Digital Trust – The Foundation of Digital Transformation

Jim Hurley
April 2018
About this Report

Information Services Group Inc. is solely responsible for the content of this report. Unless otherwise cited, all content, including illustrations, research, conclusions, assertions and positions contained in this report were developed by, and are the sole property of Information Services Group Inc.

The research and analysis presented in this report includes research from ongoing ISG research programs, including our global survey and interview work with business and IT leaders, briefings with providers, and analysis of publicly-available market information from multiple sources.

This independently-developed research report was developed, published and is owned by Information Services Group, Inc. This report is solely intended for use by the recipient and may not be reproduced or reposted, in whole or in part, by the recipient, without express permission from Information Services Group, Inc. Opinions reflect judgment at the time of publication, and are subject to change.

Unisys funded the publication of this report and has been granted the right to reprint and electronically distribute it through its website until April 30, 2019.

Lead author for this report is Jim Hurley. Design and layout is by Partho Saha and Liza Zacharia. Edited by Elizabeth Davis.
Introduction

There is no longer a comfortable wait-and-see middle ground when it comes to digital business: every business is now a digital business. Business leaders can wait and be forced to respond to market change, or they can embrace digital and lead market change themselves.

Although we have been doing digital for years, businesses in every industry are re-imagining and re-inventing digital trust to gain and retain customers, business partners and suppliers. The nexus of digital trust – convenience, user experience, reputation, transparency, integrity and reliability – all rely on digital identity and entitlements. This is where the trust in digital for customers, partners, suppliers and the digital processes and data for all stakeholders come together and where digital transformation comes alive.

This report summarizes ongoing ISG research and analyses the intimate relationships between digital transformation, the enterprise journey to cloud, digital trust, new operating models and principles of cyber, and choices that enterprises need to make about identity and entitlements for the digital transformation journey.
Digital Business Transformation

What sets digital business apart from all prior uses of digital is the re-thinking and re-inventing of the business of the enterprise, the reinvention of customer expectations and experiences and the re-invention of served markets. The digital tools enabling digital transformation and business are mostly cloud related, but, by themselves, they are like unformed clay. After market fungibility and readiness for change, closing the gaps between customer expectations and experiences, and visibility into future market states, the next critical success factors enabling digital transformation are small teams, agility and digital trust.

Small teams
Consisting of interdisciplinary talents, small digital teams are operating as innovation engines in start-ups and as sourced from service providers by very large enterprises. Small digital teams are the grease of near-frictionless acceleration.

Agility
By failing fast, learning from failure, re-thinking, re-inventing, and re-coding, small teams are adroitly navigating market seams and the gaps between customer expectation and experience. However, agile is just the cadence of the journey to the digital transformation of enterprise business, not the destination.

Digital trust
It is digital trust – earned through interactions with customers, business partners and suppliers – that is the bedrock foundation of all successful digital business transformations.

Digital Transformation’s Fulcrum is Cloud

Cloud is the lever of digital business because it delivers the speed that agile teams need to test, retest, rethink and reinvent customer and workplace resources. It supports market share and wallet share expansions.

ISG research reveals digital transformation involves a wide spectrum of cloud uses, from stand-alone virtualized workloads to stand-among cloud microservices integrating e-commerce gateway engines and operating on data housed both in data-lakes and traditional transaction databases. The agility, flexibility and speed of cloud uses for digital transformation is enabling organizations to stretch the boundaries of customer intimacy, product leadership and operational excellence.

The dominant profile of most enterprises is one of change involving a mixture of new technologies along the journey to cloud and numerous interactions between the enterprise, its employees, contractors, business partners, suppliers and customers. Rather than being restricted to front-office processes and interactions, the journey to cloud is one in which almost all business processes are being re-thought and re-invented, from sales to manufacturing and delivery. For example, cloud application workloads are occurring for business processes using intelligence and analytics, customer relationship management, industry-specific business applications, human capital management, financial planning and reporting and supply chain management application workloads.
Although regional and industry differences exist in the rate of adoption of digital cloud technologies, the average rate of change shows cloud application workloads now account for a majority of digitally enabled business processes. Before the end of 2018, fully 65 percent of all application workloads are expected to be in one form of cloud or another, and just 35 percent to be maintained as on-premises workloads. The journey to cloud is expected to accelerate further when, by 2020, eight-in-ten application workloads – customer relationship management (CRM), supply chain management (SCM) and human capital management (HCM) among others – will be operating on cloud foundations and no longer deployed on stand-alone application servers operating on the corporate network or as virtualized workloads.

