SPOTLIGHT

Sponsored by: Accenture and Palo Alto Networks

Organizations must ask themselves whether their current cybersecurity strategy and program are playing a positive role in the success of their digital transformation.

Why Organizations Should Consider Cybersecurity Transformation Now

March 2022

Written by: Cathy Huang, Research Director, Worldwide Security Services, and Christina Richmond, Program Vice President, Security Services

Introduction

The unprecedented acceleration of digital transformation since the start of the COVID-19 pandemic has been driven by a series of seismic shifts that are changing the nature of work, including the rapid move to remote working and the growing use of online platforms and channels. These shifts require an organizational pivot to a digitally transformed operating model, enabled by cloud, big data/analytics, edge, and automation solutions.

Accelerated digital transformation has ushered in a digital-first world. IDC predicts that by 2023, one in two companies will generate more than 40% of revenue from digital products and services, as compared with one in three companies in 2020 (source: *IDC FutureScape: Worldwide Digital Transformation 2022 Predictions*). Direct digital transformation investments will accelerate to a CAGR of 16.5% for 2022–2024, making up 55% of all ICT investment by the end of 2024.

AT A GLANCE

WHAT'S IMPORTANT

Organizations must ask themselves whether their current cybersecurity strategy and program are playing a positive role in the success of their digital transformation. There are three primary business benefits achieved by cybersecurity transformation initiatives:

» Empower cybersecurity as a brand differentiator

» Enable a secure digital transformation with "secure by design" or "zero trust" principles

» Ensure maximum value from cybersecurity investments and resources

In response, organizations must ask themselves whether their current cybersecurity strategy and program are playing a positive role in the success of their digital transformation.

In this Spotlight paper, cybersecurity transformation is defined as a new initiative undertaken by organizations looking to align business, technology, security, and risk programs into a single cohesive program and strategy, with the goal of achieving the following outcomes:

» Empowering cybersecurity, trust, and privacy as brand differentiators with their customers and partners

» Enabling a secure digital transformation with "secure by design" and "zero trust" principles

» Ensuring maximum value from cybersecurity investments and resources

An organization's cybersecurity should behave as an agile function, acting as a facilitator of transformation. Cybersecurity transformation helps enterprises achieve higher levels of cybersecurity proficiency, which means a significant boost in enabling better security of the brand and customer. These services provide a holistic understanding of the overall cybersecurity posture and objectives of the organization, encompassing people, technology, process, and culture.

Challenges Driving the Need for Cybertransformation

The proliferation of digital technology, tools, and processes has greatly expanded the threat surface, effectively raising the cyber-risks for organizations. IDC's September 2021 *Future Enterprise Resiliency and Spending Survey* found that 42% of organizations surveyed indicated that "cybersecurity threats and regulations" will have the greatest impact on their digital transformation and technology investment plans in the next two years.
The challenge is further compounded by the fast-growing threat landscape where cybercrime, data breaches, and ransomware attacks have increased multifold since the start of the pandemic.

Key attributes of the commonly experienced challenges faced by many CIOs/CISOs include:

- Struggling to keep pace with the complexity introduced by digital technologies and processes
- Handling the large volume of alerts generated by various IT and OT systems
- Navigating a fragmented security vendor landscape with confusing messaging
- Managing a security talent shortage
- Addressing sprawling security and technology debt

Moreover, some stakeholders may resist trends like 5G, zero trust, and secure by design as hype or an impractical security model for the enterprise, citing complexity, expense, or lack of skilled resources. However, the complications created by legacy systems needn't be the obstacle that derails the transformation of an organization's cybersecurity program. Selecting the right partners and aligning strategic investment decisions with technologies that will support the security transformation can keep plans on track.

> At the end of the day, cybersecurity is a business risk managed by IT or the security team. As the business evolves to become a digital-ready or digital-first entity, the cybersecurity function must transform from a cost center and inhibitor of progress to a value enabler and facilitator of change.

At the end of the day, cybersecurity is a business risk managed by IT or the security team. As the business evolves to become a digital-ready or digital-first entity, the cybersecurity function must transform from a cost center and inhibitor of progress to a value enabler and facilitator of change.

