UC BERKELEY

CENTER FOR LONG-TERM CYBERSECURITY

CLTC WHITE PAPER SERIES

Security and Privacy Risks in an Era of Hybrid Work

ANN CLEAVELAND | GRACE EVANS | ANDREW REDDIE | ISAAC VERNON | STEVE WEBER

CLTC WHITE PAPER SERIES

Security and Privacy Risks in an Era of Hybrid Work

ANN CLEAVELAND | GRACE EVANS | ANDREW REDDIE | ISAAC VERNON | STEVE WEBER

DECEMBER 2021

CENTER FOR LONG-TERM CYBERSECURITY

University of California, Berkeley

Contents

Executive Summary

Since the start of the COVID-19 pandemic, firms have shifted significant proportions of their workforces to "hybrid" roles, with workers splitting their time between their offices and homes. At the same time, many issues regarding privacy and security in the hybrid environment have not been clearly formulated or answered.

This paper discusses emerging privacy and security issues attached to hybrid work environments, drawing on workshop proceedings and interview data with security, policy, human resources, and other leaders from private firms and government agencies. The paper introduces high-level policy recommendations that, with further development, could potentially address these concerns. Among the key insights included:

- Hybrid work represents a significant opportunity in terms of human capital development. Many employees welcome the freedom associated with hybrid work, and firms that allow remote roles can recruit without regard to location, increasing the potential applicant pool.
- "Zero trust" architectures are well-suited for a hybrid work environment as they promise a seamless experience for employees and state-of-the-art digital security for employers, through multi-factor authentication and continuous authentication of the users and devices on a network, regardless of where they are located. Zero trust security has limitations, however; such networks can be expensive and complicated to implement, and the term "zero trust" has negative connotations.
- Employees are uncertain as to expectations concerning their privacy in the hybrid workplace, as well as how they might protect firm data, particularly personally identifiable information (PII) and proprietary data. Workers in home environments may reveal PII, as well as information about protected characteristics for both themselves and "bystanding" members of the household. For firms operating across jurisdictions, the multitude of policy regimes that govern data will make privacy considerations even more complex.
- Firms that are transparent with employees about their privacy and data protection expectations, and that provide support through training and other means, will have an opportunity to reshape norms and improve security while strengthening their relationships with workers.
- Firms face a range of novel liability concerns associated with the security and privacy risks posed by hybrid work, from leakage of data through insecure networks to potential vulnerabilities in at-home "smart" devices. These concerns will need to be addressed, for exam-

ple through liability shields or by firms' segregating home workers' personal and business devices and networks.

- Equity concerns loom large in the context of hybrid work, as whether workers are in the office or at home could lead to differences in promotion decisions or in the types of work employees are asked to perform. Firms that support hybrid work will be called upon to level the playing field across the home and office environments, and should lean into lessons from the new virtual environment, in some cases translating them "backwards" into the office environment.
- Government infrastructure investment could be allocated not only to expand broadband access, but also to improve home network security by providing secure routers and other home network equipment, ensuring workers in less privileged circumstances can participate.
- To improve labor market flexibility, policy may be needed to ensure that firms' investments in home network security are transferable to a new employer if the employee chooses to take a new job. This is a complex trade-off, as it may lead employers to reduce their investments in home-based workers. However, a set of policy-based standards that implement interoperability and "portability" could help mitigate this risk.
- The move to hybrid work has potential to disadvantage local and state governments as they compete to attract businesses to develop offices and other facilities in their geographic regions. Governments could benefit from putting shared boundaries around such competition going forward.

The shift to the hybrid work environment — an economy-wide "reset" of work location and practices — offers a rare opportunity to break through longstanding habits of personal and organizational behavior that negatively impact privacy and security. Escaping the downsides and realizing the upsides will require a combination of legislative and regulatory action, roles for industry associations, and new tools and technologies. Security and privacy in the hybrid work environment are likely to be tied tightly to productivity, equity, and innovation in the next decade. How firms and policymakers converge around new privacy and security considerations will determine whether hybrid work lives up to its promise.

