White Paper

Digital Trust: The Key Driver for Sustained Digital Transformation

Sponsored by: CenturyLink

Courtney Munroe Christina Richmond Richard L. Villars

January 2019

EXECUTIVE SUMMARY

In the early stages of digital business transformation, when companies are deploying ad hoc projects, they are trying out new ideas and various technologies. They often demonstrate an unwarranted willingness to trust potential partners, customers, and broader internet entities with very little regard for business risk. Conversely, once organizations shift to a line-of-business orientation for transformation, they become overly cautious about other entities and institutions as they look inward to develop their own program but struggle with the need to navigate the worlds of industry, government, and the public internet.

IDC finds that the companies thriving at digital business transformation understand that establishing and sustaining "trust" are crucial drivers to their long-term success. They value digital trustworthiness and commit time and resources to ensure that their information technology (IT) and network environments are a platform for building and maintaining digital trust. Digital trust enables the decisions made between two or more entities that reflect their level of confidence in each other; these decisions are based on each entity's digital reputation as well as the assurance levels provided by each entity's cybersecurity programs for a proposed digital activity. Digital trust decisions can involve one or more of the following constituencies: organizations, customers, business partners, and overseers.

Companies recognize that they require a partner that can:

- Assist in properly designing, configuring, protecting, and maintaining increasingly agile IT architectures.
- Enable dynamic network functions and services that ensure flexible and secure interconnection of cloud, core, and edge locations and data.
- Implement next-generation network-based cybersecurity practices and policies that provide an overarching platform for establishing and maintaining digital trustworthiness.

Reputation is the most challenging part of trust. While digital business trust is mostly driven by technical expertise, it is also continually being assessed by others. It requires sustained communication about the ways the organization is protecting its environment and ensuring that shared resources are properly handled. Taking explicit measures to define the controls in place — leveraging reports from third parties — and providing meaningful metrics are critical elements in any effort to demonstrate sustained excellence in digital trust.

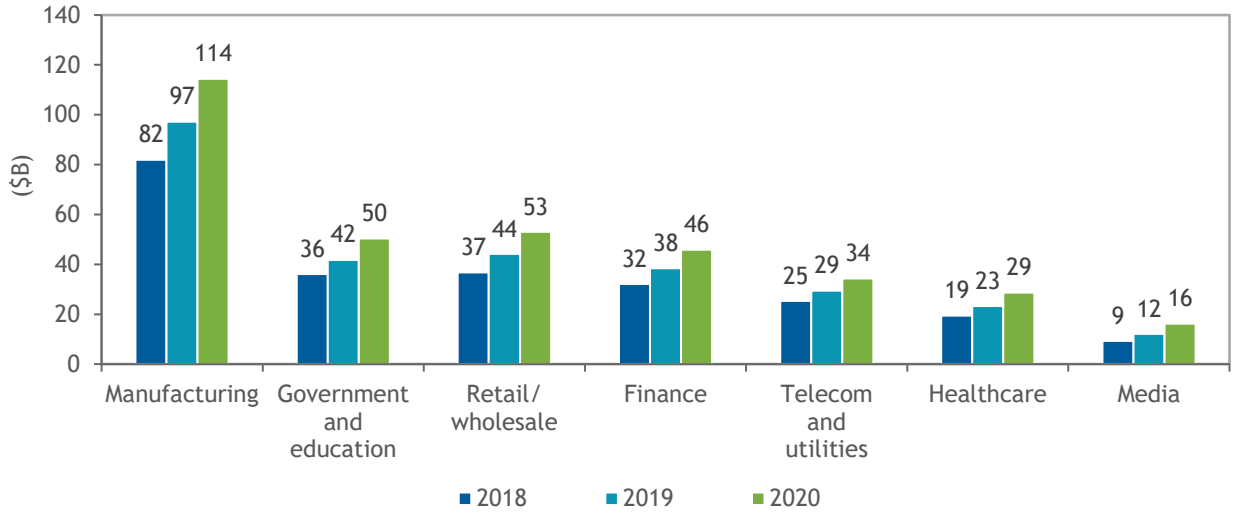
January 2019, IDC #US44565619

HOW DIGITAL TRANSFORMATION IS CHANGING THE BUSINESS CONVERSATION

In just a few short decades, information technology has moved from the back office to the front office and is now embedding itself into nearly every aspect of people's business and personal lives. We are entering an era where the distinction between the technologies and the processes that businesses deploy is so tightly linked to their customers and markets that the boundary between the internal operations of the enterprise and the enterprise's external ecosystem (e.g., customers, markets, competitors, partners, and regulators) is rapidly disappearing. Business leaders are challenged to move their enterprises to the next level, that of digital business transformation, employing digital technologies coupled with organizational, operational, and business model innovation to create new ways of operating and growing businesses. Enterprises in all verticals are planning sizable investments in technologies that support digital transformation (DX) initiatives in 2019 (see Figure 1).

