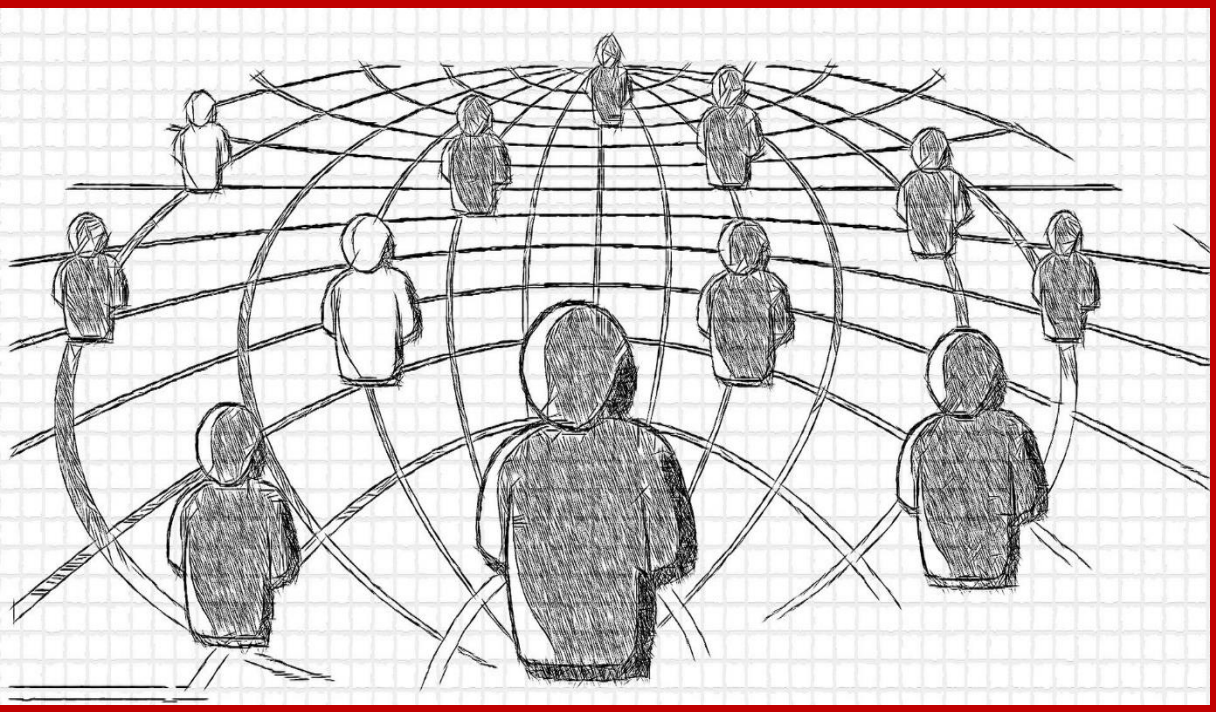
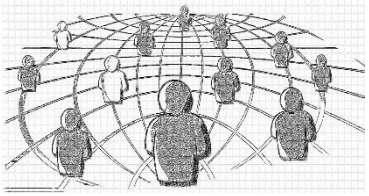
Securing Digital Transformation

The benefits it offers and guidance for a successful implementation



Craig Moan, Advent IM Senior Security Consultant

ADVENT IM



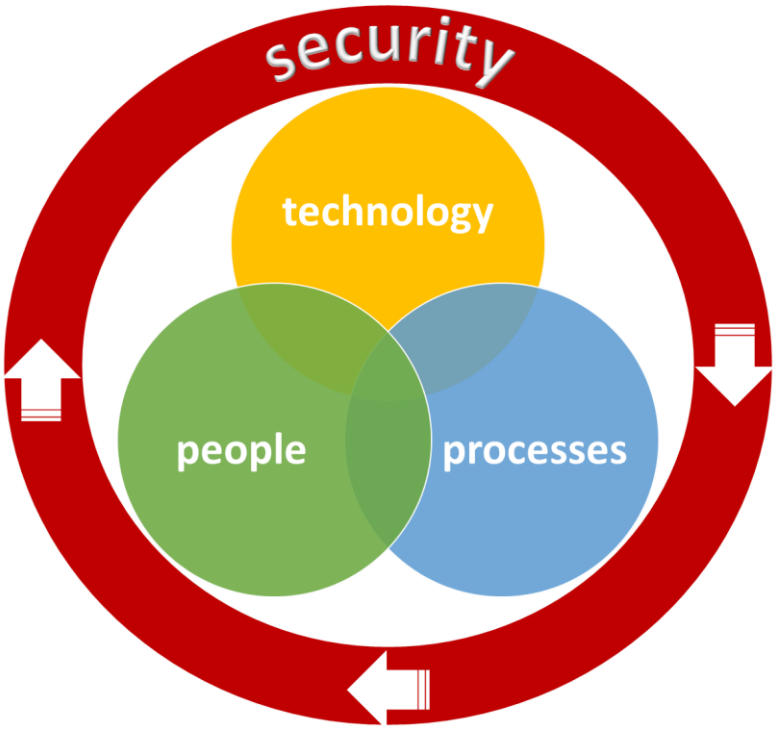
Introduction

This white paper aims to provide a brief overview of digital transformation, the benefits it can offer, and some guidance on how to secure your transformation programme to enable a successful outcome.

