CEO's Briefing

Cyber, Legal Compliance... how a CEO can sleep soundly!

This document describes the basic projects to make your business secure and compliant.

It is not an exaggeration to say that most days we meet companies who have been hacked, their reputations damaged, and money lost. Successful websites can be juicy targets; ransom-ware can bring a company to a standstill.

Many companies have demanding standards and huge contractual penalties imposed on them by their customers. And the law is tighter than ever, with big fines making headline news.

The threat of cyber makes many CEO's of mid-market companies feel exposed and uncertain. They find themselves without an obvious way to respond to this situation strategically. Perhaps your staff and suppliers looking after these issues have the necessary skills to do this well, perhaps they don't. How can you know for sure?

These are complex issues, your time is short, and finding a simple commercial and strategic approach can feel difficult.

There is often no-one around the Board table who has the necessary technical knowledge, experience, and sensible attitude to lead the approach.

Regardless of whether there is clear accountability or not, the actual approach may be "hope for the best".

For business in heavily regulated industries, security standards and good practice are culturally ingrained, but for most businesses in ordinary markets the situation is far more ambiguous.

FREEMAN CLARKE

contact@freemanclarke.co.uk
0203 020 1864

CEO's Briefing

> "Boards need to accept that secure practices might not be as convenient or simple as insecure practices."

But there is a simple solution

In our experience the underlying issue is that Boards of mid-market companies lack the expertise to feel confident. External advisors are typically selling expensive products like AI-based intrusion detection, data loss prevention software, or advanced malware protection. But they're often aiming to baffle and befuddle rather than help.

Often the starting points should be simple training to ensure your staff understand how to behave securely. And simple steps to reduce threats and to minimise impact in the event of a breach.

But long reports from experts can be very difficult to boil down into achievable plans. So many Boards end up trying to break this down, to circumvent advice, to work-around and short-cut, or even just to ignore what they know to be a problem.

Boards need to accept that secure practices might not be as convenient or simple as insecure practices. Some things might take a bit longer, or be a bit more cumbersome. But keeping your business secure is worth the investment of effort and, when done well, the positive impact enormously outweighs the negative.

But, above all, there is no longer any alternative!

This document describes the basic projects to make your business secure and compliant

But there's no such thing as being truly secure?! OK, well that's true - there is no finish line to security, but there are a set of practical basic steps that every substantial business should put in place.

Consultants, product vendors and the media would convince you that this is much more complicated that it actually is.

The truth is that we have been in business for many years and worked with hundreds of mid-market companies. During this time we have seen many security issues, hacks and breaches but in almost every case these occurred as a result of basic errors. Mistakes due to lack of care, lack of training or lack of expertise.

Yes, sophisticated attacks do happen. But they're very rare.

And even when sophisticated attacks have occurred, basic measures have allowed our clients to recover quickly with limited damage.

In almost every case, disaster can be averted by simply getting the basics right.

But the issue for the Board is how do you know whether your tech guys have got the basics right or wrong?

The following is a simple roadmap.

1. Risks and Issues Analysis

Every substantial business should maintain a list of risks and issues, with some analysis of the options and mitigations. Each risk or issue should be owned by someone around the Board table who has the expertise, time and ability to manage it. This document should be reviewed by the Board at least annually.

Every business faces risks and tolerates issues, this is inevitable. You need to know what you have, what's valuable and what's vulnerable. The list and the open discussion drives sensible, productive decision-making and avoids a culture of sweeping issues under the carpet. Instead, you can confront the real business risks, identify a proportionate response, and ensure you are looking after the things that matter.

FREEMAN CLARKE

CEO's Briefing

> "For most businesses there is a simple route to getting basic security right, accreditation to the government sponsored scheme, Cyber Essentials Plus."

Proper backup plans, disaster recovery and crisis management plans will flow from these discussions.

2. Sort Out Your Cyber Insurance

It's prudent to consider the need for Cyber Insurance but, unfortunately, not all Cyber Insurance is created equal and you need to take care to select an appropriate policy and provider.

Specifically, does the provider simply want to sell you a policy or do they take time to understand your requirements and level of risk?

Check the exclusions on the policy and ensure a member of your Board understands the cover – most importantly does it cover ransomware payments, recovery costs, and cover for loss of business. Cyber Insurance may not give you back money that's stolen from you – that generally requires Criminal Insurance.

If you have to make a claim, will your insurer specify the third party to run the recovery programme? If so, how quickly can they mobilise? If not, and you need to identify an appropriate third party, have you already undertaken a review to identify the best candidate? Don't wait for an incident to evaluate potential suppliers.

Check your IT is compliant with your policy conditions. The devil is always in the detail and your IT team or supplier need to know what they have to do to maintain compliance? Are these documented in policies that can be audited?

Finally are your suppliers' contracts clear about their liability and are they appropriately insured?

