Strategies for Securing Your Remote Workforce

Dylan Hall
Cyber Security Engineer
Afidence

Bryan Hogan
President & Co-Founder
Afidence

University *of* Dayton
Center for Cybersecurity & Data Intelligence

OHIO CYBER RANGE INSTITUTE

Overview

The global pandemic forced many companies to quickly adapt to a remote workforce model. Threat actors immediately responded by adjusting their tactics to take advantage of weaknesses resulting from this change. Many companies have not yet made the changes needed to minimize new security risks and maximize data confidentiality, integrity, and availability. This paper presents several practical strategies for securing your remote workforce.

About the Authors

Dylan Hall is a Cyber Security Engineer at Afidence, seamlessly merging a psychology background with robust technical expertise. He offers a unique perspective, emphasizing a people-centric approach to cybersecurity while excelling in vulnerability analysis, security posture assessment, and incident response. Dylan's diverse experience ranges from penetration testing and remediation planning to speaking engagements and cybersecurity content creation. He has recently honed his focus on GRC within the DoD sector, showcasing specialized knowledge in CMMC compliance and maturity development.

Bryan Hogan is the President and co-founder of Afidence, an Ohio-based technology consulting firm specializing in cybersecurity, cloud, and application development. A graduate of DeVry University, he has over three decades of experience helping organizations get the most out of their technology and cybersecurity investments. Bryan sits on several boards, is a frequent speaker at industry conferences and enjoys collaborating with the broader technology and business communities.

University of Dayton
Center for Cybersecurity and Data Intelligence
937-229-1929
udaytoncyber@udayton.edu

Find more tools at **go.udayton.edu/cybersecurity**

Strategies for Securing Your Remote Workforce

Dylan Hall
Cyber Security Engineer
Afidence

Bryan Hogan
President & Co-Founder
Afidence

Introduction

The global pandemic forced most companies to adapt to a remote workforce model quickly. Threat actors immediately responded by adjusting their tactics to take advantage of new weaknesses that emerged from this change. While many of these companies have since updated their business model to reap the benefits of a remote workforce, too few have made the changes needed to minimize new security risks and maximize their data's confidentiality, integrity, and availability. As such, this paper presents several practical strategies to secure your remote workforce.

What Was Once Considered Temporary

The pandemic compelled most companies to temporarily change their workforce and operating model to ensure continued operations. However, many of these changes have now become permanent, as companies have realized the significant advantages of these changes, including:

- Access to talent: The transition to a remote-enabled workforce has broadened access to an exponentially larger talent pool.
- Reductions in costs: Companies with a remote workforce have been able to reduce their office-related expenses, including office space, phone systems, network connectivity, and multi-function print/copy devices.
- Revenue growth: The widespread acceptance of remote work has enabled some industries, including professional services, to venture into new markets with minimal capital investment. Pandemic quarantines prompted restaurants to offer or expand take-out services, even spurring the growth of ghost kitchens. Cloud computing companies have experienced tremendous growth through cloud-centric solutions built to serve the remote/hybrid workforce.

Process and Technology Changes

Companies that recognize the long-term opportunities that the pandemic exposed are making the operational and technological changes needed to capitalize on those benefits, including:

- Broadening their recruiting strategy to reach a larger candidate pool.
- Embracing virtual meeting platforms such as Zoom, Microsoft Teams, and Google Meet as a primary means of communication.
- Shifting from legacy collaboration tools, such as on-premises file servers, to cloud-based alternatives like Slack, Dropbox, and Google Drive, specifically designed to support remote work environments.
- Accelerating the migration from on-premises business systems to cloud-based solutions, allowing for enhanced accessibility and scalability.

The Need for a Remote / Hybrid-First Cybersecurity Program
The advent of hybrid and remote work models has influenced the cybersecurity landscape, calling for a comprehensive re-evaluation and re-focusing of cybersecurity awareness and user training programs. While traditional in-office work models provide a more controlled environment where cyber risk can be better contained, remote work presents a multifaceted and complex cyber threat landscape with its many devices, unmanaged networks, and digital touchpoints. Organizations must pivot their focus towards creating a robust culture of cybersecurity that extends beyond the physical office, extending through to the digital workspaces of remote employees.

