CEO's Briefing

IT Risks, Compliance & Security

Nobody expected the Buncefield explosion, the floods of 2014, the London riots or the ransomware that infected vast swathes of the NHS, but they still happened.

FREEMAN CLARKE

No doubt you worry about growing your business and being successful, but as the business grows and becomes successful, protecting it against risks becomes a new source of worry!

New concerns range from compliance with Data Protection regulations, ensuring the business will survive a climatic event, or fall victim of a cyber-attack that destroys all your data, these all need to be considered however remote they feel. Put simply, a successful business is worth protecting.

Entrepreneurs are typically people whose personalities are more tuned to opportunities rather than threats. So it's easy to push these concerns to the back of the queue... but if you're not prepared and they do come round to bite you, it could be the end of your business.

Nobody expected the Buncefield explosion, the floods of 2014, the London riots or the ransomware that infected vast swathes of the NHS, but they still happened. One of our clients suffered minor subsidence in their building, but it required an evacuation which lasted weeks!

These are just examples of external influences on your business, there's a whole set of risks within the business that could have a similarly major impact whether that's theft of data, loss of your main client or losing long-term access to your main business system. We met a company recently whose main system failed, and to their horror they then discovered they couldn't restore their backups.

It's not practical to deal with all possible risks and issues, they have a habit of absorbing vast swathes of time and energy if you're not careful. So, you need to know the risks that you do have and then prioritise and work through the list. Some will be all but impossible to mitigate against because it is either too expensive, would take too long or be detrimental to the business. Half the battle is understanding your risks, because once you know what the risks are you can make an informed decision.

CEO's Briefing

> "Nothing should be off the agenda, every risk and issue should be logged, even contentious or unlikely scenarios.."

Face up to your risks

The first step for any Board is to bottom out the risks and issues within your business. Generic concerns about security aren't good enough, you should know specifically what and where your risks are and at the very least have a plan for them, even if that plan is "do nothing".

When we engage with a client, one of the first things we recommend is the creation of a risk and issue log. It's a hygiene thing and any IT Director worth their salt will do this soon after joining a company for peace of mind. If your business doesn't have a risk and issue log, then it's high time one was started.

Nothing should be off the agenda, every risk and issue should be logged, even contentious or unlikely scenarios.

A risk and issue log defines all the risks within the business. To be an effective tool, it needs to describe the risk, outline the likelihood, the potential damage to the business and therefore how important and urgent it is to resolve.

When creating the risk and issue log, it's important to understand the difference between a risk and an issue. A risk is something that might happen whilst an issue is something that has happened. Once the log has been created, it needs to be maintained and managed. A risk and issue log that's 12 months out of date is useless.

Risks that we've seen turn in to real-life issues that our Principals have dealt with are:

- Structural failure in a new office meant the building was immediately unavailable and an alternative site to be found immediately.

- Multiple network link failure due to cables being cut by an external contractor – no internet, no email, no files!

- An IT Service Provider going bust and leaving a company without any support or access to their servers hosted in the IT Service Provider's data centre.

- The company car-park under the office flooding and threatening the power supply to the whole building.

- 200,000 files being taken over by ransomware.

We believe an average company is affected by a serious calamity every 3 to 5 years.

> "We believe an average company is affected by a serious calamity every 3 to 5 years."

Maintaining the risk and issue log is the start of proper management of risk. Appointing someone on the board to be responsible and setting up projects to resolve or mitigate some of the most urgent important risks must be the next steps.

Keeping in with Compliance

Compliance is a risk for every business nowadays.

For example, the Data Protection Act applies to almost every business. This is more or less compulsory and is being updated when GDPR comes in to force in May 2018. Compliance is likely to require many changes to your business, not only in technology, but in your processes, policies, marketing and sales. It should not be underestimated. The government (actually the ICO) will be able to fine up to 4% of global revenues for GDPR non-compliance.

FREEMAN CLARKE

> "If your systems don't follow a least-privilege system, then you are significantly exposed to cyberattack, to fraud and to errors."

Another regulation affecting many of our clients is Payment Card Industry compliance (PCI). If you have any kind of payment processing then you will need to be compliant. PCI compliance has a number of levels depending on how you interact with payment cards, but anything other than tokenised payment processing will mean an audit, a penetration test and the need to resolve all issues raised to avoid on-going fines.