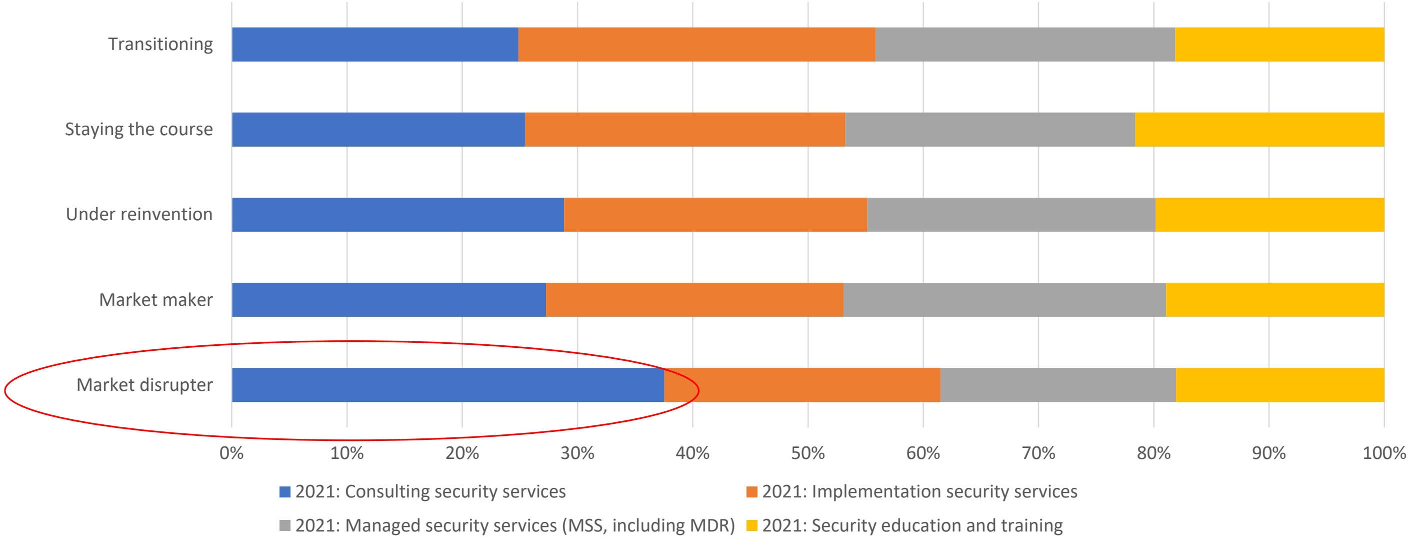
In IDC's *Security ServicesView 2020*, "market disrupters" (defined as an organization fundamentally changing an existing market) spend significantly more on IT security compared with other study cohorts:

- 6% higher than the "market maker" (an organization creating a market that did not previously exist)
- 9% higher than the "under reinvention" (an organization reinventing or repositioning)
- 17% higher than the "staying the course" (an organization continuing to execute existing strategies)

"Market disrupters" also spend more on security consulting services as seen in Figure 1.

FIGURE 1: ***Market Disrupters Spend More on IT Security and Particularly More Cybersecurity Consulting Services***

Q *What is an estimate of your 2021 IT security services budget by services segment?*



n = 1,500

Note: Sums equal to 100%.

Source: IDC's Security Services BuyerView Survey, 2020

Defining a Cybersecurity Transformation Program

Traditional cyberinitiatives tend to be based on individual projects, which means they often lack a cohesive program and strategy. Cybersecurity transformation seeks to combine multiple security technology, talent, process, and risk reduction initiatives into a single program with cross-functional support to drive broader and more effective business outcomes and move from incremental improvements. Key elements of this approach often include:

- Working across the organization to identify business objectives supported by technology change
- Understanding the customer and partner ecosystems and identifying where security can be a differentiator
- Challenging the security and risk posture of the organization, based on new technology solutions and ways of working to enable new opportunities
- Building short- and long- term road maps with clear reference architectures and vendor consolidation initiatives
- Providing regular communication to all levels of the organization, celebrating the accomplishments and progress of the cybertransformation program

For example, an insurance provider undertaking cybertransformation will want to consider the role security and technology play in enabling its internal and external workforce to securely and quickly connect to underwriting systems and how that might facilitate access to new talent pools, overseas or within certain demographics.

A manufacturer will want to consider the role of technology in increasing plant efficiency and productivity, looking at how security could help to enable new efficiencies. They may also look to how IP is better protected at regional and local levels, to ensure their competitors are not able to gain access, while also improving employee collaboration options.