Strategies to Secure Your Remote / Hybrid Workforce
Create a remote work policy or rewrite existing policy to assume remote
A comprehensive remote work policy is a fundamental element of effective cybersecurity management in a remote work environment. This policy encapsulates the organization's expectations of remote employees regarding their conduct and practices, specifically regarding utilizing company resources, adherence to data security protocols, and engagement with incident reporting mechanisms.

Given the evolving threat landscape and the rapid pace of advancements in remote work procedures, it is incumbent upon organizations to review and update their remote work policies routinely. This procedure should ensure the policy accurately represents current risks, challenges, and best practices associated with remote work.

For instance, the policy must specify acceptable behavior patterns, including:

- Proper Use of Company Equipment: Details such as proper software installations, internet usage restrictions, and regular software updates must be communicated to employees.
- Data Handling Practices: This involves guidelines on data sharing, encryption methods, and rules for downloading sensitive data.
- Use of Personal Devices: If personal devices are used for work, the policy should clarify security requirements, such as installation of antivirus software, use of secure networks, and regular security updates.
- Home Network Security: Employees should be educated about securing their home networks using strong passwords and encryption and about the risks associated with public Wi-Fi.

Moreover, the policy should enumerate the steps employees are to undertake in case of a suspected or actual security breach. This includes information on immediate points of contact, the type of information to be provided, and the expected involvement in the containment and investigation of the incident.

Effective communication of the remote work policy to all employees is critical. Information should be presented in a lucid, succinct, and readily comprehensible way. Organizations might consider organizing interactive training sessions or workshops to acquaint employees with the critical elements of the policy.

For example:

- Interactive Training Sessions: Use live sessions, webinars, or e-learning courses to walk employees through the policy, using real-world scenarios to illustrate policy points.
- Workshops: Run practical workshops where employees can ask questions, discuss scenarios, and explore the policy more thoroughly.

- Policy compliance should be monitored continuously, and violations addressed promptly and consistently. A robust feedback loop and an open dialogue with employees about the policy can lead to better understanding and adherence, ultimately improving the organization's cybersecurity posture.

Secure home networks and routers
An organization's security perimeter broadens with remote work to encompass the home networks of its employees. Unlike corporate networks, which typically utilize stringent security protocols and are continually overseen by specialized security teams, home networks often lack similar protective measures.

Guidance should be provided to employees on how to enhance the security of their home networks. Several fundamental steps include:

- Changing Default Router Credentials: Cybercriminals frequently leverage universally known default passwords to gain unauthorized access. Employees should replace default usernames and passwords with strong, unique credentials.
- Activating Wi-Fi Protected Access 3 (WPA3): WPA3 is the most recent and secure protocol for safeguarding Wi-Fi networks and enabling it can provide robust protection against unauthorized access and eavesdropping. It improves upon previous protocols by introducing higher encryption standards and individualized data encryption.
- Disabling Remote Management Features: Remote workers should deactivate remote management functionalities on their routers, which could deter potential attackers from manipulating the router remotely. These settings can often be found in the router's web interface and should be disabled unless necessary.
- Patching Home Routers: Regular updates to router firmware are integral to patching possible security vulnerabilities and augmenting the overall security of the home network. This is akin to updating one's computer software, as router updates often contain security patches to protect against known vulnerabilities.

Secure your data
The rising ubiquity of remote work has escalated the quantity of data transferred beyond the conventional corporate network, thus accentuating the need for data security. Organizations must highly value and focus on robust data management practices and employ technologies that guarantee data confidentiality, integrity, and availability.