FIGURE 1

U.S. Spending on Technologies to Support Digital Transformation by Leading Verticals, 2018–2020



Source: IDC's Worldwide Semiannual Digital Transformation Spending Guide, November 2018

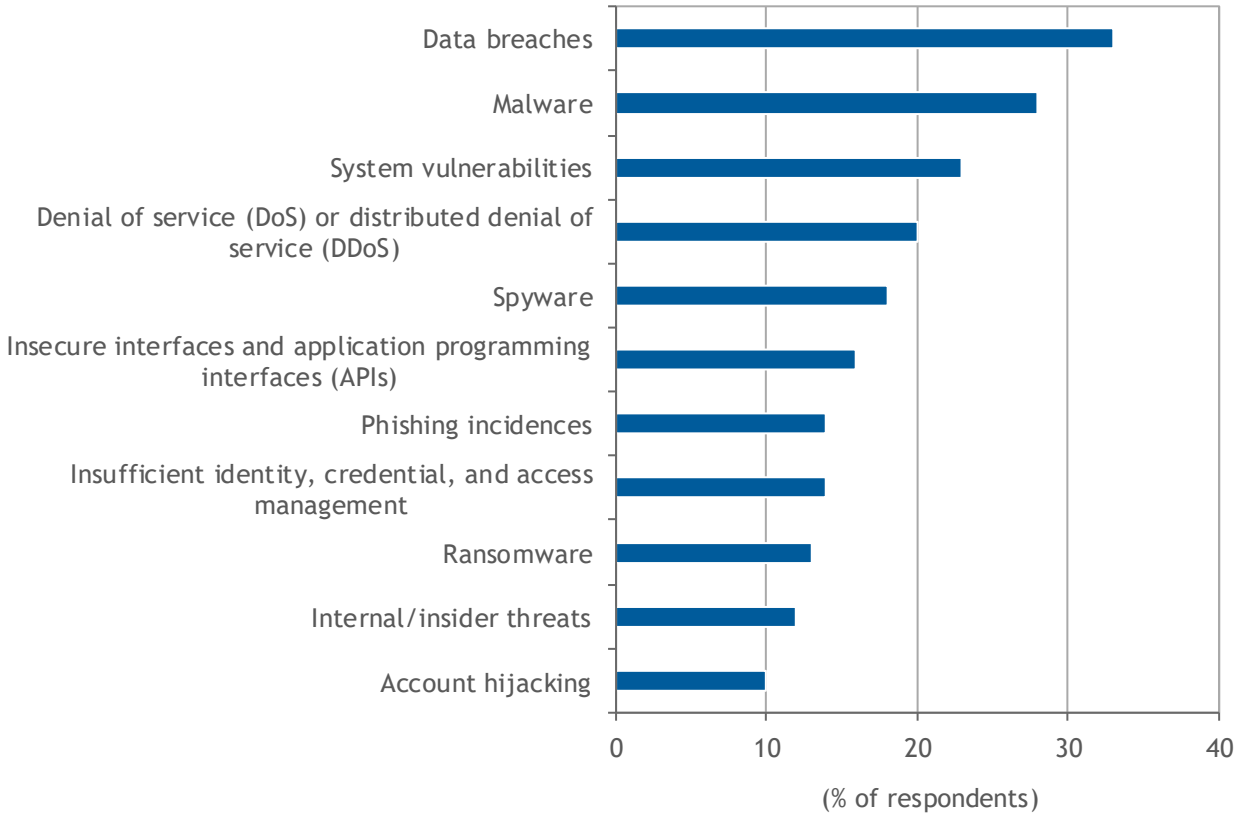
One of the most important challenges for business leaders as they move to the next level, that of digital business transformation, depends upon the establishment and maintenance of digital trust. Without trust, they won't be able to employ digital technologies coupled with organizational, operational, and business model innovation to create new ways of operating and growing their businesses.

It's no surprise that when asked about their greatest concerns when it comes to securing business operations and IT environments, enterprises state that data breaches and system vulnerabilities worry them most and these naturally erode attainment of digital trust (see Figure 2).

