FS-ISAC

Executive Risk Report

22 March 2024 | EP - 03 - 2024

Recommended Distribution | Chief Executive Officer | Chief Compliance Officer | Chief Information Officer | Chief InfoSec Officer

Revisiting Cyber Hygiene

Summary

The January 2024 release of *"Defining The Beauty Of Cyber Hygiene: A Retrospective Look"* remarks, "…a more recent study, introduced cyber hygiene as an adaptive knowledge, behavior, and attitude. It is a necessity to have good cyber hygiene among individuals and organizations in dealing with the risk of cyber attacks and other digital threats and in ensuring good health and security of users, devices, networks, and data."

Indeed, the US National Institute of Standards and Technologies' (NIST) National Cybersecurity Center of Excellence states in its document, *Critical Cybersecurity Hygiene: Patching the Enterprise*, "There are a few root causes for many data breaches, malware infections, and other security incidents. Implementing a few relatively simple security hygiene practices can address those root causes—preventing many incidents from occurring and lowering the potential impact of incidents that still occur."

Redefining Baseline Practices

Instead of establishing best practices, it is time to adopt new baseline practices. The below recommendations are an excellent way of embarking on new baseline practices.

1. Require phishing-resistant multi-factor authentication (MFA).
2. Apply zero-trust principles.
3. Employ modern anti-malware with detection and response capabilities that automatically identify and block real-time attacks.
4. Prioritize and immediately patch the highest priority vulnerabilities.
5. Protect your critical and high-risk data by identifying your data's value, classifying data by type, following the principles of least privilege, monitoring system activity, and encrypting data at rest and in transit.
6. Train employees to recognize suspicious activity and ensure they understand their obligation to report security threats.

Has your institution…

- *Enabled and required employee and customer use of MFA?*
- *Increased its cyber maturity level and began moving towards zero trust principles?*
- *Begun using detection tools to proactively identify and halt suspicious activity?*

For internal discussion…

- *What were the results of your institution's most recent phishing and social engineering testing? Are you satisfied with the results?*
- *Are you proactively sharing vulnerability and threat information with other FS-ISAC member institutions?*

Events

2024 Americas Fall Summit

27-30 October, Atlanta, GA

Cyber Range Exercise Forensic Analysis

24 April, Virtual

Charlotte Member Forum

8 April, Charlotte, NC

About FS-ISAC

FS-ISAC is the member-driven, not-for-profit organization that advances cybersecurity and resilience in the global financial system, protecting the financial institutions and the people they serve. Founded in 1999, the organization's real-time information-sharing network amplifies the intelligence, knowledge, and practices of its members for the financial sector's collective security and defenses.

Contact

Jeffrey Korte

Director and Executive Sponsor,

FS-ISAC Community Institution and Associations Council

Reach out to Jeffrey on LinkedIn

+1 703.962.7901 ext. 583