EXECUTIVE REPORT

Digital Transformation Executive Report

An Examination of Best Practices for Balancing Security, Strategy, and Productivity in Your Digital Transformation

Table of Contents

A New, Digitally-Driven Security Perspective for CIOs

The digital revolution, also known as the fourth industrial revolution, is in full effect. The way business is conducted is more dependent on technology than ever before. All businesses are in different stages of transforming their business and client engagement models resulting in massive amounts of data, adding unprecedented complexity and change to the traditional network. This shift is putting greater pressure on CIOs, moving their roles away from being an operational requirement, to a revenue-generating asset to a business' overall success. While digital transformation brings about tremendous opportunity, it also introduces larger amounts of complexity and risk to a business.

CIOs today need to reframe their position on security in order to succeed in this digital era. Having executive security leadership in place is an integral starting point that enables businesses to be more successful, so long as security is approached in a collaborative fashion during the early architecture stage. At present, security remains an afterthought at many companies[4]. CIOs can set a paradigm shift in motion by ensuring that the security side of information technology gets a seat at the table and has a contributing voice in terms of business direction. The cost of compliance and security can be an obstacle, particularly where retrofitting is concerned. At the same time, it is crucial for CIOs to recognize that when you do not put forth the right level of investment, the outcomes for the business will be far worse than the initial cost of security.

Security Challenges of Digital Transformation

The Digitally-Driven Environment Paradigm

As digitalization continues to progress, an interesting paradigm is evolving. Enterprises push technology teams to accelerate the pace of innovation, drive greater productivity and efficiency, and capitalize on new economic models. Consider the impacts of cloud and IoT: business must move at a faster pace as these technologies thrive. Technology assets have been pushed beyond the bounds of traditional constructs, with access enabled anywhere, anytime, and via any type of device. In fact, 52% of enterprises have already experienced significant disruption to their industries as a result of digital technologies.1 Things like the introduction of bring your own device (BYOD), smart offices, back office systems that are now internet-facing, and many more, have revolutionized the way CIOs work, as well as the impact they have on an organization. This is forcing a change in IT, away from a purely operational overhead to a centralized revenue generating function critical to the business. This strategy has been widely adapted around the world.

Yet despite the global adaption of digital transformation being so rapid, a large number of organizations understand that this transformation brings about large amounts of risk. In fact, according to Dell Technologies, 48% of business leaders believe that the more we depend upon technology, the more we have to lose in the event of a cyberattack.

73%

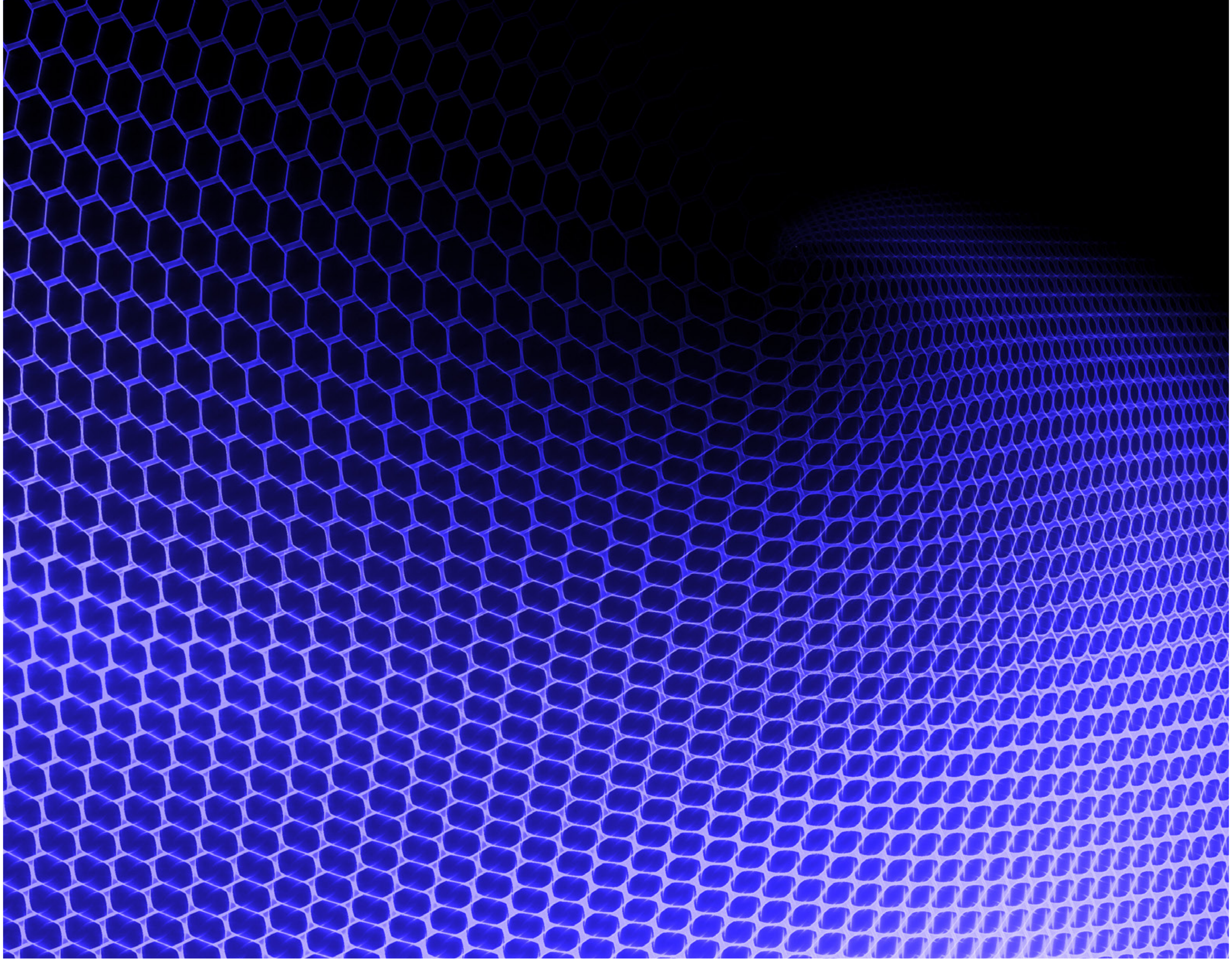
of businesses are in agreement that a centralized technology strategy needs to be a priority for their business.