Background

Digital transformation is the term given to the strategic changes made by an organisation to fundamentally change the way technology, people and processes are used to improve business operations. Businesses adapting to new technology to transform operations is not a new concept, however over the previous decade the term 'Digital Transformation' has become prevalent in both the Public and Private Sectors. This is predominately down to the speed and improvements made in technology that require businesses to keep pace with developments in order to maintain effectiveness. A great example of this in the past decade would be the widespread adoption of the Cloud - moving away from traditional, on-premise infrastructure.

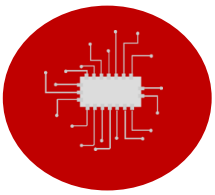
If a digital transformation project is to be successful it is crucial that the 'holy trinity' of technology, people and processes are addressed throughout the programme. Failure to do so can lead to the project becoming disjointed from the business, and the transformation will ultimately fail to deliver any promised benefits.



Effective Digital Transformation Trilogy

The next section outlines some of the drivers that would propel a business toward embarking on a Digital Transformation project.

Drivers



Adoption of New (or not so new) Technologies.

Whilst it would be easy to use businesses looking to leverage the benefits of Artificial Intelligence (AI) and Machine Learning (ML) as an example of adopting new technologies, for some however, adoption can simply mean replacing legacy IT infrastructure with more modern and better functioning systems. This might include replacing a complex Excel spreadsheet, used to manage large scale data, into a purpose-built business application that allows the data to be used and accessed more efficiently and effectively.

Customer Expectations.

The digital revolution has been key in changing consumer expectations, with many customers choosing digital methods of interacting with businesses and organisations over more traditional methods. In addition, customers expect a business to be able to leverage technology in a fashion that actively *improves* their experience as a consumer. For many businesses this can be a key driver for change, as without adapting their technologies and processes they will be unable to retain or attract new customers. A

great example of this is the modern approach to branchless banking that often sees services fully delivered through digital means. This has removed the traditional and absolute requirement to visit a branch in order to interact with a bank. Customers expect businesses to have the technology in place to make their experiences better with less effort on their part.

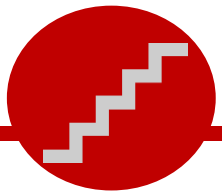
Global Events.

The necessity to respond to global events such as the coronavirus pandemic can often cause a reactive response to digital transformation. The pandemic revealed high levels of organisations who had typically either failed to organically modify or to adopt new digital ways of working. This ranged from companies scrambling around trying to provision devices to facilitate remote access, to smaller enterprises adopting technology in order to continue to operate and interact with customers. The most common reaction has been the adoption of online conferencing software. This software will change the way we all work long after the pandemic is over. Whilst global events of this nature are rare, it has undoubtedly caused businesses to reassess their current ways of working, and whether digital transformation can improve their organisations going forward.

Benefits of Digital Transformation

One of the key benefits of adopting digital transformation is that processes are likely to be highly optimised with the use of technology. This translates into boosting workplace efficiency that can lead to reduced costs and improve the operation of business functions. Organisations who have adopted digital technologies are better placed to gain valuable insights into their customers, whilst understanding their needs, and how their experience can be improved. This also allows businesses to respond to change in an agile fashion compared to those that have yet to adopt new technologies and processes. All of the above factors can enable a business to establish a competitive advantage by being able to deliver better services and products quicker than their competitors.

Next steps



8 Steps to Securing Digital Transformation

1. **Whole Company Approach.** Traditionally, changes to IT infrastructure were the sole responsibility of the IT function with little to no involvement from other areas of the business beyond initially defining the requirement for change. This often led to a

disconnect between the business requirement that prompted the change, and the system or service that was developed as a result because the developers didn't understand a particular business function. Successful digital transformation programmes involve **all** areas of the business; stakeholders are represented and engaged throughout the course of the transformation. This ensures that business requirements are considered at each stage, rather than being led by technical decisions. It is also vital that the Senior Leadership Team has suitable oversight over the project, as well as ensuring it is properly resourced to succeed. Transformations that do not adopt a whole force approach are counterproductive and unintentionally deliver outcomes that are not fit for purpose. This often requires workarounds to be introduced to the service which can introduce security risks, additional costs and delay, as these have not been fully factored into the design process.

