The IT Security Risk Assessment: The Elephant in the Boardroom

White Paper

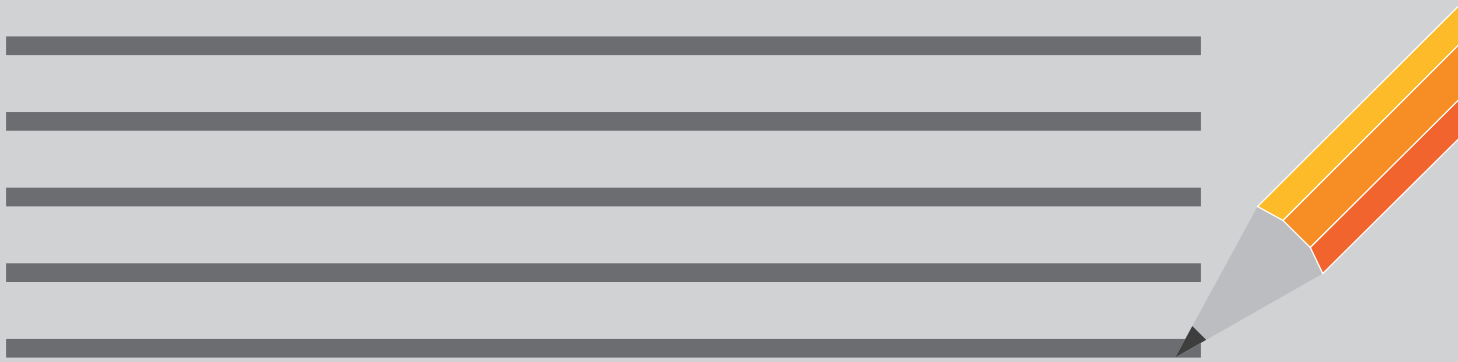
Abstract

Why every business should make adaptive IT risk assessments an essential part of their digital transformation strategy

SWIVEL

Contents

1. Executive Summary



As transformative technologies like the cloud, mobile and the Internet of Things (IoT) gradually become woven into the fabric of everyday business life, the pressure on corporate Information Security (IS) departments to maintain bulletproof data security is rising.

This paper makes the case for CEOs to release funding to prioritise the implementation of IT security risk assessments. It asserts that without assessing the risks associated with this profound technological change, corporate IT teams will lack the insights they need to defend their sensitive corporate data as they embrace their organisation's digital transformation.

It also explores the security challenges facing IT and IS departments as they seek to integrate the new with the old, without impacting the end-user experience or the performance of their systems. It outlines how security risk assessments can provide a bridge between IT, IS and other departments, enabling them to strike an effective balance – or 'identify appropriate levels of friction' – between the adoption of protectionist and, in some cases, interventionist information security policies, and the promotion of new enabling technologies capable of fostering innovation and improving business performance.

2. IT departments are losing control (and so is Information Security)

Most security industry analysts, trade media and other industry commentators agree: the IT department is losing control over its IT.

In many cases, the biggest challenge is coming from within. Gartner[1] recently stated that 38% of all spending on IT is done from outside of the IT department, with a disproportionate amount going toward digital tools. The analyst house also claimed that by 2017, that figure will have risen to over 50%, as marketing, finance, HR and sales departments buy-in digital products and services they believe will deliver a competitive edge.

Gartner also suggests that this buying behaviour is reaching a tipping point, beyond which the IT department will struggle to regain the control they have lost, as vendors, VARs and integrators 'go where the money is' and focus on nurturing revenue streams from non-IT buyers.

This shift has been driven in part by disenchanted employees who have learned that they can be more productive when they use their own devices. A recent piece of research from Ovum[2] found that 60% of information workers would prefer to choose the smartphone or tablet they use for work and 47% would prefer to use a single smartphone to manage both their work and personal lives.

These circumstances don't just sideline the IT department, however, they also present a clear problem for IS. And that problem is set to get worse unless action is taken.

