JS|HELD

PERSPECTIVES

Cyber Hygiene: Getting Buy-In from Users (Part 1 of Cyber Hygiene in 2023)

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

INTRODUCTION

As we progress through 2023, both new and old cyber challenges remain, but opportunities for improvement are present. For the upcoming year, assume the following:

1. Past challenges have not been overcome, and we still grapple with them.

2. Technology use and innovation are in an increased state of fluctuation, driven by externalities (e.g., work habit changes, vast amounts of data, commercialization of artificial intelligence, etc.).

Everyday users may find the realities daunting. They may even feel dismissive about cyber-related responsibilities, leading them to ask, "Well, what do you want me to do about it?"

Cyber experts simply want everyone to help "protect the house" by creating a more resilient organization and atmosphere. In this series, J.S. Held provides information for security professionals and everyday users alike, with suggestions to identify means of avoiding internal failures and/or a central collapse or breach of information systems. How? Through a federated approach that relies on personal responsibility and accountability.

This two-part paper focuses on what everyday users can do to help protect data, through the support of leadership and a well-established and well-maintained information security program. Specifically, this mini-series identifies how to resolve a key pain point—ensuring users know both why and how actions are being taken—and managing two evolving conditions, changes in the workplace and malicious actor tactics.

We begin by identifying who is responsible.

KNOWING THE DIFFERENCE BETWEEN ENTERPRISE AND INDIVIDUAL RESPONSIBILITIES

Information security and risk management leaders will generally focus on "the program" of the enterprise, but they, like all others, are also everyday users of technology and data assets. The knowledge gaps between the two groups can be wide even if the risks to both are similar. Moreover, priorities differ between these two groups, yet care and responsibility should not.

Therein is the core of the cybersecurity issue: understanding the nuance between stakeholder groups. Understand this issue, and many downstream challenges can be managed.

Going forward, one can expect that those tasked with data security responsibilities will focus their efforts on migration and integration into the cloud, digital transformation, increased monitoring and automation, software-as-a-service (SaaS) use, and company-wide initiatives such as "building cyber resilience" or increased testing and training. And let us not forget the chatter of Zero Trust replacing VPN.

But are those efforts, however well-intentioned, the most impactful to everyday users? At best, maybe. Everyday users have their own priorities, and, in some cases, those can counter information security best practices. Therefore, a priority for directors, officers, managers, and the CISO should be helping everyday users find that balance; it's good business and good security.

NEAR TERM CYBER HYGIENE TRENDS TO BE AWARE OF

All enterprise-driven security efforts must ask this question: "How do everyday users help reduce the organization's risk footprint?"

The key is to recognize that the solution does not rest solely within the enterprise program, though the program most certainly is the foundation. Rather, the solution rests in everyday users internalizing and valuing good cyber hygiene as a gateway to protecting their own job, while concurrently improving the organization's risk position.

In other words, the key is that "cyber hygiene" (as a practice) needs to be seen as a positive benefit to the everyday user, not a cumbersome or restrictive task or process. To achieve this, it helps if everyday users—or, more specifically, front-line observers and last-chance defenders—can internalize the impact of these three questions:

1. How is an individual's digital behavior impactful to the enterprise?

2. Why there is a need to secure remote and hybrid workspaces?

3. What insights can be used to help prevent traditional and novel attacks?

INTERNALIZING BENEFITS OF GOOD CYBER HYGIENE

Some users may practice "more secure" habits over others, but those tendencies are generally derived from experience and role. Everyday users may have tendencies that can contribute to or hinder good cyber hygiene habits. For example:

- One group of users may have an inherent desire for privacy and want to practice more secure habits but are technologically illiterate, therefore posing a risk if they make mistakes.

- Another group of users may have a natural proficiency for technological use but place little value on privacy and security, posing a risk through lack of care.

The interesting result is that despite behavioral differences, both situations could result in the same type of data loss. So, where is common ground? Personal interest.

EXPLAIN TO THEM WHY, NOT HOW

"Eat your veggies," on its own, has rarely been a compelling argument. People are inquisitive and want to understand the concept of "why." Practicing good cyber hygiene is no different. Illustrative examples help. Here are just a few:

- **Take yourself out of a potential investigation.** Demonstrate the value of segregating professional and personal use of assets (think BYOD). If your company suffers a breach, investigation will require information from most sources that touch the company. If you are comingling personal and professional data on your personal device, it may be subject to investigative exposure. Sure, some convenience is given up through strict segregation, but in the aftermath of a breach, the likelihood of personal information – from a BYOD perspective – getting scooped up as part of the investigation, or in response to a subpoena, becomes relatively low. Most everyday users do not want or need the grief of having their private and personal information becoming part of a court case.

- **Protect the company to protect your job.** Explain the risk/reward of investment, innovation, research, and development, and how these activities are the lifeblood of an organization. Loss of intellectual property can be the difference between having job security for the next 10 years at a great company versus having to update a resume because the once-great company is now bankrupt.

- **Eliminate finger pointing**. Show support for strong change management and validation processes. Doing so limits misconfigurations and accident scenarios such as "the door was left wide open." Emphasize that "tying off" these tasks minimizes the likelihood your user was the cause of the breach.

CONCLUSION

In summary, you can tell everyday users *how* good cyber hygiene may be achieved (e.g., password strength, shadow IT dissuasion, reasonable monitoring, training, etc.) but none of that explains *why* good cyber hygiene is valuable to the user and the organization.

Practicing good cyber hygiene is not just a present issue; it is an ongoing issue influencing security and risk postures. CISOs and other security leaders focusing the "carrot and stick" (behavior reprimand) and "silver bullet" (technology) approaches will be left behind. To positively alter behavior, everyday users need to be partners and understand why sacrificing some upfront convenience and efficiency could yield long term protections and rewards. Business, risk, and security leaders need to appreciate that issue too.

In the second installment of this two-part series, we will focus on the need to secure remote and hybrid workspaces and insights that help a user prevent attacks.

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.