CAUGHT IN THE CROSSHAIRS

Why every business in London is under dual attack from both hackers and the government, and what you can do about it

Ben Schneider

Director of ITGUY London

Book and cover designed by Luciene Calabria
Icons made by Freepik from www.flaticon.com

CAUGHT IN THE CROSSHAIRS

Why every business in London is under dual attack from both hackers and the government, and what you can do about it

Ben Schneider

Director of ITGUY London

Contents

"By failing to prepare, you are preparing to fail."

Benjamin Franklin

Introduction

It's hard to understate the importance of IT for businesses in 2018. Companies rely on their computer systems and communications to be able to operate, let alone grow. And yet, the number of businesses that get caught out each year by cyber attacks is at an all-time high: 46% of UK business had some sort of breach in 2017 according to a UK Government report.*

Add to this, the new data protection regulation (GDPR) that comes into force in May 2018, and the obligation to act takes on legal and financial implications for every single business: your business: our business! Unless you have in-house IT support, you are most probably going to need some help. ITGUY London can help your business navigate the treacherous waters of IT data compliance and security and hopefully, we can guide you to a safe port in the approaching storm.

* Cybersecurity Breaches Survey 2017. Link:
https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017

1
This is your data security nightmare

Have you noticed recently just how often data security scares seem to be in the mainstream news? Whether it's the NHS being practically shut down by hackers, or yet another large organisation like Yahoo, Uber or Ashley Madison having to admit it got hacked in a major way, data security has become almost daily news.

This is a hallmark of the information age we are currently living in. Yet the problem with the media reporting the very biggest hacks means that normal businesses (like yours) feel as though they are not at risk.

This is absolutely, 100% not correct.

As a Managed Service Provider (MSP) looking after a large number of businesses in London, we see normal companies being targeted by hackers every single day of the week.

As technology has become more sophisticated and flexible over the last decade, so have the hackers. All they need is a small foot in the door, and they can do real damage to an unprepared business.

But hackers aren't the only risk. Our government is another source of risk to your business, thanks to the new GDPR, the General Data Protection Regulation.

Here's a good analogy. Think of your business as a 17th-century boat in the ocean. It's loaded with valuable treasure (data), and you are the captain.

For years you've been able to collect this treasure with little real risk. The authorities have more or less ignored how you collect this treasure

and what you do with it… and the pirates who want to steal the treasure have been focused on plundering the biggest ships in the sea.

However, times have changed and now your boat is currently under attack from both sides.

To your left is a pirate ship. This is where the hackers are. They're trying every trick in the book to steal your treasure. Or lock it away and force you to pay to get it back.

They're constantly firing cannons at you. Trying to board your boat. Sneaking up on you in the dead of night. Cutting a hole in the bottom of the boat so they can obtain access without your knowledge.

The pirates are not a single organised group. They are a collection of motivated and fierce warriors, who both work individually and together for gain. They don't care what treasure they get their hands on, as they know that all treasure has a buyer somewhere.

But what makes them particularly dangerous is their R&D department. They have clever pirate colleagues who are constantly designing new weapons and finding new ways to get into your boat.

It's exhausting just thinking about their constant bombardment. The only respite comes from the fact they are attacking all treasure ships, all the time. They don't care where the treasure comes from. They just keep constantly testing the defences of all the boats until they find a weakness.

There's another boat in the sea. To your right is a military ship. This is the government.

Over the last few years, it has become more and more aware of the pirates and is a little embarrassed at its inability to control them.

So instead of tackling the pirate problem, the government has produced a list of guidelines about the defences you must have on your boat.

The list is a little vague, and none of the captains is 100% sure exactly what the government wants. What is clear is that you must protect your treasure from pirates at all costs.

And if any of your treasure is stolen or compromised by pirates, then you have to tell the government straight away.

They will then make an example of you. For a small breach, they may make you walk the plank. For more serious problems, the military ship will aim its cannons at your boat and try to blow it out of the water.

As the captain of this boat, you are caught in the middle of a big battle. And yet that's not even your primary mission.

Your real job is to steer your boat towards a specific destination (think of this as your business's goals). You get paid when the boat reaches port and not before.

For years you've been able to ignore the battle, but the noise is getting louder and louder and it's starting to take up more of your attention.

This is the point where everything changes. The introduction of GDPR and the sheer weight of criminal attempts to steal your data means you must now comprehensively and definitively defend your boat. So you can ignore the battle, and stay focused on the seas ahead.

Let me introduce a fourth boat. It's my boat. My boat is full of highly trained and experienced mercenaries. They know how to keep the pirates at bay. And they know exactly what the military wants to keep it happy.