66%

feel incentivized to invest in IT infrastructure and digital skills leadership.[1]

> “If you’re monitoring and managing the flow of where data is going to, you can use technology to improve your security posture. However, there is a balance between exposing assets and data in a self service way and enhancing security capabilities to actively secure your distributed environment.”

Matt Diamond,
VP of IT at Secureworks



How Digital Transformation Initiatives Are Impacting Security for Enterprises

This paradigm is challenging the structure of conventional security models and causing leadership to question their day-to-day responsibilities versus those of their chosen technology vendors, as well as evaluate the security postures of critical service providers from a different angle. Today, enterprise security should be a continuous process that can be a competitive edge when incorporated as part of the initial design. When considering all of the needful security elements in the digital realm, businesses face a challenging environment in which to mature information technology; one that offers organizations a highly scalable, fast-paced, and agile route to market, yet also exposes them to increased risk if not managed appropriately.

Consider, for example, Amazon Web Services. With increasing frequency, businesses are putting more assets into public cloud environments. Amazon has a shared security model, and while many companies are aware of the concept, some do not fully understand the implications, or how to evolve their security strategies to adequately fulfill their responsibilities. A mature security strategy includes the people, practices, standard and control procedures, and technology that must be brought to bear to secure a cloud-based environment. The rise of the shared security model is a primary challenge as businesses pursue digital transformation.

Concurrently, the attack surface and operational complexity are growing rapidly as enterprises and their partners continue to rely on the public cloud. This growth is further compounded as the decentralization of responsibility about access, buying, and design architecture decisions are pushed to the edges of the organization.

The decentralization of digital assets has upended the customary approach to security, and as changes continue, the necessary internal people, processes, and technology have to be implemented at the same pace, but usually are not. Too often, there is a gap between the deployment of innovative technology and the security resources necessary to support its operations.

It is true that the more organizations step away from the idea of a traditional network and infrastructure, and the more data is brought into a business, the more the business has risk of data breach. Conversely, it is important to recognize that technology can also be used to reduce risk when integrated properly, assuming you are continually assessing the state of your applications and infrastructure.

All organizations are operating their security programs at varying levels of maturity. The more mature, the more likely it is for security to be involved from the onset of a new technology initiative. With the right approach, security allows businesses to get to market faster, and with the appropriate level of risk tolerance and management. On the other hand, businesses that lack a centralized security strategy often rely on more reactive tactics, are viewed as slowing the business down. The problem is, if security is not incorporated into design decisions upfront, regardless of the technology, the security team will have to rebuild scaffolding retroactively, which ultimately disrupts go-to-market.