FIGURE 2

Top Security Concerns

Q. Which two of the following factors are your company's greatest concerns when it comes to securing your business operations and IT environments?



n = 400

Source: IDC's *Managed CloudView Survey,* August 2018

As organizations explore digital transformation, this same need for "digital trust" becomes obvious. Consumers need to trust the online websites and mobile device-based services they use. Increasingly, they also need to trust the "smart" devices, vehicles, buildings, and cities in which they live and work. At the business organizational level, companies routinely conduct interviews and audits of prospective business partners and service providers to evaluate their trustworthiness for stronger strategic relationships.

In the world of DX, everything is potentially connected to everything else. Data comes into the organization through connected assets, connected employees, and connected processes and as data streams through APIs. This data can be used to extract insights. Those insights can circle back into the organization as improved internal processes. Data also comes in through ecosystem engagements via bots, mobile devices, augmented reality/virtual reality (AR/VR), connected vehicles, and so forth. This data can be turned into actions to be taken when engaging with people and organizations in the ecosystem.

In 2018, IDC asked companies to identify their stage of digital transformation — from ad hoc projects on through to full-fledged organizational transformation. With that information in hand, we also asked them to assess the attention they are giving to digital trustworthiness. DX thrivers (those already executing on DX across the organization) were three times more likely as survivors (those still making DX investments in an uncoordinated and limited way) (50.9% versus 16.7%) to have predefined ways to measure digital trust associated with DX projects and have ways to correlate measurements to DX program success (see Table 1).

TABLE 1

Evaluating Trustworthiness

Trustworthiness Stage	Survivors	Thrivers
Other than a fundamental recognition of the importance of trust, we have not considered the effect of trustworthiness to our DX program.	1.4	1.9
The concept of digital trustworthiness has been a subject of discussions associated with our DX program.	25.0	1.9
We are actively considering the effect of digital trust on our DX program success.	36.1	5.7
We are testing some elements of digital trust in our interactions with business partners for our DX program.	20.8	39.6
We have defined ways to measure digital trust for DX projects and have correlated these measures to our DX program success.	16.7	50.9

Note: For more details, see *The Digital Trust Index: IT Executives Rate the Digital Trustworthiness of Online Institutions and Entities* (IDC #US44316718, September 2018).

Source: IDC, 2018

THE VALUE OF IT TRANSFORMATION IN ESTABLISHING DIGITAL TRUST

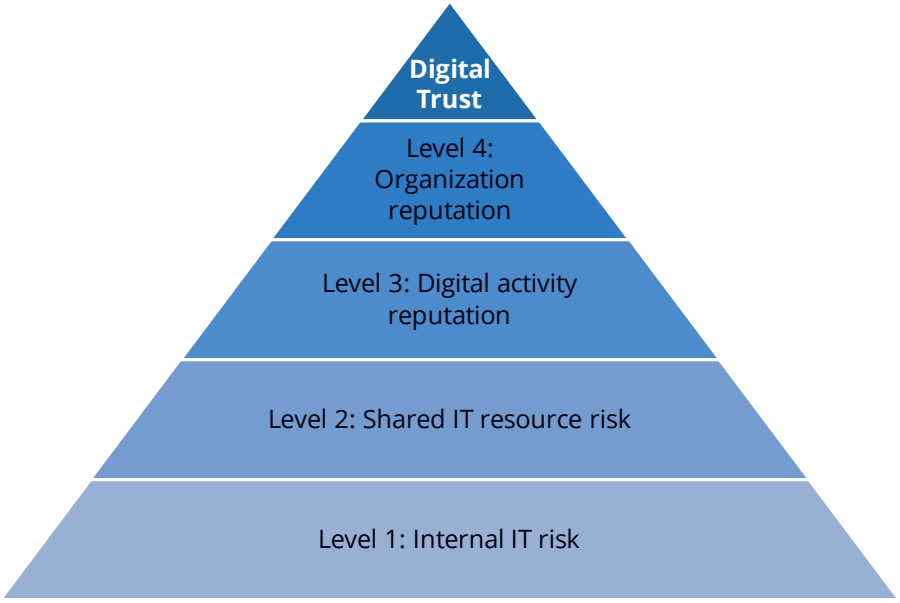
Digital business transformation requires new ways of thinking about business and IT governance that not only protect new IT architectures and new revenue streams properly but also demonstrate a level of trustworthiness among customers, partners, regulators, and other interested parties that drives economic success. IDC describes digital trust in the following way:

> Digital trust enables the decisions made between two or more entities that reflect their level of confidence in each other; these decisions are based on each entity's digital reputation as well as the assurance levels provided by each entity's cybersecurity programs for a proposed digital activity.

IDC created a digital trust framework that describes the levels of trustworthiness (see Figure 3).