2.1 Bring Your Own (security) Deficit?

In recent years, this change in employee attitudes and behaviours has given birth to the bring-your-own-device (BYOD) phenomenon, adding yet further to the host of network security issues that arise from deperimeterisation. The danger of unsecured data in the enterprise was highlighted in October 2014 when a survey from Kroll Ontrack[3] suggested that 4.6 million employees had lost work-related data in the last 12 months due to corrupted and malfunctioning personal devices or cloud services.

> *"In October 2014 a survey from Kroll Ontrack suggested that 4.6 million employees had lost work-related data in the last 12 months due to corrupted and malfunctioning personal devices or cloud services."*

[1] http://www.forbes.com/sites/gilpress/2014/10/09/gartner-predicts-top-trends-for-technology-it-organizations-and-consumers-for-2015-and-beyond/

[2] Enterprise Mobility: The Impact of Changing Employee Behaviour, Richard Absalom, Principal Analyst, Ovum

[3] http://www.krollontrack.co.uk/company/press-room/press-releases/employees-lose-employer-data-due-to-malfunctioning-personal-devices/

Cloud applications like Dropbox and Google Drive, which operate in both the mobile and desktop environments, allow users to remotely access and transfer data between personal and company devices. Since these applications were designed for consumer use, most have inadequate security for the enterprise environment. Their adoption, therefore, leaves the gateways open to highly-confidential, business critical data stored in countless clouds guarded only by a simple username and password (UNP) system. With a staggering 73% of US full time workers re-using the same batch of passwords online, nearly three-quarters (74.2%) of business owners admitting to keeping a written log or another offline system for recording their passwords and with attacks involving keyloggers becoming more prevalent too, the odds of a data breach caused by a stray UNP falling into the wrong hands are significant.

Once on the corporate network, these cloud applications create new system vulnerabilities that invite data breaches and cyber-attacks. In some cases the IT and IS departments are unaware of the risks being taken by users of these systems. In others, they are simply powerless to prevent them, having been presented with BYOD and cloud applications as a fait accompli by the board, other departmental heads and the rest of the workforce.

If and when the IS department is made aware of potential network vulnerabilities, controlling them is far from straightforward, as HR initiatives continually muddy the waters. A key driver of BYOD and cloud application adoption has been a move to adopt flexible and remote working. The mobile working trend has been made possible by recent government legislation which gives employees the right to work remotely or from home. In many cases, this leaves the employer with very little control over the employee's choice of device or internet provider. In addition, for the IS team to address this area they must first create BYOD policies and have the power and resources to enforce them.

In an attempt to address these issues, IS teams must work closer with HR departments to create policies to educate and control flexible working practices. This will not be an easy fix, however, as HR teams are under pressure to attract and retain the best people, many of whom are Millennials, a group that expects BYOD to be readily available. A recent survey from Tarckvia[4] found that 69% of Millennials say they never work in conjunction with the IT department when selecting new business apps. If this insight is anywhere near reflective of the wider marketplace then device and application usage policies and associated risk ratings need to be urgently re-assessed.

2.2 **Outsourced and out of mind**

For IS departments already struggling with securing not just the enterprise but also third party suppliers in order to avoid events like the 2013 Target breach, these issues were bad enough. But there was a new cloud on the horizon - the next big threat to the IS team's control came from cloud-based managed services.

[4] http://www.wired.com/2014/09/millennials-mobile-security/

The advent of cloud computing, together with the practice of outsourcing operational control to a remote third party, coincided neatly with the global economic downturn, giving many CFOs and FDs the opportunity to axe their budgets by turning CAPEX into outsourced OPEX.

While this model successfully served the needs of the FD and also offloaded many of the internal IT issues around BYOD to a third party, the move to the cloud presented the in-house IT and IS departments with yet another set of challenges.