Introduction

After the COVID-19 pandemic began in 2020, firms around the world shifted significant proportions of their workforces to remote roles, in what amounted to "adaptation under fire." To maintain productivity amid a rapid shift away from in-office work, many firms relaxed security requirements to allow newly remote workers to access corporate networks, vendor approval processes were abbreviated, productivity tracking software was introduced, and workers shared aspects of their home lives that were previously private as video-based meetings became standard practice.

In 2021, as the pandemic has subsided, many firms have allowed workers to return to work in the office on a part-time basis, leading to a new shift toward "hybrid work." These businesses now face an environment in which their workforces are split across remote and office-based roles, to a degree never seen before. Employees are working not only at home, but also in airports, co-working facilities, coffee shops, and other "third spaces." Although the shift to hybrid work has been a constant subject of discussion in 2021, many issues regarding privacy and security in this environment have not been clearly formulated, much less answered. This report details these concerns and offers possible routes forward.

Securing the hybrid work environment is, like other security challenges, not simply a technical problem. Decisions concerning privacy and security regimes for the hybrid work environment are often strategic in nature, and in most cases require policy discussions that evaluate costs and benefits for different actors. For example, to what extent might changes in the labor market lead firms to engage in a "race to the bottom," tolerating higher risk in security practices to retain remote employees? Under what circumstances might firms that adopt intrusive or burdensome security and privacy requirements have a disadvantage in recruiting and retaining the best talent? And how might security and privacy choices offered to a hybrid workforce amplify or ameliorate existing inequalities? With hybrid work seemingly here to stay, getting privacy and security "right" in this new environment will have profound implications for productivity, equity, and innovation in the next decade and beyond.

In this paper, we discuss emerging privacy and security issues attached to hybrid work environments, drawing on workshop proceedings and interview data with security, policy, human

resources, and other leaders from private firms and government agencies.[1] We organize insights across four categories: human capital and trust, privacy and data protection, liability and insurance, and equity concerns. We then outline a series of high-level policy recommendations that, with further development, could potentially address concerns across each.

HUMAN CAPITAL AND TRUST

Firms increasingly walk a tightrope when it comes to employer-employee relationships in the hybrid work environment, and corporate policies associated with privacy and security have the potential to significantly impact this relationship, particularly given increasing calls by employees for means to disconnect from work. Should enterprise-level security expand into some aspects of the home, and if so, how should it be implemented? Firms that adopt intrusive or burdensome security and privacy requirements for home networks risk being less competitive in hiring and retaining high-quality employees, particularly as the pandemic gives way to what has been described as the "Great Resignation."[2] Firms that tolerate more leeway in their security practices in order to retain remote employees face a "race to the bottom," making their networks more vulnerable and placing themselves at greater risk of a major cybersecurity incident.

The same shift to hybrid work that presents challenges also yields opportunities. For example, hybrid work represents a significant opportunity for firms to engage new forms of human capital, with one interviewee noting that employees have welcomed the freedom associated with an increasing number of hybrid roles. At the same time, firms can recruit without regard to location, allowing them to find the best candidate for a role, regardless of geographical location, which dramatically increases the potential applicant pool. These benefits, of course, are tempered by the potential for employees to leave firms should the flexibility associated with hybrid work — in terms of both location and working schedule — be taken away.

1 As part of this project, we carried out over fifteen individual interviews with academics and executives from industry before hosting a virtual workshop in September 2021, where participants discussed the challenges associated with hybrid work in larger groups. All engagements occurred under the auspices of the Chatham House rule. The authors would like to thank Matthew Nagamine and Rachel Wesen for their administrative assistance throughout the project.