Business application workloads that will make digital transformation journeys involving internal, hosted, hybrid, public and SaaS cloud services include: CRM (82 percent), SCM (81 percent), business intelligence and advanced analytics (81 percent), industry-specific application workloads (85 percent), HCM (85 percent), financial planning, budgeting and reporting (83 percent) and core financials (77 percent) among others.

Two common factors across these many business application workloads include the fact that there are numerous stakeholders involved and the hybrid nature of cloud, which uses identity and digital capabilities across private subscription services, public subscriptions, private workloads, hosted data centres and virtualized workloads.

The major reasons cited for moving to cloud workloads are not financial – although lower capital expenses are often mentioned – but rather speed, agility and access to digital tools as factories for digital transformation to re-invent business procedures. It is the speed to use-case optimization that makes cloud irresistible. But making this journey requires some critical capabilities, including:

**Speed:** The speed necessary to introduce new cost leadership, product leadership and intimate customer experiences is essential to the effective use of cloud as a transformative agent. Speed is what organizations gain when using digital capabilities that can amplify flexibility and agility.
**Decentralization:** A key attribute of digital transformation is decentralization of applications and data to serve local markets and customers. Today, most cloud data centers decentralize application workloads and content across the world.

**Scale:** Digital is world-wide, omni-present and scalable in response to rising and declining demand. Cloud allows enterprises to scale without large up-front capital expenses.

**Volume:** Digital processes and information are transformative and elastic, serving from small to large. It is the elastic nature of business demand supported by fungible cloud workloads that are hallmarks of the synchronous and responsive nature of digital business.

While cloud is a spoke of the transformations of digital business, enterprises report that digital trust is the hub of the journey, with digital identity and entitlement being the central clearing source. Trust in digital business is earned from customers, partners and suppliers during every digital interaction with the enterprise.

**Figure 2 – Cloud is the Fulcrum of Digital Transformation**

<table>
<thead>
<tr>
<th>Information Entropy</th>
<th>Centralized and replicated information systems</th>
<th>Edge of network gateway systems (Email and Web) plugged into centralized systems</th>
<th>Decentralized and Cloud enabled micro-service information services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business cycles</td>
<td>Five years to one year</td>
<td>One year to three months</td>
<td>Three to one month</td>
</tr>
<tr>
<td>Business applications</td>
<td>Centralized Applications</td>
<td>Gateway Applications</td>
<td>Decentralized Applications</td>
</tr>
<tr>
<td>Performance cycles</td>
<td>Annually to quarterly</td>
<td>Quarterly to monthly</td>
<td>Week to daily</td>
</tr>
<tr>
<td>Information entropy</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td>Customer multipliers</td>
<td>10x : 1</td>
<td>10x Thousands : 1</td>
<td>100x Millions : 1</td>
</tr>
</tbody>
</table>

Source: ISG Research, 2018
Digital Trust is the Foundation of Digital Business

Trust in the digital age is indispensably digital. Digital trust includes the digital experience accorded to customers and their data, and the digital experiences of business partners and suppliers. But digital trust goes beyond the custodianship of customer, partner and supplier data to include relationship attributes that can improve or impair loyalty and stickiness of all stakeholders and participants in the enterprises value chain. The attributes of digital trust include:

- Convenience
- User experience
- Reputation
- Transparency
- Integrity
- Reliability
- Security

Digital trust – and its attributes – differ according to the user and the users’ access, conditions of access and relationships. For example, customers in different regions of the world have different expectations – and legal covenants – governing what can be done with personally identifiable information (PII). The witch's brew that is convenience, user experience, reputation, transparency, integrity, reliability and security accorded to the handling of customer PII can adversely impact digital operations and results if customer expectations and experiences do not match.

**Figure 3 – Attributes of Digital Trust**

<table>
<thead>
<tr>
<th>Digital Trust</th>
<th>Customer Questions</th>
<th>Enterprise Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Convenience</td>
<td>How convenient is it to do business with this company?</td>
<td>How convenient is it to add, change and modify digital releases?</td>
</tr>
<tr>
<td>User experience</td>
<td>Are my expectations being met?</td>
<td>What is the next minimum viable sprint to test?</td>
</tr>
<tr>
<td>Reputation</td>
<td>Do my peers trust this company?</td>
<td>What digital reputation do we aspire to?</td>
</tr>
<tr>
<td>Transparency</td>
<td>Do I control my information?</td>
<td>Can we make transparency simple and convenient?</td>
</tr>
<tr>
<td>Integrity</td>
<td>Do I trust this company?</td>
<td>What is needed for the customer experience?</td>
</tr>
<tr>
<td>Reliability</td>
<td>Do I always have access - when I need it?</td>
<td>What is needed for 7x24x365 operations?</td>
</tr>
<tr>
<td>Security</td>
<td>How secure is my information?</td>
<td>What do we do to make it rock solid and repeatable?</td>
</tr>
</tbody>
</table>

