KB

BETTER TOGETHER: HOW HR PROFESSIONALS SHOULD PARTNER MORE PROACTIVELY WITH IT AND CYBERSECURITY

January 2023

Derek E. Brink, CISSP
Vice President and Research Fellow, Cybersecurity and IT GRC

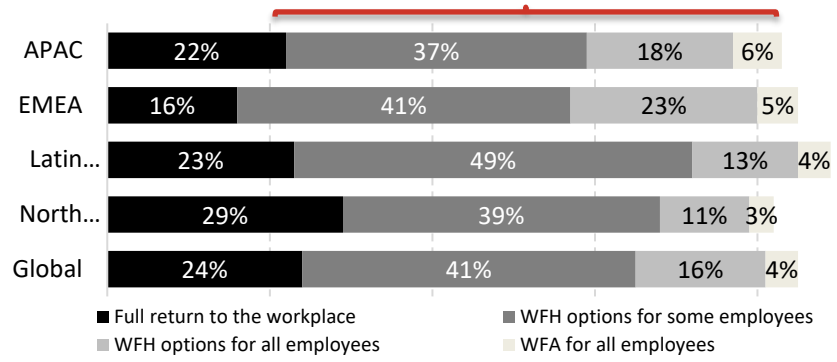
When a **remote / hybrid workforce** and a preference for highly **mobile, networked devices** and **cloud-based applications and data** has become your organization's new normal, there's an obvious opportunity for Tech pros to enhance their cybersecurity programs by collaborating more closely with powerful partners — especially their colleagues in Human Resources.

(Knowledge) work is an activity, not a place

The trends toward an *increasingly decentralized workforce*, enabled by *highly mobile, networked devices* and *cloud-based applications and data* — trends which were abruptly accelerated by the global pandemic starting in 2020 — have in fact been building momentum for many years[1]. See Figure 1.

Without question, these trends are significantly transforming the way we work, live, learn, and interact with one another — both professionally, and personally. At the same time, they are creating new cybersecurity-related threats, vulnerabilities, and risks that each organization needs to a) properly understand, and b) proactively manage to acceptable levels.

Figure 1. Across the globe, more than 50% of all organizations plan to support a full or partial remote workforce indefinitely.



Source: (ISC)[2] / Spiceworks Ziff Davis *Global Cybersecurity Workforce Study* 2021 (Global N=4,470; NA N=1,870; LATAM N=276; EMEA N=1,175; APAC N=1,149); Aberdeen, 2023

Over the years, Tech professionals in IT and Cybersecurity roles have been working tirelessly to address these challenges. Today, they are also collaborating more closely with their organization's HR professionals, who are well-positioned to play a larger and more influential role in cybersecurity than ever before, for example by:

- **Developing policies** for cybersecurity, privacy, and acceptable use that are appropriate for a remote / hybrid workforce, and for the routine use throughout the organization of its sensitive or regulated data using highly mobile, networked devices.
- **Driving policy awareness** among employees, not only during the onboarding process but also on an ongoing basis — including the organization's processes for career planning and development.
- **Delivering security awareness training** and skills development for employees, to establish and regularly reinforce safer cybersecurity behaviors — both "at work" and in their personal lives.

[1] For example, the rise of "knowledge work" was first described by Peter Drucker in *The Landmarks of Tomorrow* (1959); the idea that "work is an activity, not a place" was noted by William Draves and Julie Coates in *Nine Shift: Work, Life, and Education in the 21st Century* (2004).

- **Influencing decisions about the enabling technologies** that the organization provides for its remote / hybrid workforce — to enable reliable access, consistent security, and centralized management by IT — to help ensure that "people" and "process" perspectives are fully considered, in addition to "technology."

How IT, Cybersecurity, and HR pros can team up to focus on the human factors

The annual Verizon *Data Breach Investigations Report (DBIR)* consistently shows the importance of focusing on the human factor with respect to cybersecurity, privacy, fraud, and regulatory compliance. In the 2022 DBIR, for example, more than 4 out of 5 (82%) confirmed data breaches involved phishing attacks, stolen user credentials, misuse, or simply human error. Moreover, the Verizon 2022 *Mobile Security Index (MSI)* showed that cyber attacks on mobile devices have significantly increased (i.e., by about 45%) in the last year.

Working together, HR professionals can team up with their Tech pro colleagues in IT and Cybersecurity roles to address today's challenges more holistically, such as those described in the following table.

Table 1. Working together, HR can team up with Tech colleagues to address today's challenges more holistically.

Challenge	Business Impact	How HR Professionals Can Collaborate More Proactively with Colleagues in IT, Cybersecurity Roles (illustrative)
Devices and tools used for remote work lack appropriate policies and technical controls	Higher likelihood of phishing, account takeovers, malware, ransomware, and data breaches involving corporate data (e.g., personal devices are more prone to access compromised websites)	• Update acceptable use policies to reflect the context of a remote / hybrid workforce • Provide employees with updated training whenever working arrangements change • Provide employees with guidance specific to working remotely (e.g., maintaining privacy in a shared apartment)
Use of consumer-grade internet devices and services for work	Higher vulnerability to cyber attacks, limited performance, and complicated IT support can imperil productivity	• Advocate for robust and secure collaboration tools • Standardize on company-supported internet devices (e.g., 5G routers), endpoints (e.g., mobile phones, tablets, and laptops with common security and management solutions), and collaboration tools (e.g., video conferencing with common security and privacy settings)

Source: Aberdeen, January 2023

In addition, the Society for Human Resources Management (SHRM) offers a range of useful tips about how HR professionals can contribute to an organization's cybersecurity culture.

About Aberdeen Strategy & Research

Aberdeen Strategy & Research, a division of Spiceworks Ziff Davis, with over three decades of experience in independent, credible market research, helps **illuminate** market realities and inform business strategies. Our fact-based, unbiased, and outcome-centric research approach provides insights on technology, customer management, and business operations, to **inspire** critical thinking and **ignite** data-driven business actions.