My boat can clear a path towards your destination. My mercenaries can fight your battle for you. So you can stay 100% focused on the challenges of captaining your boat.

This book is an introduction to the data protection work we do for businesses like yours. In these pages, we will introduce you to the powerful concept of **Predict > Plan > Protect**.

This means anticipating data security problems before they happen, putting in place a data protection policy, and taking daily proactive action to prevent problems.

When you have read this, we'd love to have a no obligation chat about your business. You can call me or my team on **020 7241 2255** or email us at **info@itguy.com**

2
When it goes wrong, it's catastrophic

We live in a wonderful world of everything on demand, where practically anything you could ever want is instantly available on your phone.

With this in mind, a prime example of a data breach with catastrophic consequences was highlighted in 2015, when the discreet but highly publicised company, Ashley Madison, was hacked by a group calling itself The Impact Team. At the time, Ashley Madison claimed to have 37.6 million members worldwide.

The impetus for new members to sign up to the service was that they would remain anonymous, and 100% discreet. This was positioned as a safe service.

And so it was… until July 2015, when The Impact Team threatened to release the stolen website's user data unless Ashley Madison was immediately shut down. A month later they leaked more than 25 gigabytes of company data, including user details.

In the days following the breach, extortionists began targeting people whose details had been released, trying to scam bitcoins from them. A website was set up where people could type in their spouse's email address, to see if they had been a user.

The emotional and relationship impact on many of the site's users is documented online. What's not widely known is the financial impact on the business itself.

It's likely to have been significant. Because this was a business based on trust. It promised discretion and anonymity.

Yet don't all businesses – including yours – exist because of huge

amounts of trust with clients and customers? There is an assumption by buyers that when you transact with a business, your data is safe. It's a real shock when it goes wrong.

Here's another example, closer to home and with greater consequences for more people.

In May 2017, the NHS was forced to cancel at least 6,900 appointments and divert ambulances away from hospitals, after its computer networks were compromised by something called WannaCry ransomware.

Unlike hackers stealing data, WannaCry had a different tactic. It encrypted data held on infected computers and demanded the user paid a ransom of £230 per machine to unlock the data.

It wasn't just the NHS that was targeted. WannaCry spread to computers across 150 countries.

So why was the NHS so badly hit? Put simply, it was relying on older operating systems. The WannaCry software used an exploit in Windows 7 that had actually been patched by Microsoft a few months before… but the patches hadn't yet been applied by many NHS trusts.

The BBC reports that an assessment of 88 out of 236 trusts covered by NHS Digital before the attack, found that none passed the required cyber-security standards.

There's a real risk in me highlighting Ashley Madison and the NHS as case studies. Because I don't want you to think that your business is less at risk.

The software that hackers use to steal or lock away data doesn't care which computers it infects. It just goes looking for vulnerabilities. And when it finds them it exploits them.

Any business, of any size, is at risk without data security protection that is constantly 100% up-to-date, and an active data protection policy.

Here's a case study that our business has dealt with recently. I have anonymised it to protect the people involved.

CASE STUDY

This is a true story about a new client who contacted us when they were caught out by some social engineering and an email phishing scam. We may think we are tech-savvy. We may think we know how scams work. But even the best of us can be vulnerable, no matter what internet security is in place.

A London-based entertainment business contacted me in distress. They are a small but engaged team and have a constant roll out of new productions so there's never a dull moment - decisions are made very quickly.

Their boss, let's call her Christine, contacted me in a panic: "Someone has hacked our email accounts! We've been ripped off to the tune of nearly £12K! How did this happen?!"

In fact - they had been the victim of a clever email fraud.

A bad guy masquerading as Christine herself sent an email to their accountant, John. I will paraphrase here: "Hi John. I haven't got time to go through the usual tomfoolery. I need a BACS transfer for £11,850 to be paid immediately to a new company we are working with. This is urgent and I haven't got time to discuss it. I expect it to be done within the hour. Christine". The email looked legit and even had the usual company signature.

The accountant had only been employed for six weeks and didn't want to get into trouble or question the unusual request from his boss and paid as instructed.

The same afternoon, ANOTHER request came in asking for a larger sum to be transferred. This time Christine was in the office and John had the courage to ask, "So you want me to send another transfer?". "What other transfer?". The accountant turned white; he realised there was no request.

In the post-mortem, several discoveries were made:

1) The company had a "w" in their domain name. The alleged email from the "director" had "vv" instead of "w" in the name. So the email appeared to be

coming from companywaithaw.com but was, in fact, coming from companywaithavv.com – it took two or three checks to see that this was bogus. Further digging showed that the email originated from Panama, not Holborn.