2 Estimates indicate that 11.5 million workers quit their jobs between April-June 2021. Hsu, Andrea. "As the Pandemic Recedes, Millions of Workers Are Saying 'I Quit'." *National Public Radio*. June 24 2021. https://www.npr.org/2021/06/24/1007914455/as-the-pandemic-recedes-millions-of-workers-are-saying-i-quit; https://hbr.org/2021/09/who-is-driving-the-great-resignation

"Zero trust" architectures have emerged as one solution to this balancing act, and a growing number of firms are adopting this approach. Advanced zero trust systems promise a seamless experience for employees while maintaining state-of-the-art digital security for the organization, through multi-factor and continuous authentication of the users and devices on employer networks. Workshop participants noted the importance of thinking of network security as *location-agnostic,* and zero trust tools can support a hybrid work environment in which a person logs in from work, home, in-transit, and "third spaces." Indeed, participants extolled the value of zero trust architecture even for firms with most or all of their employees working in the office.

Advanced zero trust systems today are accessible mainly to large enterprises, and do not address the security and privacy contexts of other types of organizations, such as small and medium-sized businesses, non-profit organizations, and local government agencies. The name itself, "zero trust," also connotes mistrust between the authenticated (employee) and authenticating (firm), a branding challenge and negative valence in the public discourse that exacerbates the tensions in employer-employee relationships. Most importantly, no framework currently exists that establishes an industry standard for what constitutes zero trust or that provides safeguards for the monitoring elements inherent in zero trust technologies (e.g., location data, keystroke data). To accelerate the adoption of safe, secure, and accessible security regimes for the hybrid work environment as zero trust solutions proliferate, each of these concerns needs to be addressed.

PRIVACY AND DATA PROTECTION

The hybrid work environment also creates new considerations for privacy and data protection in an already confusing and fast-evolving privacy landscape. Across multiple interviews, we heard that a robust privacy discussion between employers and employees has yet to mature. This leaves employees uncertain about expectations concerning their own privacy in the hybrid workplace, as well as how they might protect firm data, particularly personally identifiable information (PII) and proprietary data. We heard that the gap between technology and privacy is *widening* as the workforce shifts to a hybrid mode. Adoption of new technology products is outpacing people's understanding of the privacy risks those products could introduce, and employers and employees need a more formalized process for vetting products for potential risks. Consider the following examples:

- "Always on, always listening" devices in employees' homes, such as virtual assistants or "nanny cams," are now components of the work environment. If a virtual assistant (e.g., a Siri-enabled or Alexa device) is used for both work and personal purposes or in a common space, who is responsible for managing the security and privacy settings? What are the boundaries of consent for data use and collection?
- In addition to ubiquitous video conferencing software, productivity software and digital health monitoring applications (such as COVID-19 symptom screeners) have become increasingly commonplace in both the home and on-premises work environments. Study participants noted the potential for inadvertent data collection associated with an employee's home environment, with few or no policies to address this issue. For example, should firms store video data that includes images taken from inside an employee's home? What is a firm's responsibility to report illicit activity unrelated to the business that video might inadvertently capture? Should an employee expect any degree of privacy while using an employer-issued laptop in any location?
- Participants were also concerned that individuals other than employees might have access to privileged company data (whether proprietary or PII in nature) in the home environment, in transit, or in "third spaces." Participants noted the common experience that family members and housemates were arriving at implicit agreements regarding the protection of privileged information. Participants also noted the uneven distribution of private workspaces for those working outside of the office, pointing to the examples of younger workers working from kitchen tables surrounded by roommates. These concerns beg the following questions: Do these arrangements require explicit agreements about data sharing and privacy among members of a household? How might firms integrate these concerns into training materials? Should these concerns constrain data transfer from work networks to home networks?

The multitude of policy regimes that govern data make the answers to some of these questions more complex. Many firms operate across political jurisdictions in which both laws and regulatory expectations are quite diverse. Geographic differences in consumer-oriented privacy regulation, such as Europe's General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA), already overlap with geographic and cultural differences in employer-employee relationship norms, laws, and regulation.[3] Combined with the increasing prevalence of geographic boundaries around data flows (such as data localization rules that extend to cloud storage), these geographic differences will tend to reinforce rising barriers to doing business,

3 For example, a Canadian study of employees' privacy rights with respect to workplace surveillance found a patchwork of laws and frameworks spanning criminal codes, privacy directives, and labor laws at the international, national, and provincial levels. See https://www.cybersecurepolicy.ca/workplace-surveillance

including inside global companies. Without proactive efforts to harmonize policy, standards, and practices, hybrid work might exacerbate emerging fractures across regions that have diverging digital regimes. This could become a self-reinforcing cycle with negative consequences for economic growth, technology development, and geopolitics in the coming years. Hybrid work is not a primary cause of this dilemma, but it may be impacted by it.