Leading with Cybersecurity as a Brand Differentiator

Brands have an opportunity to build trust with their customers by marketing the value of their focus on security, privacy, and trust. A sound cybersecurity program builds the foundational layer of an organization's trustworthiness and changes security from a business impediment to a business enabler.

Cybersecurity Transformation in Action

A cybersecurity transformation initiative can sound hard and expensive. The road to transformation starts with a mindset — one where you can achieve something greater than your current condition and you can bring your organization through this change successfully. The advice for organizations is to look to what they are already doing and find ways to connect existing initiatives to create an overarching program framework. Some examples of how larger initiatives could be combined are detailed in the sections that follow.

Boost Digital Transformation Initiatives with Secure-by-Design and Zero Trust Principles

Digital transformation can bring with it unintentional IT complexity — and complexity correlates with the likelihood of breaches. Against the backdrop of rising cloud adoption and edge deployments, managing and securing diverse IT resources and data sets are among the most critical IT operational challenges.

To that end, adopting security principles at the design stage is an important first step in effectively managing and securing the hybrid, multicloud IT environment. The rise of many "developer first" companies helps to shift security left and enables developers to build more secure software without slowing them down. These companies offer to embed protections in the development processes and to help improve an organization's digital transformation. This requires a nontraditional mindset toward security and trust. Zero trust, rooted in the principle of "never trust, always verify," fits with this new requirement perfectly because it is designed to protect modern digital environments by leveraging network segmentation, preventing lateral movement, providing Layer 7 threat prevention, and simplifying granular user-access control. IDC research shows that enterprises recognize the importance of assessing or redesigning the entire security architecture stack to improve the overall security posture and cyberdefense capabilities.

Rationalize and Maximize Security Resources

The key to a trusted digital enterprise is to develop a cybersecurity program that shifts security and risk management toward continuous measurement and granular access control with an architecture that supports real-time decision making. For instance, in a zero trust design, no level of trust is automatically granted to any end users nor to any computing or network resources without authenticating or authorizing. The zero trust model gives system engineers the information for risk-based decisions on who should be granted access to which resources.

Another important characteristic of cybersecurity transformation is to strengthen security by infusing it with a higher level of automation and observability. Unlike other IT infrastructure that has a feedback loop where failures can be easily identified and then fixed, security controls tend to fail silently. For example, their false negative rate is unobservable because the measure of a security control's efficacy is not what it detects or blocks but what it fails to detect or block. Continuous security control validation is not about finding individual errors. Rather, it provides the basis to understand and optimize the effectiveness of the overall security program.

In addition, the reduction of alerts and false positives can significantly help to reduce analyst burnout. Automation is not meant to replace human analysts but to create a more conducive environment for them to perform more valuable and rewarding tasks.

Build Trusted, Secure Supply Chains

Cyberattacks on the supply chain have grown in prominence since 2020. High-profile attacks like Kaseya and SolarWinds are constant reminders that it is vital to build a trusted and secure supply chain ecosystem that acts like a virtual extension of an organization and its operations, products, and services. Nearly 60% of organizations surveyed in IDC's July 2021 *Future Enterprise Resiliency and Spending Survey* indicated their major suppliers/partners required them to review and certify that they are implementing security and data protection and recovery practices to prevent disruptions from a ransomware attack as a result of increased awareness of ransomware incidents in the past 12 months.

The visibility of all third-party organizations' security postures is critical to build a trusted secure ecosystem for the future enterprise. Trust is a defining characteristic of a mature, effective ecosystem. It enables agreements to be made quickly between organizations, which reflects a level of confidence in value creation with minimized risk.

The pandemic and geopolitical tensions between China and the United States have also brought significant disruptions in value chains, including supply chains and customer value chains. These tensions have resulted in the scrutiny of digital ecosystems that leverage digital platforms to deliver scale and speed as well as federate data from connected products, assets, people, and processes. Under a transformed cybersecurity program, cyber-risk assessments should be extended to organizations' suppliers, partners, and vendors to establish acceptable risk levels.

Considering Accenture and Palo Alto Networks' Joint Cybersecurity Transformation Offering

Finding partners to help jump-start or add horsepower along the way to a cybersecurity transformation initiative can really help organizations achieve their goals more easily and in an accelerated fashion.