If your payment processing systems are on the same network as the rest of the business then all of your infrastructure will be audited leading to a potentially wide-ranging update activity that could get expensive. Fines for PCI compliance infringements usually kick in when there's a security breach, but the fines and costs can mount up very quickly, even for those companies handling just a few thousand credit cards.

If your business is in the financial services sector, then the level of compliance necessary is far more wide ranging. Compliance with the FCA is not just about data security and managing backups appropriately, it also requires companies to have personalised and firm-specific compliance or operational manuals that are embedded within its procedures and culture. The FCA has even published guidance on use of Social Media.

There are many other sector-specific compliance or regulatory requirements, for instance we deal with companies in Life Sciences and Pharma, Defence, Buildings and Construction, Legal and Accounting, Transport and Supply. The first step is to find out what regulations apply to your business, appoint someone at board level with responsibility for becoming compliant and then maintaining that compliance.

It's highly likely third party professionals will be required to ensure compliance is achieved so these activities need to be prioritised and budgeted. But professional compliance experts do tend to create very, very long lists of actions – a balanced, sensible and commercial view is needed to oversee the project.

Where to start with Physical and Cybersecurity ?

These days a security breach hits the front page every day. Why do companies fall prey to this? Normally because no-one on the Board has time or expertise to ask the right questions and to draw compromises in the right place.

There must be both physical security and on-line data security and process fidelity. In today's mobile businesses there are many ways in which security can be compromised and breached without anyone knowing about it. Here are 10 key steps:

1. Firstly, look at perimeter security, this needs to include both physical security of your office and the security of your systems. All networks make contact with the outside world and those points of contact should be firewalled. Knowledgeable and trusted experts who understand the complexities of system and firewall management need to configure this equipment and to keep it up to date. Specifically this involves minimising points of access (ports) and using secure ports for email and web access rather than standard ports.

2. Access to systems should be on a least-privilege policy. For example, when a person is given access to a system, the default should ensure that person has no rights to anything. Then privileges should be granted according to what that person needs to do in the system, building up to only include the data and processes they require. If your systems don't follow a least-privilege system, then you are significantly exposed to cyberattack, to fraud and to errors.

FREEMAN CLARKE

CEO's Briefing

> "Establish how you will handle a crisis in advance. Who's in charge if you are attacked by ransomware and decisions need to be taken on the spot."

3. All computers should use up to date operating systems which are properly patched; utilise up to date anti-virus and anti-malware systems. However these systems only work well when they know what they're up against. Newer protection systems coming on the market look for programmes acting suspiciously and will automatically shut down the programme down before it has had time to cause mayhem. These systems provide protection against new attacks (called "Zero Day") because they spot the bad behaviour of an application rather than recognise the malware itself.

4. To protect your data, it should be encrypted by default and only accessible to those with the approved rights to look at it. Where you have customer data, particularly user accounts and passwords, ask your IT team whether the data is "hashed and salted" which will make it very secure and difficult to break even if your systems are breached. It is unforgiveable nowadays to be holding customer data unencrypted (known as "clear or plain text").

5. Security systems can be bypassed by canny criminals because they know where the weak link is in the security chain, and that's your employees. Criminals have become highly adept at social engineering - manipulating humans in your organisation to their own ends. For instance, emailing your financial controller posing as you, the CEO, telling them to send money to a supplier and providing bank account details are not unusual. Many people fall for this and a lot of money can be lost very quickly. Having sound financial processes in place and spending time on training and awareness for your staff is the only defence against this kind of attack.

6. Your data and systems should also be well backed up and stored in an off-site location, preferably with no connection to your live systems (known as an "airgap"). Ensure the backups include multiple versions of the same document in case undetected corruption or malicious encryption took place at some point in the past. Having a decent data backup can be the difference between having a business post-disaster and not.

7. Bespoke software and web applications must be built by experts, using modern tools and techniques. Good developers can build secure software, but bad ones don't – and you won't necessarily know which they are! Ask whether they are designing to meet the OWASP Top 10 and consider getting an independent penetration test which can be done for well under £5k.

8. Create a "secure culture", where taking this stuff seriously is encouraged. Ensure you and the Board demonstrate good practice - for example, if you write your passwords on post-its then you should fully expect your staff to do the same... and one day you will probably be hacked as a result!