At the same time, firms that do engage in a robust discussion around privacy and data protection expectations with employees have an opportunity to reshape norms for hybrid work environments, while fostering a collegial, collaborative, and supportive work environment that bolsters relationships among firms and their employees. Participants offered several ways to take advantage of this opportunity, including investing in fresh approaches to employee training around these issues, creating mechanisms to make a firm's security and privacy commitments visible in the context of an employee's hybrid workday, and building coalitions of firms to establish consensus on expectations for security and privacy. These conversations need to occur at a deeper level than boiler-plate consent agreements and should help people make informed decisions to manage the risks associated with using digital tools in a hybrid work environment.[4]

LIABILITY AND INSURANCE

Where liability lies for privacy and security breaches that result from hybrid work arrangements remains an open question. The increasing prevalence of home "Internet of Things" (IoT) devices makes this question even more acute. Manufacturers of IoT devices for the most part remain under-burdened when it comes to product liability; the security risks are *de facto* passed on to employees and, by implication, their employers. Beyond IoT devices, a variety of liability concerns are associated with the security and privacy risks posed by hybrid work, including the inadvertent or intentional capture of employee data, as well as the increased risk of data loss as information moves between work and home networks. In scenarios where the confidentiality of private or proprietary data is breached, where does liability lie? And if liability shifts to firms, do evolving cybersecurity insurance markets have a role to play?

In our analysis, the cyber-insurance markets are relatively nascent, with existing frameworks primarily focused on consumer notification, investigation, and crisis management associated

4 Newman, Jessica, Ann Cleaveland, Grace Gordon, Steve Weber. "Designing Risk Communications." CLTC White Paper Series. December 2020. https://cltc.berkeley.edu/2020/12/15/designing-risk-communications-a-roadmap-for-digital-platforms/; Redman, Thomas C and Robert M. Waitman. "Do You Care About Privacy as Much as Your Customers Do?" *Harvard Business Review*. January 28, 2020. https://hbr.org/2020/01/do-you-care-about-privacy-as-much-as-your-customers-do

with a particular breach. The responsibility of insurance companies is governed by individual contract-based relationships between the insurance providers and their clients. This may lead to new, stronger security requirements for hybrid work in order for firms to receive coverage.[5]

In light of the privacy and security challenges, participants discussed the potential use of liability protections that would shield firms from responsibility for breaches associated with hybrid work, and weighed their appropriateness, given the extenuating circumstances posed by the rapid shift to remote work driven by the pandemic. In some circumstances, firms already attempt to mitigate liability concerns in ways that create subsequent inconveniences, restrictions, and costs for employees. It is common in government agencies and in regulated financial-sector and accounting firms for employees to carry two phones: one that is controlled by the firm and used exclusively for work, and another for personal use (though day-to-day practices sometimes blur these lines). This reality begs the question: Do we need to similarly normalize the idea of two home networks? Such a configuration may be technically possible and could help mitigate some of the liability concerns outlined above, but would require a significant shift in behavior and practice. In addition, the question of where the costs would fall is not settled.

EQUITY CONCERNS AND OPPORTUNITIES

Across our research on hybrid work, equity concerns loomed large. Participants discussed the challenges the pandemic presented for workers responsible for caregiving, who are predominantly female. Participants also focused on the large "middle" of the workforce, whose lives have not changed as much as headlines about pandemic migration might suggest, and noted that in many cases, the shift to hybrid work may have solidified existing inequities. The shift to hybrid work has certainly made reliable internet access a job requirement. Workshop participants suggested that wealthier workers have been better able to access resources to maintain online access and secure their home workspaces, and the wealthiest firms have been better able to invest in securing their employees' workspaces, whether at home or on-premises. As noted above, home environments contain and reveal PII, as well as information about protected characteristics for both employees and "bystanding" members of the household. For example, senior executives might use a home printer to print documents related to personnel decisions or a proposed merger deal, and subsequently discuss either or both with family members within earshot. Even unintentionally, this information could pose a

5 McAndrew, Edward J. "Cybersecurity Law Alert." DLA Piper. July 29, 2019. https://www.dlapiper.com/en/us/insights/publications/2019/07/surviving-the-service-provider-data-breach/

challenge for equity considerations, from biased promotion decisions to the types of work that employees are asked to perform, given their home environment.

