COMPUTER WORLD
Helping Businesses Define Tomorrow™

WHITE PAPER

How to protect your business from a security breach

COMPUTER WORLD
Helping Businesses Define Tomorrow™

WHITE PAPER

How to protect your business from a security breach

The ever increasing risk to your business...

We are seeing an increasing risk of cyber-attacks to businesses of all sizes, across the globe, with attacks being far more focussed and intelligent than ever before. The target is your data, and ultimately money. Despite the increasing risk to businesses we are still seeing a large number of organisations being blasé around the risk that is posed to them and what they can do to mitigate it. Microsoft reports that on average it takes more than 200 days to detect a security breach and a further 80 days to contain it!

READ MORE FROM MICROSOFT

Each year Allianz Insurance creates a business risk barometer. Their 2016 report indicated that cyber incidents have increased by over 25%, making cyber security one of the top 3 risks posed to businesses. We are seeing the number of connected businesses devices rise, but without an increase in the levels of security we apply to these devices we are simply increasing our vulnerability.

“The current level of security of connected devices is still low. Cyber security risk will increase as each device is a potential entry point for data breaches and inter-connectivity can increase the damage significantly, creating high accumulation potential”

READ THE REPORT HERE

Finally the types of cyber threat we face is continually growing — becoming both more personalised and sophisticated. In Symantec’s annual threat report they found that...

- In 2015 a new zero-day threat was discovered on average once a week
- Social Engineering is increasing as a form of attack, leaving your employees as the weakest link
- A 35% increase in ransomware attacks

Amongst other rising statistics, most shocking of all is the fact that over half a billion personal records have been reported to be lost over 2015. How many more haven’t been reported?

READ SYMANTEC REPORT HERE

With these growing risks to our business it is time to take the risk of cyber-attack seriously and review the layers of security within our business.

COMPUTER WORLD
Helping Businesses Define Tomorrow™

WHITE PAPER

It's time to review your protection

When reviewing the security within your infrastructure you should start by considering the 'business as usual' security measures that are looked at by most businesses, but maybe it is time to review these solutions to ensure they are still fit for purpose.

When was the last time you reviewed the following elements within your infrastructure?

- **Anti-Virus**
  Anti-Virus signatures are now considered to be old hat and whilst they are still a critical element of protection they shouldn't be the only level of protection from your Anti-Virus solution. Modern anti-virus solutions should offer threat analytics that allow data and workloads to be monitored to capture an attack prior to a signature being written. We should also ensure that our anti-virus solution will integrate with our virtualisation technology to offer deep inspection and to offload the workload from the agents to a dedicated anti-virus system.

- **Edge and DMZ Firewalls**
  Having a robust firewall solution at the edge is just as critical today as ever, however as we will read later we can no longer rely on it being the only form of security. We should ensure that web facing workloads, such as websites and email are placed within a secure DMZ, we should further consider isolation between servers and users. All firewall solutions should be up to date and also highly available, with a reliance on having internet connections a single firewall solution maybe a significant business risk.

- **Backup and Disaster Recovery**
  Backup and disaster recovery should be on top of an IT Manager's radar. Consider when was the last time you tested the recovery of your data from backup and did a complete DR test? We highly recommend that backups should be tested on a weekly basis and DR on a quarterly basis at minimum. Your backup solution should be designed with the 3-2-1 rule in mind, 3 copies of your backups, 2 different mediums and at least 1 held off-site.

- **Mail and Web Filtering**
  Mail and web filtering is a critical area of protection to mitigate the risk to your business, if we can stop users being sent viruses or indeed phishing emails as well as visiting non-trusted websites we are able to significantly reduce risk. We recommend that mail filtering should be cloud-based, this reduces the risk and network bandwidth of you pulling all mail to site before it is filtered. With web filtering an online, highly available solution is recommended.

One of the fastest growing forms of attack is social engineering. Social engineering works by turning your employees into the weakest link and utilises a number of methods such a phishing and baiting attacks to access your systems and ultimately your data.

COMPUTER WORLD
Helping Businesses Define Tomorrow™

WHITE PAPER

With the growth of social engineering there is a need to enhance security surrounding the users, these are areas where traditional security solutions are unable to assist. See our tips to enhance the security of this modern day threat below.

TIP 1

Move from an unmanaged to managed desktop estate

Zero day exploits utilise security weaknesses in the applications we use every day, resulting in security holes. Government recommendations are that applications should be updated on a regular basis to minimise risk. Also providing a standard build and automated desktop rollout will improve break fix and security of your systems.

Q. How do you rollout your desktops today?

Q. What is your patch and update policy for your desktop and server estate?

TIP 2

Improve internal network security

Whilst we spend thousands on protecting the exterior of our networks with firewall technology, the internal network is often overlooked. As many cyber-attacks are now focusing on accessing your data from within your network we need to increase internal network security.

