REPORT TO THE CISA DIRECTOR

Turning the Corner on Cyber Hygiene

June 22, 2022

Introduction:

The Turning the Corner on Cyber Hygiene (CH) Subcommittee was established to examine how the federal government and industry can collaborate to identify appropriate goals and ensure strong cyber hygiene is easy to execute. This document outlines three recommendations offered by the CSAC and provides background and context on how the subcommittee derived the recommendations.

Findings:

By the end of 2021, the public sector saw an increase of 600% in cybercrime since the beginning of the pandemic.[i] Security incidents in 2021 were often related to supply chain and infrastructure breaches. Incidents have led to the public exposure and stealing of intellectual property and other confidential data. Attackers leveraged vulnerabilities to spread ransomware. Protecting the corporate and private data of Americans, their networks, and businesses is not limited to hardening our individual systems and executing incident response. Protection also requires elevating security across diverse ecosystems and clarifying the multitude of regulatory requirements to which American businesses need to adhere.

Security Requirements

Security requirements are nothing new. Federal, local, and private mandates were made to improve the security posture of all American enterprises. Those requirements are numerous, vary widely, often intersect, and can also conflict. The language used can be convoluted, unclear, overly technical, or simply overwhelming to its audience. The lack of clarity, along with the time it takes to parse relevant information, is cause for concern. When individuals assume technical jargon is understood by all, such security requirements often go undefined and are not acted upon. The actions needed for an entity to follow security requirements are subsequently neglected due to the technical misunderstanding.

Even requirements terminology can become misunderstood in technical jargon, such as “after any significant change in the environment take action to remediate identified deficiencies on a timely basis”[ii] and “alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files”.[iii]

Relying solely on compliance and requirements will not increase the nation's security posture.

Focus

To improve security holistically, data, networks, and businesses need to be secured by elevating security hygiene and focusing security responsibility on the right actions to mitigate cyber risk. CISA must focus on the following areas for security efforts:

- Multi-Factor Authentication (MFA)
- Security Awareness Training
- Vulnerability Remediation
- Security Event Logging
- Incident Response Capabilities

• Resiliency & Recovery

Delivery in each of these areas of focus will go a long way to enhance risk mitigation and cyber hygiene across organizations and individuals.

Recommendations:

- CISA must build out its current MFA campaign by identifying additional vehicles for publicizing "More Than A Password".
    - CISA must work to enable MFA everywhere and be inventive in its publicizing. This is a large, multi-dimensional undertaking and can be interpreted differently across various actors. Numerous technical options exist to move users away from a dependency solely on a username and password. Even within the security community, there are conflicting opinions on the correct course of action regarding MFA.
        - The benefits from enabling MFA are widely known. A recent report from Microsoft estimates that 99.9% of account compromise attacks would be prevented if MFA was in place.[iv] The 2021 Verizon Data Breach Investigation Report states that "61% of breaches involved credentials."[v] A recent internal survey of small to medium sized service suppliers asked "Do you feel that using multi-factor authentication (MFA) makes your personal and business data more secure?" 38.5% responded no, with another 25.3% responding "I don't know". This signals that the value added and impact of MFA is not obvious to users.
        - CISA must brand, market, engage, and support a simple, singular message of "More than a Password" that will be memorable.
            - CISA should initiate the campaign to design original creative content for both digital and print media. CISA should create a dedicated "More than a Password" online hub with not only dynamic and creative web content, but also explicit instructions to users on how to achieve the "More than a Password" objective. A new outreach campaign needs to initially leverage social media via DHS and other government high profile figures/accounts. CISA should engage high profile, private sector companies, and celebrities to echo the campaign and have bounce back messaging to the CISA hub. CISA should target large events, such as sporting events (e.g., MLB, NBA, NHL, etc), Fourth of July Parades, back to school / first day of school outings with digital and print marketing. CISA should create network television / cable broadcasts can air media spots; a type of updated "the more you know" public service announcements. CISA should also deploy digital and print signage in state / municipal high traffic areas (e.g., transit hubs, interstate rest stops, airports).
    - CISA must incorporate messaging that goes beyond advocating or educating users about the dangers of single factor authorization. CISA must focus messaging to dispel the myth that enabling and using MFA is difficult, time consuming, and has diminishing returns.
        - Large organizations have begun adopting MFA by default in their engagements with customers. Salesforce announced they mandated a February 1, 2022 deadline for all account users to implement MFA.[vi] In May 2021, Google announced they would enforce and auto-enable Two-Factor Authentication (2FA) for new users. By February 2022, they had more than 150 million 2FA users for Google accounts,[vii] as well as 2 million 2FA users for YouTube creators. GitHub announced in May 2022 that all users who contribute code on its platform will be required to enable 2FA on their accounts by the end of 2023.[viii] Examples of successful implementations and transitions to the usage of multi-factor authentication should be shared as they occur.

