CYBER RISK ALMANAC

A handy, desktop guide for any small business worried about the big bad world of information security.
Contents:

#2 Summary
#3 Stats - size up the problem
#4 Hacks will shake the World
#6 Reasons to get focused
#8 Rules, regulations & standards
#9 Threat Spectrum
#11 Anatomy of Information Security
#12 Steps to Cyber Security
#13 Toolkit101
#14 What’s at risk?
#15 What about insurance?
#17 Where next?
Information Security - let’s help

Across the UK, small business are doing everything they can to grow and keep their customers happy. But there’s always unknowns and they manifest in risks. There’s no more relevant issue than information security and cyber threats. That’s why we’ve created the Days of Cyber campaign - the campaign raising information security awareness for SMEs. This almanac is the first in a series of resources designed to make your journey to CyberPeace of mind easier.

Whether we call it information security or cyber - matters not. We know that most smaller businesses don’t have budgets for risk management structures let alone Chief Information Security Officers (CISOs). These are for global, billion pound companies, right? Yes - but we think it’s an addressable problem. Something is better than nothing - and often some is enough. Every business can have a few defences.

This guide is designed to help you begin forging your toolkit, to power a conversation with your stakeholders. Ask yourself: What’s your information security picture - which cyber threats do you face?

As global businesses begin to upgrade & build their defences, it’s likely to be upon the SMEs, that great backbone of our economy, that the information security threats increasingly fall heaviest.

None can argue that, these are indeed, the Days of Cyber. Let’s meet its challenges as one.

I hope this document is of some use,

@JamesJWYork
Information security, sometimes shortened to Info-sec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).

- Wikipedia

£65k - 115k
Average cost of a Cyber attack for UK SMEs
- Association of British Insurers, 2015

£75.96 billion
Spent online in UK through Nov. - Dec.’15
- Centre for Retail Research

205 days
median time cyber attackers have "free reign" before a breach is discovered.

46.4%
Of the World’s population are internet users.
- Internet World Stats

$67.3bn
The current revenue of one of the biggest online brands, per YEAR.

2.16bn
Global Smartphone Users in 2016.
- eMarketer

74%
of UK small businesses suffered a cyber breach during year.
- UK Gov/PWC 2015

24 billion
Network & devices connected by 2019
- Cisco, 2015
FBI Portal Hacking

In October 2015, a group by the name of ‘Crackas with Attitude’ or CWA breached an FBI information sharing portal and also managed to hack into the personal emails of both the FBI Deputy Director Mark Giuliano and also the CIA Director John Brennan. The hack was fascinating, firstly because it was the FBI that had been hacked and extorted, the most sophisticated crime fighting agency in the world could not defend themselves. Secondly, it was a targeted attack at individuals and government systems, this was not a simple phishing scam. Thirdly, the hacking group described themselves as ‘stoners’ who were ‘high at the time of their actions’ who were extremely public about the attack. Lastly, that this attack was repeated twice more releasing thousands of government official, military police and law enforcer’s personal details. All that, despite regular tweets from the group announcing their intentions. Within these tweets, the Hacker group Anonymous was mentioned a number of times leading experts to believe that hacking groups often act in some sort of cohort. If sophisticated hacker groups began to merge and cooperate the eventual hacks could be devastating.

Wetherspoons

Many Brits love a trip to Weatherspoons for a cheeky pint, but if you knew that afterwards the pub had lost your personal details on to the dark web, wouldn’t that just leave a bitter taste?! During 2015, the Weatherspoons pub chain lost around 657,000 data sets from its website database, including card details and names. Scarily, this hack was not registered until the following week when The Financial Times were alerted by an anonymous email. They then became the bearers of some very bad news that Monday morning. Due to the new regulations issued by The Information Commissioners Office and The EU, Weatherspoons could have faced fines of up to £20,000,000. Fortunately for customers, the data stolen was from an old register, but it goes to show that all types of industry are being targeted within the UK, and regulatory bodies do not care for the age of data, data is data, and the company could still be fined. Those who think they carry old or benign data are more often than not at a higher risk, even charities have been fined £200,000 for not properly protecting their data.

