Welcome to the first IPBS newsletter of 2018. Whilst global optimism seems to be on the rise, there are still many bumps in the road ahead. Our newsletter looks at the key issues of Cyber Security and GDPR, along with details of a new cyber partner for IPBS. We also discuss how you can close the digital readiness gap in your business and our country spotlight looks at British Virgin Islands.

If you have any comments or feedback on the issues raised in this newsletter then please email me at bruce@ipbs.com and you will receive a personal reply.

Regards

Bruce Raine

Bruce Raine
CEO and Founder, International Private Banking Systems

Staying Ahead of Cyber Risk

Every day there seems to be another story of large and small companies that have been affected by a cyber security breach. It is likely the real scale of breaches happening today is far larger than the reports suggest. After all many companies will freely admit that they have been affected? With GDPR and other legislation making it mandatory to disclose data breaches for example, we are likely to see and be personally affected by more examples.

How can companies stay safe and protect their business? The starting point has to be with employees and technology solutions.

Employees need to be made aware of the risks they face when using social media, many hacks use very sophisticated profiling techniques on information that is publicly available via social media sites. This risk awareness should take place as part of a wider cyber security training program so all employees from the most junior to the most senior all have the same commitment to safeguarding data and following good security protocols around passwords and data management.

Then there is the role of technology solutions. There are a wide range of solutions and what is right for one organisation may not be suitable for another. However, all organisations should be looking to use some of the following as standard:

- Encryption is a must have for secure communications and for protecting sensitive data. This could be details of your customer records, or payment files that are created ready for transmission to a bank payment network such as SWIFT.

- Multi factor authentication is a significant step up from controlling system access via user name and logins. Compromised user credentials are a major risk to organisations but this can be minimised by using MFA. Typically this will involve something you know (a username), something you have (a smartphone) and something you are sent (a time based security token). This combination of factors ensures that only correctly verified users are granted access.
- Adopt the most stringent patching routine possible. Many hacks exploit vulnerabilities in systems or software that already have a patch or fix available. If you can keep your browser, antivirus, firewall and enterprise software up to date, you close off many of the opportunities open to hackers.

A good first step for organisations looking to strengthen their cyber security defences should be to carry out a risk assessment. If you don't have the skills to complete this, there are plenty of third party organisations that can help.

With the cost of recruiting and retaining specialist cyber security skills in-house continuing to rise, it may be worth exploring Security-as-a-Service. This is a form of always on always, up to date technology that protects your business using the latest cloud technology. This may offer the best of both worlds - enhanced security and protection at a more affordable price point.

IPBS can help advise you on all aspects of cyber security and protection. Please get in touch if you would like to know more.

Partner News: Sequrest and Cyber Security

We are hearing more and more from customers that are concerned about cyber security. That is why we have continued to look for partners that can add value to the IPBS system and we are pleased to announce that we are now partnering with Sequrest to enhance cyber security for private banks and wealth managers

Sequrest provides an end to end cyber security framework for our customer base of private banks, wealth managers and trusts etc. The agreement covers the Caribbean region and other offshore markets that IPBS already serves.

Sequrest offers a range of cyber security solutions including the latest facial recognition and biometric technology, encrypted communications and cyber intelligence. As a product and technology agnostic service provider, Sequrest is able to offer the optimum cyber security solution taking into account each institution's specific challenges. Bespoke advisory protection is then available on an on-going basis according to the organisational requirements and risk profile.

Given the nature of sensitive data that private banks and wealth managers have access to, it is imperative that institutions invest in providing robust cyber security defences. The number of threats is growing on a daily basis and this issue should be at the top of every C- level executive's agenda. There is already evidence of a cyber security skills shortage in the industry which will ultimately hinder an institution's ability to defend itself against external threats.

By partnering with a specialist in cyber security, IPBS can help organisations to focus on their core business secure in the knowledge that their infrastructure is protected to the highest standards.

Many small and medium sized institutions lack the capability or know how to mount an effective defence against an increasingly sophisticated threat. However, efficient and cost effective cyber security solutions exist that can keep an institution safe, prevent reputational damage and lower the risk of financial penalties. By working with Sequrest, you will benefit from a responsive service with direct access to cyber experts with many years of industry experience.

When Digital Transformation Becomes Transformation

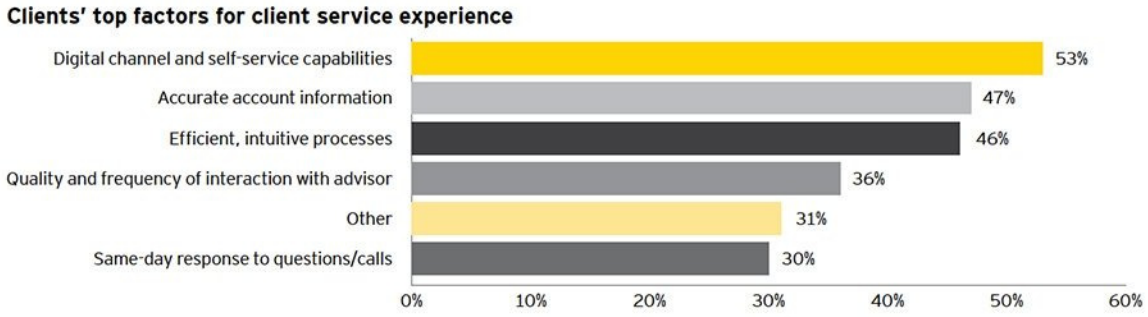
You may have seen our article by Sean Raine, VP at IPBS on how to deal with change in the wealth management industry.

