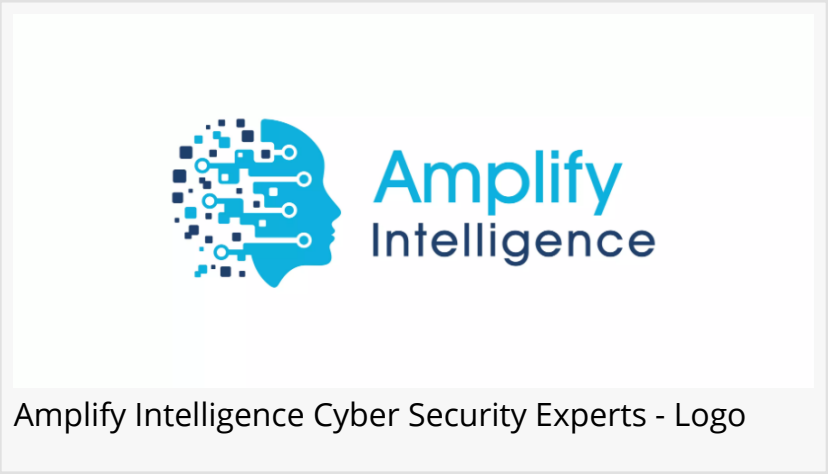
Cyber Security Compliance for Small Business - Amplify Intelligence steps up to the plate

Being able to prove Compliance with the cyber security requirements of your clients has become extremely important in 2020 - 2021!



Amplify Intelligence Cyber Security Experts - Logo

MELBOURNE, VICTORIA, AUSTRALIA, December 1, 2020 /EINPresswire.com/ -- You may be losing big business because you are not able to prove your compliance - "Cybercrime is the greatest threat to every company in the world." (Ginni Rommety) Working within a security policy framework reduces your risk of a breach, purely because your new habits make you a harder target!

> Good risk management isn't just about implementing controls, it's about measuring and validating that they effective"
>
> *Paul Byrne - Founder | CEO at AMPLIFY INTELLIGENCE LIMITED*

Amplify Intelligence wants to let you get on with business and not need to try and 'figure out how to become compliant'. - We take care of that part, and provide you with a policy and framework that results in you needing to spend less time worrying about this.

As of July this year (2020), the law has changed - if your client is any of the large financial organisations in Australia, they must be able to demonstrate 'your' minimum level of cyber security capability.

We aim to reduce the complexity of this very issue. We explain where you are strong and where you are weak, and we provide the policies and procedures that can demonstrate how reliable you are - as well as guide you towards a stronger cyber security position. You are able to demonstrate an ongoing increase in the strength of your cyber resilience.

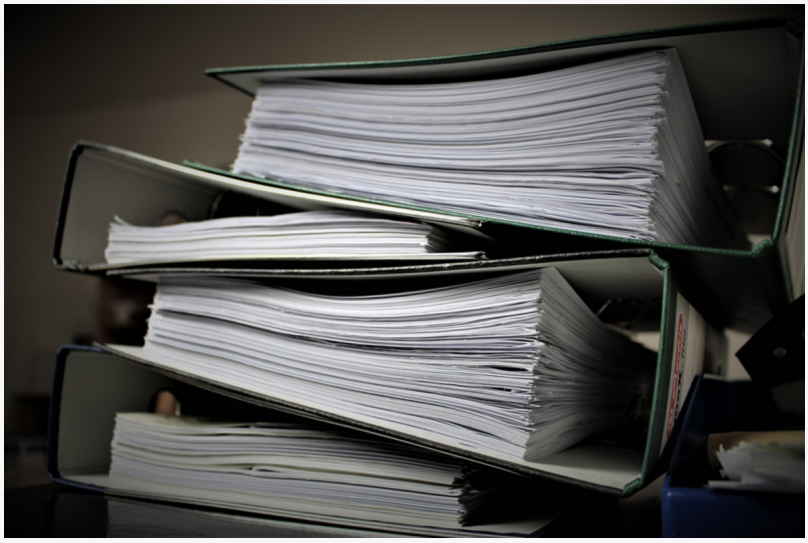
We provide the tools and documents to help you meet the standards required by your clients - We measure and examine how your business hangs together and where data can be compromised. Our recommendations will assist you in being a harder target. A criminal would

rather hit an organisation that isn't looking, and more importantly isn't updating and fixing issues as they arise.