Source: ISG Research, 2018
The General Data Protection Regulations (GDPR) – in effect in May 2018 – will affect the reputation and digital practices of every enterprise conducting business in Europe or carry out business for enterprises conducting business in Europe.

GDPR and digital trust are about digital identity and the capabilities and entitlements enabled for each participant in the enterprise’s ecosystem. This might involve PII data for the citizens of the European Union (EU) governed by GDPR, or entitlements accorded to participants in the economic value chains of ICBC from China, Berkshire Hathaway from the United States or Toyota Motor Corporation from Japan, among thousands of other businesses.

Digital trust is different for every enterprise and its use as a market differentiator will differ as well. Enterprises ignoring digital trust, digital identity and entitlements run the risk of become digital dinosaurs, while those embracing and using it compellingly as part of the customer experience will thrive.

ISG research shows the key unanswered question for most CIOs and CDOs is not whether to adopt and use the tools of digital transformation, but what can be done to accelerate it and avoid careening off the road. In summary, the research reveals the unresolved challenges include the organizing principles and operating model to create digital security for agile digital transformation and digital business. The answers to these unresolved issues involve artificial intelligence (AI)-enabled orchestrations, agile digital trust fabrics and a new operating model for cyber security.
Digital Identity and Entitlements – The Foundation of Digital Trust

The age of network security is over. It survived as the organizing principle and force multiplier for cyber security operations for more than two decades. But the era of hybrid cloud workloads, microservices, machine-to-machine communications and big-data analytics are dissolving – but will not eliminate – network security controls as organizing principles for cyber. The legacy of network perimeters as the force multiplier for cyber is merging into a new operating model for cyber security made possible by digital trust and AI-enabled cyber orchestrations.

The new age of digital trust is composed of application workloads using API-based services operating natively in the cloud, with on-premises workloads, and with decentralized and distributed microservices across many kinds of business data, application workloads and systems.

Some of the new age digital cyber capabilities – including digital deception, digital bio- and behavioural- identification, digital stealth, digital micro-segmentation, information asymmetry, software-defined networking, flow-based anomaly analytics, behavioural analytics, and AI-based cyber orchestrations – are among the capabilities that will be used to manage the risks of integrating cloud workloads and digital service transformations into the business.

One of the foundations of the new capabilities is digital identity and entitlements: the combinations of attributes identifying organizations, people, applications, avatars, bots, data and things; and what all these entities – active and passive alike – are entitled to do and under what circumstance.

Ongoing ISG research reveals that, much like transformations to digital business that are using on-premises and cloud application workloads, the allocation of spend on digital security will remain split between on-premises-enabled operations, managed security services and cloud-enabled business operations.

The research clearly indicates that, while many underlying application workloads are being re-invented and re-imagined using cloud capabilities, much of the task for digital security will focus on integrating cyber capabilities for a very hybridized world of cloud.

**Figure 4 – Digital Security Plans from 2018 to 2020**

<table>
<thead>
<tr>
<th>Year</th>
<th>2018</th>
<th>2020</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>On premises security</td>
<td>42%</td>
<td>39%</td>
<td>Decline</td>
</tr>
<tr>
<td>Managed security services</td>
<td>29%</td>
<td>29%</td>
<td>No change</td>
</tr>
<tr>
<td>Cloud security</td>
<td>30%</td>
<td>32%</td>
<td>Increase</td>
</tr>
</tbody>
</table>
Decision-makers charged with navigating cyber security for an enterprise’s digital transformation journey have some simple choices to make regarding what to do about the hybrid nature of digital trust, digital identity and entitlements for, with and to the cloud. These choices include:

- Digitally segmenting communities of trust
- Trusting cloud providers to deliver security
- Using on-premises security products for hybrid cloud
- Reusing today's cyber force multipliers of identity and access management (IAM) and security information and event management (SIEM) for hybrid cloud
- Using a cloud security fabric for hybrid cloud

Digitally segmented communities of trust

In the new world of elastic hybrid cloud services, the old-world approach that depends on network firewalls and appliances simply does not work. There is no way to mediate access rules by spinning up and down cloud-based elastic microservices using network firewalls. Instead, the way forward is by building digitally segmented communities of trust, where assets, users, business procedures, application workloads and service entitlements are dynamically allocated on the fly. Digitally segmented communities of trust deliver more convenience, greater assurance, more transparency, better user experiences and more control.

