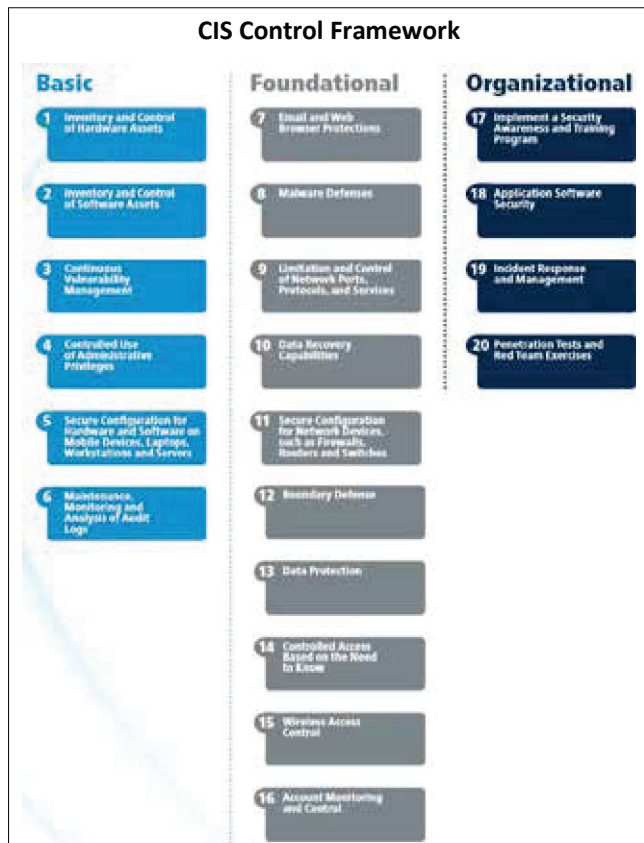


IT and cyber security – Why IT matters and what should you expect of your software suppliers?

By Andy Nightingale, Managing Director, from Worksmart Limited

In the April edition of T-CNews, I wrote about the regulatory and economic changes that were affecting the financial services industry and the subtle, but important, impact this was having for software suppliers to the sector. In summary, I argued that financial services firms were now expecting their software suppliers to really understand these changes and respond by offering pragmatic and high quality, market proven software solutions.

Building on that article, in this edition of T-CNews I want to stay on the subject of the changing expectations of financial services firms but this time, focus on the key area of IT and cyber security and what that means for both financial services firms and their software suppliers.



“It was so simple then...”

Ten years ago, the norm was for software suppliers to offer just that, i.e. regulatory software that, once configured, could be installed on customer sites and, barring any upgrades, left to run. Change began with some software suppliers offering additional services, typically ‘downstream’ implementation training or ‘upstream’ regulatory consultancy. However this seldom, if ever, included hosting as an offer. There were several reasons for this such as data centres being in the early stages of development, however by far the biggest reason was corporate IT policy. For corporate IT, data

security was everything and trusting software suppliers, even the most trusted suppliers, with their data was deemed too big a risk.

Slowly however, things changed.

First came the rising cost of IT infrastructure and as these costs increased, alternatives were developed, e.g. offshore corporate data centres. Although offshore data centres brought their own challenges, they served to begin unfreezing the mindset of corporate IT. This was further helped by global software suppliers, e.g. SAP, having the confidence to offer hosted or SaaS solutions. The final factor which changed the mindset of corporate IT from dismissing hosted and SaaS solutions to positively favouring them was the growing cost of data security and the rise in the incidence and complexity of cyber threats. Although other factors no doubt played their part, e.g. new regulation such as GDPR and the rising expectations of the regulator, these factors were arguably the key drivers towards favouring the outsourcing of regulatory software.

As this mindset changed towards positively favouring outsourcing the hosting of regulatory software, so came a significant change in financial services firms’ expectations of their software suppliers. First came a deepening of the relationship as buying an ongoing service was very different to the previous simple, ‘purchase and install’ relationship. Secondly, corporate IT expected their software suppliers to mirror or exceed their own high standards of security and service availability as well as maintaining alignment with the latest IT industry standards.