In an industry where there is a continual downwards pressure on fees and asset flows, the impact of shifting demographics and technology expectations are driving a step change in the user experience demanded by customers. Wealth managers need to respond accordingly by reshaping products and services and investing in transformational technologies.

One of the biggest changes in our industry is that the so called millennial generation are increasingly turning to digital channels to perform their bank activities and shunning traditional branch based or call centre banking.

Two worrying facts for wealth managers; the consumer's smartphone will become the main banking channel and third party financial aggregators have the potential to know more about your customer's financial position than any human advisor.

Against this backdrop of seismic changes some wealth managers have had their head in the sand. A 2016 PWC survey indicated that only a quarter of wealth managers offer digital channels beyond email capabilities. Another survey this time from Ernst and Young showed that digital channels and self service capabilities were the top rated factor for client service experience (see diagram below).



(Source: Ernst & Young - Global Wealth Management Survey 2016 – The experience factor)

It is clear that firms that do not respond to change simply won't survive in the medium to long term. Why? Research shows that 85% of High Net Worth Individuals (HNWI) use 3 or more digital services in their day to day lives. More than two thirds of HNWI use online or mobile banking and more than 40% use online channels to review portfolio or investment markets. These people want and demand that same consumer experience they get from Amazon, Uber and Apple in other areas of their lives, and banking is no different.

Digital readiness gap

The upshot of this digital readiness gap is that the sector is vulnerable to a digital disruptor, one that uses innovation to address current HNWI needs in a convenient and user friendly manner, including the use of robo advisers to efficiently service customers and deliver what they want, how they want it and when they want it.

If any of the above sounds familiar then it is time to take action now.

Digital has become a key accelerator for evolution and institutions must redouble their efforts to build a future ready digital infrastructure that provides a unified customer experience. Digital should not be feared. It has the power to enable you to deliver existing and new services in a way that is efficient and cost effective.

But how can slow moving and risk-averse wealth managers make the necessary changes if they lack the digital skills required? One option is to look at strategically partnering with a FinTech innovator/disruptor. They will bring the speed of development and access to new capabilities the market is looking for.

According to Mckinsey, "digital has the potential to generate significant cost reductions through robotics and automation, change business models with digitally assisted advice, and drive disproportionate market-share gains through digital acquisition and servicing of clients."

It is likely that the institutions that benefit most will be those that embrace the opportunity to close the digital readiness gap. Of those institutions that are already digitally enabled, they need to continue to build on these offerings. These institutions will be in a position to better compete in the market by combining the best of technology and human service and are likely to remain relevant if not thrive in the future.

You can read the full version of this article which first appeared on Bobsguide here

---

GDPR: Sorting the Facts From the Fiction

The General Data Protection Regulation (GDPR) comes into force on 25 May 2018. However, there is growing misinformation emerging around the regulation in the Caribbean and we risk losing sight of what this new law is about. Polly Pickering, Managing Director of IPBS partner eShore explodes the top three myths.

Myth #1: 'We're a Caribbean based company so the GDPR doesn't apply to us'
Even if Caribbean-based companies have no physical presence in the EU, they can still be subject to GDPR if they process an EU resident or visitor's personal data in connection with goods or services offered to those individuals. Given the cross-border nature of offshore financial services and legal organisations with offices overseas, including in the EU, personal data will likely be subject to GDPR.

Myth #2: 'My data is stored in the cloud so it's not our responsibility to remain GDPR compliant'
Controllers and processors of data share responsibility for meeting GDPR. Businesses utilising personal data for business purposes cannot pass the duties to their cloud or security provider that are processing or storing personal data on their behalf – the data controller is still responsible for compliance.

Myth #3: 'Our personal data is in the database so we are not subject to GDPR'
GDPR applies to all data, meaning all collected data connected or associated with a person in the EU will be considered under GDPR protection based on the person's name, ID number, or physiological, genetic, or other factors.

Conclusion
You need good data processes when onboarding client information with a clear policy over security, access controls, retention, labelling and incorporating additional eDiscovery controls. This will make the responsibility of data management less problematic.

GDPR fines for non-compliance can be substantial and this should be addressed in the boardroom for both emergency budget consideration and also brand impact and marketing/public relations risks.

Fines will be 'effective, proportionate and dissuasive' so contingent on the violation level the penalties from 2% up to 4% of the total worldwide annual turnover of a company will be imposed. This speaks volumes in respect to 'impact' to a company's bottom-line.
GDPR is a cross departmental concern at every business level and not just an IT only issue. It has the potential to affect every component of most businesses. Disregarding or miscalculating the importance of the regulation or pending deadlines could be disastrous.

Reviewing the lengthy GDPR articles means appraising what information rights relate to your company but a review should also consider liability and duty. One responsibility tied in is consideration of announcements of IT attacks and data breaches. How, who and when you have to notify the regulator, clients and manage the breach should be again part of a good Business Continuity Plan (BCP). Above all, ensure a proactive policy and training is present in the company's overall philosophy.

Please get in touch with eShore for any queries related to GDPR and compliance +1 (345) 946 3673 or info@eshoreltd.com.

