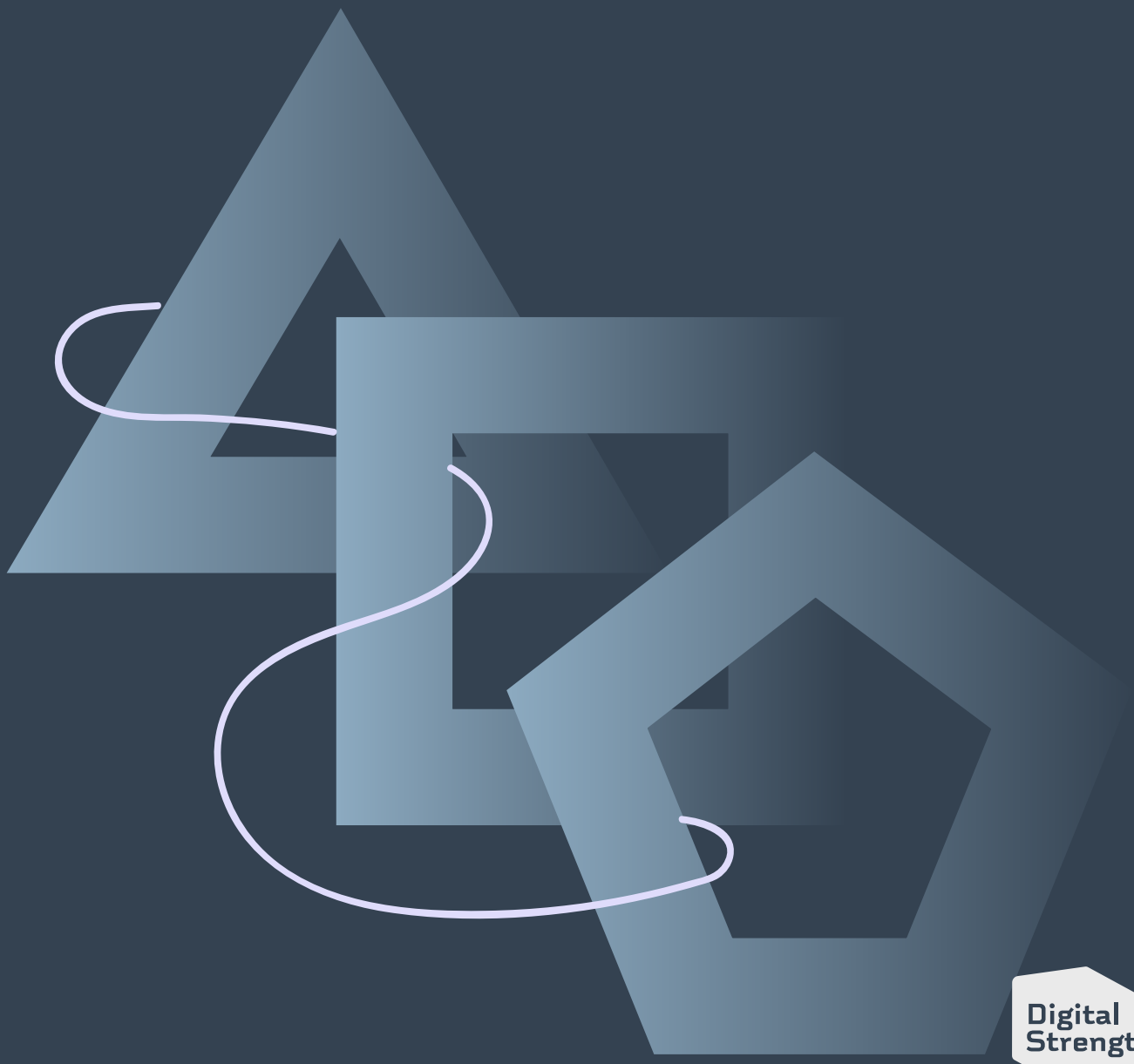
Securing Your Digital Transformation



Digital Strength
by HELLOSIGN

Contents

Clicking on the titles will take you to the different sections.

About the Digital Strength Program

In this digital age, the pace of change is increasing exponentially and every organization faces existential threats from new and existing competitors. The Digital Strength program is crafted to give everyone within an organization – from the C-Suite to the production line – an understanding of what digital transformation means within a global context, and guidance to achieve the digital transformation journey in your own organization.