2.3 **Cloud concerns**

> *An IDG Cloud Computing survey[5] in 2014 found that 56% of CIOs were uncertain about their ability to enforce their security policies on a provider's site, while 45% were concerned about unauthorised access on what they deemed to be 'untrusted' networks.*"

Having relinquished control, it became apparent to some enterprises that the threats to their corporate data hadn't gone away, and yet more had emerged as a result of the new model. Issues relating to the ownership and sharing of cloud platform usage data emerged. In fact, an IDG Cloud Computing survey[5] in 2014 found that 56% of CIOs were uncertain about their ability to enforce their security policies on a provider's site, while 45% were concerned about unauthorised access on what they deemed to be 'untrusted' networks.

The net result? The time and resources that should be released by the remote managed services model are instead being ploughed back into working with the vendor to ensure their security practices align, especially as their businesses change over time. What's more, they also have to ensure that the physical, administrative access to the data centre is robust and has the latest malware protections in place, and that the service provider is monitoring effectively for new threats. The same 2014 IDG study highlighted that 44% of CIOs were unsure as to whether they could effectively audit their provider, while 42% worried about questionable privileged access control at the provider's site.

In all, it's clear that the IT and IS departments have come under incredible pressure in recent years, both internally and externally. If CEOs want to implement digital transformation strategies, or innovate with new concepts and models, they need to ensure that both IT and IS are in a position to help them achieve their strategic goals. This means arming them with the right powers to protect the areas of the business that are crucial to future prosperity.

The first step on this road is to ensure appropriate risk assessments are performed prior to the approval of new initiatives. With the promise of a network revolution on the horizon, thanks to the advent of the Internet of Things (IoT), taking this step now should be viewed as critical to the future of both IT and IS.

[5] http://www.idgenterprise.com/report/idg-enterprise-cloud-computing-study-2014

3. The Internet of Things (IoT); IT's friend or foe?

Many IS teams are already struggling to control threats to their IT network caused by early digital transformation initiatives like BYOD and the cloud. But, such problems haven't altered the focus of CEOs who (probably correctly) believe that digital transformation strategies continue to be essential to remain competitive and achieve growth in technology areas such as multichannel, e-commerce and m-commerce.

Indeed, Gartner's recent survey of CEOs[6] and senior business executives found that growth remains a top priority and technology-related change is viewed as the primary tool to achieve that growth in 2015 and 2016.

In particular, the CEOs surveyed felt digital transformation will be driven by mobile technologies for customer engagement (81%), data mining and analysis (80%), cyber security (78%), the Internet of Things (65%) and cloud computing (60%).

The standout finding from this survey was the meteoric rise of IoT. While the IoT phenomenon may be the next big thing in the eyes of the board, however, it threatens to be the next big headache for IS teams.

Pressure from the board forced through BYOD and cloud before it was fully secure. Excited by the prospect of IoT, the board now runs the risk of repeating this mistake, without fully appreciating how much higher the stakes are this time around.

Gartner[7] claims that few organisations have established a clear strategy to take advantage of a connected devices boom, indicating that the IT and IS departments will be left facing similar pressures to those faced when deploying BYOD projects. This will leave them with little or no control over the increasing threats to network security.

3.1 Will IoT be the straw that breaks the IS department's back?

Just as the cloud enabled the widespread implementation of BYOD projects to better link employees, it promises to be the driving force behind IoT, connecting vast amounts of data across our physical and virtual worlds. Once connected, billions of devices will then be able to exchange information and take autonomous actions based on continuous input, leaving IT departments facing a paradigm change that will potentially transform and revolutionise their role in the business. However, these transformations will pose unprecedented data privacy and security challenges to IT and IT security professionals, according to Forrester.[8] Now their areas of concern will range from customer facilities and homes,

[6] http://www.gartner.com/newsroom/id/3033618

[7] http://www.itproportal.com/2015/02/05/businesses-unprepared-iot-says-gartner/

[8] https://www.forrester.com/Brief+CIOs+Will+Architect+And+Operate+The+Internet+Of+Things/fulltext/-/E-RES116625#endnote10

through the Internet to the enterprise. Sensors and gateways outside the perimeter will be easy to access yet must remain tamper resistant and tamper evident, even though constantly connected. This challenge will leave IS teams with a stream of decisions about where and when to deploy additional identity, authentication, and encryption technologies without upsetting a whole new range of users.