FIGURE 3

The Digital Trust Platform



Note: For more details, see *Digital Trust: The Key Driver for Digital Transformation* (IDC #US43986218, June 2018).

Source: IDC, 2018

The digital trust framework describes and categorizes four levels of the most common elements of digital trust that inform the decisions made by individuals and organizations:

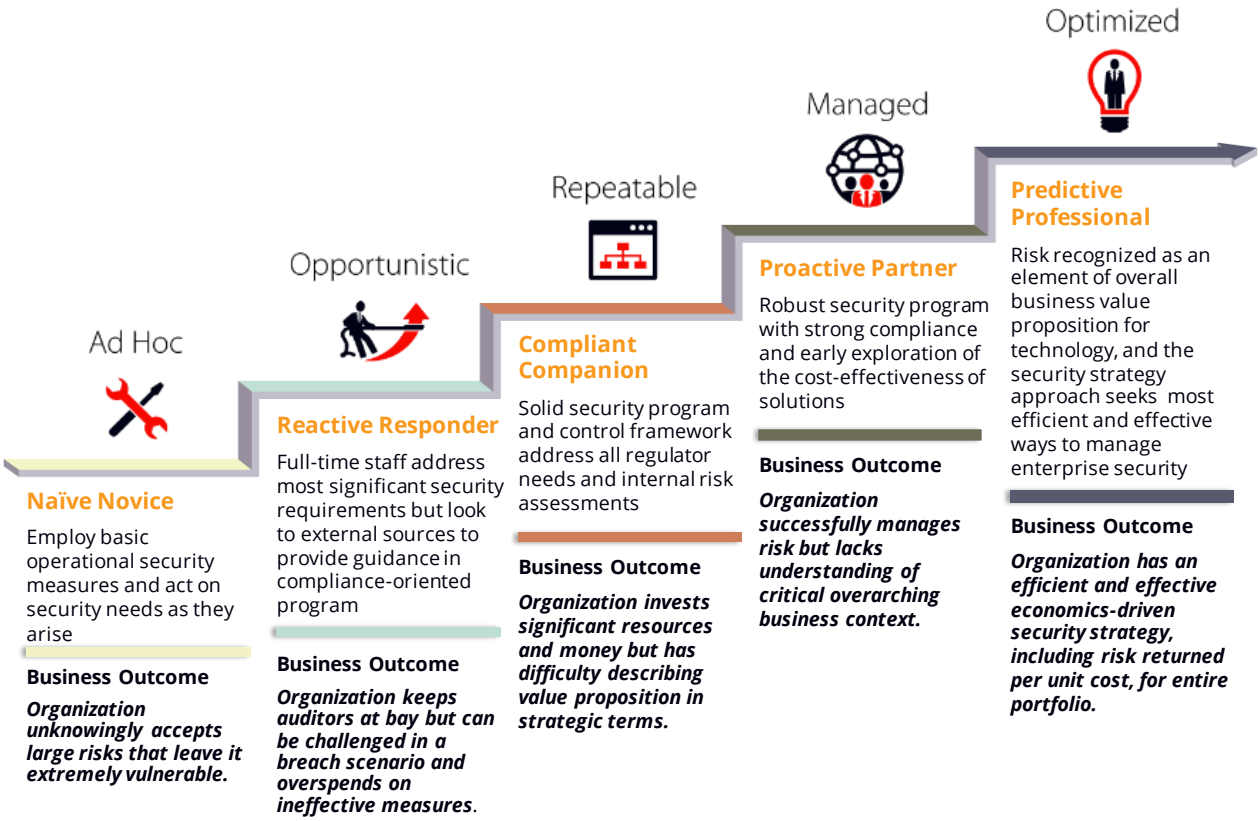
- **Level 1:** Internal IT risk addresses the internal, traditional cybersecurity posture and risk management activities of an organization.
- **Level 2:** Shared IT resource risk addresses the managed risk of the shared technical resources for the digital activity.
- **Level 3:** Digital activity reputation addresses the quality of an organization's reputation in providing or performing some specific digital activity.
- **Level 4:** Organization reputation addresses the quality of an organization's overall reputation for all its digital activities and usually all of its public actions.

Level 4 is primarily the provenance of business leadership. Levels 1-3, however, are all places where IT organizations must play a leading role. The key challenge for the IT organization is to ensure the integrity, fidelity, and control of all data and applications that underpin innovative digital services, without which there can be no establishment and continuance of digital trust.

Level 1 of the digital trust framework should be a given for any organization: implementing a security program that properly addresses the breadth and depth of risk and compliance needs. IDC recommends evaluating the program using a maturity model such as that illustrated in Figure 4.