We will cover an explanation of what digital transformation involves, the roles and responsibilities around digital transformation, as well as the cultural aspects of a digital change. Over the course of the program we will detail tips and tricks, potential barriers, clues into the ideation approach, and how to move towards seeing digital as an ongoing process.

By the end of the program, participants will be fully conversant about digital transformation, and will be armed to be the change agents within their own organization to implement digital broadly.

No matter whether you are just beginning the journey of transformation or are well on your way, the guidance in this program will be useful to you. Early adopters, those mid-way on the transformation journey or those yet to begin will all find something of value from this program.

Welcome to the future!

I. Introduction

While we have shown that digital transformation is something that involves the entire business (rather than being simply an IT project), it is certainly the case that IT will have an important part to play in delivering many of the technology aspects of digital transformation.

As with any IT projects – especially ones that touch at the very heart of what the organization does – security is an area that must be recognized and respected. In this course, we'll look at how organizational culture can drive the correct way of looking at IT security, and attempt to balance the high levels of security responsibilities (governance, risk, and compliance) with the more prosaic issues of relevance within organizations.

We'll discuss the issues around building intuitive and user-friendly systems, and show how approaching this process from a design-led perspective will help drive higher levels of security.

Finally, recognizing that the digital transformation process is often a big change within organizations, we'll discuss the issues around change management and adopting an appropriate cadence for change.

II. Security Implications of Digital Transformation

In the previous course, we pointed out repeatedly that digital transformation is a business change rather than just a technology one. That said, there is no disputing that the "digital" in "digital transformation" is a good indication that technology will be a big part of your transformation.

And technology, of course, must bring to mind security related questions.

In days past, cyber security and core business have often been seen as adversarial. Lengthy security requirements were often seen as hurdles rather than enablers. But in a rapidly-changing world, and with organizations needing digital technologies to drive their innovation, this divisive view no longer works.

We contend that security should never be an afterthought when it comes to digital transformation. Expecting to "bolt on" or retrofit security into an already-implemented digital product is a fraught approach and introduces an unacceptable level of risk. Security is firmly a part of a transformation strategy, and should be considered an enabler of grand potential.

Before we look into the ways security empowers digital transformation, it is important to understand historical perspectives and the cultural norms that have been created. It is only through an understanding and empathetic view of the dominant paradigms that we can hope to change those paradigms into the future.

III. Perspectives Diametrically Opposed

It is almost comical to hear how various protagonists in the security vs. business conflict view the other party. The adversarial nature of the roles is, unfortunately, a huge barrier to innovation and organizational transformation. While a stark generalization, it is useful to hear how each side views the other.

SECURITY PROFESSIONALS – CONTROLLING THOSE PESKY END USERS

The most emphatic of security professionals can still view business users as the biggest possible threat to their organization's security posture. At they see it, end users spend their days looking to find new ways to avoid security policies, and, as a matter of course, have their passwords conveniently written on a Post-It Note as a matter of course.

These security practitioners see business personnel as individuals whose access to applications and data needs to be controlled, less they, either inadvertently or not, cause a data breach that puts the entire organization at risk. They know that employees, though well-meaning, may inadvertently show a Trojan horse exactly where the front door to the castle is.

The fundamental perspective of individuals on this end of the spectrum is one of control, limitation of access, and tight compliance with process.

Of course there is nuance in all of this. Security professionals can be prudent and still apply due diligence without being overly controlling. Often it comes down to honest communication that maintains understanding and mutuality.

END USERS – AVOIDING THE "DEPARTMENT OF NO"

The perspective of end users, at least the most extreme of them, is that the security department is a barrier to them doing their jobs and something to be avoided at all costs. You also might see them banging their heads on the desk because they forgot a new password, and refuse to use a password manager.

Frustrated by seemingly endless impediments to agility that the security and/or IT department puts in place, these end users have seized the bull by the horns and self-chosen and self-implemented point solutions.

Their modus operandi is to choose whatever tool does the job as they require it, and to implement that tool directly. While this approach certainly delivers agility, it also introduces risk, potential duplication, and a nightmare of application sprawl.

When applied to digital transformation specifically, this polarized approach to security can lead to negative outcomes as we shall detail in the next section.

IV. Security Starts in Leadership

Leaders of today have a very important opportunity: to be an enabler of digital technologies in partnership with security and compliance. This isn't, unfortunately, always viewed as a positive. Some see security as a reason and justification for blocking the adoption of new technologies.