  - "More Than a Password" is solution agnostic. As such, it's realistic to gather multiple voices to sign on and subscribe to the common objective of eradicating single factor authentication. CISA must collaborate with a multitude of influential companies, spread across a variety of industries and sectors, to come together to amplify the "More Than a Password" message. That unified voice should express a commitment to it being "the path forward" for the betterment of the American public.
  - CISA must utilize mechanisms to disseminate "More Than a Password" that illustrate, in great clarity, the consequences and risks associated with not enabling MFA solutions.
    - In the same way that the American public were made aware of the risks of not wearing seatbelts in cars, the public needs to know that choosing to continue to use just a username and password comes at a price.

- CISA must take all available steps to ensure that companies working with the federal government fully adopt MFA by 2025.
  - CISA must work to obtain commitments across sectors and industry to enable MFA solutions and remove the ability for single-factor authentication. This goal will encompass not only technical solutions, but also the processes, training, communication, and socialization of a new way of being secure online.
  - CISA must work to obtain commitments across sectors and industry to enable MFA solutions and remove the ability for single-factor authentication. This goal will encompass not only technical solutions, but also the processes, training, communication, and socialization of a new way of being secure online.
  - CISA must set the deadline of 2025 to ensure the success of this effort. By having a goal date, the "More Than a Password" messaging is better amplified, and expectations are clearly established and communicated for new requirements to partner with both government and industry. The new branding of "MFA by 2025" advances beyond explaining the security expectations, towards declaring that those not using MFA solutions demonstrate negligence in their business practices.
  - To drive to the adoption of MFA solutions by 2025, CISA must establish mechanisms to make this transition a reality. CISA must create and implement the following mechanisms:
    - CISA will garner a commitment from numerous influential high-tech companies to enable MFA by default on their products and services. This coalition can come together and collectively enable this new default functionality at the same time, as an "industry move." CISA will feature these companies as industry partners of government.
    - The CISA coalition will publicly communicate its support of the CISA commitment to "MFA by 2025" initiative.
    - CISA will enlist non-profits, educational institutions, national, state, local and tribal governments, and the extended security community to amplify and publicly support the narrative that single factor authentication is eradicated by 2025.
    - CISA will work closely with small and medium-sized businesses (SMBs) to help them move beyond passwords. An avenue for this can be through additional guidance on CISA's public-facing website.
    - Through CISA, the US Government will lead by example and ensure that government agencies have a path forward to meet the goal of having "MFA by 2025."

- Recommend that CISA launch a "311 National" campaign, to provide an emergency call line and clinics for assistance with cyber incidents for small and medium businesses.

- Across the country, municipalities have leveraged the "311" model as a tool to connect residents, businesses, and visitors to Customer Service Representatives ready to help with general government information and services.
    - CISA must adopt a 311-like experience that acts as a security lifeline. If a small business or member of a local community believes they need support due to a security breach, compromise, or attack, where can they turn? "311 National" envisions locally managed support structures across the nation that are staffed with security response personnel who can assist those in need by providing education, guidance, and real incident response efforts. This will serve as a 311 helpline for information security issues.
    - A combination of local government agencies, higher education institutions, and help from the private sector must come together with security awareness content, incident response playbooks, staffing support, and community outreach / engagement mechanisms. City services, such as 311 lines, government websites, and/or mobile applications that are already in place for citizen engagement would become the proxy for connecting with those in need.
    - CISA should communicate with the city of Austin and the University of Texas who are currently prototyping and testing this idea. In the long-term, once the idea is proven to have impact and value, CISA could reproduce the service in major metropolitan areas across the United States.

Conclusion:

The recommendations outlined above are the initial steps in a long journey toward securing the American public and businesses. CH work is expected to continue for the next six months as CSAC continues to work on recommendations for the remaining scoping questions.

Beyond, CSAC will apply extra efforts towards the remaining recommendations of:

- Security Awareness Training
- Vulnerability Remediation
- Security Event Logging
- Incident Response Capabilities
- Resiliency & Recovery

Appendices:

The following Turning the Corner on Cyber Hygiene subcommittee members contributed towards this report:

- George Stathakopoulos, Chair
- Alex Stamos
- Nuala O'Connor
- Steve Schmidt
- Bobby Chesney
- Matthew Prince

Member subject matter experts:

- Matt Kehoe
- Jordana Siegel

Other contributors:

- Big Thanks to Mayor Steve Alder and the City of Austin

[i] CompTIA Blog, dated 04/21/2022 - https://connect.comptia.org/blog/cyber-resiliency-begins-with-people-and-process-not-technology
[ii] Unified Compliance, https://www.unifiedcompliance.com/products/search-controls/control/12497/
[iii] Unified compliance, https://www.unifiedcompliance.com/products/search-controls/control/12045/
[iv] Microsoft Blog, dated 08/20/2019 - http://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/
[v] Verizon's 2021 Data Breach Investigations Report – https://www.verizon.com/business/resources/dbir/2021/masters-guide/
[vi] https://security.salesforce.com/mfa
[vii] https://blog.google/technology/safety-security/reducing-account-hijacking/
[viii] https://github.blog/2022-05-04-software-security-starts-with-the-developer-securing-developer-accounts-with-2fa/