2) The bad guys had worked out (probably by web research and possibly phoning the company) that Christine was the boss and also what the account department's email address was.

3) The company had no protocol for dealing with new payments with new suppliers. This demonstrates how important it is to ensure that any new payment for a new client/employee/anyone is verbally confirmed by the accounts team and the decision maker.

ITGUY assessed the company's IT. There was a problem. Although they had a reasonable firewall, their computers were up to date with Windows updates and even had an antivirus system in place, they did not have email filtering (which checks whether emails being delivered are authentic or not).

The email domain that the spurious email came from was blacklisted by the email filtering engine ITGUY deployed. This may have caught the suspicious email or at least alerted us that there was something dodgy happening.

The company never got their £11,850 back. But they now don't leave their IT security to chance. They employ a professional company to ensure they are covered.

And they have also learnt an equally important lesson which no computer program can do for you.

Educate your team about internet security.

Social engineering, false emails, warning pages on websites must all be viewed with a high level of caution.

3
The five main risks to your business

There is good news. While it's impossible for anyone to second guess what hackers will come up with next, it is totally possible to protect your business to very high levels against existing threats and the ways hackers work.

This is why we promote the concept of **Predict > Plan > Protect**.

The first thing you must do is assess your business against the five main risks, and put in place preventative measures.

Please don't attempt this yourself. Like any technical subject, the devil is in the detail. You want seasoned experts who are used to doing this day in, day out.

These are the five main risks:

1) Cyber attacks

Hackers are attacking computers all the time. Literally 24/7. Because humans aren't doing the hard work; it's software that's doing it for them. Software roams the internet looking for vulnerabilities in computers and networks that it can exploit. When it finds something, it notifies its human controllers to take a closer look.

There's a surprising number of different ways that hackers will target you:

- **Malware**: Software that has been created solely to disrupt or damage your computer system, or give someone access to it.
- **Viruses**: Software that can copy itself onto other computers.
- **Rogue security software**: Malicious software that misleads people

into believing there is a virus on their computer and tricks them into paying money for a fake malware removal tool. Often this actually introduces real malware onto the computer.

- **Privilege escalation**: The act of exploiting a bug, design flaw or oversight in an operating system to give the hacker access to higher levels of control over the computer.
- **Spyware**: Software that watches what you're doing on your computer, and sends that information back to the hacker.
- **Trojan horses**: A piece of software that looks like it's doing one thing, whereas actually, it's secretly doing something bad.
- **Worms**: A piece of malware that replicates itself across a network in order to spread to other computers.
- **Botnets**: A network of computers infected with malicious software and controlled as a group, without your knowledge.
- **Spam**: Undesired and unsolicited email. Some spam really looks like a real email, which can easily go undetected in a busy workplace. And that leads to…
- **Phishing**: Fraudulent emails that appear to be from reputable companies, trying to get people to reveal personal information such as passwords, bank login details, etc.
- **Rootkit**: A set of software tools that enable a hacker to gain control of your computer system without being detected.
- **Blended attacks**: Where hackers combine several of the techniques already mentioned to attack your computers and spread to other networks.

2) Data breach

Where a hacker gets into your system and steals data, or locks it and demands payment to unlock it. Data can also be breached by rogue employees on site – imagine a member of your team putting an unauthorised USB into their computer and taking a copy of your data.

A data breach can also include losing a device that's not protected. Something as simple as leaving your laptop on a train is a data breach. Under GDPR you must report every data breach to the Information Commissioner's Office. You really also have to tell those people affected – your clients. Not good. Not good at all.

3) Data loss

You try to switch on your laptop one morning and you see the blue screen of death. So long as you have a proper up-to-date verified backup, this is an inconvenience – a speed bump. This is a basic protection. But you'd be surprised how many businesses risk their data every day.

A good backup system runs constantly, so as new data is created a backup of it is being made. You might have a copy of this data in your business, for speedy restores. But you will certainly want to keep a copy offsite in the cloud. Both sets of data should be encrypted so everything's safe.

Backups should be regularly verified and tested. You don't want to discover that your backups have been corrupted, just at the point you need them… this is how you lose a month's worth of data. When was the last time you tested your backup system and verified the data?

For many businesses, a serious data loss could be a fatal blow. Interestingly, a device failing is treated as a breach under GDPR if the data goes on to be lost. Comprehensive data backup protects you in many ways.

It's also worth noting that under GDPR, you must keep a list of failed equipment and how it was safely disposed of.

4) Cloud computing

The cloud is now a mature and readily accepted way to store and handle data. It offers you so much flexibility to access data on any device, wherever you are, that for most businesses it's the right solution. There are many downsides of course.