57%

of businesses are struggling to keep up with the pace of change.

93%

are battling some form of barrier to becoming a successful digital business in 2030 and beyond.[2]

“I don’t believe data privacy and security are barriers to digital transformation—rather, they’re part of it. If a business is doing a digital transformation and not bringing those two aspects along, then it will be a failed journey.”

Rob Scudiere,
SVP of Engineering and CIO at Secureworks

Further, as a consequence of a digital transformation, the number of systems that weren't designed to be exposed to the internet has become glaringly apparent. Financial institutions, for instance, are grappling with legacy backend systems that were never intended to be IP accessible from the internet. Often, people bring these systems online and introduce a higher level of security risk than would be engendered by a modern system built from the ground up. As all companies are working to capitalize on new economic models, the pressure to modernize legacy systems intensifies.

Another byproduct of digital transformation initiatives that affects security is the myriad of tools that people have at their fingertips to improve their efficiency. While they are empowered to achieve more, faster, they are also able to carry out activities independently that often create threats in the environment. For example, users who use openly available development and runtime environments sanctioned by corporate IT, create new business applications for consumption by others, often referred to as Citizen Developers, who are ignorant of security best practices exemplify this tendency of creating inside risk, although often unintentionally. Digital transformation allows decentralization of technology innovation and speed advances of businesses in their respective markets, but also creates more insider threats. While not of the malicious variety, these types of threats expose companies to more risk due to a lack of understanding of how to develop new capabilities effectively and securely in a decentralized model.

+50%

of businesses are making do with outdated technology that can't work fast enough, suffer from data overload, privacy and cybersecurity concerns.[2]

Data Privacy and Security Concerns Create Barriers

Data privacy and security concerns are also a frequently-cited barrier to the progress of digital transformation. It is true that the cost of data privacy today is higher that it was historically, largely as a result of new and growing compliance requirements, such as GDPR. But do these security concerns have to be barriers?

Not necessarily. In fact, data privacy and security should be more accurately considered an enabler to any digital transformation. You have to maintain security and data privacy practices regardless of your initiatives. However, focus will likely shift to changing how sensitive data is actually anonymized, such that the high-risk data you are carrying is minimized. Going forward, Personally Identifiable Information (PII) will be significantly more expensive to maintain in comparison with traditional information. This will impact all businesses differently, depending on individual goals for digital transformation.

As mentioned, data privacy and security are adding to the overall costs of digital transformation initiatives; expenses can originate from numerous dimensions, especially when leveraging technology partners.

According to Gartner, IT services will be a key driver for IT spending in 2019, when the market is forecast to hit $1 trillion, an increase of 4.7 percent from 2018.[3] As dependence upon IT service providers increases, a new dimension of security considerations surface, including:

- Onboarding
- Understanding security practices
- Whether third-parties leverage subcontractors
- Legal terms and how they impact your own customer base
- How to operate in different countries

SaaS, Boundless Networks, and Well-Resourced Hacker Communities Shift the Threat Landscape

With many digital transformations comes a higher dependency on cloud-based SaaS tools, like Microsoft Office 365, for instance. This introduces the capability to build content in disparate locations beyond the data center, whether from a mobile, tablet, or user compute device. This gives users in an organization greater freedom to communicate and collaborate, leading to beneficial business outcomes. However, failing to properly configure security and data privacy that is compatible with Microsoft prior to the introduction of the tool into your overall business strategy generates risks. As a result of greater freedom, end users are now responsible for security risks within the shared security model that previously did not exist.

