CISA
CYBERSECURITY
ADVISORY
COMMITTEE

REPORT TO THE CISA DIRECTOR

Turning the Corner on Cyber Hygiene

September 13, 2023

Introduction

The Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) established the Turning the Corner on Cyber Hygiene (CH) Subcommittee to examine how the federal government and industry can collaborate to identify appropriate goals and ensure strong cyber hygiene is easy to execute. To prevent a “boil the ocean” scenario, the subcommittee narrowed their focus to three sectors: K-12 public education, hospitals, and healthcare, and water supply/delivery/treatment. These areas of focus coincide with the Department of Homeland Security and White House objectives for defending the systems and assets that constitute critical American infrastructure. The CISA Director tasked the Committee with advancing the following scoping questions:

1. How can we encourage technology companies and software providers to develop products that are secure-by-design and secure-by-default to move the burden of security away from small and medium enterprises?
2. What specific actions should we recommend, that will materially improve technology product safety, and how do we best communicate these in a way that resonates?
3. What is the best way to evaluate progress toward all technology manufacturers building safety into their technology products?
4. How can CISA best support "target-rich, cyber-poor” entities in these sectors?
5. Which services and resources will make the most difference, and how can we most effectively measure a reduction in risk to these entities?

Findings

The subcommittee engaged in a series of discussions with industry and sector panelists and experts to inform the Committee’s tasking. Briefers shared feedback, concerns, and insights with the subcommittee, bringing details about the challenges that exist towards becoming secure. It became clear that due to entities varying in levels of size, complexity, and maturity, there is no “one size fits all” solution to apply. For example, the healthcare sector has many different government agencies, at both a federal and state level, that provide oversight. This is compared to the K-12 education sector, where there are minimal cybersecurity capabilities and partnerships between federal and state governments and school systems. Throughout the sector discussions, the subcommittee regularly heard the idea that it is easier to maintain cyber hygiene within larger, well resourced, well-tuned service providers and systems. It becomes a more challenging situation at smaller institutions with legacy systems and technology. According to Andrew Hildick-Smith (WaterISAC), 10,000 of the largest 143,000 Public Water Systems (PWS) provide water to 90% of the U.S. population, yet only a portion of those PWS have operational technology (OT) that is at risk to cyber-attacks. The threats are not just focused on OT specific to that sector, rather the majority of the cybersecurity incidents that occurred since the beginning of 2021 were ransomware attacks. Successful OT attacks were almost as common as successful information technology (IT) attacks and compromises. With the majority of PWS being smaller, they are not well positioned to defend against the most basic IT security threats. After speaking to the health, water, and education sectors, a pattern of issues that were common in the sectors was identified:

Lack of Authoritative Guidance

- There are no reference architectures or easy to use best practices documented and followed within or across the sectors.

- For those who are making investments into partners to assist, as they do not inherently understand cybersecurity, there are no resources to know whether they have invested in a good security program or service provider or a bad one. There is nobody saying, “you have done the right thing” in these circumstances.
- There do not seem to be any collaborative arrangements across groups of utilities or service providers, those with the ability to influence and support with their expertise or experiences do not have a reliable way to engage others in the sector needing such support.

Lack of a Path Towards Funding

- Cybersecurity investment is lacking as it is rarely viewed as a top priority for spending.
- It is rare to have a dedicated budget focused on improving the security posture of their organizations, therefore progress is often made when combined with other deliverables or value add-ons.
- Cybersecurity grant programs along with state revolving loan programs primarily exist at a regional or state level but sector entities may operate across regional or state boundaries.
- Raising water rates or costs to the consumers to incorporate cybersecurity as a normal cost of business is not simple, due to regulations and oversight of utilities providing public services. You simply cannot pass on the costs as you would in a more commercial private sector situation.

Lack of Expertise

- Cybersecurity skills are often seen as something unique to normal subject matter expertise in the sectors. At best, perception is that this is an extra area of focus or work that needs to be absorbed along with other primary roles and responsibilities.
- There is not a wide range of staff resources available. Sometimes, a single individual is put into a position to do everything.
- Due to a lack of IT staff, many utility companies outsource their IT work and consider it complete, regardless of if that IT outsourced partner has the cybersecurity skills or not.