Cloud providers

Although trusting cloud providers is a seductive option, cloud providers will never customize their environments to the digital security needs of each customer and will never agree to accept the risks of cyberattacks, outside of normal availability service-level agreements. For example, no cloud provider can operate a high-volume business acting as a custom job-shop, and none will accept the financial and reputational risk of data breaches and digital security events, thefts, ransomware attacks or other cyber-attacks.

On-premises security products

Unfortunately, on-premises cybersecurity products do not translate to the cloud. For example, network appliance and next-gen firewalls do not – and cannot – operate in dynamically allocated container and microservices resource pools that are changing constantly. The only places where it is possible to use on-premises network security tools is in dedicated hosting racks operated in single-tenant mode, exclusively for the use of the enterprise. And then this is not cloud, it is simply a private hosting service in some other data center.

Reusing IAM and SIEM for hybrid cloud

Reusing IAM and SIEM systems for C=cloud is also a seductive – and common – approach seen in some of today’s early digital transformation efforts. Integrating IAM services is generally easier to make work, depending on whether the IAM service is cloud-ready or not and whether it has an API library for use with agile cloud application development. The situation with SIEM is a bit more complex but early evidence appears to indicate these systems are translating to the cloud for post cyber security event forensics and analytics. The benefits of taking some of today’s client-server cyber security technology to the cloud may include lower training and less staffing. However, the downside of this approach is that it increases costs, if not by twice, by at least by 50 percent. And depending on the event rates and storage rates, costs for cloud uses for SIEM could mushroom well beyond two times more.
Cloud security fabrics for hybrid cloud

The other option to consider – and one that is becoming more commonly used in the market – is the use of microservices security fabrics that are native to cloud workloads while integrating these with existing IAM, SIEM and non-cloud workload systems on-premises. The big benefits of this approach are a consistent set of security services operating across the enterprise’s business operations and digital operating environments. Another benefit is that costs should be lower than taking client-server security to the cloud. The initial drawback may be training, familiarization and coding when integrating these native cloud security service platforms into client-server workloads. In theory the use of a Cloud-native API service for IAM and SIEM is alluring but fabrics and API-based “as a service” versions of IAM and SIEM have very different operating, scalability, speed, and financial characteristics. The usual candidates for considering and using a common cloud security fabric include:

- Roll your own
- Pre-packaged appliance form factors
- Software service segmentation fabrics
- Managed cloud services
- Cloud subscription services

Rolling your own fabric is a fool's errand: it will bog the enterprise down with the costs, staffing and processes required to become industry security technology experts. The entire purpose of API-driven micro security services is for enterprises to leverage the expertise of security experts.

Using security appliances make sense when processes are well understood, are standardized and unlikely to change much. Cloud and digital

Figure 5 – Attributes of Digital Trust, Software Segmentation Fabrics -vs.- IAM and SIEM

Source: ISG Research, 2018
trust transformation are somewhere between infancy and teenage years depending on the enterprise: it is not ready for appliance-sizing yet. Appliance versions of cloud security fabrics should probably be delayed for now.

The last three options – using software segmentation fabrics, managed services and cloud services are really one and the same when they deliver dynamic allocation of resources and assets for digital transformations. All deliver much greater agility, convenience and customization for customer expectations and experiences. The differences between the three include whether they are consumed as a managed service, a cloud service or as a software fabric. All three rely on a common segmentation security fabric for delivering digital trust. The differences also include how scalable and elastic each alternative is to demanding application workloads.

Typically, managed services are used where processes are not changing as rapidly and where fixed contracts can be used to better manage costs. If this is the primary value proposition of the managed digital trust service, then the obvious place to start is not going to be managed services but will be software fabrics or cloud services for digital trust. More demanding workloads may be better served by API-based cloud services for IAM and SIEM, while the most demanding workloads will be best served by native microservice cyber security fabrics.
Summary Recommendations

The path taken to digital trust for digital business is one that will define the future success of goods-producing-and-selling industries as businesses add new levers for differentiation in addition to competitive advantages of price and cost leadership based on operational excellence. Digital business means producers and sellers of business and consumer goods will have to re-invent and re-imagine the customer experience and product leadership market at the same time as they re-invent and re-imagine digitally driven operational excellence.

