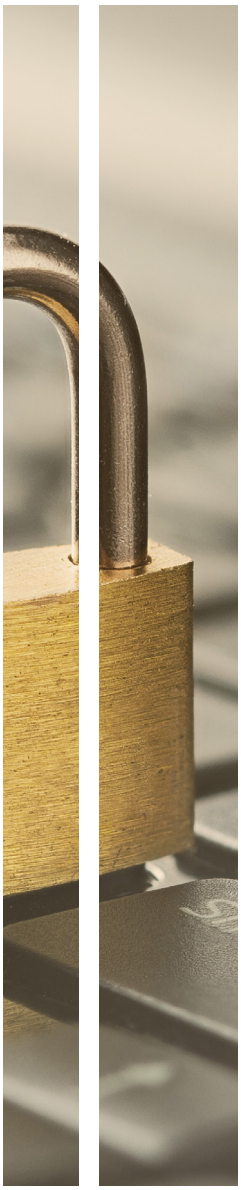
Cybersecurity M&A Momentum: Digitalization to Drive Accelerated Demand and Total Available Market Expansion



As C-suite executives focus intensely on corporate **digital transformation** efforts, cybercriminals are following suit and adjusting tactics to exploit the resulting **massively broader cloud attack surface**. This big new challenge is driving record growth in cybersecurity mergers and acquisitions (M&A) and investment.

During a recent panel I participated in at S&P Global's 451Nexus technology conference, 451Research shared that **Information Security (InfoSec) spending in the first three quarters of 2021 more than doubled compared to 2020 and 2019**. Such out-sized growth in cyber spending ties directly to the digitalization wave, accelerated by the global COVID-19 pandemic.

In addition to creating greater vulnerabilities and risk, the rapid shift to cloud-first is catalyzing a blizzard of regulatory development and enforcement activity (e.g., in data / privacy protection, access control and risk quantification). Elevated breach and legal dangers to organizations mean that underinvestment in cybersecurity is no longer an option; consequently, cyber spending as percent of information technology (IT) budgets will continue to rise.

> *"InfoSec is in the middle of retooling for a cloud-first world. Where cybersecurity once protected the network perimeter and assets within, it is now charged with securing our entire digital world. The network includes the entire Internet and everything touching it, meaning that today's attack surface is broader than ever. Rather than just servers and laptops, security must protect data and applications wherever they reside. That can be in transactions, communications or physical assets from planes to pacemakers to pipelines.*
>
> **Don More, Managing Director, Lincoln International | S&P Global 451Nexus Panel**

Zero Trust Paradigm Becomes Fundamental to Modern InfoSec

Legacy Cybersecurity 1.0 was built on the concept that anything outside the network is untrustworthy, while inside the network is trusted. In modern organizations, employees and machines directly access cloud applications, data and services, **rendering the perimeter defense model obsolete**. Consequently, **one can never trust and must continually verify the IT ecosystem**.

The **Zero Trust model** is rapidly becoming the cornerstone of Cybersecurity 2.0, because it requires that only the right, legitimate parties gain access to accomplish permitted activities, wherever IT resources reside.

The emerging shift to **Zero Trust requires a redesign and replacement of security infrastructures** across cloud, network, endpoint, identity, cloud and data security. This makes Zero Trust the most potent thematic driver for sector spending growth, investment, M&A and initial public offering (IPO) activity.

(continued next page)

Modern InfoSec Expanding from the Digital to Physical World

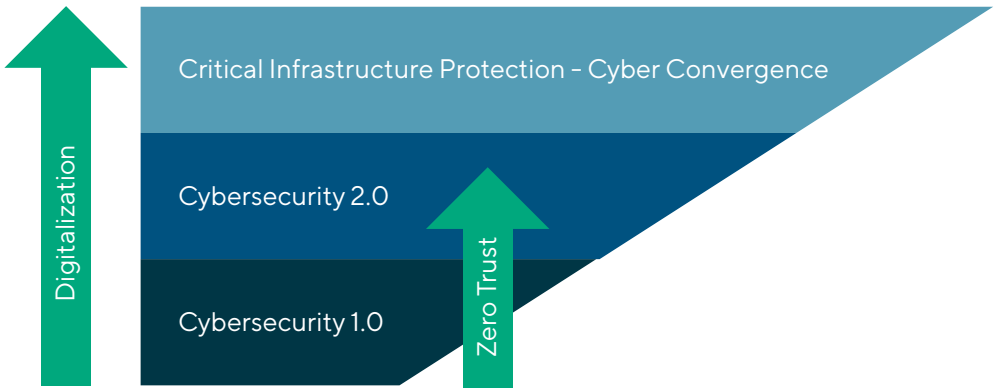
Digitalization is also pushing IT-OT (information-operational technology) convergence, necessitating the protection of both digital and Internet protocol-enabled (IP-enabled) physical assets. This is opening up **vast opportunities to extend cyber investment to smart buildings, industrial control systems, vehicles and all manner of devices**. Historically, critical infrastructure protection (CIP) spending has been separate and distinct from cyber, and both markets are roughly the same size. Progressive overlapping of cyber and CIP, and the extension of Zero Trust to the physical world, will be the most potent cyber spending growth drivers in coming years, while greatly expanding the cyber total available market (TAM).

Lincoln Perspective

For investors and business owners weighing their InfoSec investment strategy in 2022, Lincoln International highlights several implications of the digitalization wave, and resulting shift to Zero Trust-led Cybersecurity 2.0 and CIP-Cyber convergence:

Valuation Outlook: We forecast the overall cybersecurity sector will maintain valuation over-performance in 2022, as spending continues to grow materially faster than other technology sectors. Further, the cybersecurity TAM is growing rapidly due to digitalization, expected Zero Trust refresh and the expansion of digital to physical security (see graphic below).

Cybersecurity TAM Expansion Will Drive Persistent Outsized Growth and Valuations



Deal Activity Outlook: Record cash available to invest, by financial sponsors and on public balance sheets, combined with the desire to participate in the digitalization-fueled cyber spend boom, will support continued frenetic consolidation and growth investment activity in 2022.

Navigating Robust Valuations: In cybersecurity, industry revenue multiple-based valuations correlate closely with revenue growth, resulting in above-average valuations. In this high growth, high valuation sector, the best way to invest is to focus on companies that are class leaders in solution areas benefiting directly from Zero Trust, Cybersecurity 2.0 and CIP Convergence, and that are valued below the revenue multiple implied by their growth.

For other perspectives, visit us at www.lincolninternational.com/perspectives.

To learn more about Lincoln's cybersecurity, InfoSec and technology, media & telecom capabilities, connect with a member of the team at www.lincolninternational.com/technology.
