October 2024

ICIT

The Security Challenges of a Hybrid Workforce

Jim Routh
Fellow, Institute for Critical Infrastructure Technology

www.icitech.org

Table of **Contents**

About ICIT

The Institute for Critical Infrastructure Technology (ICIT) is a nonprofit, nonpartisan, 501(c)3 think tank with the mission of modernizing, securing, and making resilient critical infrastructure that provides for people's foundational needs. ICIT takes no institutional positions on policy matters. Rather than advocate, ICIT is dedicated to being a resource for the organizations and communities that share our mission. The views and opinions expressed in this essay are solely those of the author(s) and do not necessarily reflect the official policy or position of ICIT. Any assumptions made within the analysis are not reflective of the position of any entity other than the author(s).

To learn more, please visit www.icitech.org

CyberRisk ALLIANCE | Thank you to our Strategic Partner **CyberRisk Alliance** | www.cyberriskalliance.com

The Security Challenges of a Hybrid Workforce

The shift to hybrid work models has introduced a range of new security challenges for enterprises that are not yet managed effectively. The significant increase in the enterprise attack surface due to employees and third parties accessing company resources from remote locations requires new thinking on the types of controls that offer effective risk management in the future. Maintaining consistently applied cybersecurity controls with the shifting attack surface is beyond the current capabilities of most enterprises today, resulting in an increase in cyber incidents and related supply chain disruptions.[1]

The COVID-19 pandemic was a catalyst, changing how we work with technology and, most significantly, where we work.[2] This change extended the attack surface for all enterprises, requiring additive controls for effective risk management. Since the end of the pandemic, enterprises have attempted to encourage employees to return to work in corporate offices without much success. It appears likely that the shift toward remote and hybrid workers will continue globally.[3] This change comes from the societal shift in how we work and the evolution of technology choices by both enterprises and digital consumers.

[1] https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/#:~:text=In%202023%20alone%2C%20more%20than,theft%20constituted%20over%201.1%20million
[2] https://www.upwork.com/press/releases/the-future-of-remote-work
[3] https://www.officernd.com/campaign/resources-hybrid-report-work-trends-2024/

Identity, Access Management, and the "Last Mile"

Unfortunately, ensuring that only authorized personnel have access to company systems is more complex when employees are not physically in a company office. The "last mile" of networks,[4] which includes unsecured home networks, many types of personal devices, and reliance on public Wi-Fi, contribute to vulnerabilities that cybercriminals are increasingly exploiting. Experts estimate that about 70% of passwords used for home routers are weak meaning that enterprise (customer, employee, financial, etc.) data are potentially exposed.[5] In hybrid environments, the risk inherent in "last mile" connectivity means that the security of the enterprise's corporate data depends on how the home router is configured and the endpoint security of personal devices.[6] The difficulty in monitoring and enforcing security policies outside a controlled office environment further complicates efforts to protect sensitive information.

Hybrid work models also exacerbate the challenges of identity and access management,[7] including the growth of using SaaS applications both inside and outside corporate networks to supply core functions for employees and 3rd party service providers.[8] Traditional authentication methods, such as passwords, are insufficient to manage these risks. Phishing attacks and social engineering tactics are more likely to succeed in a hybrid work setting.[9] The blend of remote and in-office work demands robust, adaptive security solutions to manage these risks and protect organizational data from evolving cyber threats.

[4] https://www.ncta.com/whats-new/the-last-mile-explained
[5] https://www.forbes.com/sites/leemathews/2021/10/28/70-of-passwords-for-home-wi-fi-networks-are-terrible/
[6] https://www.ncta.com/whats-new/the-last-mile-explained
[7] https://www.upwork.com/press/releases/the-future-of-remote-work
[8] https://www.spendesk.com/blog/saas-statistics/
[9] Phishing attacks and social engineering tactics are more likely to succeed in a hybrid work setting

Balancing Personal and Work Data Protection

Remote and hybrid workers also find it challenging to balance personal support needs (e.g., family members and home support staff) with work requirements for data protection. Conventional data protection controls were embedded into proprietary network architectures combined with endpoint devices when away from the office. Next-generation network computing for the enterprise is now more likely to include software-defined networking capabilities (SD-WAN) that provide better performance at a lower operating cost. This approach requires a different configuration of data protection capabilities pushed to the network edge that supports diverse endpoint devices. Enterprises need to educate their employees on specific practices to more effectively manage the risk of the "last mile" to protect the company and themselves. Currently, enterprises depend on remote workers to follow effective cyber resilience practices, which may be too tall an order. For example, 65% of digital users apply the same passwords across personal and corporate accounts.