However there are steps that IT and IS can take to re-assert their control.

4. Taking back control

This paper has highlighted how many CEOs are pinning their hopes for growth on digital transformation. However Forrester[9] claims that the road to success for many businesses will be far from straightforward. In fact, the analyst house feels that many boards are ignoring the complexity, or simply misunderstanding the level of cultural change needed to implement effective digital transformation programmes.

> *"Forrester claims that the road to success for many businesses will be far from straightforward. Many boards are ignoring the complexity, or simply misunderstanding the level of cultural change needed to implement effective digital transformation programmes."*

One key area that Forrester picks out is the outdated approach of many enterprises to large scale change management. In particular, the analyst house claims that organisations must learn to embrace iterative, customer-centric innovation to enhance both the customer and employee experience. It is crucial that IT and IS feed into this process.

In addition, claims Forrester, firms must learn to interact with their customers in a whole new way[10]. While the analyst house feels that winning, securing and managing loyalty will be easier with IoT initiatives, success will also rely on meeting and exceeding customers' expectations for data protection and privacy. These issues are an organisational challenge and not one that can be dealt with effectively if boards allow IoT projects to be commissioned without the IT team's involvement and IS's oversight.

Indeed if the board doesn't learn from the mistakes of BYOD and fails to give the IS department the necessary control over IoT deployments, the impact could inflict far more damage on corporate reputation than past BYOD related data breaches. In reality, because of the key role customer data will play in IoT-led growth strategies, if a data breach was to occur it would severely impact the trust of existing and new customers, and ultimately threaten to derail IoT-led growth strategies. However, because data is the lifeblood of all IoT initiatives, Forrester[11] believes this presents

[9] http://blogs.forrester.com/martin_gill/15-04-01-why_do_digital_business_transformations_fail

[10] https://www.forrester.com/CIOs+Drive+InternetOfThings+Strategies+Forward+With+Effective+Data+Protection+Practices/fulltext/-/E-res119904

[11] https://www.forrester.com/Brief+CIOs+Will+Architect+And+Operate+The+Internet+Of+Things/fulltext/-/E-RES116625

IT teams with the perfect opportunity to work alongside all key business units from the outset of each IoT project to ensure appropriate information safeguards are put in place. As a result, the IT department will now be working with the information security team, the app development team, the enterprise architects, and the product line-of-business teams to ensure that full visibility, security management and proper development practices remain central to the IoT effort.

Only when this co-operation is in place will it be possible to securely embed IoT into the digital transformation strategy, avoid past errors with BYOD and cloud and progress toward meeting the CEO's growth targets.

However, while this new level of integration will enable the IT and IS teams to showcase their skills and experience, they will also be constantly challenged by other departments and the board to provide evidence to support their IT security recommendations. This means they'll have to find a way of changing the attitudes of other departments towards data security, and especially risk assessments, if they are to prove their business case.

4.1 A fresh approach to the culture of risk

With that in mind, the role the IS and IT departments play will be crucial to the future success of the organisation. Any effective change in organisational culture must include a fundamental change in attitudes and behaviours towards data protection and privacy. The good news is that there are a growing number of Chief Digital Officer (CDO) or a Chief Privacy Officer[12] (CPO) roles being created, and many large companies have already separated out the IT and IS functions, providing the Chief Information Security Officer (CISO) with a direct reporting line to the board. Nonetheless, these moves alone won't be enough to establish a data model that meets all the needs and expectations of the business, employees and customers.

The main challenge facing any CISO or indeed CDO or CPO comes from many businesses having an ad-hoc security culture created on the fly. All too often, internal departments and senior executives are choosing to ignore security policies and the IT and IS teams are not empowered to enforce them.

