JS|HELD

PERSPECTIVES

Cyber Hygiene for Remote and Hybrid Workforce (Part 2 of Cyber Hygiene in 2023)

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

Copyright © 2023 J.S. Held LLC, All rights reserved.

INTRODUCTION

In the first part of this mini-series, we identified that showing everyday users how to secure data may not be as important as highlighting why data security matters. The "why" helps everyday users appreciate and internalize the need for cyber hygiene by demonstrating personal interest, which can improve buy-in. Now, let us close the series with two pertinent 2023 issues.

GOODBYE TO THE PERIMETER

Evolving externalities, including the pandemic, forced a change in work habits: remote, and subsequently hybrid, workspaces became the norm and will likely persist. For the fortunate ones who kept working during lockdowns, many turned a piece of their home, dining room table, or couch into their new office.

Advances in technology, such as mobile devices and high-speed residential internet connections, allowed a good portion of service industries to operate. But, with benefits and efficiencies come potential risks: in this case, the possible erosion of the security perimeter, which may result in financial and operational impacts not previously seen in an office-only environment.

From a financial perspective, costs are incurred through acquisition of security tools (e.g., monitoring, VPN connections, devices). In the future, information security and financial leaders, together, must manage business related expenses and determine which solutions meet business demands to deliver appropriate return on investment.

Operational impacts to everyday users are a result of changed work habits. A professional workspace has inherent security controls not found in a home office, hotel, or even in a hybrid workspace (e.g., "hoteling" office arrangements can reduce financial real estate burdens but can also come with unintended or hidden security risks). So how are these risks minimized?

POTENTIAL VULNERABILITIES IN REMOTE AND HYBRID WORKSPACES

Home offices offer convenience, but conveniences may generate lax behavior. "Who is going to break into my home to get into my digital files anyway, right?"

Well, driven malicious actors will follow a bread crumb trail if it is attractive, and a remote workspace is attractive because of the potential soft areas to exploit, such as:

- Poorly secured home routers and devices.
- Sloppiness or laziness of security protocols (e.g., failing to use VPN access, collaborating through non-work authorized means or devices).
- Distracted or inaccessible workforces causing operational degradation.
- Social engineering attacks taking advantage of a dispersed workforce.
- Over-access to data, or poorly secured data resulting from an unsecured facility.

While many issues will be maintained through enterprise programs, such as device management and identity controls, additional controls and support can be added.

GOOD PRACTICES FOR CYBER HYGIENE FOR REMOTE AND HYBRID WORKFORCES

A few good practices for mitigating the risks associated with remote and hybrid workforces include:

- **Mandatory VPN**. This comes with a cost but can be offset by reduced real estate costs.
- **Home office support.** Assist users to lock down or separate home systems (e.g., change default passwords

Copyright © 2023 J.S. Held LLC, All rights reserved.

on routers or hide Wi-Fi visibility so only whitelisted devices can access the network).

- **Make collaboration easy.** Protocols get circumvented for an "easier way." Get security and business teams to work together to find a productive and secure way to do business while avoiding "shadow IT" workarounds.

As mentioned in Part 1 of this series, achieving a secure environment is more than a matter of technology; achieving a secure environment also requires personal interest and personal responsibility. Therefore, tying these controls and support efforts to "why" data security matters will help motivate everyday users to invest personally.

With that in mind, let us close with some tactics to help everyday users prevent traditional and novel attacks.

VALUE PRIVACY TO ACHIEVE SECURITY

Whatever their reasons, people have differing attitudes toward digital privacy. But with a little help at the organizational level, perhaps some consistency in behavior can be achieved. For information security and risk management leaders, be mindful that promoting a culture of personal privacy could result in a more secure corporate operating environment.

Remember, with in-office safeguards reduced, each user expands the attack surface. Even informal controls, such as walking over to a colleague's workspace, are gone, impacting how we handle both benign and sensitive information. For example: water cooler chats have been replaced by group instant messages, but water cooler chats are generally forgotten over time, whereas the internet never forgets.

