INCISIV

In partnership with:

>_cmd

Digital Transformation & Security: Executive Learnings & Insights

This Market Snapshot, is part of Incisiv and CMD’s effort to deliver management and executive level insights on the digital transformation process.

Unless otherwise indicated, all data in this Market Snapshot is from this Incisiv’s industry data pool.

Unprecedented challenges and threats due to the global pandemic have compelled businesses to redefine and accelerate their digital transformation roadmaps.

Led by a need for improved stakeholder experience (customers and associates) and operational efficiencies, security and adoption of new technologies are among the top objectives of the transformation programs.

Top 3 challenges faced by an organization as they implemented their digital transformation programs

- Security
- Budget Allocations
- IT Infrastructure

Embedding security into the scope and design of a digital transformation roadmap reduces risk and improves digital resilience

Digital transformation initiatives and focus differ by digital maturity

Digitally mature organizations

Focus: Modernize IT infrastructure and increased investments in security solutions for increased security

Organizations that have completed their digital transformation journey or are more than halfway to completion have an increased focus and budgetary allocation for security solutions.
These organizations believe that robust security and stakeholder go hand in hand.

Organization who have completed their digital transformation journey are willing to spend more.

Key reasons:

- Lessons learned and realization from executing the digital transformation roadmap that security is the foundation of enhanced stakeholder experience

Digital laggers

Focus: Operational capabilities, data and Infrastructure migration

Organizations that have just started their digital transformation journey or are still in the planning phase are more focused on operational capabilities and infrastructure. These organizations focus their top priorities around stakeholder experience and operational efficiencies.

Organizations that are still in the early stages of their transformation journey are unsure of their investments in security solutions.

Key reasons:

- The value of security investments is not clear
- Ownership of security is outside the transformation journey of an organization.

Initially, a vast majority of organizations considered security requirements outside the scope of digital transformation.

Now digitally mature organizations have realized the importance of including security requirements and solutions as an intrinsic part of the core digital transformation roadmap.

Robust security is a foundation element that is an essential must to realize benefits from digital transformation programs.

Firms are turning their focus on a mix of emerging technology and solutions that have been around for years to build the foundation of their security architecture

2 Factor Authentication (2FA)

Authentication is a form of access control. A 2FA process requires 2 different authentication factors to establish authority. This means that a user must prove their identity in 2 different ways before being granted access, thereby increasing security.

Privileged Access Management (PAM)

Critical apps like web, database, and application servers run on Linux. A layered approach to PAM gives visibility and control to protect Linux accounts and credentials. Proactive management and ongoing reporting become easy and repeatable.

Guardrails

Guardrails are quiet security tools that mainly focus on threats that are most likely to be exploited and are susceptible to attack instead of focusing on every vulnerability. Guardrails integrate with open source and commercial security to pin down urgent fixes and implement the same.

Real Time Authentication

A Real-Time Authentication process requires approvals for any changes made to commands or files in a system. It is like an additional security protection layer to ensure that the right changes are made. Approvals can be policy-based or manual.

#1 Objectives of the digital transformation journey

Key objectives of the digital transformation journey for most organizations are improved stakeholder experience, operational efficiencies and increased cost saving, improved productivity, and enhanced security. However, the COVID-19 pandemic has changed this to a large extent. Even though organizations identify customer centricity as the top objective of their transformation journey, companies are increasing their focus on employee experience (work from home) and operational efficiencies related to policies, regulations, and processes. E.g.;

- In healthcare or retail organizations, objectives of digital transformation have pivoted to streamlining operations or increasing productivity
- In travel and hospital, the objective of digital transformation has pivoted to flexibility and improved visibility

CXO’s

50%

of CXO’s have selected Improved Regulatory Compliance as their primary objective and Improved Associate Experience as their secondary objective.

Managers

78%

of managers have selected Improved Customer Experience as the primary objective and Improved Security as their secondary objective.

COVID-19 is the primary reason for accelerating digital transformation journey for

100%

of the organizations in Banking, Healthcare and Retail.

> “
>
> Cmd has brought us a massive paradigm shift in how we audit logs – they have enabled us to intelligently automate the mundane and empower our previous talent to focus on the more exciting aspects of their jobs.
>
> **- Tomas Honzak**
> **Chief Information Security Officer, GoodData**

#2 Decision influencers: Primary influencers in selecting security solutions for digital transformations

The role of a CTO has evolved from just keeping track of emerging IT trends, policies and generating ideas to improve an organization's product or service. Now, the role of a CTO is supporting the digital transformation of a company and impacting overall business strategy. Since IT innovations and strategic business transformations are at the heart of a digital transformation journey, it is natural for a CDO or CEO to be responsible for leading it while leaning on CIO/CTO to support core technology aspects.