Talk Talk

Teenagers can be annoying, rude and thoughtless, but master criminals? This was a hack that shook the world because of both the ages of the offenders and also how easily they managed to hack into one of Britain’s leading telecommunication companies. So far, five people have been arrested, ages ranging from 15 to 20 for managing to hack into Talk Talk’s servers and steal around 157,000 sets of personal data including names, addresses, credit card numbers, account numbers and sort codes. As a result, Talk Talk shares lost around a third of their value prior to the hack with an estimated cost of repair at around £35,000,000.

US Office of Personnel Management

This breach was one of the biggest ever of US government systems. Still not proven, this was suspected to be masterminded by Chinese hackers who purportedly stole a staggering 19,700,000 sets of financial details from those whom had ever been subject to a government background check. A further 1,800,000 other sets of personal files we’re also taken but details of these have not been disclosed. When your government is successfully breached by hackers it does not exactly instil confidence in the average citizen. This hack demonstrated the advanced abilities of hackers and proved that absolutely no-one is beyond their reach.
Having an information security policy and risk management model seems like a “big company” problem - but with a basic framework - any SME can visualise and plan for unknowns.

Once you’ve created an Information Security structure, the heavy lifting is mostly done! You can then simply maintain it. Keeping abreast of news, developments and asking lots of questions to whomever is handling, building or helping make your digital technology.

One stride, then a few relaxed steps.

A few lines of extra procedure (Worth the effort?)
3 REAL reasons to get focused
(On your information security)

Probability

If massive businesses can and do get hacked - what’s protecting you? If you don’t get your info-security picture clear (with the resources you do have) you’re increasing the probability something can, and will, go wrong. If you don’t know your odds, take stock.

TIP! Ask all of your digital suppliers for details on their information and data security protocols. You may get some good ideas and expose some unknown gaps in your own business’s big picture.

Solvency

Even if your business is swimming in capital (wow, can we have some!) your board, investors and team will be pretty p*ssed off if all flies out the window on a handful of cyber security breaches. Your bottom line and future prospects will be better served by talking about this risk at the very highest level of your company - with a culture of managing cyber security issues running in the business’ DNA.

TIP! Run a simple ‘Cyber War game’? Stress test with your digital systems and finances to see what the cost would be of emailing, calling and speaking to your customers and fixing the underlying scenario.

Reputation

Reputation. Trust. They are two key pillars of successful business. Most SMEs don’t have the budget to start from scratch if either of these are shattered. Plus, having a strong bespoke cyber security process is something you can share with your key stakeholders, pre-empting any concerns they may have.

TIP! Sharing your cyber review process with key customers and suppliers shows your business cares, is pro-active and meeting the real threats. It can’t damage your reputation - not doing it? That could.

“Our fatigue is often caused not by work, but by worry, frustration and resentment.”
-Dale Carnegie

Legality. There’s another very important reason to pay attention to cyber risk.

The rules are likely to get tougher - the government has a lot of focus on cyber threats to the UK economy.
Whilst businesses are reaping the benefits of operating online and now earn £1 in every £5 from the Internet, cyber attacks are now considered a serious threat to UK businesses. The latest figures reveal that 74 per cent of small businesses, and 90 per cent of major businesses, has had a cyber breach of security in the last year.

Source: UK Government. (‘Phreaking’ out about Cyber.)
EU General Data Protection Regulation (GDPR)

Said to be the most important EU legislation for the industry in 20 years, the long awaited GDPR is set to transform the way companies collect, store and secure personal data. It will also amend the rights those individuals have to then access and challenge the data those companies have stored. The intention is to create a standard single regulation that all those trading within the EU will have to follow. Although the regulation is to apply to all companies within the EU, it will be the firms with over 250 employees that will face the toughest requirements. Non-compliance with GDPR could see your company fined 5% of global turnover or £80,000,000, whichever the larger figure. Focus within the GDPR is directed towards:

- Privacy, consent & rights.
- The ‘right to be forgotten’.
- Data Governance.
- Appointment of a data protection officer.
- Data breach notifications.

ICO Standards

The Information Commission’s Office is the UK’s independent information rights authority. The Data Protection Act 1998 and the Privacy and Electronic Communication Regulations 2003 are its primary standards and a breach could result in prosecution, undertakings, audits or fines of up to £500,000. Compliance with ICO standards is mandatory, and proposals are under way for beefed-up rules:

- Reporting back to ICO investigations within 24 hours.
- Mandatory data processor within company to report breaches.
- Data Processor must detail specific breach notification information.
- Obligatory requirements to notify individuals where possible adverse effects are likely.
- Penalties will increase unto £1,000,000 or 2% of the company’s global turnover.
The Threat Spectrum is hyper-complex. Now, consider SMEs in the centre of it all...

