WHITE PAPER

PREVENTION IS BETTER THAN CURE: SECURITY FIRST

PREVENTION IS BETTER THAN CURE WHEN IT COMES TO IT SECURITY

Introduction

It’s an important time for understanding how IT security can protect your business.

In 2016, cyber-attacks were already reported to have increased by 25%[1]. But then came an unprecedented few months of high-level targeting of businesses and political institutions that showed just how sophisticated and intense these attacks were becoming.

Unfortunately, keeping up with this ever-changing threat can be a challenge for all but the biggest organisations. Which leaves most small to mid-sized businesses exposed at a time when the rising risk of being attacked is matched by the increasing cost of being a victim.

This white paper discusses the risks associated with cyber-crime, what they might mean for your business, and why we believe your IT security strategy needs to stay ahead of the game by focusing on prevention, not cure.

A more dangerous digital world

The threat of cyber incidents (including cyber-crime) is currently the #1 business concern in the UK, and among the top three corporate concerns worldwide, according to a recent report by Allianz.[2]

In fact, this is the fifth year running that there has been an increase in perceived risk. And with high profile occurrences appearing more frequently in the news – such as the recent WannaCry attack on the NHS[3] and the external interference in the US Presidential election[4] – it’s not hard to see why.

Attacks by hackers, organised crime, data breaches and the spread of viruses make up the majority of cyber incidents. Yet the reasons behind them can vary considerably, from purely financial to data and identify theft.

Given the increasingly sophisticated nature of these attacks, and their high-level profile, it’s easy to understand why so many small and mid-sized businesses seem unmoved in keeping their IT security up to scratch. Either they underestimate their risk of exposure to being targeted, or they simply don’t have the ability to keep up.

> CYBER RISK IS NOT GOING AWAY AND PEOPLE AROUND THE WORLD ARE RIGHT TO BE CONCERNED. INCREASING SOPHISTICATION OF CYBER ATTACKS POSES A HUGE RISK FOR BUSINESSES, WITH THE POTENTIAL FOR CAUSING LONG-LASTING AND COSTLY BUSINESS INTERRUPTIONS – AS WELL AS DATA PROTECTION ISSUES.

Derren Stephenson | Head of Operations and Cyber Security (CISSP) of Seriun

[1] Allianz Risk Barometer: Top Business Risks 2016
[2] Allianz Risk Barometer: Top Business Risks 2017
[3] The Economist, Daily Chart: Ransomware attacks were on the rise even before the latest episode, May 2017
[4] Symantec Internet Security Threat Report Vol 22, April 2017, pp14-20

How cyber-attacks can impact your business

Only last year it was estimated that cyber-crime costs the global economy nearly $445bn a year.[5]

Symantec's Internet Security Threat Report 2017 details a sudden rise in email malware rates, with 1 in 131 emails now determined to be malicious. Meanwhile, ransomware detections have increased by a massive 36%, with the average cost of ransoms being demanded from businesses growing to $1077 (up from $294 the previous year).[6]

There is also an increased threat to our 'Internet of Things' approach to business, with greater office connectivity and a reliance on cloud services failing to be balanced with increased security. A key component of this problem could be that the number of average cloud apps used by a business is often severely underestimated – with Symantec detailing that the average is 928 apps, while most CIOs thought they were only using 30 or 40.[7] Regardless, attacks through these weak spots seeking data, financial gain, or to merely disrupt, are gaining momentum.

Impact on reputation is another much overlooked cost of these attacks, especially when it comes to loss of data. And this is set to become a bigger threat in May next year with the introduction of **GDPR**.

How GDPR will affect security measures

The EU General Data Protection Regulation (GDPR) is officially described as being the **"most important change in data privacy regulation in 20 years."**[8]

Coming into effect on 25 May 2018, it aims to bring balance to data privacy laws across Europe, with a view to giving greater protection and empowerment to the data of all EU citizens. However, tightening of this regulation also means businesses will face heavier consequences for breaching rules.

The Allianz Risk Barometer 2017 report suggests that time is already running out to prepare for this crucial change in the business landscape, stating that **"It will impose significant liabilities and penalties on companies doing business in the EU or with EU citizens. Costs to comply with the legislation will be high, the penalties of not complying could be even higher."**[9]

With fines for non-compliance potentially as high as 4% of a business' annual global turnover (up to $20 million)[10], it is essential companies get serious about better protecting their data – and quickly.