Cybersecurity threat actors have recognized the extended enterprise attack surface and have pivoted to tactics designed to exploit the vulnerabilities. The year-over-year growth of cyber incidents involving compromised credentials is 71%, which is significant evidence for threat actors regularly using compromised credentials to escalate privilege and cause business disruption at scale. Another increasing trend is software supply chain attacks, such as the compromise of Snowflake, that use weak software developer credentials to compromise SaaS accounts, enabling criminals to infect the software distribution process with malware, impacting the customers of the software provider.

[10] https://www.marketsandmarkets.com/Market-Reports/software-defined-wan-market-53110642.html#:~:text=The%20software%2Ddefined%20wide%20area,the%20SD%2DWAN%20market%20growth

[11] https://techreport.com/statistics/cybersecurity/password-reuse-statistics/#:~:text=Main%20Password%20Reuse%20Statistics,-Up%20to%2065&text=of%20their%20accounts.-,More%20than%2050%25%20of%20workers%20worldwide%20like%20to%20use%20the,81%25%20of%20company%20data%20breaches

[12] https://datadome.co/guides/credential/compromised-attacks/#:~:text=There%20has%20been%20a%2071,increase%20in%20compromised%20credential%20attacks.&text=The%20average%20cost%20of%20a,cybercriminals%20is%20US%20%244.45%20million.&text=Poor%20password%20security%20practices%20are,majority%20of%20compromised%20credential%20attacks

[13] https://thehackernews.com/2024/06/snowflake-breach-exposes-165-customers.html

The Evolution of Third-Party Governance

I believe, based on two decades as a CISO, that cybersecurity professionals should both implement and design cybersecurity controls. Conventional or established controls will weaken over time as technology uses evolve. When technology usage changes regularly, it is folly to presume that all conventional control objectives and requirements never need to change. This is certainly the case when relying on 3rd party governance controls, often referred to as "Third Party Risk Management" (TPRM).

TPRM control frameworks, methods, and tools are well-established and have been used in highly regulated environments, like financial services, for several decades. The cornerstone of conventional TPRM controls is a supplier risk assessment questionnaire that provides the enterprise with self-attested information from the vendor on an annual basis. I remember working to develop the original version of the standard information gathering (SIG) questionnaire used today and currently supported by the Shared Assessments organization.[14]

The standard approach is for a supplier to provide answers to questions across a broad spectrum of cybersecurity controls to help the enterprise determine the risk of working with that vendor. The process may take weeks as the supplier needs to carefully provide answers and then the enterprise should thoroughly analyze the results. The benefit of using the SIG is that it has been somewhat automated with questions tailored to the type of service or product being offered by the vendor. Auditors and regulators are very familiar with this approach to TPRM and applying different ways of testing the efficacy of the control assessment process.

However, this conventional approach to TPRM is outdated and no longer valid given the rapid maturity of supply chain management practices. Emerging practices in operational risk management rely on near real-time information-feeding models that identify deviations in patterns, triggering automated workflow to manage risk. An annual assessment of vendor risk is insufficient to manage the risk of a software supply chain disruption from cyber or other types of threats.

[14] https://sharedassessments.org/

An alternative approach for an enterprise is to analyze the universe of third-party vendors and identify specific categories of service providers and product providers based on categorical risk attributes. As an example, a professional service firm with access to customer records operating in the Far East, say Vietnam, has a very different risk profile from a professional service provider operating in the US with employees working in development centers. They are both professional service vendors, but the risk profiles differ significantly. Therefore, since categories should be defined by the control requirements required by the specific risk profiles, these two professional service firms belong to different categories commensurate with the distinct control requirements that should be enacted.

Once vendor categories and control requirements are defined, it is time to apply a few data science fundamentals to creating and managing a vendor risk score. In simple terms, risk scores can use a numeric scale from 0.0 (no risk) to 5.0 (highest risk). An initial score is calculated based on how well the vendor meets the required controls for their product or service category. This score can be manually created by an analyst, automated by completing a questionnaire that specifies the control requirements, or a combination of both.

Returning to the example, the onshore service provider may be asked to use a secure browser with data protection features for every employee. In contrast, the offshore vendor may be asked to apply continuous identity verification with screen protection controls that are additive for employees and contractors working remotely.

