advanced
People. Partnership. Solutions.

Reimagining your business means imagining the risk – and then mitigating it

Digital transformation, the process of disrupting the way you do business by harnessing the opportunities of digital technologies, is high on the media agenda.

Whether it's a profound disruption, or more of a phased approach to transformation that is required to support business innovation, what is clear is that reimagining your business will involve the need to drive change. This change may involve leveraging digital technologies to deliver a customer-centric approach, and unlocking the potential of staff to focus on the customer and enhance every single interaction. Or it may be about changing the role of IT so that leaders can stay ahead of the game, confident in the data insights they are getting from a connected digital business.

The good news is that reimagining your business is within easy reach for any organisation with effective planning. This white paper will cover how best to prepare for any risks that change may bring, what to consider and, reassuringly, provide insight and tips to work towards implementing best practices for success.

Mitigating risk around innovation

Every business has unique requirements and therefore has its own set of risks. When considering areas of innovation, the consequences of not getting it right can be far reaching, especially when considering how pervasive technology has become and how reliant most businesses are on technology. This can be as extensive as being unable to perform basic business operations; impacting upon customer services; and even the potential to damage a brand's reputation.

Assessment must be the first step in mitigating these risks. Leaders need to consider in detail the factors that may affect the business when embarking upon a process of reimagination, to ensure the right balance is struck between risk and function. For example, how reliant is your business on existing technology, from running all your systems through to delivering business-critical services?

In addition to the operational impact, it is also vital to ensure your business remains compliant with the rules and regulations that govern your industry, and the British industry as a whole. This is particularly important in the current climate, while the UK undergoes a period of transition during Brexit negotiations, alongside uncertainty around the impact of the forthcoming European Generation Data Protection Regulations (GDPR) due to come into force in May 2018.

The key advice here is to be prudent, invest time in thoroughly assessing the threats, then plan and prepare for those risks to ensure you are best placed to achieve success.

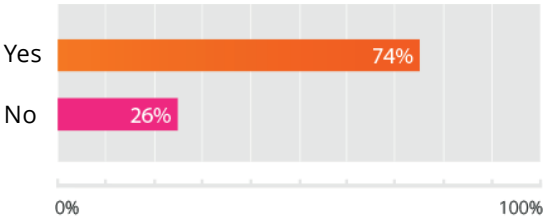
Another consideration is that, when reimagining your business, data privacy and cyber security

Reimagining your business

should be the driving force behind any transformational journey. Worryingly, there is an apparent reluctance of UK industry to accept the level of threats faced in today's digital world.

Our independent Trends Report revealed 26 per cent of British businesses admitted to having no protection against a cyber-attack. Couple that with the fact that a shocking 46 per cent of respondents claimed that data security is not a deciding factor in adopting digital technology, and the threat becomes much more real.

Is your organisation prepared for a cyber attack?



So what are the most significant security risks facing an organisation about to begin the process of reimagination? They fall into two main categories: external and internal threats, and both need to be considered a potential risk to businesses looking to thrive in a digital era.

The outsider threat

Online data security – the obvious but overlooked threat

Recent Government research into cyber security has found that two thirds of large businesses experienced a cyber breach or attack in the past year; TalkTalk, Camelot and Tesco are illustrations of this. It is no surprise then, that the Government has announced a £1.9 billion investment into online security. Some consider this to be a drop in the ocean towards what needs to be achieved in this area.

"We've seen a seismic shift in the security space in the past year; it feels like we're in the midst of a cold war arms race and every business and individual must now keep up with the significant problems arising from organised digital crime. The fact that the new National Cyber Security Strategy has almost doubled previous funding commitments, both reassures and reaffirms the significance of cyber security to every aspect of British life." - Private Sector Professional

Data privacy and protection – the threat of unclear data journeys

Every organisation is accountable for their customers' data. Each is responsible for knowing exactly where that data is headed in order to remain compliant and reduce potential security risks. This is especially important for those organisations which have several different systems or third parties handling their data.

For example, for the financial services and public sectors, it is critical to know the exact movement of Personally Identifiable Information (PII) so that, should a customer ask for their data to be removed, they are able to meet that request efficiently.

Critically, the requirements being introduced by the GDPR will demand that most organisations make significant enhancements to their privacy control environment, and rethink the way they collect, store, use and disclose personal information. Such complex changes will take time. With many businesses choosing to wait to see what impact Brexit will have on these new regulations, the risk here is that they will then find they have failed to allocate sufficient time to prepare should the regulations be fully enforced in the United Kingdom.