Although market advantages driven by cost leadership will remain absolute for companies in some industries, market differentiation will increasingly flow to those that are exploiting cloud-based digitization to improve customer, product and service experiences simultaneously. The challenge for all companies and all industries is that anyone can and will use new digital business capabilities to re-imagine and re-invent upstream customer experience. Once re-imagined and re-invented, it will be difficult for cost leadership to compete by itself as the single market lever.

Delivering against customer expectations and not just customer experience will change every industry – some sooner than others – and is one of the imperatives of digital business transformation. The foundation of this transformation is digital trust, and this is anchored by the choices made for digital identity, entitlements as part of the cyber security strategy.

Digital transformation involves a fundamental re-thinking and re-imagining of the operating model for cyber security. The force multipliers and operating model for digital security for digital trust is no longer perimeters and controls of network security but is a combination of digital trust involving digital identity and entitlement fabrics and AI-enabled cyber orchestrations.

In the era of digital transformation, digital trust is table stakes: a requirement that, if not met and delivered as part of the experience for stakeholders of the enterprises value chain, will upend brands everywhere. Enterprises that are first to adopt and exploit digital trust fabrics will realize competitive advantages driven by combinations of deeper customer intimacy, operational excellence and product leadership. These in turn will create a virtuous cycle involving rapid customization, convenience and market agility.
Sponsor Perspective

Scalable Digital Trust

Protecting assets critical to an organization’s continued operations without impeding productivity is a boardroom concern. Historically, enterprises attempted to achieve this balance by applying static security controls onto existing IT infrastructure.

The static control approach that worked when critical assets sat behind fixed perimeters failed when perimeters dissolved. In a fixed perimeter environment, digital trust was easily established between an organization and an employee when the employee was in the office, behind a firewall and on an approved device. In today’s digital world, competitive advantage is gained by making data and systems open and available to more than just employees on approved devices. Digital trust in digital business is earned from customers, partners and suppliers during every digital interaction with the enterprise.

Effective security identifies critical assets by the business value assigned to them and protects them appropriately. This means establishing digital trust based on the identity of the user as opposed to the device. It means scaling digital trust to accommodate the dynamic nature of employee, customer, partner and supplier digital interactions where trust levels must be adjusted based on time of day, location or data being accessed. Adaptability must be achieved in a matter of minutes, without extensive security policy updates that require cross-organizational coordination to implement. And, in the event of the inevitable cyberattack, resilience must be guaranteed by providing trusted users with a secure, segmented enclave that provides access to the critical assets required to ensure continued operations.

Unisys Security Solutions protect enterprise critical assets by establishing digital trust and providing secure access to trusted users. We build security that scales to secure user’s digital identity and data on any device operating within the enterprise, the factory floor or out in the field. Our solutions help enterprises reduce their attack surface, easily comply with regulations and simplify the complexity of today’s network security. Combining expert consultants, advanced software and managed security services, Unisys enables you to build security into the fabric of your digital transformation.
About Unisys

Unisys is a global information technology company that builds high-performance, security-centric solutions for the most digitally demanding businesses and governments on Earth. Unisys offerings include security software and services; digital transformation and workplace services; industry applications and services; and innovative software operating environments for high-intensity enterprise computing. We build better outcomes securely for our clients across the Government, Financial Services and Commercial markets.

For further information contact Christopher Kloes, Vice President of Security Sales, at christopher.kloes@unisys.com to or visit Unisys.com/stealth to learn how Unisys Stealth® micro segmentation can help transform your business.
Jim Hurley
Director

Jim Hurley is a Research Director at ISG with a focus on the business impact of emerging technologies and digital transformation, digital security, regulatory compliance, blockchain, big data analytics, privacy and risk management.

Prior to ISG, Jim led software lines of business for smart grid electric, gas, and water utility industries; led benchmark research for Symantec, ISACA and The IIA; headed industry research, analysis, and advisory for risk management and security with Aberdeen Group; led numerous lines of business in the computer industry; was responsible for many successful software and security products; and designed experimental high energy superconducting magnet systems and software. Jim is a graduate of Boston University and is a certified information systems security professional (CISSP).
Digital Trust – The Foundation of Digital Transformation

April 2018

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 700 clients, including 75 of the top 100 enterprises in the world, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; technology strategy and operations design; change management; market intelligence and technology research and analysis. Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,300 professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data.