The first is the need to protect data. When we talk about the cloud we

really mean servers or data centres that are not under your direct control, in your building. If you can access that data on any device… then what's to stop a hacker?

We recommend putting in place two-factor authentication, or even multi-factor authentication to help secure cloud systems. You may have experienced this when logging onto your online banking. You put in your password, and then either have to give an extra piece of information. Or perhaps respond to a prompt on your phone. Or enter a code texted to you.

There are lots of different ways to do it. The key is striking a balance between solid security and annoying your staff every time they need to access data.

5) BYOD

This stands for Bring Your Own Device. It's where you allow your staff to use their own mobiles – perhaps even their own iPads – to access company data. This is convenient for them and reduces costs for you. But it directly takes away your 100% control over how your data is accessed.

You need a very clear policy to address how data is encrypted, and issues such as which apps your team use to access data. As well as what happens when they lose their phone. What happens when they upgrade to a new device (and sell their old device on eBay). You should also consider the risks of jailbreaking (where the operating system is bypassed).

4
The 6th and biggest risk: Your business's reputation

Since 1998, UK businesses have been bound by the Data Protection Act. Which now seems like a very old piece of legislation.

After all, the world was very different back then. Google had only just been invented. YouTube was seven years away from creation. Mark Zuckerberg was only 14 years old and was six years away from creating Facebook in his Harvard dorm room.

We literally live in a different world now. According to the latest figures from Ofcom, the average adult now spends 20 hours a week online. That's double the time we spent surfing the web 10 years ago.

You can see why this law quickly became out of date. In 2016 the EU adopted the General Data Protection Regulation (GDPR), a major and far reaching piece of legislation that 100% affects your business.

The ICO – Information Commissioner's Office – has published extensive guidance to make sure your business is compliant.

If you hold and process personal information about clients, staff or suppliers, you are legally obliged to protect that information. You must:

- Only collect information that you need for a specific purpose
- Ensure it is relevant and up to date
- Only hold as much as you need, and only for as long as you need it
- Allow the subject of the information to see it on request
- Keep it secure

It's that last one that's most relevant to you in a data security context. GDPR places a duty on all organisations to report certain types of data breach to the ICO.

And as the ICO writes on its website: "Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly."

You know what that means in practical terms? If an employee leaves a laptop packed with unencrypted data on a train, you not only have to tell the ICO within 72 hours, but you might also have to tell everyone whose data was on that laptop.

The ICO also publishes the names of businesses and directors involved in enforcement action.

Can you imagine a bigger threat to your reputation than having to tell your clients you lost their data? Or a news article about a data breach coming up every time someone Googles your business?

What a nightmare. There are some high fines for GDPR breaches – up to 2% of your turnover. In my mind, the greatest threat is to the relationship people have with your business.

The ICO provides a practical guide to IT security (you can search for it online). In summary, it suggests you:

- Assess the threats and risks to your business
- Get in line with Cyber Essentials (a UK government scheme that describes five key controls for keeping information secure)
- Secure your data on the move and in the office
- Secure your data in the cloud
- Back up your data
- Train your staff: What to look out for (such as phishing attacks) and what to do
- Keep an eye out for problems. This means constantly monitoring systems

- Know what you should be doing
- Minimise your data
- Make sure your IT contractor is doing what they should be (we like this one).

CASE STUDY

Austen Hall: Preparing for GDPR and Cyber Essentials Plus accreditation.

Austen Hall is a legal firm specialising in legal and business services for aviation and super-yachts. As their IT support company, ITGUY London manages all aspects of their IT systems, including backup and security.

Laura Austen, the Manager at Austen Hall, approached ITGUY London in 2017 for advice on how to tackle the requirements of GDPR and to assess what processes and systems should be implemented prior to the May 2018 deadline.

"As a responsible legal and business advisory services company, Austen Hall takes legal compliance very seriously. We wanted to demonstrate that we embrace the six principles of GDPR. From a legal perspective, we felt confident that we could navigate the compliance procedures. However, when we investigated the IT requirements, we were much less certain. ITGUY talked us through the IT-based concepts that GDPR covers and helped to map out the tasks we needed to undertake."

Our initial step involved identifying all locations of data (paper and electronic) stored within the business. This allowed us to identify

the companies Austen Hall needed to contact and identify their GDPR procedures.

The second step was to create a checklist so that Laura and her team could see, at a glance, what services needed to be secured, backed up and what recovery methods needed to be tested to ensure successful data restoration.