For software suppliers, this was a ‘game changer’.

For Worksmart, this has meant a single hosted offering for a major high bank in 2008 developing into a mature hosting offer that complements our traditional on-premise offer for all our products and, for our new SM&CR product Accord, a true SaaS offering. But what was the journey that has taken us to this point?

“It’s very different now...”

Corporate IT now expects software vendors to meet a minimum set of standards. But what are these standards? There is a number of bodies, national and international, providing frameworks for IT and cyber security and guidance on how to implement these frameworks. The most well-known ones are; BSI (British Standards Institute), ISO (International Organisation for Standardisation) and CIS (Centre for Internet Security). The emphasis may differ, but all these frameworks provide guidance across a range of areas to help companies, i.e. financial services firms and software providers alike, to develop the required standards.

For Worksmart to ensure our software, particularly our hosted and SaaS propositions, remain credible to our customers, has meant a sustained focus on every part

of our business, i.e. from the physical security of our data centres, to malware software and even HR policies. Adopting the Framework from the CIS in 2016 gave Worksmart the structure and standards to work towards and, importantly, to audit progress against.

Doing so has not been easy. It has required a significant effort supported by sustained investment and, equally important, management focus over the last three years to make happen. However, it must be done.

The evidence is clear that every business is at risk of a cyber-attack. The latest government statistics show over four in ten (43%) of all businesses and charities experiences a cyber breach or attack in the past year. IT and cyber security threats are continuously evolving, it's important for businesses to safeguard themselves by following global standards and recognised best practice for securing IT systems and data against attacks.

Alongside our investment in our software products themselves, our investment in our IT and cyber security and defences has enabled us to win and retain over 50 customers. It wouldn't be an understatement to say that implementing these controls has transformed Worksmart into being trusted partner to some of the UK's largest financial services brands.

What Does This All Mean?


Having software providers that offer a hosted or SaaS solution is attractive for financial services firms. It saves cost and passes responsibility for ensuring compliance with legal, e.g. GDPR, and security standards to their software providers. Conversely, for software providers, offering these services increases sales revenues and offers greater potential for building customer trust and retention.

Additionally, the regulator is now making it clear that regulated firms have a clear responsibility to conduct rigorous due diligence on potential software suppliers and maintain this oversight throughout the life of their relationship.

However, this opportunity comes with the significant responsibility of not only providing regulatory software that enables our customers to both comply and gain business advantage when doing so. It also means 'going the extra mile' to ensure our customers software and the data held in that software is safe.

It is now common practice for firms when buying software to investigate its features, underlying architecture and product roadmap. Indeed, many firms now require technical questionnaires to be completed as part of the procurement process. These questionnaires touch on the software supplier's capability to protect the software and data held in that software. In our experience however, the degree of investigation into data and cyber security varies wildly between financial services firms. Moving forward, thorough investigation into data and cyber security should, and will likely, be as commonplace and thorough as investigating software functionality and roadmap.

Therefore, the key question for prospective software suppliers alongside functionality and roadmap should be; 'if we buy your software, how do you intend to protect it and our data held in it?' The clarity and thoroughness of the response will tell you everything you need to know about your prospective software partner.




"Worksmart has been key to ensuring that we have met the requirements of the rules"


Lisa Nowell, Chief Risk Officer, Masthaven Bank

Contact our experienced SM&CR implementation team via email at; info@worksmart.co.uk or call us on; **01908 613613**

Visit; www.worksmart.co.uk for more information



brought to you by Worksmart, the UK's leading, award winning, supplier of SM&CR software



assign
model
manage
report

"The basic principle of the Senior Managers Regime is that of responsibility and accountability. A senior manager has to take responsibility for the activities under their control. Likewise, they should be accountable for that responsibility"

Andrew Bailey, CEO - FCA, 2018