To be effective, a TPRM function needs to set up subscriptions to online resources across multiple dimensions, including, but not limited to, cybersecurity. These daily data feeds provide inputs to a risk model that compares the information to the vendor profile and determines the change to the risk score based on deviation from the established pattern. In other words, the vendor risk score should be updated every day. The primary input is from the daily data feeds combined with the opportunity for a TPRM analyst to modify the risk score manually. When the vendor risk score increases beyond a pre-determined threshold, say a score of 4, an automated workflow generates an email to the vendor requesting a response to the event that triggered the risk score increase. The TPRM analyst can lower the risk score based on the vendor response, essentially rewarding the vendor for proactive and resilient behavior. In a conventional questionnaire-based approach vendor risk score changes annually, but in this case, the vendor risk score could potentially change daily.

In the above proposal, annual questionnaires are no longer needed to drive the definition of vendor risk. Instead, vendor risk is calculated daily based on many factors, and data science automates the workflow, reducing the burden on an analyst to initiate risk management activity. This approach increases capacity for operational risk management while lowering the dependence on human analysts to initiate risk management operations, resulting in more effective risk management at a lower operating cost. As a bonus, a TPRM analyst now has more marketable skills that significantly increase her ability to manage operational risk.

There are other opportunities to design new controls to manage the extended enterprise attack surface as part of a TPRM program. For example, service providers that use remote workers should be asked to deploy continuous identity validation capabilities. Originally, IT and cyber professionals used a binary authentication model. If a user provided the proper credentials, usually user ID & password, they were allowed access. If the credentials were incorrect, they were not allowed access. This binary model of authentication is based on an event and a singular outcome: allowed access or not.

An alternative model considers a non-binary approach to the authentication process where behavioral attributes are compared with an established pattern and can change access at any time, even after completing a binary authentication event. Many authentication solutions that do not require passwords use some variation on continuous authentication. For example, a remote worker can use a version of continuous identity validation to ensure she is using the laptop. For example, when she leaves her laptop or looks away from the screen, the screen goes into sleep mode until she returns, preventing shoulder surfing by others who happen to be in the same room as the laptop. This control is more effective for employees with access to sensitive information than several conventional controls used when workers are in a single location. Enterprises that deploy these types of additive controls, which are available on the market today, significantly reduce the extended enterprise attack surface created by remote workers.

Real-Time Risk Management and Continuous Authentication

Passwords have served the industry very well for the past 60+ years,[15] but they were never designed for digital users needing to access several hundred digital assets that each require a secure login.[16] The volume of digital assets that require authentication is well beyond the average person's ability to remember complex passwords. Migrating to continuous authentication options causes two outcomes that are historically uncommon together:

1. A much-improved user experience
2. Better security

The application of continuous authentication with a focus on data protection opens a range of control options for the enterprise to effectively manage the cyber risk of the attack surface extended by remote workers. An enterprise can significantly reduce the probability of a cybersecurity breach by reducing the dependence on credentials that must be issued, stored, and processed. When remote workers are forced to work at home with others (family members or shared households) it increases the risk of others shoulder-surfing and getting exposure to sensitive information. Continuous authentication capability recognizes this situation and puts the screen to sleep in real time when the user is not viewing the screen. Even if the threat actor can capture an image from the laptop's screen, the image will include a digital watermark identifying the laptop owner, making it difficult to monetize the data in the image. An emerging set of new controls is referred to as continuous identity assurance that combine biometric measures with pattern matching to offer consistent data protection to protect digital consumer privacy.[17]

These new control capabilities are open to enterprises and cybersecurity professionals who recognize the need to design new control capabilities to address the extended enterprise attack surface of remote workers, both employees and third parties. The evolution of digital identity management capabilities gives enterprises the choice to move toward continuous, real-time risk management for employees, contractors, service providers, product providers, and customers alike. Many of these options use biometric (e.g., facial recognition, voice recognition, keystroke dynamics) attributes that can be easily compared to established patterns. Any deviation from the pattern can trigger risk management action in near real time.

Enterprises today must consider the necessity of *designing* new cybersecurity controls. Continuously verifying user identity based on a range of diverse attributes or biometrics adds a dynamic layer of security that complements other technical, administrative, and physical controls, thereby creating a more secure and resilient work environment for all parties. The result decreases enterprise attack surface making it easier to manage with hybrid workers.

Third party governance practices must evolve to real time, data-driven practices that enable an enterprise to respond to changes in risk posture rapidly while enabling remote work with the controls essential for cyber resilience. The list of new controls and technical solutions for remote and hybrid workers available to an enterprise is growing every day. Enterprises need to make the right investments in these capabilities to more effectively manage cyber risk and reduce the attack surface of remote workers requiring new control design specific for the way people work today.

[15] https://www.nytimes.com/2019/07/12/science/fernando-corbato-dead.html
[16] https://www.morningstar.com/news/globe-newswire/9121266/people-have-around-170-passwords-on-average-study-shows
[17] https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html

ICIT

www.icitech.org