The CIO/CTO takes responsibility for developing data processing strategies, technology needs, security, and assessing IT skills during the transformation journey.

32%

of all respondents have selected the CIO as the primary decision influencer.

67%

of CXO's have selected the CTO as the primary decision influencer in the digital transformation journey.

36%

of all respondents selected the CTO as the primary decision influencer.

100%

Organizations in the banking/financial and retail sector have the CTO lead digital transformation.

> Cmd helped us identify and normalize our deployment process allowing us to focus on cloud edge use cases. We were able to actualize our digital strategy plans faster than we thought was possible.
>
> **- Will Tarkington**
> **Director, Head of Security at Zenefits**

#3 Framework: Most preferred security framework

When it comes to security, organizations prefer taking proactive measures to prevent threats and attacks. Center for Internet Security (CIS) standard is the top choice for most organizations. It provides the foundation organizations need to start building their digital transformation strategy.

It is closely followed by the International organization for Standardization (ISO) framework. ISO frameworks have wide adoption in many industries like energy management and medical devices.

CXO's

100%

of CXO's have selected CIS as the most preferred framework.

Managers

39%

of managers have selected CIS as the best security framework.

36%

of managers have ISO as the preferred security framework.

The main objectives of security frameworks are to:

- Provide a measurable way to examine the security of an organization
- Create security benchmarks
- Identify key strengths and weaknesses
- Provide risk mitigation strategies

The top 3 security practices that are important for the success of digital transformation initiatives are:

- Threat Detection
- Cloud Security
- Privilege Access Management

Source: State of Digital Transformation - 2021 by Cmd and VIB

#4 Spend: How much should you spend on security?

The global pandemic has changed the way organizations invest in security solutions. The shift to a remote, distributed work environment has increased the need for security around access management and network security. Digitally mature organizations that have recognized the benefits of digital transformations are increasing their spending on effective security solutions.

However, digital laggers(organizations that are yet to implement digital solutions or are in the first stage of their transformation) are more skeptical about their spending on security solutions.

56%

of respondent's advocate spending >10% of digital transformation budget towards security.

71%

of respondents from companies with revenue > $1Billion are willing to allocate 10% or more of their digital transformation budget towards security.

16%

of the respondents believe that <5% of digital transformation spends should be allocated to security.

> Cmd saved us 50% in compliance costs and from hiring 3 additional engineering head counts.
>
> **- Tomas Honzak**
> **Chief Information Security Officer, GoodData**

Key challenges

Organizations feel that Budget Allocation for security tools is the top challenge faced while securing digital transformation programs.

Source: State of Digital Transformation - 2021 by Cmd and VIB

Digital transformation doesn’t come easy.

Leaders must evolve into transformers of their organizations’ culture and strike the right balance between short-term improvements and long-term value.

An integrated digital transformation plan should emerge with clear cross-functional ownership and provision for core features like security and infrastructure to ensure success.

Execution roadmap: Short term improvements will provide long-term value

4 key actions organizational leaders should consider to integrate security as part of their digital transformation journey

Align security strategies to business goals

This aligns actions with business goals and ensures a balance between risk mitigation and enabling innovation.

Find a balance between risk and reward

Understand whether the risks posed by digital transformation processes out-weight the cost of mitigating them through security solutions.

Drive productivity and convenience

Digital transformations should support new business models that appeal to customers. Models such as secure use of online resources for secure sign-on.

Build a security culture

Security solutions must be the drivers for larger business goals. Businesses need to embed security at the very core of their systems and processes.

In partnership with:

>_cmd

Cmd, based in beautiful Vancouver, Canada, delivers runtime security to global brands, financial institutions, and software companies that need infrastructure detection and response capabilities. The Cmd platform observes real-time session activity and allows Linux administrators and Developers to take immediate remediation action. Organizations will sleep easier and save time and money by securing their infrastructure with Cmd.

www.cmd.com

INCISIV

Incisiv is a peer-to-peer executive network and industry insights firm for consumer industry executives navigating digital disruption.

Incisiv offers curated executive learning, digital maturity benchmarks and prescriptive transformation insights to clients across the consumer and technology industry spectrum.

www.incisiv.com