To overcome this and for any digital transformation programme to be a success, the IT team, the CISO and the CDO/CPO must work together to define an accurate estimation of risk.

Only this will prevent the company's IT security resources from being used to protect the wrong things, resulting in valuable data being put at risk. Indeed this is already an integral part of IT governance frameworks such as COBIT and not something that businesses can afford to ignore any longer.

Any such risk assessment must take a holistic view of the entire business, including areas of digital transformation, to assess what is 'business-critical' and must then implement strict policies that must be adhered to at all levels.

It is true that the risk assessment has historically been a long-term strategic tool for many businesses. However once internal departments begin to run their own technology innovation projects without the involvement of IT and IS, the risk assessment may become redundant. In addition, the

[12] http://blogs.forrester.com/heidi_shey/15-05-01-do_you_have_an_effective_privacy_organization

speed of business transformation can leave monolithic risk assessment procedures lagging behind. In many cases this has caused IT and IS to either overspend or underspend on protecting business assets or put resources into protecting the wrongs things altogether[13] - yet another reason why experts claim that IT and IS departments have lost control of IT.

There is no 'one size fits all' solution to IT security and there is certainly no 'one risk assessment secures all' solution to recommend. But neither should IT security risk assessments be viewed as the enemy of digital transformation. In fact, new, adaptive authentication solutions now enable IT and IS to breathe new life into legacy risk assessment procedures and security policies.

Risk is a difficult area to discuss. On the one hand those driving initiatives forward need to understand the risks these initiatives bring to the business and take responsibility for their mitigation. Equally, however, IS departments also need to understand that, from a commercial perspective, some risks are worth taking. Just because these conversations are difficult does not mean they shouldn't take place.

> *"There is no 'one size fits all' solution to IT security and there is certainly no 'one risk assessment secures all' solution to recommend."*

4.2 How risk-based authentication can revive the risk assessment

> *"Adaptive risk-based authentication solutions are the catalyst to help all parties to agree on the right level of visible security appropriate to the access being requested."*

Adaptive risk-based authentication solutions are the catalyst to help all parties to agree on the right level of visible security appropriate to the access being requested. They require a collaborative inter-departmental approach and they serve to remind the user of the security risks associated with whatever it is they are doing.

The most powerful and protective step is to define policies based on each access request. In taking this approach, an appropriate level of 'friction' is integrated into the authentication process, ensuring that the user, even a BYOD user, is conscious that they are moving into a secure environment and must proceed in accordance with whatever enterprise security policies have been agreed for that environment.

This is particularly important for those involved operationally in IoT deployments, given the potential volume of sensitive data.

Unlike old fashioned risk assessment measures, this method creates the required flexibility to cater to any changes in business strategy, while introducing proportionate levels of security friction into the user experience, according to the gravity of the access request.

[13] http://www.computerweekly.com/feature/IT-security-risk-assessment-in-the-real-world

> *A director that accesses the server from a tablet while travelling poses a very different risk to when they are logging in from their secured laptop in head office."*

