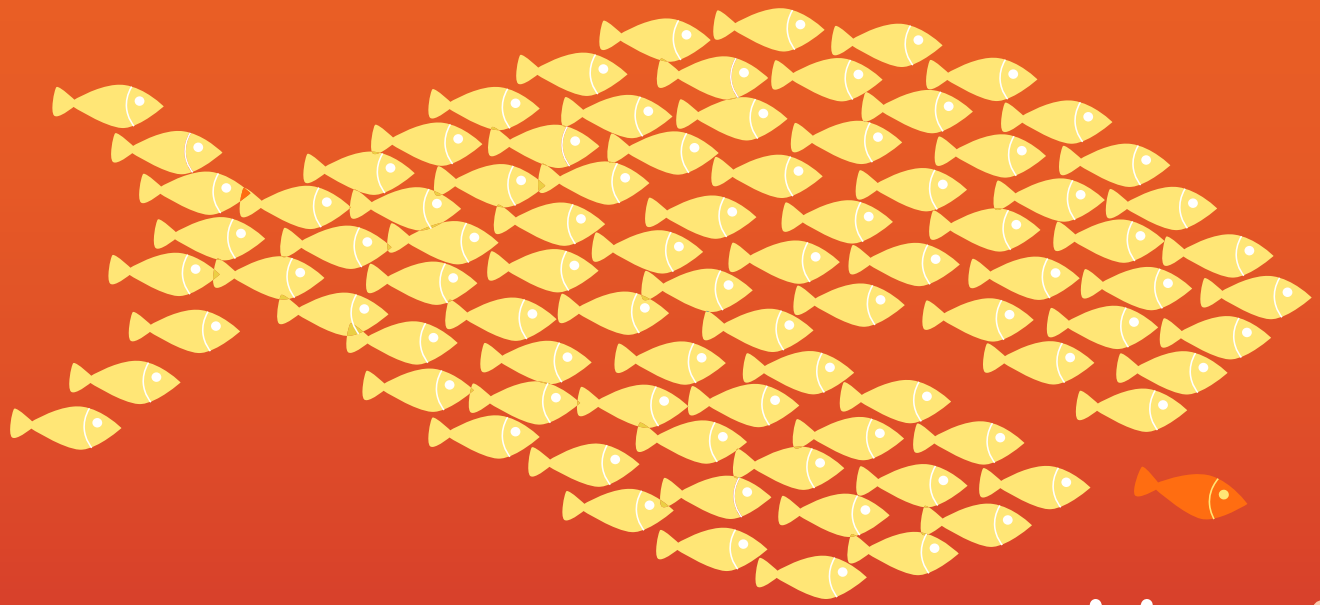
THE SCALE AND ASSOCIATED COSTS *of IT security* AND COMPLIANCE

The future of IT in business

Maxxia

“The risk of fraud and online crime, both real and perceived, is costing each UK small business up to £4,000 per year”

– UK’s Federation of Small Businesses (FSB)



Maxxia

Introduction

Data and online security is now a major worldwide talking-point; and businesses of all sizes are frantically trying to ensure they are protected from cyber attacks, security breaches and data loss. During the recent Heartbleed bug, one of the internet's most widely used encryption tools (deployed in approximately two-thirds of websites) was 'hacked' meaning highly-sensitive data was compromised all over the globe.

According to the World Economic Forum, if attacker sophistication continues to outpace defender capabilities (resulting in more destructive attacks), a wave of new regulations and corporate policies could slow innovation, with an aggregate impact of approximately US$ 3 trillion by 2020.

But what does this mean for you and your company's bottom line? Well, failure to adequately secure your organisation's data or comply with data regulations could not only result in a security breach, but also high fines for failing to comply and protect sensitive information. On top of this, your brand reputation may be damaged beyond repair, therefore costing your business customer lifetime value and future revenue.

To help you better understand security and compliance and also protect your business against potential breaches and the associated financial ramifications, we've created this helpful e-guide. Read on to find out what's needed to protect your data, your company reputation and your profits.

Types of threat and security costs

93% of large organisations and 87% of small businesses had a security breach in the last year
- PwC Cyber Security Report

Before it's possible to protect your organisation against security threats and their associated costs; it's first necessary to identify the different types of threats. Any risk to your organisation or data will come from five clear areas…

1. Systems failure or data corruption
2. Infection by viruses or malicious software
3. Theft or fraud involving computers
4. Other incidents caused by staff
5. Attacks by unauthorised outsiders (including hackers)

Given the cost of a security breach or data loss, it's unsurprising that organisations are allocating more of their budget to protection tools and policies. According to the PwC report, businesses typically spent 10% of their IT budget on security; with small and medium sized companies allocating slightly more (12%).