Prevention is a key element in IT security

The benefits of preventing problems happening with your business clearly outweigh the costs of cleaning up after an attack – because those costs won't just be financial, but will also have long-lasting effects on productivity and reputation.

[5] Net Losses: Estimating the Global Cost of Cyber-Crime, CSIS/McAfee
[6] Symantec Internet Security Threat Report Vol 22, April 2017, pp10-12
[7] Symantec Internet Security Threat Report Vol 22, April 2017, p8
[8] EUGDPR.org
[9] Allianz Risk Barometer: Top Business Risks 2017, p14
[10] EUGDPR.org

> STUDIES SHOW THAT IT TAKES, ON AVERAGE, 90 DAYS FOR BUSINESSES TO DISCOVER THEY HAVE BEEN HACKED. OFTEN THE INCIDENT IS IDENTIFIED, NOT BY THE BUSINESS ITSELF, BUT BY THE CUSTOMER OR ANOTHER STAKEHOLDER, WHICH IS ANOTHER REASON WHY CYBER RISKS POSE A HUGE THREAT TO A COMPANY'S REPUTATION. THE FACT THAT COMPANIES OFTEN ONLY RECOGNIZE THE LOSS WHEN AN ATTACK HAS ALREADY HAPPENED MEANS ALL THEY CAN DO IS TRY AND PREVENT FURTHER DAMAGE. THIS IS WHY PREVENTION IS SUCH A KEY ELEMENT IN IT SECURITY. MANAGING CYBER RISK HAS TO BE AN INTEGRAL PART OF ANY COMPANY'S RISK MANAGEMENT STRATEGY.[11]

Jens Krickhahn, Practice Leader Cyber & Fidelity, at AGCS Financial Lines Central & Eastern Europe

What businesses should be doing to prevent attacks

There are several preventative measures that are recommended to implement as part of a solid IT security strategy:

In-house protection and policies

Implementing simple preventative procedures against cyber-incidents should form the core of your strategy. For example, the renewed use of malicious emails in a wide range of cyber-attacks is worrying, but installing up-to-date firewall technology can protect against a lot of these types of external threat.

These emails also rely on deceiving victims rather than exposing technical vulnerabilities. Which means that educating staff about identifying emails of a potentially harmful nature – and not clicking on attachments, following links, or disclosing information – is easy enough to do and can be quickly implemented.

Similarly, maintaining strict policies of website and device use while connected to the company network can help safeguard against some disruptive attacks.

Partnering with the right provider for long-term protection

Cyber-crime is becoming increasingly sophisticated and changes in type and intensity all the time. It is no longer simply an external threat, as attacks on your data can now happen from within your network. So, while installing standard network protection and educating staff about easily preventable issues is essential, it should only form the basis – not the entirety – of your IT security strategy.

Partnering with an external IT security provider is often the only way to ensure long-term protection against both external and internal threats. Having a dedicated team assess your business needs and practices, and tailor a security solution just for you, can provide peace of mind – especially for those small to mid-sized businesses without an internal IT team of their own.

Any partner you hire needs to be a Certified Cyber Security Professional (CISSP), with the proper accreditation to demonstrate their expertise. You should also look out for a team with the capacity to offer you a range of digital security options to ensure every risk is countered.

A lot of businesses remain blasé about IT security. But with potentially devastating cyber-attacks on the rise, and the penalties for breaching the new data privacy laws about to become heavier, it could only take one event to cause irreversible damage to your business. Which is why it's essential to prevent attacks ahead of time, as there might be no cure strong enough to save you afterwards.

[11] Allianz Risk Barometer: Top Business Risks 2017, p10.

Seriun

Seriun provides support to local and large organisations, Betfred, O2 & others. We invest in leading systems to deliver exceptional services to thousands of working people.

Our IT security expertise ensures we can offer our customers everything from next-generation firewalls and the latest updated anti-virus software, to self-healing Virtual Private Networks, content filtering and mobile device management. Protecting your business around the clock in a more dangerous digital world.