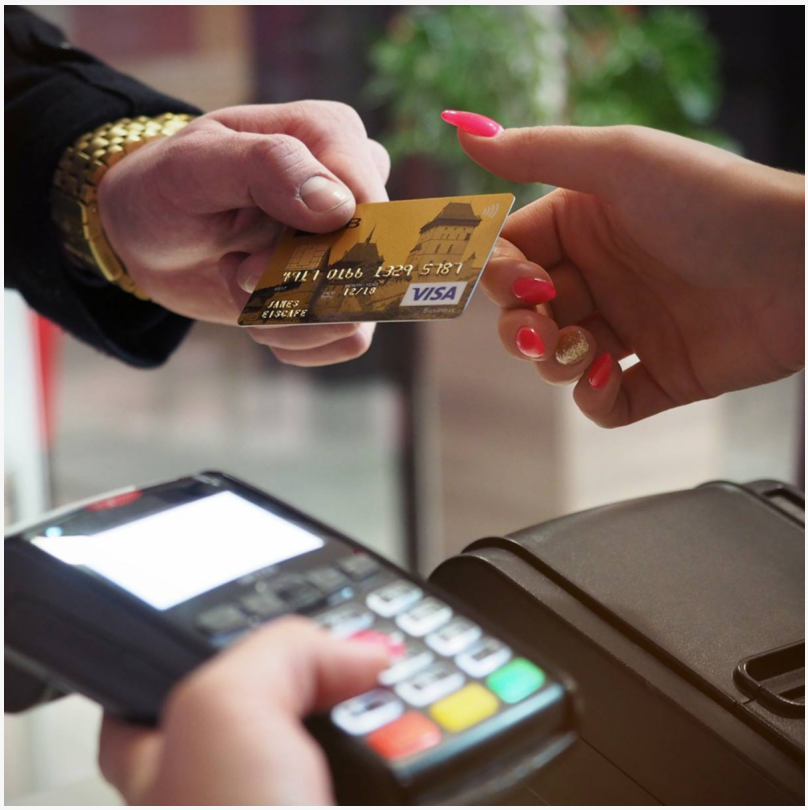
"A majority (86% of KPMG survey participants) said they would consider removing an SME supplier if it suffered a data breach".

What this means is that your compliance with the regulations is not only your responsibility, but the responsibility of those that employ your services. Many of the larger organisations now require you to understand how compliant your business is, so that they can gauge your risk to their data.

When a small business expands, there is often a greater need for external resources covering basic business functions such as accounting, IT, training, hiring and sales. The rising need for cyber protection is usually ignored - or just not part of the scope increase.



cyber security compliance paper work



Protecting credit card information protects your customers

Instead of recruiting a new salesperson, small companies should to find cyber security expert advice in order to fix any data security issues well before they even begin to compete for a federal contract - being able to demonstrate that you are aiming for compliance indicates less risk to your client should a data breach ever occur.

So why are small companies targeted more frequently than larger ones? Almost all cyber threats are for personal data, and will usually be used on a credit card. While larger businesses usually have more data to steal their networks are rock solid, small enterprises have fewer security measures and therefore offer softer networks - making it much easier to steal customer data. This is the very reason for the law change mentioned above. Small business is now the weakest

link in this information chain, and because of this, larger companies now need to prove your cyber resilience to both their customers and to the regulators.

If industry trends hold true, then the cost of cyber insurance will continually be on the rise - because customer data is becoming more and more valuable to hackers. One of the recommendations made by the cyber insurance industry, specifically in relation to reducing your premiums, is to be able to demonstrate your willingness to reduce your own cyber risk footprint through increased compliance and use of a strong in-house security policy.

Compliance cannot be ignored any longer, the risk to you as a SME grows by the day, and the government has stepped in and drawn a line in the sand.
Learn more about compliance at Amplify Intelligence https://www.amplifyintelligence.com/cyber-security/services/compliance/

Paul Byrne
Amplify Intelligence Ltd
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
