GLOBAL BANKING & Finance review®
Global Insights & Analysis of the Financial & Business Markets

Why you don't need to break the bank to achieve good security?

By **Andy Miles,** CEO at**ThinkMarble**

With a seemingly endless succession of major breaches making the headlines and increased regulatory demands from the newly enforceable GDPR, cyber security has swiftly become one of the leading priorities for most organisations. Leading analyst house Gartner has predicted that worldwide spending on security will increase by eight percent this year, to reach a global value of £71.71bn by the end of 2018.

Few organisations feel the pressure of investing in security more keenly than those in the financial services sector.

Financial information is one of the most widely sought-after datasets among criminals, with the financial industry used to adhering to strict regulations long before the GPDR came into being. Consequently, the financial sector has the second highest investment in security in the UK.

With seemingly large budgets to play with, there is a trend for most of the investment in cyber security to be drawn towards whatever the newest and shiniest technology solution on the market happens to be. There are some extremely impressive solutions on the market and incredible developments being made in fields such as artificial intelligence, which appear to offer a nirvana like state of security at the push of a button. But throwing money at it isn't going to solve the problem. In fact, it is a serious mistake to think of security as a purely technology-based issue that can be solved simply by investing in more technology.

https://www.globalbankingandfinance.com/why-you-dont-need-to-break-the-bank-to-achieve-good-security/

Instead,a strong security stance requires the trinity of People, Process and Technology (PPT) to work effectively and efficiently together. A security vulnerability can appear in any element of the business and a holistic approach that covers all employees and operations is vital for a good defensive strategy.

People

 Andy Miles

When you hear the word ‘vulnerability’, the natural assumption is that of a software or hardware vulnerability, a glitch in the system that is negatively impacting the performance of the affected solution. But what if it is the people within the organisation that are, in fact, increasing the risk to the business?The human element of an organisation is often seen as the weakest link by cyber criminals, and many attack tactics have been developed specifically to take advantage of employees. Phishing emails in particular have become the de facto delivery tool for most attacks, with 91 percent of successful breaches beginning with a spear phishing email, according to research from multiple sources.

A good email security awareness and training solution can help to address this threat, but it’s also imperative that employees are made aware of the risks and are trained to spot signs of phishing and other social engineering techniques aiming to deceive them. Simulating a phishing attack against your workforce can be a good way of raising awareness, and all staff should be trained in the right processes if they suspect an attack.

Aside from training around specific threats, firms should seek to foster a cyber security culture in the workplace, with individuals taking their responsibility to reduce threats seriously. This approach starts from the top, and business owners should take responsibility and dedicate at least an hour every month to cyber security. Whether this is

getting in some reading or attending a seminar, it is important for decision makers to understand the latest threats and developments and be seen to be leading by example.

Process

Alongside the awareness and engagement of the workforce, the organisation also needs to ensure it has the right processes in place to ensure its security is robust. This is particularly important for financial organisations where activity is centred around large sums of money and sensitive personal and financial data. Any activity involving at-risk data or transactions should be governed by strict processes to minimise the risk of an attacker exploiting the system through social engineering or malware. Ideally, organisations should be conducting a 360° review on a weekly basis not only to identify key data and Intellectual Property (IP), but also the procedures and practices associated with keeping this information secure.

For example, implementing two-factor authentication (2FA) for processes such as authorising high-level payments or sharing sensitive data. 2FA uses a separate communication channel, such as a mobile number or even biometrics, to verify user identity, making it much more difficult for an imposter to trick their way into acquiring data or payments.

As well as the day-to-day working practices of employees, implementing good processes around key, and somewhat basic, IT functions like patching and updating software will also go a long way in preventing attacks. The majority of malware utilises old exploits that have been patched by software vendors, so ensuring systems are up-to-date will help mitigate this risk.

Ideally, an organisation should be constantly updating its systems, and should consider automating this process to reduce the manual, time intensive nature of this activity. At a minimum, all organisations, not just financial institutions, should be keeping up with the monthly 'Patch Tuesday' release from Microsoft, which delivers the latest essential patches.

Technology

Finally, people and processes must of course be coupled with good technology. Companies should at the very least be equipped with solutions to facilitate threat detection and vulnerability scanning and should be performing regular penetration tests on their systems.

The technology aspect goes beyond simply which solutions to purchase however, and security should be ingrained in every investment the company makes at a design level. For example, if the company is considering taking on a new cloud platform, security should be the priority. Factors such as the provider's security policies, data storage location and use of 2FA need to be considered on equal measure with the service's functionality.

With a security strategy that centres on PPT, financial organisations can minimise the risks to the funds and data they hold without investing ever-increasing amounts to chase the latest solution to hit the market.

https://www.globalbankingandfinance.com/why-you-dont-need-to-break-the-bank-to-achieve-good-security/