How can privacy and security decisions advance equity and opportunity in a hybrid workforce? Firms that support hybrid work will increasingly be called upon to create a level playing field across the home and office environments. Our research suggests that firms should lean into lessons from the new virtual environment and in some cases translate them "backwards" into the office environment. For example:

- **The flexibility of hybrid work can be an upside for equity considerations.** Multiple interviewees noted that the ability to hire remote workers expands their applicant pool and allows them to hire the best person for a role, regardless of their geographical location or time zone. One participant noted, for example, that "work is no longer a location, it is a state of mind," and the ability to work online could reduce potential barriers to entry for workers who are financially or otherwise unable to relocate for a job.

- **The entire security ecosystem can be strengthened by investments in enterprise-level support for workers, wherever they are.** By investing in setting up "professional" and "personal" profiles on home devices, home-based virtual private networks, and other technologies, firms can help the most vulnerable workers become more resilient to cyberattacks. Workshop participants noted that some firms are already working on tools to separate personal and work accounts on home networks. The more sophisticated and expensive of these types of tools have historically been provided to senior managers more often than to line employees, but equalizing digital security across the workforce will only become more important as professional and personal profiles migrate to augmented and virtual reality environments.

- **Hybrid work can force a reexamination of power imbalances between employers and their employees.** Tools used to monitor employees while they are logged in that are unacceptable to those working from home may no longer feel acceptable in the office environment. Employees who have become accustomed to affirmative consent mechanisms in the virtual environment (e.g., agreeing to record a meeting) may reasonably come to expect parallel consent mechanisms in the office environment.

Policy Recommendations

Considering these insights, we propose a diverse set of policy interventions that could have a positive impact by enhancing security for hybrid workers while supporting equity. These include a combination of government and company policies that will have a greater impact if supported by industry consortia, associations, or other standard-setting bodies.

1. **Use infrastructure investment to enhance the upsides of both the equity and security agendas.** Through the recently passed bipartisan infrastructure deal (Infrastructure Investment and Jobs Act), the U.S. Federal Government is set to invest approximately $65 billion in broadband to improve internet access, speeds, and pricing, with two-thirds of this funding to be allocated to the Department of Commerce Broadband Equity, Access, and Deployment Program. Broadband is a necessary ingredient for workers in less privileged circumstances to participate effectively in the hybrid labor market, but connectivity alone is not sufficient. A more refined policy should re-purpose some of these funds (or expand the overall pool of investment) to subsidize other parts of the hybrid work environment, including, for example, secure routers and other home network equipment. "The last mile" for internet connection (such as the coaxial cable from the street to the home router) should now extend fully into the home network and reflect the security and privacy requirements associated with hybrid work, regardless of whether the home is rented or owned. Several details would need to be worked out, including establishing appropriate standards for subsidized equipment, clarifying tax treatment for subsidized products and services, and setting rules around the dual-purpose nature of the home network. (For example, is a subsidy for workers in the home also *de facto* a subsidy for entertainment and gaming at the end of the workday?) Participants also highlighted the importance of allocating resources both to build out the internet and to regulate and protect it, noting that overwhelming focus has been on the former thus far.