Several measures can be implemented to bolster data security:

- Implement Data Encryption: Data encryption is crucial and applicable to data at rest (stored data) and in transit (moving data). Encryption converts data into an indecipherable format, ensuring its protection, even if intercepted during transmission or extracted from a misplaced or stolen device. Various encryption methods, such as Advanced Encryption Standard (AES) for data at rest and Transport Layer Security (TLS) for data in transit, can be used.
- Enforce Access Controls: An essential step is enforcing access controls based on the Principle of Least Privilege (PoLP). With the PoLP, employees receive only the minimum access needed to perform their duties, reducing the risk of data leakage or misuse. Access controls could be role-based, where permissions are tied to an employee's role within the organization, or context-based, where permissions are granted based on a combination of factors such as location, device, and time.
- Secure Cloud Storage and Collaboration Tools: Cloud storage and collaboration tools have become indispensable for remote work. However, if not properly configured, they can inadvertently expose sensitive data. Organizations should

establish lucid guidelines and protocols for using these tools. This includes correctly setting privacy controls, training employees on safe sharing practices, and routinely auditing these settings and practices to ensure compliance.

Embrace multi-factor authentication
Multi-factor Authentication (MFA) is a security protocol requiring users to present two or more unique types of evidence, or factors, to authenticate their identity during logins or transactions. These factors may include something the user knows (such as a password), something the user possesses (like a physical token or smartphone), or an aspect of the user's inherent physical identity (biometrics), among others.

MFA presents a formidable obstacle to cybercriminals by introducing an added layer of complexity to the authentication process. This complexity makes it significantly more challenging for attackers to gain access, even if they acquire a user's password. MFA can markedly augment an organization's security stance, especially in a remote work environment, where users frequently connect from diverse locations and networks.

To fortify security, the following MFA methods can be employed:

- Authenticator Apps: Applications such as Google or Microsoft Authenticator generate time-sensitive codes that users input during the login process. This method avoids potential SMS intercepts but requires users to install the app on a separate device.
- Hardware Tokens: These devices generate a code when activated. While they offer robust security, they come with increased costs and the inconvenience of carrying a separate device.
- SMS-Based Codes: Upon attempting to log in, the user receives a unique code via SMS that must be entered to gain access. While convenient, this method is not impervious to interception, so its use should be considered based on the sensitivity of the information being protected.

MFA should ideally be deployed across all systems and applications an organization utilizes. However, organizations should prioritize implementing MFA for high-risk accounts, recognizing that this may only be viable due to cost or compatibility issues. Such accounts may include administrator profiles, accounts with access to sensitive data, or accounts capable of conducting high-risk transactions.

In choosing among various MFA methods, organizations should evaluate these options within the context of their specific needs. Factors for consideration should include the sensitivity of the data or system, the user experience, and the cost of implementation and management.

Implement complex passwords, and consider password managers
Password security serves as a central tenet of cybersecurity. The integrity of an organization's IT infrastructure often hinges on the protective layer of passwords, thereby concreting their role as the first line of defense. The strength of this defense significantly depends on the complexity of the passwords and the strategy adopted for their management.

Contrary to the notion of complex passwords being merely arbitrary character sets, they should ideally constitute a deliberate set of uppercase and lowercase letters, numerical digits, and special characters. A password of optimal complexity typically ranges from 12 to 16 characters. Such complexity effectively thwarts standard attacker tactics, including

brute-force and dictionary attacks, by significantly increasing the computational time and effort needed for an attacker to discover the password and gain unauthorized access. Nevertheless, the draw of complex passwords is often undermined due to a propensity towards easily guessable or weaker passwords. This tendency predominantly stems from the challenge associated with remembering intricate passwords and a need to understand their importance.

The following strategies can address these challenges:

- Use of Password Managers: Password managers have emerged as a powerful solution. These tools manage numerous complex passwords under one primary master password. This approach relieves users from the mental strain of memorizing various intricate passwords, requiring only the retention of the master password. Advanced password managers further elevate user convenience by offering functionalities such as password generation, automatic fill, and cross-device password vault synchronization.
- Enforce Password Policies: Organizations can enforce password policies requiring users to periodically create and change complex passwords. These policies should also discourage password reuse across different accounts.
- Provide Security Awareness Training: Regular training sessions can educate employees about the significance of password security and how to create and manage complex passwords.

