MD's briefing

*Growing Data and Cyber Security Risks for **SMEs***

Smell the coffee

SME owners/MDs focus their efforts on growing their business and being successful, which is no different to our focus at Peritus. New laws around data protection and the ever-growing cyber security threats to businesses of all sizes are a real concern, and one that has potential to cause huge issues with reputational damage as well as restrict growth.

Working with leading experts in this rapidly expanding area, it is amazing to see how laissez-faire many owners/MDs are when it comes to protecting themselves. Many businesses say they are 'covered' for new laws like the GDPR, it's 'the new Y2K isn't it?' 'Brexit will remove this European law?'

"The commercial consequences of non-compliance could be crippling, and most business owners/MDs do not understand the potential risks to their reputation and most valuable asset – their business."

What does 'covered' actually mean?

Can you prove your business is compliant?

Have you trained your people on the threat of potential cyber-crime?

Have you mitigated risk as much as possible across your business?

The government has a clear strategy to 2021 to make the UK the safest place in the world to trade, therefore laws around data will undoubtedly become more stringent, even after Brexit. With the introduction of new e-privacy laws in the coming months and the fact **directors could be made personally liable for data breaches, why would you not take this seriously as a business owner/MD** when you work so hard to be successful?

0116 2688728
info@perituslearning.co.uk
https://perituslearning.co.uk/peritus-protect/

Peritus
The Learning Experts

The SME - Created by an **SME** for an **SME.**

MD's briefing

*Growing Data and Cyber Security Risks for **SMEs***

Data compliance - Key to modern business

Like it or not, at Peritus I recognise none of this is going away, however like many MDs I do not have the time or patience to submerge myself into the world of data compliance and cyber security. Therefore, we have selected a compliance champion, and we have provided the necessary resource and budget to comply with data laws in order to protect ourselves as much as humanly possible to mitigate the risks of cybercrime.

"74% of SMEs haven't made any provisions in their accounts to deal with a potential attack or issue."

(PolicyBee)

Worryingly there are 5.4M businesses in the UK, £2.4M PAYE registered, and approximately only 600,000 data controllers that are registered with the Information Commissioners Office (ICO), which to many is the most basic of requirements. What are the tens of thousands of other businesses doing when it comes to data and cyber security? I would anticipate very little! This essentially means many UK businesses could be trading illegally, which I can't imagine any of us set out to do.

Data claims culture - Opening the floodgates

The fines for non-compliance with the GDPR are certainly a threat with potentially 4% of annual turnover being attributed. This, for many SME owners, could have a serious impact on dividends and an ability to re-invest back into their business to support growth. However, having presented alongside the ICO at recent events, they clearly stated their intention to support businesses who have made 'reasonable' efforts to become compliant.

A greater threat to most businesses, no matter the size or sector, is the data claims culture building in the background. The case of Vidal-Hall Vs Google saw the claimants sue Google on the basis they were 'distressed' that Google had collected their data unlawfully. In practice this means no personal or financial damage is required and distress is all that needs to be proven to have a successful claim.

0116 2688728
info@perituslearning.co.uk
https://perituslearning.co.uk/peritus-protect/

Peritus
The Learning Experts

MD's briefing

*Growing Data and Cyber Security Risks for **SMEs***

"The ICO recognises that many organisations would still fail a GDPR audit. There is still time, however the ICO states effective data protection requires clear evidence of commitment and ongoing effort."

"Only 40% of all data in the cloud is properly protected against attack. People assume that if it is in the cloud they are safe."

(NCSC)

Looking at this logically means **every past and present customer could have a claim against most UK businesses of at least £1000 per data claim.** Therefore, if you hold lots of personal data this could be expensive if you are non-compliant or get things wrong.

When we talk about the data claims culture taking shape, just type 'data claims' into Google and you may be alarmed to see the raft of companies available to support people with a claim for financial, emotional distress or both, where they believe their data has not been handled correctly by a business. I can see the adverts on TV now in the same vein as PPI claims over recent years. Just so you are aware, the PPI claims deadline is the 29th August 2019, so data claims are an ideal replacement!

A key change to the GDPR legislation is the requirement to report any data breaches to the ICO. Therefore, if you have been the victim of cyber-crime in your business this may compromise the personal data you hold, which in turn you must report to the ICO. If you are not GDPR compliant, nor have trained your people sufficiently, this could result in fines and claims made against you, on top of the cost of a cyber-crime incident, which in effect provides your business with a double whammy.

Simply it could be one of your employees opening an unsolicited email and causing systems and data to be affected. The core problem here is the lack of basic training for employees around all aspects connected to data and cyber security.

