Protect yourself from embarrassment, financial loss and ruin

WHITEPAPER: SPRING 2018
AUTHOR: STUART MULLEN
SUBJECT: CYBERSECURITY

serenitydigital

CONSULTANCY | CREATIVE | TECHNICAL | ACQUISITION

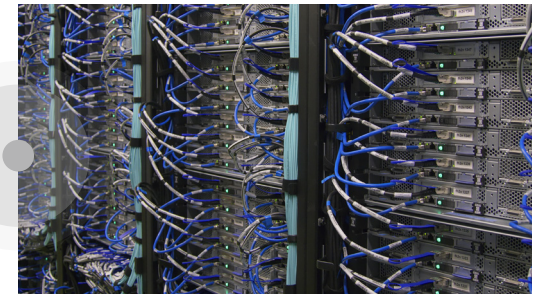
Identifying risks & implementing solutions

In the 21st century it's almost inevitable that at one time or another, you will have a digital product or facility which will need protection from unauthorised access.

Therefore, it is crucial that you utilise cyber security experts to employ technologies, protocols and controls which are intended to defend your data from hacking attempts.

Businesses stand to lose assets, reputation and revenue, as well as facing huge legislation fines when they are subject to security attacks and breaches.

We protect organisations against the mistakes many make and build in solid foundations, robust architecture and modern protocols and architecture to avoid the worst case scenarios from occuring.



"Cybercrime damage costs to hit $6 trillion annually by 2021"
(CSO[1])

Ticking all the boxes

Most organisations believe that they are unlikely to be the target of an attack, but the question is not if you will be, but when.

For many businesses, they are still unclear about how vulnerable they are and as many as *"45% mistakenly think that they are not a viable target".* ***(YouGov[2])***

We know that cyber crime is big business, therefore securing our systems and our clients' data has always been an essential part of our service. By utlising a combination of expert consultation, education for our client and prospects and long term planning, together we can create a strategy which ticks all the boxes.

What we're seeing

We work with organisations of all sizes, and see the issues business owners and digital teams face when trying to protect their systems. IT Security is essential, however so often we see prospects who have fallen foul of one (or many) of the following pitfalls:

COMPLACENCY
Whilst larger organisations tend to have a realistic appreciation of the threats they face, small-medium enterprises often don't imagine it will ever affect them, but all organisations connected to the outside world are at risk.

PLUGGING THE WRONG GAPS
Some businesses understand that there are threats, but do not know where the gaps are that make them vulnerable. Hackers are normally resilient and gifted, they will keep searching for flaws, so plugging them all is essential.

SOFTWARE PAST ITS SELL BY DATE
Out-of-date software can cause a variety of problems. Cyber criminals do communicate with each other so as soon as a flaw is known, it can be exposed and used against you. These flaws can become easier to expose as the software gets older.

INSECURE/OUT OF DATE PLUGINS
Insecure web plugins make any infrastructure vulnerable to attack. Every time you work with a supplier, consider how much they know about the external facilities they implement on your behalf. If they can't explain why it's safe, get a second opinion from someone who can.

LIMITED WEB SERVER SECURITY
Without sufficient web server security hackers could gain complete access, not just to your website, but also to sensitive user data being stored on it. An intelligent hacker may also implement changes without your knowledge - Would you like customer purchases to be redirected to the wrong payment provider and an alternative bank account?

NO SSL
We have seen many organisations without an SSL certificate. This serves to keep communications between a website and an internet browser secure. It essentially keeps visitors to your website secure and protected, and more and more consumers look for this now before entering a site. Therefore, it's not just important for everyone's security, but also for engagement.

WEAK PASSWORDS
This is a very common issue within businesses and it can be difficult to police individual passwords, however human error, through the creation of poor passwords, is the easiest way for data breaches and attacks to occur.

INSUFFICIENT DISASTER RECOVERY
Despite all your planning, you cannot guarantee that the worst will not happen. But if it does, you must have have procedures in place to limit the damage. Avoid embarrassment through a clearly defined and tested procedure which can bring you back from the brink in an appropriate timescale.

Proactive and responsive strategy

You can avoid sleepless nights, unnecessary stress, financial loss and embarrassment by following a well considered implementation of the correct policies, procedures and best practice.
Our 9 tips below will put you on the right track to mitigate a large percentage of cyber attacks:

KEEP ABREAST
Whether this is existing or upcoming legislation such as General Data Protection Regulation (GDPR), it's important to stay updated so you're not caught out. If you don't feel confident in being able to stay abreast of changing legislation personally, work with a supplier who has the skills necessary in keeping you safe and well informed.

STAY VIGILANT
Implement facilities, procedures and staff education which allow you to monitor how your systems are being used. If you spot something which doesn't look right, then it probably isn't. Encourage your peers to alert you to potential risks as and when they see them.