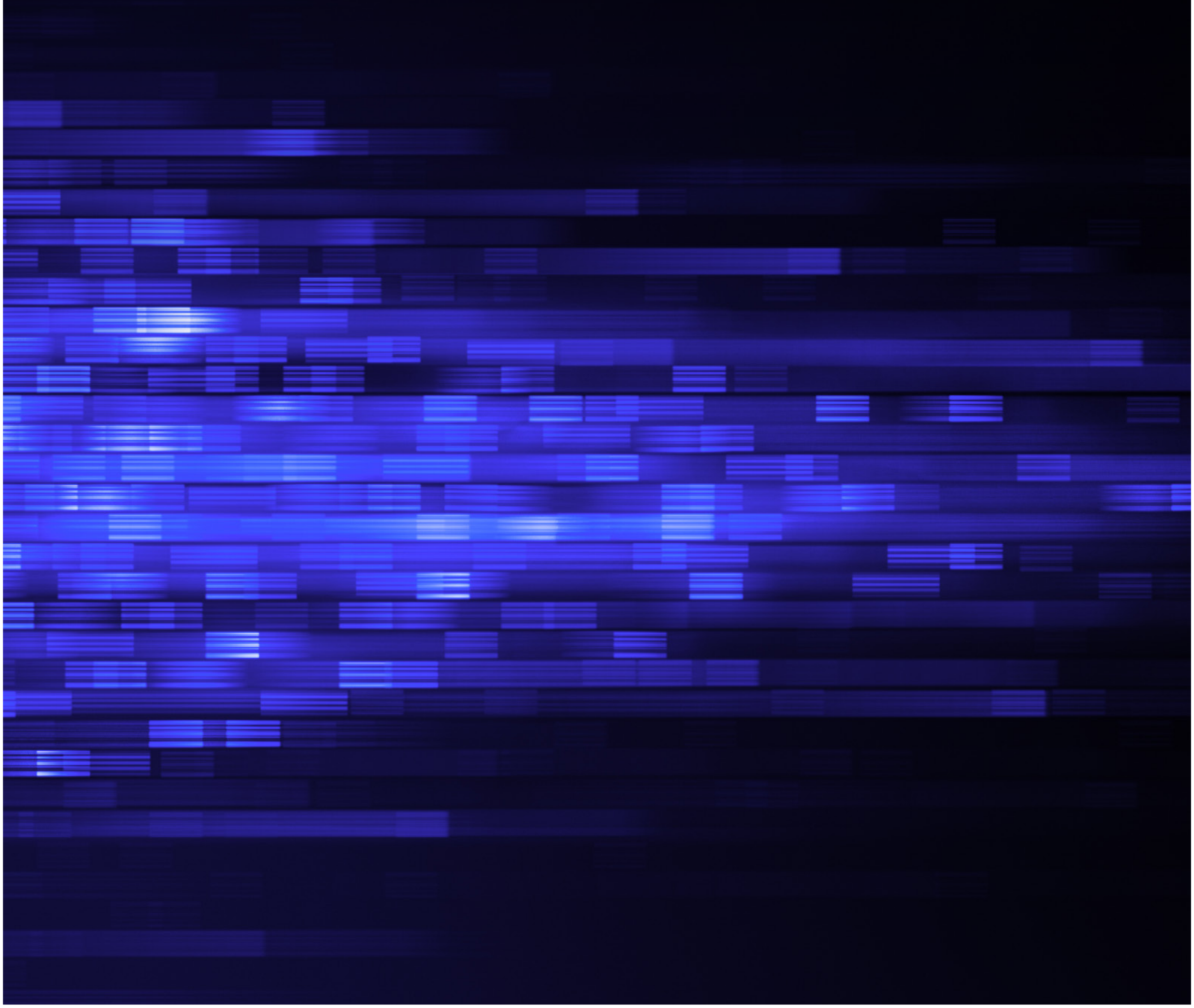
The attack surface has expanded because computing no longer takes place in internal data centers exclusively. Data has become the crown jewel, and enterprises must understand precisely what data they have, as well as where it is traversing both inside and outside the corporate network. It is a daunting challenge.

Added pressure comes from understanding the identity and access privileges of individuals who need to interact with data. This obligation is not focused merely upon onboarding an individual at their entry or departure; it involves the full lifecycle of an employee at an organization, and the onus is on all businesses to ensure the right identity and access management governance model is in place. The ideal governance model is flexible enough for people to do their jobs successfully, but exerts enough control to understand who is getting access to what data, and for what purposes.

It's also critical to note that today's prevalent attacks are wildly evolving. The hacker community is very well resourced; they have the ability to collaborate and monetize new techniques at a pace much faster than an individual vulnerable businesses can, thanks to on-demand collaboration and infrastructure resources.

“Two-factor authentication and vulnerability patching may seem like extremely fundamental security practices, but we often see organizations failing to implement these important security hygiene practices.”

Rob Scudiere,
SVP of Engineering and CIO at Secureworks



Essential Actions for Protecting Business in the Digital Era

Despite the complex security challenges facing organizations on their digital transformation journey, all is not lost. A well thought out security strategy that enables the business while reducing risk is possible and ensuring it comprehends some of the following tactics, ensures credibility.

