywalker/2019/01/31/cybercriminals-have-your-business-their-crosshairs-and-your-employees-are-in-cahoots-with-them/#1d051b8a1953)
5. Source: Verizon (https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief-emea.pdf)
6. Source: Microsoft (https://www.microsoft.com/en-us/microsoft-365/enterprise-mobility-security/advanced-threat-analytics)
7. Source: Cybercrime magazine (https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/)
8. Source: HM Government (https://www.ncsc.gov.uk/collection/supply-chain-security)
9. Source: HM Government (https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security)
10. Source: Forbes (https://www.forbes.com/sites/cognitiveworld/2019/06/27/investing-in-the-internet-of-things-security/#65b3a7b23d59)
11. Source: Google Web Fundamentals (https://developers.google.com/web/fundamentals/security/hacked/)
12. Source: Google Search Console (https://search.google.com/search-console/welcome)
13. Source: Google Web Fundamental (https://developers.google.com/web/fundamentals/security/hacked/request_review)
14. Source: (https://readwrite.com/2013/02/22/the-severe-impact-natural-disasters-can-have-on-small-businesses-infographic/#awesm=~o8FvvENnpjlhVh)
15. Source: (https://www.redcross.org.uk/get-help/prepare-for-emergencies)
16. Benjamin Franklin never said this. The internet is lying to you about that! (https://quoteinvestigator.com/2018/07/08/plan/)
17. Source: (https://searchdisasterrecovery.techtarget.com/essentialguide/Essential-guide-to-business-continuity-and-disaster-recovery-plans)

IF IN DOUBT CALL THE EXPERTS OUT

WHAT SUCURI WEBSITE SECURITY DOES FOR YOU

Alert

Remove malware from your website as soon as it appears.

Secure

Know about security issues immediately with regular notifications.

React

Stop future hacks with our Web Application Firewall.

Improve

Make your site even faster with our built-in CDN.

Heart Internet

Heart Internet

www.heartinternet.uk