The C-Suite's reaction to digital transformation closely parallels what occured in the past decade in response to cloud computing technologies. Many more conservative leaders did their utmost to block the adoption of cloud technologies – whether for good intentions or otherwise. History has shown us that these attempts to block progress where somewhat futile, and often lead to the very consequences they were designed to avoid.

This opposition to cloud came from many different angles – maybe leaders felt threatened or inadequate, maybe they worried about how cloud would impact upon their regulatory compliance, or maybe they were concerned about their already deployed capital investment. Whatever the cause, it wasn't a realistic or practical position to take.

Most forward-looking organizations, and the executives within them, have realized that allowing the adoption of cloud technologies within the context of a broad governance framework is the approach most likely to deliver the best of both worlds – agility and security.

The process of digital transformation is similar and there are numerous potential unintended consequences of centralized attempts to block it. In the same way that trying to curb cloud adoption can sometimes lead to a burgeoning number of unsanctioned and potentially unsafe applications, so too can the blocking of digital transformation initiatives lead to a sub-optimal and piecemeal approach towards digital adoption.

The leadership of the organization therefore has a hugely important part to play in giving end users access secure, user-friendly, and compliant platforms; ones which empower them to begin and continue their digital transformation journey. But the responsibility doesn't solely rest with management – end users also have a part to play.

V. End Users Doing Their Bit to Make Digital Transformation a Safe Process

As we pointed out in the last section, management cannot take the approach that sees it blocking digital transformation simply because of perceived security risks. It is the role of management to give workers access to platforms that keep organizational data safe, while also allowing them space to be agile.

But the end users also have a part to play in keeping organizational data safe and the security within the digital transformation process. It should be seen as a partnership between the leadership and end users.

While it may be a cliché to talk about the apocryphal worker who stores all of his or her passwords on a Post-it note affixed to their monitor, like the best kinds of apocryphal tales, it isn't far from the truth.

Often the tensions that exist between technology leaders and end users can be exacerbated by an unwillingness on the part of end users to comply with reasonable security requirements. It is important that the two sides collaborate to develop reasonable ground rules and then comply with them.

Building a culture that encourages communication of the "why" when it comes to security can help in these situations. Employees should understand the context behind security concerns – it is often hard for business users to visualize what are, often, nebulous concepts. Business users also have a tendency to feel that security concerns are overblown and security is unlikely to actually impact upon them – having IT specialists explain security clearly and in plain speak can be powerful when communicating the stakes.

While processes and systems undeniably need to be user-friendly, users also need to make a determined effort to understand the significance of their actions. The smallest security holes matter, and individuals have the opportunity (and the shared responsibility) to secure these leaks.

VI. Is Security the Enemy of Digital Transformation?

Digital transformation is a business-wide movement that has its focus on change, agility, innovation, connectivity, customer/stakeholder engagement and – fundamentally – disruption. In the view of many at the cutting edge of transformation, the security function can feel like friction against these aims.

In recent research[1], <insert footnote - i-scoop.eu/cyber-security-cyber-risks-dx/ > over 75 percent of respondents stated that they believe security is brought in too late to digital transformation projects. The subtext for all of this is that those involved in the digital transformation process see security as being about rules, regulations, and lockdown. The findings suggest that many believe security adds too much process and complexity to projects, thus slow down the transformation project.

This perspective, and the polarized views held by both parties in this relationship, is an outdated one. Sure, the business wants new tools and processes which optimize the way it interacts with its various stakeholders – prospects, customers, and employees alike. But security, rather than being against those aims, simply wants to help achieve them within the context of robustness.

Security is a complex topic, and security within the context of digital transformation is even more complex. The security posture, therefore, much like other aspects of digital transformation requires strategy, prioritization, and collaboration. Security needs to be a part of the conversation and not just an afterthought. Rather than either trying to avoid the security conversation outright, or thinking about how to carve off some of the transformation budget to fund security, the security construct should be an integral part of the entire digital transformation business case.

Let's explore how to make this happen in the next section.

1 Cybersecurity: security risks and solutions in the digital transformation age. (n.d.). Retrieved February 28, 2018, from https://www.i-scoop.eu/cyber-security-cyber-risks-dx/

VII. When Should Security Teams Get Involved in the Digital Transformation Process?

A question often asked as organizations embark upon a digital transformation process is when security teams should be engaged. This is, in our view, the wrong question to ask. It implicitly looks at security as separate to digital transformation, and helps to create and perpetuate an adversarial culture in which security personnel are pitted against transformation team members.