2. **Security at Pace.** Digital transformation often involves introducing agile working practices to deliver new systems and services, at pace. This can prove challenging for other elements of the security function that are traditionally be more static in their approach. Functions such security governance, change management and risk assessment all have to adapt to integrate with agile practices in order to ensure security assurances are delivered at the same pace as the rest of the digital transformation. This can often include radically rethinking how security operates at the operational and tactical levels.

3. **Changing Threat Landscape**. The adoption of new technologies can increase the threat profile of a businesses. This could be due to more centralised services being delivered across the organisation, or increased connectivity potential; making it easier for a hostile actor to move laterally around a network. Information Security personnel play a vital role in understanding whatever changes a digital transformation project is planning and how it may change the threat profile of the business, in order for the appropriate security controls to be implemented.

4. **Embrace Security Automation.** Digital transformation offers a great opportunity to integrate better security automation within any new digital infrastructure. This automation can help address some of the more high-risk areas that are too labour intensive to be effective. Functions such as SIEM, Vulnerability Management, Threat Intelligence and Asset Management, are all capable of being highly automated to provide a better level of security for an organisation. Increased security automation helps free security professionals to be partners to the business; enabling them to scan the horizon and plan to meet future security challenges faced by an organisation. Overall, this will assist in contributing to an increased security posture for the business.

5. **Authentication Oversight.** In a similar vein as the previous point, digital transformation provides the perfect opportunity to address complex authentication issues present in most organisations. This can include ensuring that all authentication is controlled and centralised, thus removing the need for decentralised privileged user accounts that manage the diaspora of some difficult-to-control elements of IT infrastructure. Introducing tooling to assist in centralising authentication as part of the digital transformation, greatly reduces some of the most significant risks associated with privileged user management. These accounts are often targeted by attackers as they provided a greater level of access to information and system resources making it easier for them to establish undetected persistence on a network.

6. **Understand Compliance.** Every organisation, regardless of sector, will have its own legal, regulatory and compliance requirements that must be considered as part of any digital transformation programme. These requirements must be fully understood and conveyed to the transformation teams so they can be planned in from the outset, avoiding any unnecessary disruption, delay and cost at a later date. Involving personnel from the GRC and Legal departments at an early stage will help any programme help mitigate the compliance challenges that could be faced as a result of the digital transformation.

7. **Training Is Key**. Digital transformation has a tendency to focus on the technology and the underpinned processes. However, the third strand of the technology, processes and people holy trinity, is often overlooked. Digital transformation will present difficult challenges in addressing the 'people' component of a programme. This can be divided into two separate elements. The first is identifying the technical knowledge and skills gaps that are present; lack of personnel trained in data analytics or DevOPs can be used as an example of skill gaps that would be a barrier to the successful outcome. The second is understanding the training that will be required for the wider organisation as a result of the transformation; upskilling personnel to use new technology, applications, or business processes that are present because of the transformation. It is vital that any programme addresses the people component of transformation, without doing so will condemn it to failure regardless of how good the technology and processes are. People will continue to underpin everything, and it is key that they are trained to adapt to the change to help the programme succeed.

8. **DevSecOps Over DevOPs.** One of the many benefits of a digital transformation programme is the ability to rapidly develop and deploy code to support agile delivery. It is also one of the biggest areas of risk that can easily undermine any attempts to secure the transformation programme. In order to address this, security must be integrated into the software development life cycle. This will allow Developers to fully incorporate security throughout application development which will allow greater confidence in faster, more agile code releases.

Conclusion

The benefits of digital transformation for any business are clear. However, what is less clear is how to embed key business functions, such as security into the programme to enable a successful transformation outcome that delivers all the expected benefits. Fully involving security from the outset can support identifying the necessary security requirements for the programme, which can then be managed throughout the transformation. This will enable seamless integration of security for other areas of the programme into each proposed transformational change. Businesses should also be bold in their adoption of technology to improve security which will free up vital security resources to focus other high-risk areas where automation is not yet possible. Organisations should also be aware that digital transformation will not eradicate the security issues which are plaguing them, technology cannot be used as a 'fix all' solution where poor process already exists. Automating bad processes will still result in a poor security outcome regardless of how good the technology is. However, digital transformation will allow these complex problems to be simplified and centralised to enable better security management that will assist in responding to the security challenges that will be faced in the future.

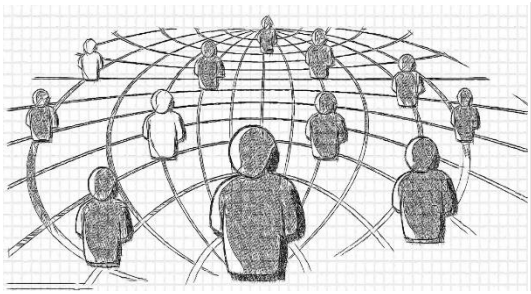
advent-im.co.uk

0121 559 6699

0207 100 1124

@Advent_IM

bestpractice@advent-im.co.uk



Securing Digital Transformation

The benefits it offers and guidance for a successful implementation