"If you've been playing poker for half an hour & you still don't know who the patsy is, you're the patsy."

Warren Buffett
Let’s turn on some tactics

“An ounce of prevention is worth a pound of cure.”
Benjamin Franklin
Imagine this graphic is your business.

**BAD THINGS** 
Stuff happens, right?

**RANDOMNESS**
‘Because as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don’t know we don’t know.’ (What he said.)

**TALENT**
The body cannot live without the mind. Your team are the first line of defence for information security - train them. Senior directors must understand as well as set procedure and trajectory.

**BRAND & CULTURE**
Around the current talent is a brand, it can be quickly damaged or affected by lapses to any constituent systems or procedures. It’s the ever-present.

**PRODUCT /SERVICE**
The beating heart of a business is its means to pay the bills. It can be influenced and effected by forces outside the control of the body of the business. It must be resilient to them.

**GATEWAY(S)**
These are where your internal silos interact with the external world, business to business or business to consumer. Through these gateways comes risks and out goes your product and service.

**INSURANCE SHIELDS**
If you want to invest, insurance is one of the tools you can use. These are forcefields that can be raised around a business entity - each protecting against certain types of problems (laser beams - in this illustration...).
They can only be raised once shots are being fired at the body, or bad things have gotten inside. They prevent further damage, allowing the body time to heal, and act as a catalyst to the healing process.

**RISK FILTER - PROCUREMENT**
As things interact with your business, controls the processes filter definable and identifiable emerging risks. In turn, they review and plug those gaps.

**RISK FILTER - LIQUIDITY**
You must decide how to budget to filter risk, and its downsides, from your business. Manage it internally, or transfer it with investment?
Based on the GCHQ “Steps to Cyber security”

Information security encompasses a range of company procedures - why not go and grab a cuppa and figure out which are most relevant to yours.

Anti-Malware
Make sure you HAVE, maintain, update and review all your defensive software and hardware regularly.

Network
Make sure your systems aren’t leaving a window open a sliver. Perform regular vulnerability scanning to see where your weak spots are.

Information Management
Make sure you know where and how information exists and is managed in your business. (Pictures help loads!)

Secure Process & Access
Secure your processes with strong procedures - from complex passwords to reviewing protocols with your tech-providers.

Flexible Working
Ensure flexible working environments are equally matched by a “built to fit” security procedure.

Removable Media
Ensure key data cannot be easily removed, and lost, and that mobile media storage is adequately secured and tracked.

Incident Logging
Record, review and iterate your stance when incidents do occur. It’s not about witch-hunts, it’s about transparency and security for your customers.

Employee Permissions
Control and audit your key employee permissions, ensure the company has strong knowledge of who can access, change and control “what”.

Do you need any experts to help with a particular area? Maybe we can help you find one.
When you consider risk, the first thing that pops into your head is usually the potential downside. (Cost.) Risk either sits wholly on your bank balance, or you can take steps to pay that risk down. First, you must know where you stand.

Risk management sounds complex, but it’s simpler than it sounds. Putting an extra lock on a window costs you twice - the price of the lock and the labour of whoever puts it on, of course. The same logic applies to your CyberWorry. How could you spend time and money to make any further probability of loss reduced. You need to shrinks your risk profile. Here are some things you could do before you spend anything other than time and brainpower. Build a picture for your budget, before investing it.

Procedures Sheet(s)

Keeping your company’s data protection, HR and %insert your need here% policies organised is difficult. Before we get you started on your Cyber Threats Procedure, why don’t you make a master sheet. (If you’ve already got one, go you.) See the big picture.

Regulatory Check-list

Some rules you simply have to follow. The government, EU and local jurisdictions (especially the USA) will require you be sticking to the law - and self-monitoring. You need to make a check-list and know where rules apply to your business. Thankfully, there’s lots of help.

Technology ‘Mind-map’

Grab a sheet of paper. Put your business in the middle, then add all the places where technology is connected. Tick next to those headings if you think Personal Information for customers, or colleagues, is present. If you’re using third parties - give them a star, remember to ask them how they manage their Cyber Threats.