The third step was to recommend gaining Cyber Essentials Plus accreditation. This two-stage process gets our clients thinking about what is involved in IT security. Whilst it is not a requirement for getting "GDPR-ready", if your business has gone through the process, you will know what you need to do and the GDPR process will be easier to understand and prepare for.

Laura said:

"Having ITGUY manage our Cyber Essentials project for us was a great move. After auditing our systems and preparing them for external assessment, they were on hand at every stage so that the process went as smoothly as possible."

5
How to protect your business

Let's grab that list from the ICO and take it even further. Because you need a reality check: Most businesses that get into trouble either with hacking, data loss or with the ICO, could have prevented the problems if they had taken more urgent action, earlier.

Our policy of **Predict > Plan > Protect** is there to stop you getting into trouble. This stuff is complicated and detailed. But it's not rocket science. There are very clear guidelines and procedures to keep your business safe.

To protect it at the highest possible levels. To have verified and trusted data backups in case there is a problem. To have policies and procedures that protect your business from the threat of legal problems.

This is what we recommend to protect your business:

Lock down your business: Every loophole can be closed and hacking opportunity shut off. You really need to implement a multi layered security solution. There's a balance between inconvenience and security, but most businesses can be made very safe most of the time. Add in thorough continuous encrypted data backup, and the business is protected no matter what future problems arise. You might even choose to test system security using an ethical hacker, who will help you add extra layers of protection.

Ensure every piece of software is always 100% up-to-date: Patches and updates to software and operating systems are released all of the time. They need to be applied immediately and ideally automatically. Companies

like Microsoft and Apple fix problems as soon as they become aware of them. Businesses get caught out when they don't apply these patches quickly. And yes, I know that sometimes glitches arise from installing patches. But currently greater security trumps all other concerns. That's going to be the case for the foreseeable future.

Train your staff properly: Your people are one of your greatest data security risks. They need basic training about what to look for, and what not to do. Even the smartest people can do the stupidest things. For example, you might test all of your staff with a safe spoof email, and see who clicks on malicious links or opens dodgy attachments. Those people would then benefit from further training.

Regularly review security and policy: It's constantly changing and needs some attention to stay constantly up-to-date.

Keep a GDPR evidence file: It's not good enough to just say you meet guidelines. You have to be able to prove it. It's worth asking your IT support partner for regular reports showing where patches have been applied, and that antivirus is up-to-date.

Get someone else to do it for you: You don't do your own accounts. You wouldn't represent your business in court. There are trained professionals who do this for you. Why would you try to DIY something as critical as data security? It's actually cheaper to pay someone who knows what they're doing. They will do a better job in less time. And at less cost overall.

Which leads to my final word on this…

6
How we can help you

Everything I've written about in this book – my business can help you with. It's what we do. We're data security professionals as part of our work as Managed Service Providers.

We live the concept of **Predict > Plan > Protect** with our clients. Stopping them getting into trouble in the first place, and sorting out the mess when there is an issue.

We now support more than 250 people in London. I started the business myself more than 13 years ago.

I understand the typical problems faced by many of these businesses – namely, that you're not an IT expert! Over the years, we've tried and tested all the best IT hardware and software and we've pulled together a portfolio of services that we know best meets the needs of our customers.

Please don't DIY your data security. There's too much at stake. Let experts set up and maintain your system and data in a professional way.

They may never say it out loud to you, but your clients expect you to act in this highly professional way. They expect you to keep their data safe, and ensure it can't be stolen, lost or compromised.

The next step from here is for us to perform a security audit on your business. There'll be a small investment for us to do this.

We'll work with you to assess what the risks are in your business, and make a series of suggestions to bring your company up to standard. And of course, we can carry out the work for you if needed (although there is no obligation for you to buy anything from us, ever).

We'll use **Predict > Plan > Protect** to take all of this hassle away for you.

Let's have a no obligation chat about your business. You can call me or my team on **020 7241 2255** or email us at **info@itguy.com**.

itguy

www.itguy.com

This is your data security nightmare

There's a perfect storm brewing for businesses in London. And it's all to do with data security.

Think of your business as a 17th-century boat in the ocean. It's loaded with valuable treasure (data). And it's currently under attack from two sides.

To your left is a pirate ship. This is where the hackers are. They're trying every trick in the book to steal your treasure. Or lock it away and force you to pay to get it back.

To your right is a military ship. This is the government. It's so keen that you protect your treasure from the pirates, that it's insisting you arm your boat in a very specific way. And it's prepared to blow you out of the water if you don't comply.

This book is your pilot craft. It explains how your boat got into this situation. And gives you a clear path towards your destination, keeping the government happy and the hackers at bay.

Ben Schneider is an acknowledged data security expert and the owner of ITGUY London.