In the selection of a password manager, due diligence is crucial. Key considerations should involve robust encryption standards for password storage, a zero-knowledge architecture that restricts even the service provider from accessing the user's data, and a secure password recovery mechanism.

Patch, monitor, and secure your endpoints
Endpoint devices, including laptops, smartphones, and tablets, are significant components of an organization's network. Frequently serving as the most vulnerable link in the security chain, these remote computing devices become prime targets for cyber-attacks.

A three-pronged approach may be adopted to secure these devices:

- Patch Management: This is an essential aspect of maintaining secure endpoints. Software vendors regularly release patches to rectify bugs, address vulnerabilities, or introduce new functionalities. Routine installation of these patch updates can fortify endpoint devices, preventing exploitation due to known vulnerabilities. For instance, Microsoft's 'Patch Tuesday' provides regular security updates that should be promptly installed to reduce potential exposure.
- Use of Antivirus or Anti-malware Tools and Firewall Solutions: These are integral to endpoint security. Such tools safeguard against malicious software and unauthorized access while monitoring network traffic for potential cyber threats. For example, reputable solutions like Bitdefender or Norton can offer comprehensive security suites that include these functionalities.
- Implementation of Advanced Endpoint Detection and Response (EDR) Solutions: EDR solutions offer real-time monitoring and threat detection by integrating artificial intelligence and machine learning technologies. This proactive approach allows for a quick and efficient response to identified threats. A solution such as CrowdStrike's Falcon platform can provide robust EDR capabilities.

Despite the unique challenges a remote work environment presents, such as unsecured networks or the lack of physical access to devices, robust endpoint security can be

sustained. This is achievable using secure remote access technologies, regular security audits, and comprehensive user training.

Implement an incident response plan that revolves around a remote workforce
Maintaining an Incident Response Plan (IRP) is becoming compulsory in the world of remote work. An IRP provides a systematic approach to managing the aftermath of a security breach or suspected attack by fulfilling its primary objective to limit damage, manage recovery effectively, and reduce costs associated with downtime and reputational damage.

The increasing prevalence of remote work presents unique challenges to incident response, making it imperative for organizations to revamp traditional IRPs to cater to remote work scenarios. It's not just about reacting to an incident; instead, it's about managing the intricacies of remote work incident response.

An essential step is identifying the types of incidents that might occur in a remote environment, such as malware infections, unauthorized access, or data breaches. Once these potential incidents have been detected and identified, a detailed initial response guide should be made available to all workers outlining the immediate steps to mitigate further damage.

Assigning roles and responsibilities is another crucial aspect of an effective IRP. Establishing a dedicated incident response team comprising of roles including incident response manager, security analyst, and communications manager is essential. In a remote work scenario, this team may need to coordinate with external partners such as cyber risk insurance providers or third-party forensic investigators.

Further, the IRP should define a clear communication strategy to manage information flow during an incident. This strategy should define which communication channels to use, who should be involved in the communication loop, and the nature of the information to be shared. It is also important to consider preserving data confidentiality, integrity, and availability during such communication.

Finally, the plan should be tested and refined regularly through simulations and tabletop exercises to help identify gaps and provide practical experience to the response team and participating users.

Cultivate a cyber-aware team
It is important to consider cybersecurity a shared endeavor. Cultivating a cybersecurity-literate workforce is one of the most effective strategies to bolster an organization’s defenses. Employees who are well-versed in recognizing and responding to potential threats form a formidable defense against cyber-attacks.

Implementing an effective cybersecurity awareness program involves several stages. The first step is to educate employees about the various threats they may encounter, including phishing attacks, ransomware, and social engineering schemes. This knowledge will empower them to promptly identify and report potential threats, reducing the risk of a successful breach.

However, more than imparting knowledge is required. Practical training sessions should be conducted to equip employees with the skills they need to protect themselves and the organization. For instance, they should be trained to create strong, unique passwords, secure their home networks, and securely store, share, and retrieve sensitive data.