- **Remember the Basics: Two-Factor Authentication and Vulnerability Patching**
  It may seem obvious, but remembering the basics of security is key. Two-factor authentication should always be enabled. It is of equal importance to maintain a vulnerability-patching program that is timely and indexed onto the highest threats that are coming in. Those two fundamental actions are still incredibly important.

- **Systems Integration for a Cohesive Security Architecture**
  Businesses today need to integrate systems and create a cohesive security architecture. You must ensure that systems you are supposed to be monitoring are integrated, as well as enabling automated responses. The environments of today are extremely dynamic, especially in the cloud, and your ability to assess and continuously monitor those environments must be equally so. It will not be long before all systems are codified, which necessitates software-driven responses in order to keep up with the speed and scale of business. In the past, a proverbial fence was built around crown jewels. Now that malicious actors have new ways to impact your posture, such as credential theft in order gain administrative control and bypass the perimeter, the way security detects threats based on “trust” of the individual user behavior is critical.

- **Training and Awareness**
  Security needs to be top of mind for everyone, regardless of role. Training, education, and awareness about phishing attacks are not negotiable, particularly if they can reduce the risk of stolen credentials. This is not exclusive to employees; it includes the C-suite and board. In fact, the higher the position, the higher the target for intellectual property. Furthermore, high-level roles are more likely to be traveling, handling higher value data, and are engaged in more critical business process and so on. Accountability must go along with training, and tone from the top will help to reinforce this.

- **Visibility**
  Visibility is critically important to the successful execution of digital transformation. Simply put, you can’t defend what you can’t see, and because digitalization is fast-moving, some components of business will operate outside of internal infrastructure as they see opportunity, but need speed and scale to be able to execute. In the name of innovation and advancement, employees incentivized by growth metrics may work outside of the standard model of governance and established practices, putting assets in places where the security team has no visibility. This creates a natural tension between time to market and risk tolerance. Establishing full visibility and management capabilities, while implementing processes that govern but allow “fail fast” innovation are crucial to balance business enablement with security.

59%

of enterprises believe their workforce isn’t sufficiently security savvy.[2]

64%

of organizations admit to not acting on intelligence in real-time.[1]

- **Effectively Introducing Automation into Threat Remediation**
  On the advantageous side, greater visibility into different parts of the security environment is becoming more widely available. On the other hand, all of these parts are shifting and moving constantly, which brings about the challenge of getting remediation in place efficiently for known vulnerabilities, and using technology to orchestrate and automate actions to contain security threats with higher confidence.

  Automating the remediation of the threats in a way that continually drives more efficiency, shortens the cycle time, and decreases the cost of the remediation, is one of the biggest security challenges of the digital era, but can be done!

- **When It Comes to New Technologies, Emphasize Security Before Design and Deployment**
  Leaders need to ensure that security is a continual, and iterative design process between IT, Security and Citizen Developers who together aim to achieve a common goal. This means putting the emphasis on security during design when it comes to new technologies. As organizations become more mature, security efforts extend beyond a checkbox review of new technology purchases and become an enabler for faster risk reduced growth.

- **Future-Proof Your Security Strategy to Continually Advance Effectiveness**
  The end state of digital transformation shifts continuously; understanding this is key to future-proofing security strategy. Individuals will need to be able to access any number of devices, as well as communicate through the open internet and into different areas of the company. The right security strategy should anticipate those needs as table stakes. People, processes and technology must remain agile and prepared for the continued digitalization of business as we know it today.

- **Make Security Part of Business Nomenclature at the Top**
  Cybersecurity is a C-level conversation. Driving revenue growth and richer client interactions while reducing business risk is a shared objective across all leaders and must be communicated to all employees as such. Part of future-proofing your security strategy relies on aligning it with the direction of business and forming partnerships between business leaders so that security is viewed as an enabler to the vision, and not just a necessary, pre-execution checkbox. If check boxes are required pre launch you have already failed.

- **Iterate Your Security Strategy to Evolve with the Business**
  Because technology and security change so quickly, security strategies must be revisited regularly. It needs to be a constant reevaluation process with periodic adjustments depending on both the changing direction of the business and technological advances. Remember that security is a living, breathing strategy, and now that digitalization has taken hold, it will need to continue to adapt as more information and systems become accessible globally.

