Cyber Talk

DIGITAL TRANSFORMATION

ENDLESS OPPROTUNITY OR CYBER APOCALYPSE?

In 1946, when scientists dedicated ENIAC, the world's first electronic, digital computer, no one could have predicted the many trajectories computing technology would follow. The worldwide installed base now numbers 1.333 billion computers.[1] In addition, there are 3.3 billion smartphone users around the world.[2] By 2020, IDC predicts IoT endpoints will top 30 billion.[3]

Moving from analog devices to digital processors connected through wired and wireless networks spurred widespread changes. The transition fostered new computing models such as software as a service (SaaS), virtual environments, peer-to-peer blockchains, and many others. Through these platforms, the digital transformation offers organizations across all industries unprecedented flexibility to improve operating efficiencies and creating new ways of doing business.

In this paper, we'll discover how omnipresent computer processing, combined with total global connectivity and expanding attack surfaces, comes at a steep price. A digitally transforming world offers endless opportunities, but is it moving us even closer to a cyber apocalypse? Organizations are already threatened by the fifth generation of increasingly dangerous cyberattacks.[4] Once familiar corporate security perimeters have ballooned into a unified global threat surface, requiring organizations to reconsider their cyber security strategies and practices.

Mad rush to digitalization

IDC reported that 85% of surveyed enterprise decision-makers need to make significant inroads into digital transformation in the next two years, or they'll fall behind competitors and suffer financially.[5] Thirty-seven percent have started their transformations by integrating and executing on a digital-first approach.[6]

A digitally transformed business offers rewards, including increased worker productivity, improved business performance management, better customer experiences, and the development of new digital-based revenue streams. In healthcare, telehealth is a growing area to help minimize unnecessary office visits. Banks are continuing to improve customer online experiences. AI is being touted to help predict when customers will need financial help.

Manufacturers are realizing that how they develop products has a huge impact on the customer experience with their offering.

However, moving to a digital business model comes with risks. The digital transformation has thrown the doors wide open to cyber criminals who are investing their time and resources to exploit any and all gaps in your cyber security.

1 Statista, Installed base of personal computers (PCs) worldwide from 2013 to 2019 (in millions), as viewed, September 24, 2019. https:// www.statista.com/statistics/610271/worldwide-personal-computers-installed-base/
2 Statista, Number of smartphone users worldwide from 2016 to 2021 (in billions), as viewed, September 24, 2019. https://www.statista. com/statistics/330695/number-of-smartphone-users-worldwide/
3 "State of Digital Business Transformation," IDG Communications, 2018
4 Gil Shwed, Gen V Security. https://www.checkpoint.com/gen-v-cyber-security/
5 "40 Stats on Digital Transformation and Customer Experience," by Blake Morgan, Forbes, May 13, 2019
6 "State of Digital Business Transformation," IDG Communications, 2018

> By 2020, 100% of large enterprises will be asked to report to their board of directors on cybersecurity and technology risk at least annually, up from 40% today.[7]

Transformation platforms

Diverse computing platforms allow organizations to economically run their workloads on processors that others own and that reside outside the organization's premises. These are often beyond the reach of on-site security measures. Digital cloud-based apps and services make software as a service (SaaS) a prime example.

SaaS

SaaS providers process the workloads your organization needs for marketing automation, customer relationship management (CRM), and a host of other critical functions. They reside in each SaaS provider's data center or in third-party cloud facilities. The SaaS market is estimated to hit $100 billion in 2019 and grow at almost 30 percent per year.[8] Using network or next-generation firewalls to safeguard the integrity and privacy of SaaS workloads is not effective. Neither can they guard against dangerous account takeovers by cybercriminals.

In addition, since SaaS applications come from outside your data center, employees can run unauthorized SaaS applications on your network without information technology's knowledge or approval. Shadow SaaS can introduce network threats and abuse bandwidth. Disgruntled insiders with access can also participate in illegal activities from sites outside of IT control.

To avoid this path to the cyber apocalypse, organizations must have security that's purpose-built to protect SaaS workloads and detect unauthorized SaaS running on their networks.

7 "Digital Business Requires Cybersecurity," Gartner, 2019
8 "SaaS Spending to Hit $100B This Year: Still Just 20% of Enterprise Software Market," by Ed Targett, CBR, June 28, 2019

Virtual, Cloud, Hybrid Environments

Likewise, when organizations want to run on-demand workloads with high cost efficiency, they can opt to run applications in different ways. This includes virtual environments on site, off-site in cloud facilities such as on AWS and Azure, or in hybrid on-site data center/cloud environments. In any case, legacy security measures leave virtual environments exposed to malware and data breaches. Whether on-site or off-site, virtual machines can spin up and spin down between security scans, causing them to miss threats entirely. The architecture of virtual environments causes workloads to travel "East-West" from virtual machine to virtual machine rather than "North-South" in and out of the data center. This means, most processes in virtualized and hybrid data centers never see a firewall or antivirus protection.

To minimize risks, dedicated security that protects virtualized workloads is essential, as is tight coordination among dev-ops, IT, and cyber security teams.

Mobile computing

Increasingly, employees, customers, contractors, and click workers, such as ride-sharing drivers, contribute to an organization's computing workloads using their own smartphones, tablets, and laptops. BYOD policies mean that most workers' phones are largely unprotected from cyberattacks. Attacks on mobile phones and other devices are the first step in many broader cyberattacks. Typically, a victim downloads a malicious app, opens an infected email, visits a malware-laced website or uses unsecured Wi-Fi. The malware steals the victim's login credentials, giving the attacker entry into a private network where the attack continues. Some malware can take over a device's camera and microphone to spy on the victim as well as access the victim's contacts and appointment calendars. And what about the mobile apps that are easily placed on a phone?

Apps purchased from official Apple and Android app stores are not entirely safe. Clever attackers use techniques like time bombs and droppers to evade app-store malware screenings. As is the case with the aforementioned platforms, typical corporate cyber security does not cover mobile-device computing. Only purpose-built mobile security will prevent damaging mobile attacks that could escalate into a global malware outbreak.

Raising success rates with digital transformations

Management consulting firm McKinsey & Company determined key factors that survey respondents said helped their organization meet digital transformation initiatives.[9] Here is a brief list of those factors:

- Digital self-serve technology made available for employees and/or partners
- Senior managers fostering a sense of urgency to make transformation changes

9 "Unlocking success in digital transformations," Survey, McKinsey & Company, October 2018

- Management team establishing clear transformation change story
- People in key roles ensuring collaboration between those in different departments
- Senior leaders encouraging employees to experiment with new ideas

In addition, before launching digital transformation initiatives, teams need to secure sizable budget and include the right people with the right skills. The digital transformation journey is neither easy nor guaranteed, but it is possible to apply the security that can help you avoid a cyber apocalypse.

Conclusion

The continuing rapid growth of the digital transformation in its many diverse forms is a mixed blessing for people and businesses. On one hand, digital technology offers us improved customer experiences. It affords organizations new opportunities to disrupt business practices, but it ratchets up competition for business executives. Similarly, the transformation adds massive complexity for IT and cyber security professionals who have to make new technologies work and keep them safe from evolving threats.

Adding cyber security technologies piecemeal as you bring new platforms online increases complexity, overwhelming IT and security staff members. Today's cyber security requires multi-platform, multi-device protection against all threats, backed with intuitive central management and forensic analyses that helps you combat sophisticated, unknown cyber threats.

To learn more about preventative, consolidated cyber security architecture that can help you meet the challenges of the digital age, visit Check Point Infinity.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com