2. **Support labor market flexibility.** In the current tight labor market environment, many employers are looking for ways to "lock in" highly valued employees in a variety of ways. Employers may seek to make "asset-specific investments" in hybrid work environments for their employees, providing infrastructure, software, physical space upgrades, and other enhancements that are non-standard and could not be used by the employee if she leaves the firm. Such benefits could help cement relationships and increase the costs to employees of leaving the firm for another employer. Future government policies should do nothing to disincentivize employers from making investments in employees' hybrid work

environments per se, but if labor market flexibility is a public policy objective, rules may have to be adjusted to ensure that such investments are transferable to a new employer if the employee chooses to take a new job.

This is a complex trade-off, as employers will logically reduce their investments if the home-based technology upgrades they provide can at any time be carried elsewhere by the employee to the benefit of another firm. Firms have long faced a similar dilemma when investing in training and education programs, however, and have found a way to mitigate these risks over time.[6]

Public policy can accelerate the process of firms' investing in the hybrid work environment. For example, a set of standards that implement interoperability and "portability," perhaps reinforced by preferential corporate tax treatment for firms that adhere to those standards, would work against lock-in on all sides — an undesirable outcome where an employee would be tied to an employer by an unrecoverable infrastructure investment. Some firms may still bear excess costs if they lose a larger proportion of their employees to other firms, but this risk is unavoidable, and could motivate firms to compete to retain employees in other ways.

3. **Update policies and practices on competitive bids for facility and job location.** Governments at the city, state, and national levels have long offered incentives, such as tax holidays and infrastructure investments, to attract the development of business facilities, such as headquarters, factories, and other facilities, based on the assumption that such projects will bring jobs to their local areas.[7] The recent competition for Amazon's "HQ2," which eventually landed in northern Virginia, and Tesla's decision to move its headquarters to Austin, Texas serve as two recent examples of this phenomenon, as tax incentives ostensibly drove corporate location decisions.[8] The mainstream of regional economic development theory has long argued that these competitions asymmetrically benefit firms over governments (that is, governments pay more than they should, given the expected

6 Rogers, Margaret. "A Better Way to Develop and Retain Talent." *Harvard Business Review*. January 20, 2020. https://hbr.org/2020/01/a-better-way-to-develop-and-retain-top-talent.

7 Wilson, Reid. "States, cities rethink tax incentives after Amazon HQ2 backlash." *The Hill*. February 17, 2020. https://thehill.com/homenews/state-watch/483127-states-cities-rethink-tax-incentives-after-amazon-hq2-backlash

8 Kang, Cecilia. "Northern Virginia Is Keeping Amazon's 25,000 Jobs, and Wants You to Know It." *New York Times*. February 15, 2019. https://www.nytimes.com/2019/02/15/technology/amazon-virginia-crystal-city.html ; Chokshi, Niraj. "Tesla Will Move Its Headquarters to Austin, Texas, in Blow to California." *New York Times*. October 7, 2021. https://www.nytimes.com/2021/10/07/business/tesla-texas-headquarters.html

benefits).[9] The move to hybrid work has significant potential to further disadvantage governments, since bids are often competitive and the range of potential locations that can reasonably compete to attract jobs will likely be much larger.

Governments would likely benefit from putting some shared boundaries around this competition going forward via regulation or legislation. Indeed, the economics literature suggests that the zero-sum game fostered by these policies incentivizes a "race to the bottom," which leads to companies competing for increasingly large subsidies and does not leave municipalities and state government with long-term guarantees.[10] Workers, who often do not benefit directly from these location subsidies, might also benefit from constraining the competition. Bounding this kind of competition is challenging, given the number of governments impacted, and the different levels of resources, risk tolerance, and political sensitivity that each is likely to have. Counterintuitively, this is an area where a consortium of large firms in a particular sector might benefit themselves in the longer term by taking a leadership position and jointly committing to an upper bound of incentives that they might ask from governments to protect and bolster their business. An industry association that represented the five largest technology firms in the United States, for example, could in principle agree on a formula to limit subsidy asks to some specific ceiling, as long as this can be done in a manner that does not constitute collusion.