9. Establish how you will handle a crisis in advance. Who's in charge if you are attacked by ransomware and decisions need to be taken on the spot. GDPR makes specific requirements about notifying the ICO if you suffer a security breach – who is responsible for making this happen; failure to do so will result in a fine.

10. Get certified – this will give a focus and purpose to your efforts to improve security. A good place to start is Cyber Essentials Plus certification. This will provide you with a government standard accreditation that directly demonstrates to you, your company and your customers that you take security seriously and that you're working to ensure their data is held securely and your systems are well managed. We know of clients that have won new customers simply because they stood out from the competition by having Cyber Essentials Plus accreditation.

FREEMAN CLARKE

> "Standard processes are actually empowering for staff. They know what they can (and can't) do and trust across the business is increased."

Reputation is Everything

Aside from the obvious operational and financial impact of a cyber attack, data leak or compliance related prosecution, the most traumatic result will be on you and your company's reputation.

If Customers know you've had a breach, their trust may be lost and they may never buy from you again. Certainly you can be sure that they will tell their network of contacts. For example, TalkTalk lost over 100,000 customers and £60m as a consequence of the hack on their systems in October 2015, not to mention a free-falling stock price.

Not only will it affect your reputation with customers, but it will go hand-in-hand with making it harder to attract the best people to work with you or remain with you moving forwards.

You can be sure that after such a calamity, your competitors will be leveraging your failure to their advantage and your business partners and businesses that you work closely with may start to distance themselves from you to limit collateral damage.

It's possible that suppliers will remove or reduce your credit terms and it's almost a certainty that your insurance costs will increase or you may not be able to find cover at all.

None of this sounds good for anybody's reputation, but today's fast moving and competitive environment, it's just not worth it. In the event of a cyber-attack, Cyber Insurance will help cover the cost of repairing your reputation and getting systems back up and running, but it is Criminal Insurance that you need if you want to be covered for money stolen. Never settle for Cyber Insurance thrown in with your normal business insurance, get proper advice and know what you're buying.

Process is Good

Having a set of standard business processes is an important part of creating a robust business that can provide the solid foundation for compliance and improve security.

Standard processes are auditable and reduce your reliance on key people. If they are followed consistently this will help ensure your business remains secure. Most of the time, particularly with social engineering, criminals need to get someone to do something that doesn't follow the normal way of working, whether that's clicking on a link in an email they think has come from their friend or giving away their password to someone who's rung them to fix a problem on their machine they didn't know they had.

It may be boring, but following a process could save your business many thousands of pounds and gives people confidence that they're doing the right thing. This is particularly the case in any part of the business that directly manages your company's money; the finance team is an obvious target for hackers.

Standard processes are actually empowering for staff. They know what they can (and can't) do and trust across the business is increased. Directors are freed up to do more value-adding tasks and reliance on key individuals is reduced, which reduces risks and makes the business more scalable.

FREEMAN CLARKE

> "Secure systems improve the reliability of your business and improve the service to your customers."

Take the time to write good processes and ensure they're understood by the team and then regularly check their use. A good process is one that is transparent in its working through an auditable trail of activity. It is also simple and easily understood and potentially comes with a policy as well.

Too Scared to Work?

It would be very easy to get sucked under by all this stuff about business risk and compliance, but it's not supposed to swamp your business and, when done well it's an enabler for growth rather than a barrier to growth. Good security rests on a well organised business with a simple structure. Achieving this also empowers staff, frees up managers and makes the business more scalable.

The risk and issue logs helps you understand your business in better detail and prioritise ways of making it more robust. A regular review of the log by the Board is a useful discussion that helps align the Board and how they're thinking.

Secure systems improve the reliability of your business and improve the service to your customers. Processes mean that it's easy for staff because they don't have to make things up and typically things get done faster. Whilst a lot of these things will protect your business, they will also improve and drive your business forward.

Don't expect to get everything changed and sorted out in a short timescale. Creating the secure and standardised environment that comes with resolving these issues will take time, but if you set an agenda and a plan with some ownership on the top table, they will get done.

Freeman Clarke
The UK's largest and most experienced team of fractional IT Directors.

Phone
0203 020 1865

Email
contact@freemanclarke.co.uk

Locations
London & South East
Thames Valley
Southern Home Counties
West Midlands
East Midlands
North West
North East
Singapore