We should ensure that we deliver a secure enterprise class wireless solution, most devices we use today are severely limited when it comes to being able to connect to a wired network, our guests also expect to be able to access the network. An enterprise class wireless network is able to offer high performance blanket coverage whilst delivering robust security from attacks.

Q. How do you deliver wireless networking to your business?

Network isolation is also key, if one system is compromised this could allow free range of travel to all the other systems on your network. As standard many enterprise wireless solutions are able to offer guest isolation. We should also look to provide isolation between our servers for the same reason by utilising the latest in network virtualisation technologies.

TIP 3

Plan for the cloud

Whether we like it or not our data is heading for the cloud, our users are used to being able to access their data and applications any place, any time, on their smartphones and tablets and as such our business data is following suit. We call this shift of business data and applications from IT control to the users control shadow IT. With the introduction of shadow IT, IT loses control of the security and resiliency of the data. Many IT departments try and block technology that is seen to enable shadow IT such as DropBox by using IT policy or trying to block services at the edge of the network. However realistically the only way to beat these cloud technologies is by joining them and matching the functionality that our users desire whilst maintaining control of the data security and resilience.

Q. Have you created a cloud strategy for your business?

Q. How are you protecting your data in the cloud today?

We recommend business have a cloud strategy, allowing them to start the journey to the cloud in the most secure manner. Our steps are as follows:

STAGE 1 **Plan**
Without a plan in place, your users are going to introduce shadow IT and you will lose control.

STAGE 2 **Protect**
Whether you have put your business data in the cloud or not, you can almost guarantee in the mobile/cloud era that your data will be in the cloud. You should introduce technologies that allow you to protect your data at source, to ensure even if it gets in the wrong hands it won't be accessible.

STAGE 3 **Enable**
In preparation for the migration this is a good time to invest in enablement training for your users and IT team to ensure they get the most out of your cloud investment. By offering training you will ensure that users are knowledgeable about the business approved systems and won't feel the need to turn to shadow IT.

STAGE 4 **Migrate**
Once you have a robust plan in place, understand how to protect your data and your employees are enabled, it's time to migrate to the cloud in a planned manner with minimum impact to the business.

TIP 4 **Cyber-Security education**
With cyber-attacks taking many different guises it is important that both IT administrators and end users are educated on the risks they could pose to the business. For IT administrators there are a variety of courses and certifications available. CompTIA offer a good starting point with the Security+ certification which offers a wide variety of study options. For user training you should investigate a mixture of e-learning, awareness campaigns and bite-size instructor led courses.

Q. Do you educate your users about how they can help avoid cyber-attacks?

TIP 5 **Identity Management and Authentication**
There is increasing demand on users to be remember multiple passwords and accessing data and applications in multiple locations. Together this introduces a larger attack area for your data. Where the desktop used to be the central point of access to all of your applications this is increasingly becoming a large amount of web services accessed from a multitude of devices. Social engineering focuses firmly on gaining credentials and other key information from end users to allow unwarranted access to your systems. As such multi-form factor authentication and centralised application launchers should be considered. Not only do these solutions allow ease of management across all applications for IT administrators, they allow the users to quickly and easily find what they need and ultimately offer a higher level of security for your data.

COMPUTER WORLD
Helping Businesses Define Tomorrow™

WHITE PAPER

ComputerWorld is the largest provider of expert business IT solution and services in the South West and Wales. Over the last 25 years it has grown to become one of the UK's most trusted providers of best-in-class IT consultancy, support, procurement, recruitment and training for all kinds of business and educational establishments – both large and small.

Areas of expertise

Virtualisation & Cloud

We design, deliver and protect custom built virtualised solutions – bringing our customers the latest technology that allows them to focus on where their business is going, not just where it is!

Networking

We provide fast and secure networks for enterprises of all sizes and across all sectors, from education to heavy industry.

Microsoft Technology

Nobody knows more about how to maximise your Microsoft investment than ComputerWorld's engineers, most of which are MCSE qualified or greater. Our team has been offering expert Microsoft solutions since day one and bring to the table an unparalleled amount of experience, whether you're looking to migrate to Office 365 or for traditional Microsoft services.

Desktop Transformation

IT departments are finding ever increasing demand to deliver the flexible working environments their employees need to fully optimise their output. We work alongside industry-leaders in business mobility to help businesses realise the true potential of their workforce and to combat Shadow IT.

Security

ComputerWorld's security consultants have all of the expert knowledge and certifications needed to offer businesses the most robust solutions for all aspects of IT security. We work in close partnership with some of the industry's most respected hardware and software vendors.

Contact ComputerWorld today

enquiries@computerworld.co.uk

01454 338 338

Apex House
Turner Drive
Westerleigh Business Park
Yate
Bristol
BS37 5YX

computerworld.co.uk