FLAG SUSPICIOUS EMAILS AND CALLS
Most of the time if something is too good to be true, it probably isn't. Don't be tricked into divulging sensitive information unless you are 100% sure of the person you are communicating with. Work on a suitable internal policy to provide guidance to your staff to mitigate against phishing scams and ask them to flag them up immediately.

ENFORCE PASSWORDS
Without proper guidance and education, staff are not necessarily aware of the risks to businesses when not having passwords and safe computing practices in place. To keep data and your infrastructure safe, strong and secure passwords are a must.

PROTECT SENSITIVE DATA
Sensitive data should never be stored or transmitted without appropriate security measures in place, whether that's password protection and/or encryption. Ensure that data which is no longer required is removed and deleted from systems (including email, backups and cloud storage).

CHECK YOUR PLUGINS
Outdated or insecure plugins leave your website and IT infrastructure vulnerable to attack, so it's essential you continue to check and update plugins. Your supplier of choice should be doing this for you. If they aren't it might be time to ask why?

KEEP YOUR DEVICES SAFE
This is really basic, but ensure your staff are aware of the risks to mobile devices and mobile data. Take care of your IT. Do not lose that USB stick full of customer data (in fact don't have a USB stick full of customer data in the first place) and do not leave your devices unattended or easily pick pocketed.

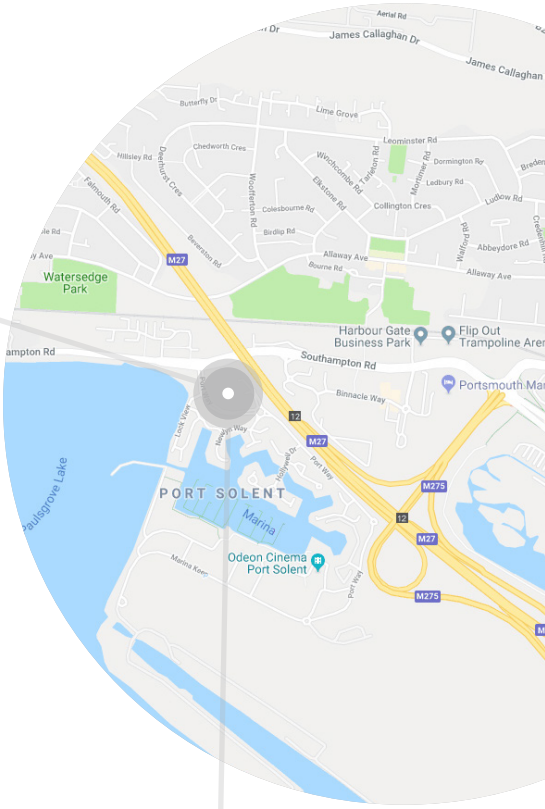
IMPLEMENT A DISASTER RECOVERY STRATEGY. NOW.
Disasters happen. They occur when you least expect it and they are hugely inconvenient. By having a set of policies, tools and procedures to enable the recovery of vital technology and information in the event of a disaster, you limit the risk to your business, your customers and your reputation. Take backups, store them safely and consider how quickly you can revert to them when the worst happens.

INVEST IN A GOOD SECURITY PARTNER
Find a supplier who asks about and understands your company objectives, and covers the bases. These includes everything from server security, website encryption, malicious software prevention, cyber security education and circumventing data breaches.

In a nutshell

As the use of digital devices has now become an everyday part of most peoples lives, awareness of the importance of cybersecurity has grown. However, it is minefield so knowing where to start can feel like an impossible task.

If data protection, privacy and cybersecurity are areas you are concerned about and wish to take a little more seriously, then please get in touch to begin a conversation with our experts.



Get in touch

Whether you're after project assistance, have a new project you'd like us to help with or just fancy meeting over coffee, we'd love to hear from you.

Our normal office hours are from 08:00 until 17:00, Monday to Friday, but we're normally contactable via email at most times when there is an emergency. We'll always aim to get back to you within 24 hours of your contacting us.

+44 (0)2392 985 750

hello@serenity.digital

https://serenity.digital

Office 6, Pure Offices, 1 Port Way,
Port Solent, Portsmouth, Hampshire
PO6 4TY

You can also find us on social networks:

How to find us

Our office is found in sunny Port Solent, near Portsmouth on the South Coast.

Please follow signs to Port Solent from the A27 (going West) or from the M27 (going East). Upon entering Port Solent we're in the two office buildings directly on the left - follow the road to the first roundabout and take the exit left into the car parks. We're in the Pure Offices car park, please use the phone at Reception to let us know you've arrived.

Whitepaper references

CSO[1] - https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html
YouGov[2] - https://duo.com/assets/pdf/duo_security_poverty_line_survey_9_26_17.pdf

serenitydigital