FIGURE 4

IT Security Maturity Distribution Across Stages



Note: For more details, see *IDC MaturityScape Benchmark: IT Security in the United States, 2016* (IDC #US41000516, February 2016).

Source: IDC, 2016

Organizations at the top of the maturity stack know that security is built not just on technology but also on vision, risk management, people, and process. And thriving organizations are those that leverage:

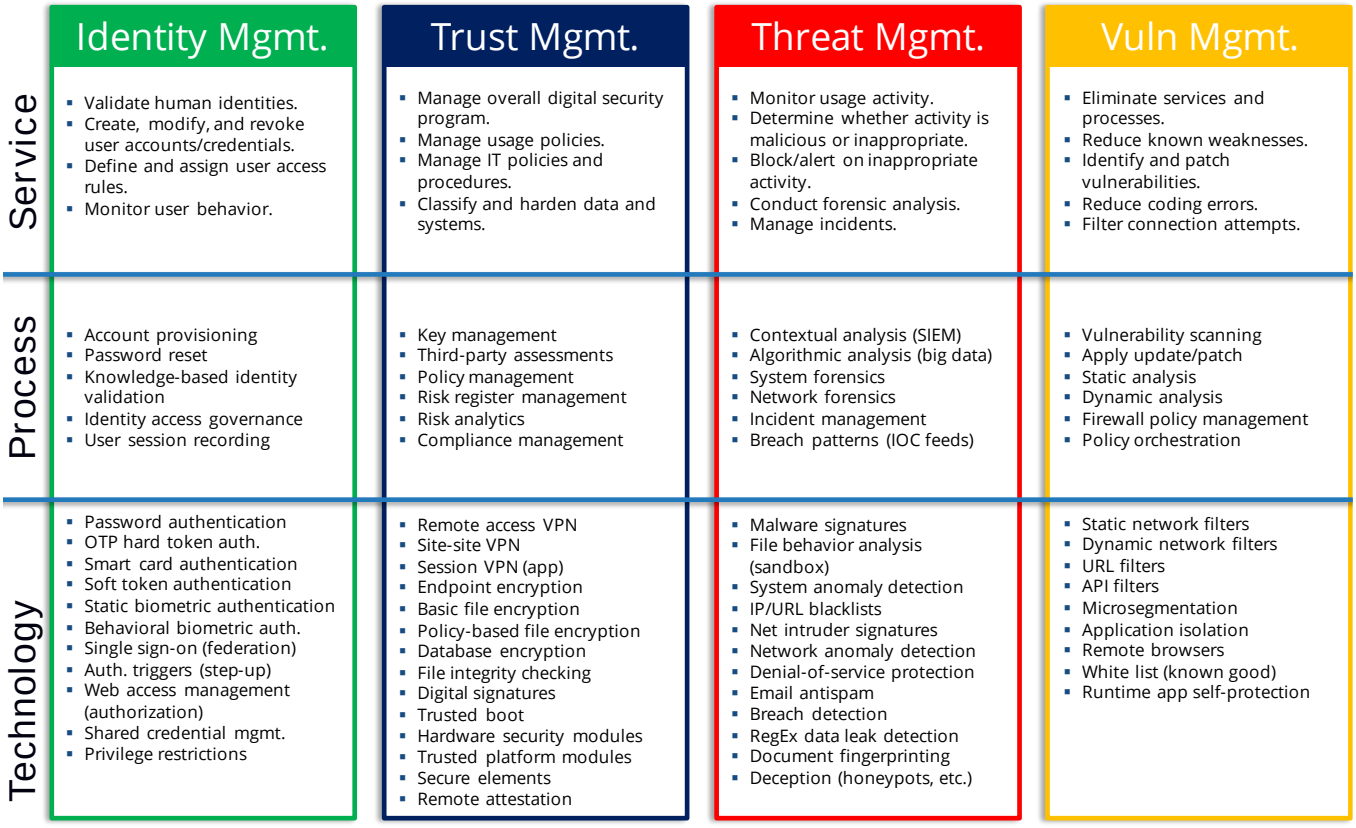
- IT agility to ensure the delivery of inherently and consistently secure compute, data, and network infrastructure in cloud and on-premises locations
- Adaptive/automated networks to allow an organization to securely and quickly process internal business and external customer transactions, maintain operations, and provide a high level of customer engagement
- Next-generation network security to reduce the risk and complexity associated with DX transformations as well as digital activities once established

In particular, the process and technology subdomains describe the following key disciplines found in Figure 5:

- **Identity management:** All manual and automated processes as well as technical solutions associated with human users, accounts, and credentials including provisioning/deprovisioning, authorizations, password resets, authentication, and access control
- **Trust management:** All manual and automated processes as well as technical solutions associated with governance, risk, and compliance including audits, policy management, third/fourth-party due diligence, encrypted communications, data encryption, digital signatures, and integrity hashes
- **Threat management:** All manual and automated processes as well as technical solutions associated with reacting and responding to and recovering from threats, attacks, breaches, compromises, and incidents including security operations and alerts, intrusion detection, threat intelligence, forensics, and incident management
- **Vulnerability management:** All manual and automated processes as well as technical solutions associated with IT system resources including asset inventories, configuration management, vulnerability scanning, patching, penetration testing, firewalls, and isolation/separation/filtering

FIGURE 5

Digital Security Functions



Note: For more details, see *Digital Trust: The Key Driver for Digital Transformation* (IDC #US43986218, June 2018).

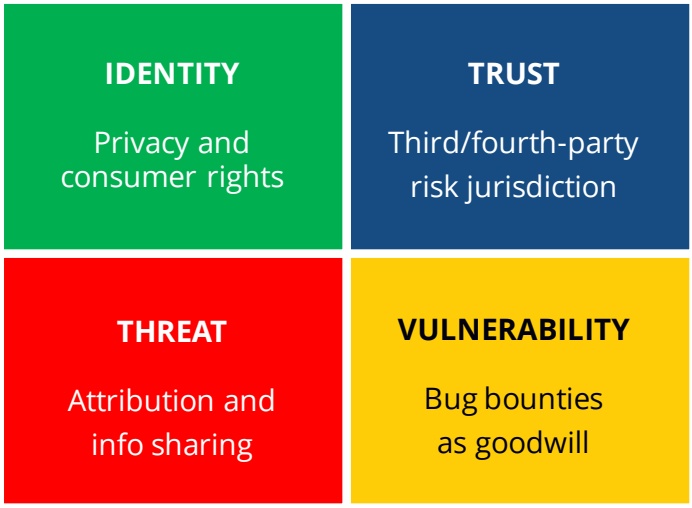
Source: IDC, 2018

The second part of the risk-oriented prescription for digital trust (Level 2) requires securing the resources exposed externally to business partners and customers. The application environment and technical architecture are shared in some way, and thus more care must be given to ensure that the shared level of risk is appropriate for the digital activity being performed. Essentially, this level involves addressing the same control requirements as Level 1 but applied in digital transformation scenarios — ones that typically involve more advanced, distributed, and dynamic architectures that are shared among participants.

To achieve Levels 3 and 4, the four disciplines of cybersecurity (identity management, trust management, threat management, and vulnerability management; refer back to Figure 5) are projected outward as signals or indicators of trustworthiness that can develop and support an organization's IT security reputation. Figure 6 illustrates some examples of engagement that can bolster digital reputation.

FIGURE 6

Levels 3 and 4 — Digital Reputation



Note: For more details, see *Digital Trust: The Key Driver for Digital Transformation* (IDC #US43986218, June 2018).

Source: IDC, 2018

IT Agility

Impact on IT Organization

The foundational elements in building digital trust revolve around IT: internal IT risk and shared IT resource risk. These elements of trust are necessary for any digital activity as time and again some IT breach leads to a loss of trust and ultimately to lawsuits and other losses. The challenges faced by IT organizations across all traditional and cloud-based IT domains include:

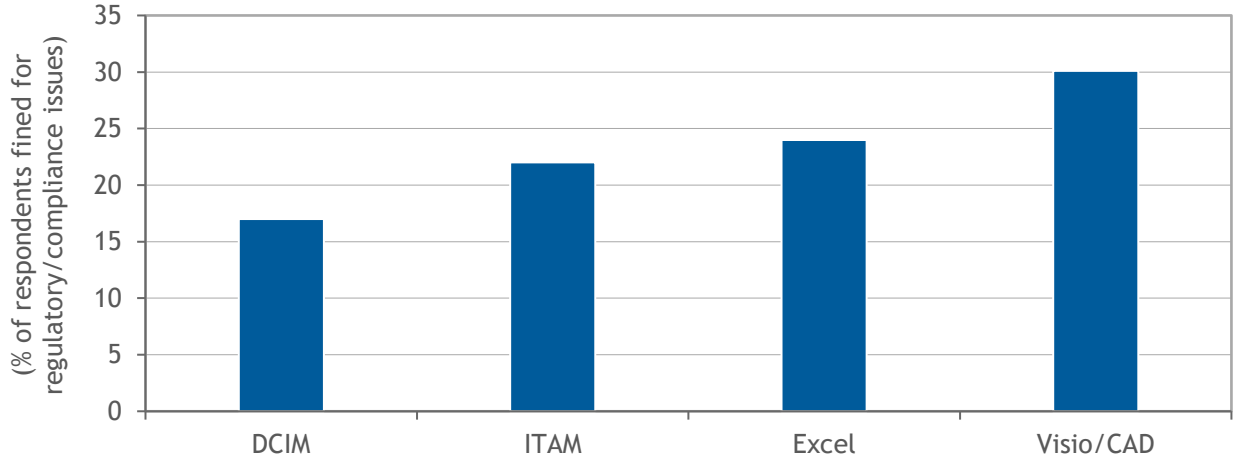
- **Managing vulnerability:** All processes as well as technical solutions associated with IT system resources including asset inventories, configuration management, vulnerability scanning, patching, penetration testing, firewalls, and isolation/separation/filtering