These changes are openings for social engineering attacks. Having lost "face-to-face" time, everyday users are more susceptible to manipulation, and while these tips may appear basic, they are valuable:

- **Limit what hits the internet.** Whether it is posting personal information (e.g., travel plans, birthdays, opinions, etc.) on social media or digital conversations (e.g., instant messages, message channels, emails, video calls, etc.), encourage discretion. Somewhere, somebody may be watching, lurking, and collating that information to use against you or your organization.

- **Make a friend; use the phone.** Not too long ago, walking over to somebody's workspace to chat was standard operating procedure. Picking up the phone is not a replacement, but it is close. It may nip an attack in the bud and build some good interpersonal relationships too.

- **Doubts are okay.** Are you and other employees in the organization applying the "does it feel wrong" test? A pressure tactic is red alert territory, but even seemingly benign commentary should raise an eyebrow. Does a stranger seem to know too much about you? If a caller says something to the effect of, "Hey, I work for Company X and I saw you traveled to [insert location] last week. So cool! Can we chat about what your company is offering?" feel free to reply, "I'm sorry, who are you?" Reluctance to trust is okay.

- **Be on the lookout for the weird.** Are devices acting up? Are connections unusually spotty? Is it difficult to access productivity software and tools? Erring on the side of caution is a good thing because everyday users generally do not have the insight to distinguish the difference between a legitimate technical difficulty or potential attack. Pick up the phone and ask somebody who knows better.

CONCLUSION

At first glance, these tactics may not appear as overt cybersecurity solutions, but they are because of the focus on neglected (bolded) portions of the following triad: **people**, **processes**, and **technology**. All three need to work in tandem to achieve good cyber hygiene. The bolded items need some attention, as cybersecurity has traditionally been so technology-focused, often leaving people and processes overlooked.

In closing, let us use a sports reference to demonstrate how small, incremental gains can be huge dividends: if you move the ball three and a half yards on every play, every possession results in a touchdown. That's how to stay ahead in the cybersecurity battle.

Copyright © 2023 J.S. Held LLC, All rights reserved.

ACKNOWLEDGMENTS

We would like to thank our colleagues Ron J. Yearwood, Jr., CISSP, CISM, CIPM and George Platsis for insights and expertise that greatly assisted this research.

Ron Yearwood is a Senior Managing Director in J.S. Held's Digital Investigations and Discovery group. Mr. Yearwood has more than 30 years of experience combatting the foremost criminal and national security threats. Mr. Yearwood has substantial experience advising and collaborating with clients on incident response, cybersecurity preparedness/resiliency/risk mitigation, and complex investigations. Having spent more than 23 years with the Federal Bureau of Investigation (FBI), Mr. Yearwood led strategic and investigative operations against hundreds of criminal and nation state cyber threat actors. During his tenure in the FBI Cyber Division, Mr. Yearwood served as a representative to the White House Cyber Response Group.

Ron can be reached at ron.yearwood@jsheld.com or +1 904 375 7792.

George Platsis is a Senior Director in J.S. Held's Digital Investigations and Discovery group. Mr. Platsis is a business professional, author, educator, and public speaker, with an entrepreneurial history and upbringing of over 20 years. He has designed and delivered solutions, and led teams, to improve breach readiness, enterprise-wide and business-unit specific incident response programs, and estate hardening for a series of Fortune 100 clients in healthcare, media, financial services, manufacturing, defense, and commercial electronics industries, including support of clients in the small and medium business space. Additionally, he brings complex investigation and emergency management experience to businesses and individuals seeking to reduce their risk posture. George is a Certified Chief Information Security Officer.

George can be reached at George.Platsis@jsheld.com or +1 321 346 6441.

This publication is for educational and general information purposes only. It may contain errors and is provided as is. It is not intended as specific advice, legal or otherwise. Opinions and views are not necessarily those of J.S. Held or its affiliates and it should not be presumed that J.S. Held subscribes to any particular method, interpretation or analysis merely because it appears in this publication. We disclaim any representation and/or warranty regarding the accuracy, timeliness, quality, or applicability of any of the contents. You should not act, or fail to act, in reliance on this publication and we disclaim all liability in respect to such actions or failure to act. We assume no responsibility for information contained in this publication and disclaim all liability and damages in respect to such information. This publication is not a substitute for competent legal advice. The content herein may be updated or otherwise modified without notice.

Copyright © 2023 J.S. Held LLC, All rights reserved.