To identify any weaknesses in your data privacy provision, ask yourself:

- What data do you hold?
- Do you have permission to use this data?
- Are you able to track and audit your data processes?
- How do you collect, store and use this data? Is it secure?
- What compliance issues are there in your business/industry?
- Do third parties have access to your customers' data?
- If so, how secure is their infrastructure?
- Do they have permission to use this data?
- Can they track and audit their data processes?
- Are employees adhering to data privacy controls?

Reimagining your business

By answering these questions, organisations can quickly identify areas of weakness in the data journey, to ensure as part of their process of reimagination, they can put in place tools and processes to reduce the risks.

Although the risks associated with the data journey will vary between industries, there are some mainstay tips that should be considered when reimagining your business.

Top tips on data journey risk mitigation when reimagining your business:

> Implementing data encryption processes will ensure only the authorised recipient is able to access the data and, if it does fall into the wrong hands, it's integrity remains intact.

> Ensuring you understand implicitly where your data is traversing, for example, is it travelling within the public or private cloud?

> Deploying perimeter facing services and web services that can audit and track the usage of data. For instance, Security Event and Incident Management (SEIM) systems will identify and correlate when a breach happens and where the fault lies.

> Installing next generation Firewall – it's no longer as simple as protecting what is allowed into or out of your organisation, now, the focus is on learning what is normal and abnormal online behaviour in order to identify breaches at the earliest point.

The insider threat

Reimagining your workforce, or disengaging them?

While an engaged and productive workforce is a key component towards business success, reimagining how your workforce operates can be a detrimental risk factor, particularly when change is imminent. Culture is the foundation upon which every business is built, and changing this can pose a very real risk as employees deal with the knock-on effects. The scope of the transformation your business is engaged in will determine the level of risk associated with your people.

To identify whether your workforce is at risk of disengagement, think about:

> The potential impact of removing functionality from employees if you intend to invest in new, efficiency-driven technologies.

> How you intend to communicate these changes and maintain that dialogue.

> Whether you will consult with the workforce to garner support ahead of the changes

> How employees could be retrained or moved into positions that focus on offering more value and delivering greater business efficiencies.

Engaging and educating your workforce into the risks and opportunities any new technology or transformation may pose is key to gaining their support, unlocking their potential and maintaining their loyalty.

The data security attack from within

High profile external data breaches, such as those experienced by TalkTalk and Sony, are thankfully very unusual. Conversely, one of the biggest risks for many businesses, but one that is worryingly overlooked, is the insider data threat posed by the workforce.

Human error, such as leaving user names and passwords open, or leaving laptops and memory sticks on trains, can circumvent the most stringent security policies. While it would be almost impossible to completely remove an organisation's internal threats, it is possible to greatly minimise them and limit the potential damage they could cause.

As part of any business reimagination, considerations surrounding internal risk should be of significant importance; spending millions on transforming your business through technology could be wasted if the internal threat isn't minimised.

"Data sovereignty and security is no longer simply stopping people and threats getting in, it's more about stopping information getting out." - Private Sector Professional

Reimagining your business

Top tips: how best to be prepared to mitigate risk

1) Be clear on what you want to achieve from your reimagined business; knowing your objectives will allow you to identify the best route to take, and the associated risks.

2) Conduct a thorough risk assessment: ultimately, you need to be fully aware of the risks in order to mitigate them; then, coordinate a risk plan.

3) Ensure data security is top of your agenda: don't join the quarter of businesses who are not prepared for a cyber-attack.

4) Don't apply onerous processes with little to no value. For example, if something is freely and publicly available, then trying to protect and secure it will simply be wasted effort.

5) Don't look for the perfect solution, instead focus on finding the 'right' solution for your organisation, and strike a balance between risk and function.

"I don't believe cyber security is holding us back. Whenever we're looking at digital transformation, we always consider the security risks when evaluating availability and resilience of the system. We see this as a significant importance to maintaining the reputation of our organisation – if we get a breach, we lose trust – it's as simple as that." Mark Smith – Head of IT and Operational Systems at Monitor

Conclusion

Successfully reimagining your business can offer a multitude of advantages, from enhancements to the service you offer customers to the way you interact with them. However, keep in mind that the negative impact of getting it wrong can pose a significant threat to your business-critical activities.

The risks outlined in this white paper are real, and represent the organisational landscape today, as we increasingly rely on digital processes.

Risk planning and mitigation has never been more important, or complex. Businesses are having to adapt to a continuous raft of change: evolving consumer behaviours, data protection, cyber security, mobile and remote workforces; the list of considerations seems endless and, when combined with the prospect of reimagining your business, can feel overwhelming.

But it needn't be. Key to successfully reimagining your organisation is effective planning and risk mitigation; in short, plan for risk, reduce the risk.

More information

w oneadvanced.com
t +44(0) 8451 605 555
e hello@oneadvanced.com

Ditton Park, Riding Court Road, Datchet, SL3 9LL