The SME - Created by an **SME** for an **SME.**

MD's briefing

*Growing Data and Cyber Security Risks for **SMEs***

"70% of business leaders & managers admit they haven't taken any action to protect their business & employees from an incident of fraud"

(Take Five)

The weakest link

Currently only 20% of all UK businesses provide the necessary cyber and data security training for their employees, which is astonishing considering people are your 'on-going' weakest link. I have talked to many business owners who have focussed purely on the technical security elements of systems and processes. Whilst this is incredibly important, the behaviour of your people is your greatest day to day risk therefore they must be aware of how to keep your business safe.

Simple facts to consider if you have an issue:

- The average costs to an SME go into the thousands of pounds, even without calculating the reputational damage inflicted (£25,736 Hiscox)
- National Cyber Security Centre state 46% of SMEs suffered at least one cyber security breach or attack in 2017 and 43% of SMEs still have no plan in place to deal with the issue.
- Ironically 49% of SMEs believe that it is unlikely to happen to them! (Take Five)

"In the opinion of the experts on cyber fraud, they claim there are two types of businesses; those that have been hacked and subject to cybercrime and those that will be!"

Legally through the GDPR it is the responsibility of the business to train staff to an appropriate level. In the event of a breach, which now must be reported, first and foremost the ICO will investigate your training records. Part of the law requires you to have an up to date training register for all appropriate employees and regular refresher training provided. So why are businesses not providing this and protecting themselves when the data claims culture is building rapidly?

0116 2688728
info@perituslearning.co.uk
https://perituslearning.co.uk/peritus-protect/

Peritus
The Learning Experts

The SME - Created by an **SME** for an **SME.**

MD's briefing

*Growing Data and Cyber Security Risks for **SMEs***

After an Attack SMEs reported that;

89% felt that the attack had impacted their reputation

30% reported a loss of customers

25% received negative reviews on social media

26% were unable to grow in line with previous forecasts

93% suffered operation limitations

(Cyber Streetwise & KPMG)

Reputation is king - Building trust in the digital age

There are some businesses who have taken the bull by the horns and are targeting competitors who they suspect are not compliant. Through marketing tactics, they are using their own compliance status to promote to customers, suppliers and stakeholders to demonstrate they are a modern thinking and trustworthy business to work with.

Reputation is king when building trust in the digital age. Data leaks, cyber-attacks and compliance-based prosecutions can provide a catastrophic impact on the credibility of you and your business. Therefore, recovery can be nigh on impossible for some, as damaging news travels so quickly in today's business world. Customers, suppliers and your people will question their trust in associating themselves with a business who did not invest to protect them.

Understanding the commercial risks

There will come a point soon where non-compliant businesses could start to experience a whole range of complications and restrictions. Banks may require proof of compliance to lend and for retention of existing lending. Accountants may have to make provisions in accounts for potential claims made against non-compliant businesses, therefore directors' drawings could be seriously affected. The business you have built to sell could be devalued by up to 50% on sale, which is a frightening concept.

We are already starting to see some mortgage lenders requiring proof of compliance for the GDPR before they will consider lending to self-employed people.

0116 2688728
info@perituslearning.co.uk
https://perituslearning.co.uk/peritus-protect/

Peritus
The Learning Experts

The SME - Created by an **SME** for an **SME.**

MD's briefing

*Growing Data and Cyber Security Risks for **SMEs***

"57% of SME owners didn't believe that fraud in the form of invoice redirection were a genuine risk to their business"

(National Fraud Intelligence Bureau)

You protect the rest of your business, right?

Every business owner believes in protecting their asset against a whole raft of potential business issues through a range of insurance products, which is seen as a given! So why are so many business owners not protecting themselves against the threat of data breaches and potential cybercrime when this is such a rapidly growing area of risk?

Typical responses are;

- The GDPR is difficult to understand.
- We don't have the resources or budget to implement new laws.
- We won't be affected by cybercrime, this is a big business issue.
- To train our people will be time consuming and costly.
- How on earth do we keep up with the changing world of data and cyber security?

These comments are perfectly plausible, however can any business really afford to ignore the commercial consequences of doing nothing, or getting this wrong?

Peritus Learning

Innovators of the UK's only online data and cyber protection product for SMEs – Peritus Protect - £99+ VAT per month
Developed by an SME for an SME.

Phone: 0116 2688728
Email: info@perituslearning.co.uk
Website: https://perituslearning.co.uk/peritus-protect/
Locations: Leicester, London, North America (Toronto)

Steve Walker, Managing Director – Peritus Learning