Accenture is one of the world's top IT services providers with deep industry knowledge, client reach, and global leadership in cybersecurity services. It is also known for its end-to-end security capabilities and broad IT and business services portfolio. Accenture's operational expertise and large-scale complexity management make it a particularly attractive option for companies in heavily regulated industries such as financial services, critical infrastructure, healthcare, and public sector. The company has many sourcing and commercial models that tie to value (e.g., level of fraud, incidents reduction, cost reduction) and ensure that it has skin in the game.

Palo Alto Networks is a leading security solutions provider that has achieved average year-over-year revenue growth of 32% over the past two years. The strong growth is attributed to the company's efforts to strengthen in several important enterprise security segments, such as high-end firewall, cloud security, SD-WAN, and security automation. Its recent Bridgecrew acquisition is an example of how Palo Alto Networks is expanding in the cloud security spaces.

Accenture and Palo Alto Networks, over the course of the past five years, have built a strategic partnership to help organizations navigate and accelerate their cybersecurity transformation through the use of best-of-breed security technology and services. With rigorous customer satisfaction and quality assurance reviews, together with strong governance and closed-feedback processes, Accenture and Palo Alto Networks help to ensure continuous value creation for customers. The typical outcomes include:

- Unlocking business and digital transformation, while protecting the enterprise
- Implementing a zero trust strategy that results in simplified hybrid networks across platforms, reduced costs, and improved user experiences
- Transforming security operations with real-time intelligence and responses
- Effectively improving security and business outcomes while efficiently managing investments

A case study with a major pharmaceutical company indicates that Accenture helped it to create a more scalable, reliable, and secure architecture, moving 80% of the company's applications to the cloud and reducing the internal datacenter footprint. The transformation also accelerated the delivery of data services and capabilities, helping to increase secure connectivity and collaboration with the overall life sciences ecosystem and external partners.

Challenges

We are at a tipping point of digital transformation. Data security, confidentiality, integrity, availability, and resilience are now key issues for any organization. Businesses also face increasing pressure to ethically use data and comply with a complex web of industry and regional regulations. The urgency to transform cybersecurity to proactively address these data-driven complexities is real. However, the available offerings in the market are loosely defined and utterly confusing at the moment. Accenture and Palo Alto Networks have joined forces to help customers understand their cybersecurity transformation offering and deliver on the promise of its value.

Conclusion

A holistic understanding of the organization's overall cybersecurity posture and objectives is required to advance the cybersecurity program from passive IT function to true business enabler.

However, any successful transformation requires a change in mindset. Ultimately, cybersecurity transformation is a people-centric process that is powered by modern tools and automation capabilities. It is much more than a piecemeal adoption of technology.

To achieve success, CIOs/CISOs need to:

- Ensure that the necessary security policies, workflow, and training are in place and that security/IT staff are reskilled or upskilled to meet the new standards and the new norm.
- Create a solid cybersecurity culture based on clearly understood standards for governance, compliance, and accountability in which all workers are equipped to avoid being the "weakest link."
- Embrace the future-proof technologies and platforms, which are the only ways to realize the outcomes. Dealing with escalating threats is not humanly possible without artificial intelligence (AI), machine learning (ML), and other modern security technologies.

About the Analysts

***Cathy Huang,** Research Director, Worldwide Security Services*

Cathy Huang is the research director for IDC's WW Security Services research practice. In her role, Cathy collaborates with other worldwide and regional analysts to develop a set of thought leadership and actionable research for IT buyers and suppliers. Specifically, she develops core research around managed security services, security consulting, and integration services within the program. She also incorporates IDC's Future of Trust and other FoX agenda to drive new research such as cloud security services and secure edge services for the program.

***Christina Richmond,** Program Vice President, Security Services*

Christina Richmond is the Program Vice President for IDC's Security Services research practice. She is responsible for the day-to-day management of the program. Core research coverage for the team includes, but is not limited to, security consulting, integration, and managed services. In addition, the team looks at services that help organizations adopt emerging technologies like Cloud, Edge, and IoT as well as key focus areas such as Risk, Data Privacy and Compliance.

MESSAGE FROM THE SPONSORS

Accenture and Palo Alto Networks have developed a Cybersecurity Transformation solution to help clients secure the evolution of their technology estate and proactively reduce modern cyber risk. Cybersecurity Transformation addresses multiple security challenges that can be overcome with a holistic cybersecurity platform available from Palo Alto Networks and combined with Accenture's deep services and deployment expertise to achieve economies of scale and long-term cost savings.

For additional information on Cybersecurity Transformation, please read our blog or visit our website.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.