3. Behavioural and Awareness Training

The weakest link in any business is often the people. Some of your staff may struggle to understand the issues or to know what secure behaviours really are. What do you really expect of them?

Lots of companies have security policies that no-one reads. Perhaps people have found ways to circumvent the rules that are tacitly approved by managers who are busy and under pressure to deliver results.

If managers write passwords on Post-its and access email from insecure home computers then your people will see this and do the same.

Is your finance manager empowered to challenge an email that looks like it's from you calling for an "emergency payment"? How are suppliers' bank details verified? Are your IT staff confident enough to call out poor security practices from senior managers?

For a few hundred or a few thousand pounds you can arrange awareness training.

4. Cyber Essentials Plus

For most businesses there is a simple route to getting basic security right, accreditation to the government sponsored scheme, Cyber Essentials Plus.

Specifically, this scheme identifies the basic technical measures to ensure your kit is being properly looked after, your network is properly setup and that access is being properly controlled.

Most importantly Cyber Essentials Plus requires all these things to be independently checked! Don't ask your existing IT supplier to do it – get an independent assessor!

The total cost of this accreditation should be just a few thousand pounds and it should take just a few weeks from start to finish. We advocate that every mid-market business should attain Cyber Essentials Plus accreditation as a basic step.

FREEMAN CLARKE

contact@freemanclarke.co.uk
0203 020 1864

> "Typically pen test findings are divided into High, Medium and Low priority."

It certainly isn't the whole answer, but it's a big step forward for a lot of companies. Note the "Plus" – this means you're externally accredited, we strongly advise this step.

5. Penetration Test

A penetration test is an assessment by an expert company of your website and network to find weaknesses.

Most companies can have a full, detailed penetration test for just a few thousand pounds.

This is essential if your website includes custom software or any kind of ecommerce services! Poor technical practices can result in custom software being full of holes and these are well documented in a standard list known as the OWASP top 10. This list are the standard vulnerabilities that almost all hackers focus on – ensure your penetration test includes checks against this list. Simple!

Typically pen test findings are divided into High, Medium and Low priority. All High and Medium priority issues should be addressed immediately.

Low priority issues can be assessed on a case by case basis.

6. GDPR

The General Data Protection Regulations came into force in Spring 2018 with much fanfare. Since then it's all gone a bit quiet, and a lot of people are hoping this has now gone away!

But the rules are in force, the penalties for breach are high, and the measures necessary to be compliant are (mostly!) sensible and worthwhile anyway.

Most businesses can organise an expert assessment of their GDPR compliance for a few thousand pounds.

The recommendations can be complicated and GDPR compliance can be a long process so the necessary work will need to be planned out as a series of projects and this will need to be led by a member of your Board who is commercial and sensible in their approach.

GDPR compliance can be daunting, but the steps to compliance are generally useful steps towards well-managed and well-organised back office systems. These steps help companies to run efficiently, smoothly and to make the best of their data which is a valuable asset.

So, quite apart from the legal requirement, GDPR is a useful tool to help you ensure good practice in your administration departments.

7. ISO27001

ISO27001 is a more serious information security and management standard. Some companies have this standard imposed on them by corporate or government customers.

But, regardless of this, if your business is complex or has specific security requirements then ISO27001 provides you with a means to embed a "security culture" in your business. For example if you manage sensitive data or valuable IP; if you want to demonstrate your credentials to demanding corporate clients; or if you plan for your business to offer important IT services, then ISO27001 gives you a means to drive security into every aspect of your business operations.

Although external assessment might only cost a few thousand pounds, the project to implement the necessary changes in your business can be large and invasive. But

FREEMAN CLARKE

> "All these measures are sensible and will make your business more secure and will help you sleep soundly."

that's why companies which are accredited to ISO27001 are able to brag about it – this standard is demanding and it means something.

And secure systems and practices are generally more effective and reliable as well!

All these measures are sensible and will make your business more secure and will help you sleep soundly. But, also, in the event of a problem you can refute criticisms or accusations of negligence because these are the sensible steps.

And, finally, simple well-maintained systems and practices are generally far more effective and reliable as well as being more secure. Secure tech is a better basis for a streamlined and profitable business, as well as being safer!

If you want to discuss any of the information in this briefing then get in touch. We can recommend suppliers who can undertake audits, insurance, pen tests and accreditation.

If you want to discuss how tech can help to grow your business whilst staying secure then contact us directly.

You might also find this interesting: 13 key steps to cyber security for non-technical Board members.

Freeman Clarke: We are the largest and most experienced team of fractional CIOs, CTOs and IT directors.

Phone
0203 020 1864

Email
contact@freemanclarke.co.uk

Locations
London & South East; Thames Valley; Southern Home Counties;
West Midlands; East Midlands; North West; North East, New York, Singapore

FREEMAN CLARKE