In a remote work world, the cybersecurity awareness program should also cover topics specific to remote work. This might include information on the risks associated with using public Wi-Fi networks, the importance of securing personal devices used for work, and how to identify and report suspicious activities while working remotely.

Creating a cybersecurity-conscious culture requires continuous effort. Regular updates on emerging threats, best practices, and refresher training sessions are crucial to maintaining a well-prepared workforce. A cybersecurity-literate workforce can significantly enhance an organization's resilience in the face of ever-evolving cyber threats.

Work with your cyber risk insurance agent

The cyber risk insurance policy is a critical yet often underutilized aspect of a comprehensive cybersecurity strategy. This policy provides a safety net by mitigating the financial repercussions of cyber threats. The process of becoming insured is valuable, as it facilitates a detailed assessment of an organization’s security posture and identifies specific gaps and needed changes. The shift to remote work has expanded the threat landscape, making it prudent for businesses to reassess their insurance needs. The insurance agent plays a pivotal role in this process, helping organizations understand their existing coverage and identify potential blind spots.

Insurance policies should ideally encompass a broad range of cyber threats. Ransomware attacks, data breaches stemming from employee negligence, and incidents involving third-party software and services are notable areas that require attention. Moreover, coverage should account for both direct and indirect costs associated with cybersecurity incidents. Direct costs include remediation expenses and potential fines, while indirect costs may include business interruption, reputational damage, and customer loss. Organizations should ensure their policy includes coverage for incident response costs, including forensic investigations, public relations efforts, notification costs, and legal fees.

Conclusion

As the shift towards a permanent remote workforce unfolds, addressing cybersecurity challenges becomes mission critical to safeguard businesses. This involves not just an understanding of increased cyber threats but also the implementation of robust security measures. Success in this new era demands both organization-wide commitment and fostering a security-centric culture among workers. This journey may be complex; however, with strategic planning, collaboration, and commitment, becoming more secure in a remote-work world is a possibility and an achievable reality.

Sources

- Reimagining the postpandemic workforce, McKinsey & Company (July 7, 2020), https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/reimagining-the-postpandemic-workforce
- Covid's Long Shadow Still Spreads Over Commercial Real Estate, Forbes (March 17, 2023), https://www.forbes.com/sites/miltonezrati/2023/03/17/covids-long-shadow-still-spreads-over-commercial-real-estate/?sh=75c03c4127ae
- Microsoft Teams monthly users hits 280 million, UC Today (March 23, 2023), https://www.uctoday.com/unified-communications/microsoft-teams-monthly-users-hits-280-million/#:~:text=More%20of%20the%20tech%20giant%27s,per%20cent%20year%2Dover%2Dyear
- Zoom revenue and usage statistics, Business of Apps (April 26, 2023), https://www.businessofapps.com/data/zoom-statistics/
- NIST Cybersecurity Framework, https://www.nist.gov/cyberframework/framework
- Microsoft Digital Defense Report, https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022
- IBM X-Force Threat Intelligence Index 2023, https://www.ibm.com/downloads/cas/DB4GL8YM
- Security Intelligence, https://securityintelligence.com/articles/most-common-cyberattack-patterns-2022/
- Owl Labs State of Remote Work, https://resources.owllabs.com/hubfs/SORW/SORW_2021/owl-labs_state-of-remote-work-2021_report-final.pdf?utm_campaign=State%20of%20Remote%20Work%202021&utm_medium=email&_hsmi=180908804&_hsenc=p2ANqtz-_QqLl-7bQetJbJYOdCoskUzSr2pErrPvrTL353dUDu9e3aetTHyMlktMDf-N_opd0g0eg2lZzzzMM4MFaCkoOPa9Edt73hZO7QXJGYUaOVMIId_nk&utm_content=180908804&utm_source=hs_automation
- PWC Global Workforce Hopes and Fears Survey 2022, https://www.pwc.com/gx/en/issues/workforce/hopes-and-fears-2022.html