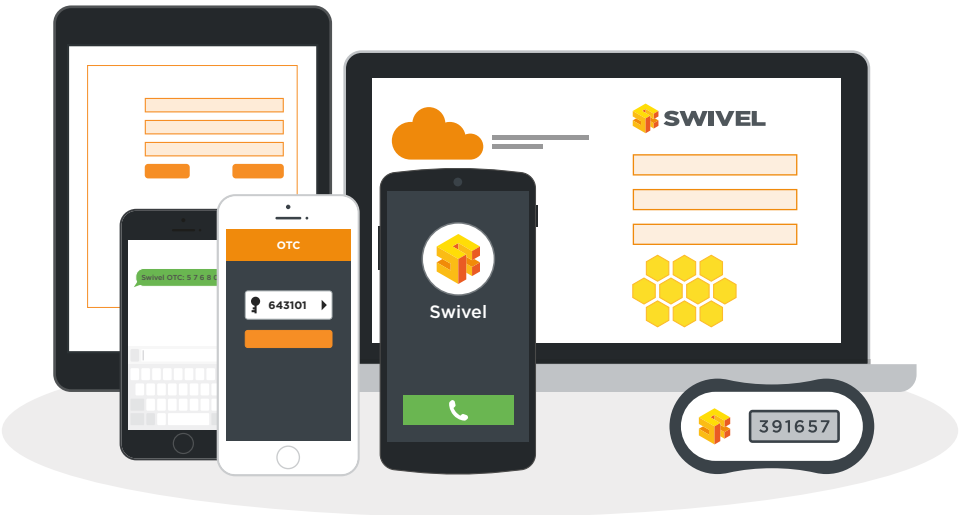
Going beyond 'per-service' and 'per-user' policies to create an additional layer of granularity means that friction can be reduced when it is appropriate to do so but also increased as dictated by increases in circumstantial risk produced by the demands of today's business environment. A director that accesses the server from a tablet while travelling poses a very different risk to when they are logging in from their secured laptop in head office.

A variety of factors should be taken into account here, with different rules being applied to different stores of data. Such factors include the sensitivity of customer and company data being protected, the firm's legal and compliance obligations as defined by the authorities in the company's host country, details of commercial agreements with partner organisations, responsibilities to shareholders or investors, together with any internal sensitivities associated with employee records, or financial forecasting.

But it is not just the behaviour of genuine users that should be considered, how a potential attacker is likely to behave is of equal importance. An access attempt from a country that an enterprise considers to be hostile, for example, can and should be treated with greater suspicion that other access attempts.

> *Only by conducting detailed, controlled, collaborative and ongoing risk assessments can an IS department create fluid, responsive security policies that support both a convenient user experience and provide adequate commercial protection."*

Only by conducting detailed, controlled, collaborative and ongoing risk assessments can an IS department create fluid, responsive security policies that support both a convenient user experience and provide adequate commercial protection. Most importantly this process is a vital part of the new way of team working between IT, IS and other departments.



5. Conclusion – how understanding the 'IT risk' is key to digital transformation success

As change in the digital world continues apace, there will be many barriers that threaten to impact the effectiveness of digital transformation projects. A lax and dated approach to security should not be one.

Indeed there is an urgent need to ensure the past failures associated with BYOD and the cloud don't continue. Given the scale of investment needed in both time and money for most organisations, and the evidence put forward in this paper, the first essential step towards digital transformation is to agree on the risk associated with each and every digital initiative. The next to is to ensure the involvement of IT and IS every stage of development. Finally, it is up to the IT and IS teams to work together to identify and implement security and authentication platforms capable of adapting to the unique requirements of their enterprise. Only then will they be able to guard the network's gateways in accordance with their new IS policies.

With all this in mind, the responsibility for success or failure cannot lie solely at the feet of IT. CEOs and boards must give their IT and IS teams the power to work with other key teams in the organisation to understand their needs, and then to collectively and collaboratively support the right 'risk' decisions which meet the short and long-term goals of the business both at the overall project and at individual transaction authentication levels.

6. About Swivel Secure

Established in 2000, Swivel is a pioneering global network security solutions provider. Its adaptive, multi-factor authentication platform, underpinned by PINsafe, the company's patented one-time-code extraction technology, is recognised as a leading standard in authentication technology. Swivel's range of risk based authentication tools helps enterprises manage the increasing data security risk posed by cloud services and bring your own device policies.

Swivel's established user base includes major blue chip companies as well as SME and public sector organisations. Customers vary from UK NHS Trusts to multi-national logistics organisations, educational institutions, high street retailers, financial institutions and one of the world's largest IT hardware components manufacturers.

Swivel is the only authentication technology accredited for Microsoft Office365 that offers primary support for a tokenless environment.

Swivel has an extensive worldwide network of channel partners supported by offices in the UK, US, Europe and Russia. It is a member of the Marr Group, a global investment business.

SWIVEL