But if this budget allocation seems excessive, consider this… when a large pharmaceutical company took nearly a month to discover that an attacker had accessed its internal network; it took over 100 man-days and cost over £100,000 to resolve the issue. So perhaps 10-12% of the IT budget is a cost worth paying to be protected.

Maxxia

“64% of organisations will focus more on managing reputational risk than they did five years ago”

– IBM Data breach statistics

Maxxia

Suggested security measures

To protect your organisation against the financial risks of a security breach or data loss, it's worth making sure that your company's IT manager is implementing the following measures (as advised by the Information Commissioner's Office).

- All computers should have a firewall, spyware and anti-virus software installed
- Operating systems need to be able to receive automatic updates
- Patches or security updates should be downloaded to cover vulnerabilities
- Limit employee internet access to only the sites they need to complete their job
- Advise employees not to share their passwords

In regards to sensitive data, ensure that it's encrypted, backed-up regularly and the back-ups are stored at a separate secure location (a legal requirement). To ensure data is protected even at the end of a computer's operating life, either destroy the individual hard drive or use specialist software to effectively 'wipe' the hard drive.

In addition to the preventative measures mentioned above, ensure that your organisation is compliant with all industry-relevant data regulatory bodies such as the Financial Conduct Authority (FCA), the Payment Card Industry Data Security Standard, ISO 27001 and the Data Protection Act 1998. Failure to comply could result in hefty fines for your business.

Maxxia

More than half (53%) of the organisations surveyed revealed they did not conduct daily backups

– Iron Mountain

Maxxia

Backing-up and the costs of not doing so

We all know that backing-up is the process of copying existing data onto a separate device so that it can be stored separately and safely. This protects the business in the event of a security breach or catastrophe and allows it to continue operating. Yet, according to Iron Mountain, 30% of businesses that don't back-up every day stated that it was not an efficient use of their time.

From a data security standpoint, customer and company data is a high-value commodity for fraudsters, with some paying up to $150 for 6GB of user credentials; but it's your company's responsibility to protect this data and information. Although it will take more than just backing-up to prevent a security breach; if the worst was to happen, your company would still be in possession of the backed-up company/customer data which it could update and protect almost immediately.

The other benefit to backing-up is that in the event of a natural disaster (such as the flooding seen in the UK this winter); a company could simply resort to the back-up data to continue trading at a safer time and place. This may not seem like a vital requirement for businesses, but according to the Strategic Research Institute, companies who are unable to resume processes within 10 days of a natural disaster are unlikely to survive more than a year.

So considering the potential for lost brand reputation, lost future revenue, large fines from data regulators and the likelihood that the business will fail within the next 12 months; backing-up now seems like an unquestionable necessity for all businesses.

Maxxia

“Gartner expects the cloud-based security services market to reach $4.2 billion by 2016”

Maxxia

Future security threats

As technology continues to develop and mobile devices become even more popular, organisations are going to have to implement more advanced security policies to manage BYOD (bring your own device) operations and Wi-Fi networks. With more employees accessing the internal company network using their mobile devices, businesses are at greater risk of data compromise from an employee (whether intentional or otherwise).

In addition to this, the use of Wi-Fi networks as a means of connecting to the internet is also likely to pose a greater risk. Researchers at the University of Liverpool have shown for the first time that Wi-Fi networks can be infected with a virus that can move through densely populated areas as efficiently as the common cold spreads between humans. Even more concerning is that the virus is only ever present on the Wi-Fi network and therefore untraceable on individual computers.

To combat these advancing security threats, anti-virus protection tools will become more agile, responsive and cloud-based. FireEye's cloud-based anti-virus tool will quarantine all inbound traffic (unlike traditional methods which only quarantine known threats) and release it only once it's proved to be safe.

These new approaches to security will require the latest equipment, software and monetary investment, but the associated costs of implementation wane in comparison to the potential losses.

Prepare to reduce risk and costs

If you believe your organisation needs to bolster its security and back-up procedures to protect itself against current and future intrusions… make sure you have the right tools for the job. Hopefully this e-guide has illustrated just how costly a security breach can be to your business… both in terms of brand reputation and also lost revenue.

At Maxxia, we're not security specialists but we can give your organisation risk-free access to the latest security solutions without the initial capital expenditure. As an industry-leading asset finance company, we can help you source the best technology and also create manageable monthly payments. When you need to upgrade your equipment, we'll simply remove the old tools and provide you with the latest versions on a new lease.

The result is that your company can be protected against the latest security threats and comply with even the strictest regulatory bodies – all without a large investment, tying up capital or the need to worry about residual asset value.

With the inherent benefits of superior security and data protection coupled with the minimal risk involved in asset finance; securing buy-in and funding from the board should now be a much easier process.

Maxxia

To find out the role asset finance can play in supporting your business, simply speak to one of our experts on 0845 643 1319 or email contact@maxxia.co.uk

www.maxxia.co.uk | Maxxia