4. **Advancing, standardizing, and rebranding "zero trust."** As noted above, zero-trust architecture is a promising approach to better secure the hybrid work environment now and in the near-term future, as it abandons traditional "moat-and-castle" models of network security and instead continuously evaluates user behavior on the network. But zero-trust architecture, given its relative infancy in implementation, still represents a high-level umbrella concept that encompasses a variety of technologies and practices that differ widely in implementation.[11]

   The U.S. Government has already taken initial steps toward standardization. The National Institute of Standards and Technology (NIST) has developed a framework, NIST 800-207, that outlines general principles for zero trust, such as continually authenticating

9 Wilson, Daniel J. "Beggar thy neighbor? The in-state, out-of-state, and aggregate effects of R&D tax credits." *The Review of Economics and Statistics* 91, no. 2 (2009): 431–436; Bartik, Timothy J. *Making sense of incentives: Taming business incentives to promote prosperity*. WE Upjohn Institute, 2019.

10 Mazerov, Michael. "Should Congress Authorize States to Continue Giving Tax Breaks to Businesses?" Center on Budget and Policy Priorities. February 18, 2005. https://www.cbpp.org/research/should-congress-authorize-states-to-continue-giving-tax-breaks-to-businesses

11 Rose, Scott, Oliver Borchert, Stu Mitchell, Sean Connelly. "Zero Trust Architecture." SP 800-207. NIST Information Technology Laboratory Computer Resource Center. August 2020. https://csrc.nist.gov/publications/detail/sp/800-207/final

and authorizing user access, monitoring user behavior, and revoking access to resources when no longer needed. The market for tools to implement zero trust architecture, however, remains fragmented. Three approaches to zero-trust that are well-documented include enhanced identity governance that defines access for authenticated users; micro-segmentation of networks, which allows access to data in defined tranches; and software-defined network perimeters that use an overlay network. As these technologies mature, policymakers might consider discussions focused on converging standards for both government networks (e.g., OMB's Federal Zero Trust Strategy) and enterprise.[12]

Part of this effort might include rebranding the term "zero trust," as workshop participants noted that this label may carry a negative connotation if users feel they are not trusted, or that the network itself cannot be trusted. Refocusing zero trust around addressing bad actors on the network and providing "layered security" may support more widespread implementation. The importance of branding and psychology should not be underestimated, as nearly all CISOs we spoke with stressed the importance of organizational culture, the "human-in-the-loop" model, and behavioral and usable security. The current push by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) toward zero trust implementation in federal agencies could include investments in collective resources and expertise for usable security, and could leverage the power of CISA's bully pulpit for re-branding.

12 n.a. "Federal Zero Trust Strategy." Office of Management and Budget. n.d. https://zerotrust.cyber.gov/federal-zero-trust-strategy/

Conclusion

The shift to the hybrid work environment represents an economy-wide "reset" of work location and practices, and offers a rare opportunity to break through long-standing habits of personal and organizational behavior that negatively impact privacy and security. Escaping the downsides and realizing the upsides will require a combination of legislative and regulatory action, coordination within and among industry associations, and the continued development and implementation of new tools and technologies. This matters tremendously because security and privacy in the hybrid work environment will be tied tightly to productivity, equity, and innovation over the course of the next decade. How firms and policymakers converge around new privacy and security considerations will determine whether hybrid work lives up to its potential of greater flexibility for workers and greater access to talent for firms.

About the Authors

Ann Cleaveland is the Executive Director of the Center for Long-Term Cybersecurity.

Grace-Alice Evans is a Non-Resident Fellow at the Center for Long-Term Cybersecurity.

Andrew Reddie is the Research Director for the Center for Long-Term Cybersecurity.

Isaac Vernon is a student in the UC Berkeley School of Information and a Research Assistant for the Center for Long-Term Cybersecurity

Steve Weber is the Faculty Director for the Center for Long-Term Cybersecurity and a Professor in the UC Berkeley School of Information

Acknowledgments

We are grateful to the security experts who contributed as interviewees and workshop participants. This project was made possible by gifts from Fortinet, EY, and Zoom, Inc. in support of independent academic research.

CLTC

Center for Long-Term Cybersecurity

UC Berkeley

Center for Long-Term Cybersecurity
cltc.berkeley.edu
@CLTCBerkeley