- **Managing new threats:** All processes as well as technical solutions associated with reacting and responding to and recovering from new threats, attacks, breaches, compromises, and incidents including security operations and alerts, intrusion detection, threat intelligence, forensics, and incident management
- **Managing trust assurance:** All processes as well as technical solutions associated with governance, risk, and compliance including audits, policy management, third/fourth-party due diligence, encrypted communications, data encryption, digital signatures, and integrity hashes

Put simply, the first steps for establishing digital trust are ensuring consistency in the configuration of systems; enabling rapid, IT-wide responses to changing threat conditions; and providing a single "version of the truth" for the deployment and use of all resources. This last element is often overlooked, but in a survey of 400 IT and datacenter facilities managers, those that leverage dynamic infrastructure management solutions such as datacenter infrastructure management (DCIM) and IT asset management (ITAM) are a third to half as likely to be fined because of regulatory or compliance failures (see Figure 7).

FIGURE 7

Dynamic Infrastructure Management Users Less Likely to Be Fined for Regulatory/Compliance Issues



n = 398

Note: ITAM and DCIM are considered "dynamic" methods of infrastructure management. Visio/CAD and Excel are considered "static" methods of infrastructure management.

Source: IDC's *Datacenter Facilities Infrastructure Management and Operations Survey,* January 2017

Today, a new generation of IT agility options are emerging built on a standard hardware (e.g., hyperconverged) platform and software-defined foundation. They deliver a standard portfolio of cloud services (instances, containers, serverless) that make it possible to deliver consistently configured compute, storage, and network resources. As these IT agility systems also provide automation capabilities, IT teams can quickly implement configuration changes/patches across the entire environment in response to emerging threats or changes in compliance policies. Most importantly, the standard orchestration services embedded in IT agility solutions provide a data-based foundation for audits and governance risk assessments, which are at the heart of digital trust efforts.

Adaptive Networking

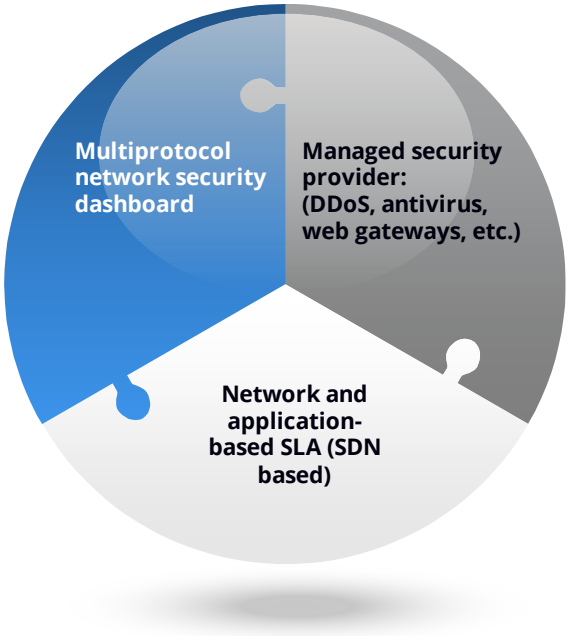
Impact on IT Organization

The emergence of cloud-based applications and hybrid access protocols presents significant IT challenges. Applications must be configured, integrated, and synchronized securely across a diverse range of network protocols. This requires enterprises to nurture and train new skill sets while developing a talent pool to meet new organizational requirements. The proliferation of connected devices will also add management and security complexities to this process. There is a significant level of effort and investment underway for implementing security at the chip level leveraging Trusted Platform Module (TPM); however, an overarching requirement will continue to be policy management and event reporting, with the capacity for network management system oversight and updates. This will go well beyond the capacity of most enterprises.