It is our strong advice, therefore, that security practitioners should be an integral part of the transformation team. It is, once again, analogous to best practices for moving to cloud computing; rather than making decisions and then engaging security/IT in the process, these practitioners should be part of the process from the outset.

We need to be clear – this is not about layering a security fabric on top of an already executed digital transformation process, but rather making security a part of the fabric itself. With security practitioners as part of the transformation team, innovation can occur with proper respect to the security requirements.

Obviously, as with other people involved in the transformation process, leaders need to ensure that the individuals they involve in the process have the correct mix of creativity, practicality, and strategic/operational knowledge. This doesn't preclude security practitioners as a class, by the way, but merely reminds us that digital transformation a very human thing at its core. All stakeholders likely have some personal development to focus on – this is as true for the security side as the house as for the business one.

Later on in the Digital Strength program we will take a deep look at the human element related to digital transformation and the best ways to find the people most likely to be able to drive good results.

First steps, however, are to ensure robust frameworks are in place, and change management is one area that this is particularly critical in. This applies to organizations embarking on the digital journey as well as ones that have already started, but without thinking about the security context. While early is generally preferable when it comes to security, it's never too late to think about the issues.

VIII. Governance, Risk, and Compliance Issues

While the main thrust of this course was to give guidance around security to those involved in the digital transformation process, it is important to think broadly around the issues of governance, risk, and compliance (GRC) as well. While GRC, much like security, can be seen as a blocker to rapid innovation and agility, good GRC frameworks can also make the digital transformation process more efficient.

The relationship between regulation and digital transformation is complex and sometimes ambiguous. Transformation can potentially improve regulatory control and compliance by increasing transparency and auditability, and reducing manual errors. On the other hand, regulators often (justifiably or not) fear that digitalization may fail to protect customers and come at the expense of security, compliance, and business continuity

The fact of the matter is that digital transformation does not happen in isolation, but is closely tied to operating processes and systems that the organization has. As such it is important to consider both the internal and external regulations that relate to the specific areas that are candidates for digital transformation.

It is useful to include an early assessment of risk in order to optimize the transformation process. This isn't just as it relates to internal processes, but also business processes which touch customers.

This process is made all the more difficult for organizations that operate within multiple jurisdictions. Policies and regulations obviously differ from market to market, and even among different regulators within a country – digital transformation efforts need to be considered within the context of the overarching regulatory framework, with thought given to how digital initiatives might broaden their reach into other markets or jurisdictions.

Regardless of the breadth of impact, the onus is on compliance teams to understand their part of the transformation process. Rather than being blockers, they can be stakeholders in the process – these functions need to evolve to become consultants to the innovation process — analyzing the risks involved and providing solutions to ensure compliance and minimize other risks.

This is a significant challenge and change as it requires that compliance staff better understand IT, and develop and use new, dynamic models to assess operational risks and establish better controls to safeguard the process. It also means that the ultimate decision of whether to take a risk will now lie with the business — not the compliance team. This is a drastic change from today's culture of control to a new collaborative culture of risk.

About HelloSign

HelloSign simplifies work for millions of individuals. Over 60,000 companies world-wide trust the HelloSign platform – which includes eSignature, digital workflow and electronic fax solutions with HelloSign, HelloWorks and HelloFax – to automate and manage their most important business transactions. For more information visit http://www.hellosign.com

About Ben Kepes

Ben Kepes is a business leader, a technology evangelist, an entrepreneur, and a commentator. Ben covers the convergence of business and technology. His areas of interest extend to leadership development, startup activity, digital transformation, and enterprise software, as well as articulating technology simply for everyday users.

He is a globally recognized subject matter expert with an extensive following across multiple channels. His commentary has been published on Information Week, Computer World, Forbes, Wired, ReadWriteWeb, GigaOm, The Guardian and a wide variety of publications – both print and online.

Ben's insight into the business of technology, and the technology of business has helped organizations large and small, buy-side and sell-side, to navigate a challenging path to a successful future.

Ben is passionate about technology as an enabler and enjoys exploring that theme in various settings.

hellosign.com/digitalstrength

Author: Ben Kepes

Let's stay connected!
Join the Digital Strength's LinkedIn Group