Cyber Insurance

Cyber Insurance is relatively new to the UK - most businesses have yet to take advantage of this product class. Despite that, there are a number of prominent insurance carriers creating products especially for the SME community - with a range of coverage solutions. It’s free to get a quote - although information is needed from you first.
"I genuinely believe that digital agencies - and their clients - will all need cyber insurance in the future.

It’s something we’re already exploring - despite the fact it’s not a widespread product, yet [in the UK].”

Richard - Managing Director, Mohara.co

Mohara is a digital agency, based in Brighton. Shared with thanks.
Your business entity is fully bearing the cost of unknowns. If bad things happen, you have to pay to fix or remove them from your path.

You rely on internal measures and your company’s risk immune system to deal with anything that’s thrown at you.

Insurance doesn’t stop bad things happening - it does react to them, throwing up a shield around your business. Giving it time and support to heal. It will return you to your original state, but can’t leave you better off - only you control your destiny.

Imagine all your worries are in one bubble. Certainty, complete peace of mind, is in another, right next to it.

Now imagine them overlapping. The more they overlap, the better the cover - the higher the cost of transferring the risk to the bubble of “certainty”.

The more overlap, the more cover. And who’s making the promise matters, too. Got it? Hope so.

Financial Strength of insurer is also a measure of the value of their “promise” to you.
We work with a panel of top insurers, a service we’ve christened, CyberPeace™. We can source a range of different packages from the insurers for you to choose between. Not every product is the same - each insurer may also offer slightly different modules of cover - here’s some key examples that are typically available. If you’ve mapped your risk, you should be in a great position to quickly identify (with a bit of reading and a cuppa) which product fits your stated needs appropriately.

Incident Response
This module is often offered to help with cyber incidents as and when they arise. It can often include legal advice hot-lines and experts on hand to advise on what to do next.

Data, Notification, Fines
These types of module offer broader cover for third party obligations. They also offer first party costs associated with data loss or use, and any potential fines that may be incurred by the business - in the event of your unintended failing to meet regulatory obligation.

Business Interruption
Many SMEs find that their traditional Business Interruption cover doesn’t extend to cyber risks. These modules specifically apply to Interruptions caused by, hacks and malware. If your system has been knocked out and you’re losing money - this helps. If you subsequently lose new business because of that - you may also receive cover.

Extortion*
Increasingly, SMEs and businesses are the target of extortion. These modules offer cover when a third party is trying to prevent you accessing/using your key systems, attempting to plant malware, post your confidential information in the public domain or damage your reputation on social media. If all their support fails - you’ll be reimbursed for any ransom you’ve been forced to pay - but only if insurer help to prevent or uncover the incident fails to deter the criminals.

Errors & Omissions*
If you’re coding could be at fault, or your processes for vetting coding - you could be liable for costs.

Forensics
Knowing an incident has happened is one thing, figuring out how it happened and preventing a repeat of it is critically important. Worse still - hacks have been found to gestate for 200+days before discovery.

Media Liabilities
These days, any modern business has a content strategy that might include social media or blogs. There’s a number of modules on offer that provide cover for defence against alleged Intellectual Property rights breaches and defamations.

Cyber Crime
Phishing, phreaking, social engineering. There’s a lot of scams out there - most products offer specific cover to contain the effects of being duped - others imply that it’s a unifying force effecting all their modules of cover.

Crisis PR*
Your reputation is critical to business growth. This module will offer a communications expert to guide you through reputational issues - should your brand or business name hit the press for the wrong reasons.

How does it work?
- Apply, we’ll help you.
- Get a free quote
- Consider if it fits your needs
- Order cover
- Get on risk
- We’ll stay in touch & help even more!

*THE CYBER RISK ALMANAC, 2016
Without breaking a sweat, you’ve made some notes, drawn a couple mind-maps and built a picture of your information security. Now you’ve made a start, you can figure out what your possible budget should really be for your defences. If it’s already optimum - well done!

You can more readily identify which areas of your information security are most vulnerable to threats - and spend some of your budget on reinforcing their defences. Start delivering that plan as soon as you’re able.

“No plan survives contact with the enemy”, so say folks in the military. Perhaps you should consider if there’s any time or budget left to get a backup for the procedures and experts, too. Thankfully a quote is free.

Where next...

Information Security Procedure

Expert Assistance Planning

Backup for Backups Insurance

Share your experience Join the campaign.

#DaysOfCyber
If you would like to know more about the Days of Cyber campaign, please visit DaysofCyber.com

Campaign Partners