Devices are developed with smart security-enabled chipsets, but this should be the last barrier of defense. Unless enterprises restrict and isolate vital aspects of their LAN and WAN environments, a holistic approach to network-based security will have to be developed that expands security beyond the network parameter to embed consistent security protocols across all network layers (see Figure 8). A comprehensive security dashboard is a must for enterprises that face a range of security threats. Depending on their network environment, this could include distributed denial-of-service (DDoS) mitigation, remote access security, and backup and disaster recovery. Service providers have a comprehensive view of millions of threat attempts emanating from endpoints spanning the globe and are best placed to provide enterprises with the best scenarios for a defensive strategy.

FIGURE 8

Key Elements for Network Security



Source: IDC, November 2018

Key Product/Tech Developments Required

The complexity of managing a hybrid networking environment demands an efficient network security strategy, and embedded security across network layers in a consistent framework is a logical choice. While a dashboard can provide an integrated view of threats and developing trends, predictive analysis is an additional tool that can be adopted to manage security.

Artificial intelligence/machine learning (AI/ML) technology is already a tremendous tool that is used extensively in managing network operations. It is used to flag anomalies for adaptive networking where resources can be marshaled to the appropriate points as necessary. Thus it is natural that AI/ML can be adopted for network security. AI can automate processes that can detect and block anomalies and malicious actions at a much faster pace than humans. ML is complementary in that it can be instrumental in the deterrence and preempting of unknown security threats by building up a knowledge base of known threats and continuously learning to block possible vulnerabilities. Once a defense system has been implemented, an executive dashboard for monitoring and reporting is indispensable. As mentioned previously, the dashboard can comprehensively integrate and summarize the performance of multiple and disparate network elements. With their deep and broad access to global network traffic patterns, service providers are adequately positioned to provide this perspective as well as prescriptive, proactive deterrence across the network spectrum.

Benefits Gained

Network security is essential for the mitigation of negative business impact due to cybersecurity threats. Deterring distributed denial-of-service attacks that can slow down transactions is also important to maintaining operations and the required level of customer engagement. A robust network security layer that can deter crippling network-centric attacks from packet floods is essential, as is tracking network layer attacks. The network is a major line of defense for cybersecurity threats, which can cripple enterprise operations and bring business transactions to a halt. The network edge, with billions of connected devices, web gateways for information, and financial transactions, is a potentially vulnerable point of attack for a wide range of malicious threats that have proven to slow down or even cripple business operations.

Implementing a comprehensive network security strategy that protects all aspects of network operations is essential. Network traffic management at the edge of the network will be a crucial issue in the coming years. Implementing a heuristic network management policy for traffic management that leverages DPI and event management will be both cost-effective and secure aware. It will be cost aware because analytics at the edge will discard irrelevant data at the edge. It will be secure because only network-based security tools will deter malicious attacks from traversing the enterprise WAN.

A network dashboard that can provide an in-depth analysis of network traffic by isolating and identifying traffic anomalies to specific devices, ports, and IP addresses is invaluable for enterprises. Enterprises can implement application-focused security and traffic policies, thereby optimizing network bandwidth and leveraging service provider QoS tools and capabilities.

ESSENTIAL GUIDANCE

The evidence that digital trust drives the success of business transformation continues to build. This trust requires more direct attention because it evolves from being implicitly intuitive into a strategic characterization of the progressive digital transformation enterprise. This change requires measurement of trustworthiness by involving all key constituencies — employees, business partners, customers, and overseers.

Digital business transformation requires new ways of thinking about delivering and using IT and network assets as well as cybersecurity. These efforts are not just properly protecting new IT architectures and new revenue streams but also demonstrating a level of trustworthiness and control among all interested parties that drive economic success.

Your organization's digital trustworthiness is ultimately linked to both technical risk and reputation. Your organization will need to ensure that it's technically adept at securing all the DX projects and IT environments that you adopt. Often, this can be achieved most quickly by leveraging a partner with the IT, network, and security expertise required to control data, applications, and digital services across edge, core, and cloud locations.

The reputation part of digital trust is mostly driven by technical expertise, but it is being assessed by others — business leaders, business partners, and customers. Your team must look for technology partners that can help you communicate to all about the ways an organization is protecting its environment and ensuring that shared data resources are properly handled. Rather than waiting until a breach to take this step, DX thrivers are those that take explicit measures to define the controls in place and provide meaningful metrics as a way to demonstrate excellence and reinforce trust.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com