> ***“Mature organizations know that security is a continual conversation with those in the buying, designing, and implementation process. It’s an open discussion with the security team, not an afterthought or a pre-deployment checkbox.”***
>
> ***Rob Scudiere,***
> *SVP of Engineering and CIO*

The Benefits of a Hand-In-Hand Relationship Between Security and Digital Transformation

Security as a Catalyst for a Competitive Edge

Now that security is top of mind for virtually all organizations, the consequential level of scrutiny put forth by partners and customers has risen significantly. To the benefit of businesses, security can be used to improve client conversations about what you are bringing to market and how you are doing so securely. Security becomes a key differentiator when you are able to demonstrate that your strategy and efforts go beyond those of your competitors, particularly where compliance is involved.

If you embrace digital transformation and your security program is software-driven, integrated, and automated, it will accelerate the pace of change in the organization and the delivery of products, services, and solutions you are able to bring to market. When you weave security into the fabric of your offerings, it can be a differentiator or disruptor to competitors who may not be able to move as quickly, nimbly, or as agile.

"A partnership between IT, Security and Citizen Developers will have mutually beneficial outcomes. Risk will reduce, system availability and visibility will increase and client's will receive value faster!"

Matt Diamond,
VP of IT at Secureworks

Achieving Balance Between Security, Strategy, and Productivity

In today's digital climate, it is incumbent upon the CIO to establish a clear strategy. Productivity should be based on measurable progress, of which security is an outcome. Strategy has to be focused on achieving a digital transformation that will yield greater productivity for end users, and consequently yields a greater level of security in a more automated, iterative way. Security and productivity are strategic prerequisites that CIOs needs to be able to prove through measurements as they move their businesses through digital transformation.

The Security Strategy of Tomorrow

The legacy security model based on building a fence around the "crown jewels" is fading quickly, and five years from now, you can expect a complete inversion of that concept. A true, zero trust model is rising to the forefront, with early innovators providing commercially available products for consumption.

The effective security strategy of the future will be software-defined, driven, and defended. More of what businesses are working on is codified in software, giving security the ability to detect and respond automatically; this will become the status quo. If your security strategy doesn't evolve to add these capabilities, you will begin to slow the pace of innovation in the business and increase the risk from insider threats.

“From a security perspective, the right people, processes, and technology approaches enable scale. Business leaders have to make sure they’re not designing themselves into a technical cul-de-sac by adopting technology today that is “easy” but will undermine the digital transformation goals of the future.”

Matt Diamond,
VP of IT at Secureworks

Security and Productivity are the Rewards of Digital Transformation—Not the Obstacles

Digital is not going away.

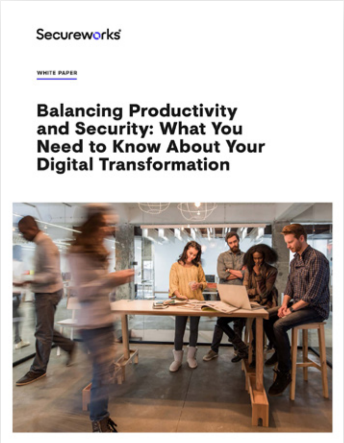
The threat landscape is evolving, and demands for technology enablement will only intensify. Realize that the complexity and the sprawl of your environment will only grow, so the need for an effective decentralized security partnership approach is required. It's not an easy situation to contend with, and CIOs need to make sure they have a sound strategy for people, processes, and technology that's aligned with where business is going.

Security strategy absolutely must enable the business so that you're able to accelerate where business is going, or at least move in lockstep. Your ultimate goal should be to execute digital transformation with two outcomes -- efficiency gains and risk reduction – not just the former.

With the right partnership between Security, IT and Citizen Developers, it's more than possible.

> ***"Building a fence around the crown jewels is an "outdated" strategy that doesn't enable your company to achieve business success!"***
>
> ***Rob Scudiere,***
> *SVP Engineering and CIO*

Want to learn more?
Click on the assets below to continue learning



Secureworks

WHITE PAPER

Balancing Productivity and Security: What You Need to Know About Your Digital Transformation

Secureworks

CHECKLIST

Essential Actions for Protecting Business in the Digital Era: A Checklist

Sources:

[1] Executive Summary: Embracing a Digital Future-Transforming to Leap Ahead. Dell.

[2] Report: Realizing 2030: A Divided Vision of the Future Global business leaders forecast the next era of human-machine partnerships and how they intend to prepare. Dell.

[3] Gartner "Gartner Says Global IT Spending to Grow 3.2 Percent in 2019" October 17, 2018 by Jennifer Garfinkel

[4] Security remains an afterthought in DevOps, Aaron Tan, TechTarget

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500 Atlanta,
GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817
www.secureworks.com.au

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp

Availability varies by region.