Recommendations

Our recommendations include focusing CISA’s resources on providing guidance in four areas: security foundations (secure-by-design), road mapping financial assistance towards a more secure future, technical support during exploitation, and security related technical expertise. CISA should increase their velocity, become the authoritative voice for cybersecurity in the United States, and focus on reaching out to the widest audience possible. Furthermore, CISA should identify and publicly share performance targets that illustrate success.

The subcommittee has observed CISA independently taking action in the following areas:

- Director Easterly and FEMA’s Deanne Criswell Announce $375M in Funding for FY23 State & Local Cybersecurity Grant Program.
- CISA publishes K-12 cybersecurity roadmap.

- ***CISA serves as the unifying voice for security guidance.*** Because of the role that CISA holds within the US Government, one that is focused on collaboration and influence with interagency partners, CISA should find unique and creative collaborations to advance its primary mission. Many agencies and organizations (e.g., Office of the National Cyber Director, Cyberspace Solarium Commission, Departments of Education, Health, Environmental Protection Agency, etc.) find themselves coming to similar conclusions around how to protect critical infrastructure and CISA should take a lead role in blending these ideas and strategies together in a singular vision and voice that allows both private and public sectors to achieve meaningful security outcomes.

- *Define sector specific communications that are themed around "Understanding My Risk & Readiness".* Create accessible, easy to understand, discoverable, yet authoritative, security guidance to address actual sector risks.
  - The materials will have real world user stories, and security best practice examples of fixes.
  - CISA should search far and wide for examples of best practices, pilot programs, and opportunities for increasing understanding.
  - Clearly define the threat landscape, allow for quick risk assessment, and quantify if the existing risks are relevant to Americans working in the three critical sectors. Sector members need to be able to answer the following questions quickly and correctly: "What threats should I be wary of?", "Now that I understand my risk, am I vulnerable?", and "Based on what's happening out there, what's the likelihood that it's happening to me?"
  - Highlight the importance of multi-factor authentication (MFA), end of life (EOL) software removal, patching, etc.
  - These vignettes will see the threat and attacks from the impacted parties' perspective, and highlight the warning signs, things to watch out for, and call outs for each stage of the attack on what preventable measures would need to be in place to prevent the attacker from being successful.
- *Create a roadmap to action to overcome financial barriers.* Most of the health, water, and education sectors want to be secure, but simply do not know how. They lack the first steps and are often deterred by the financial barriers to entry. CISA must highlight a path to financial assistance.
  - Answers must be provided to the following questions, "Where does one turn to get the financial resources needed to be secure?", and "How does one position trade off and prioritization decisions that put security needs first?"
  - Once someone decides to make the investment in security solutions or service providers, CISA should publish tips and tools to identify effective IT / cybersecurity partner companies that will be successful in assisting via outsource arrangements.
- *Establish key security metrics.* You cannot fix what you do not measure. In an effort to establish a more secure future, companies need to know how they measure up in the security landscape.
  - CISA needs to establish key security metrics that allow the sectors to know if they are making meaningful and effective security changes that reduce their attack surface.
  - Data on its own is not enough, performance indicators per sector should have context and take data and turn it into information that allows operators and sector businesses the ability to make new and informed decisions on the security posture of their companies.
  - These security metrics will be published by CISA to find common language across sectors to show the current health of an institution and to illustrate if they are indeed able to deliver on intended security outcomes.

The recommendations outlined above are the initial steps in a long journey toward securing the American public and businesses.

Appendices:

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

- George Stathakopoulos, Subcommittee Chair, Apple
- Marene Allison, Former Johnson & Johnson
- Steve Adler, Former Mayor of Austin, TX
- Brian Gragnolati, Atlantic Health System
- Royal Hansen, Google
- Doug Levin, K12 Security Information eXchange (K12 SIX)
- Ciaran Martin, Former National Cyber Security Centre
- Nuala O'Connor, Walmart
- Matthew Prince, Cloudflare
- Robert Scott, New Hampshire Department of Environmental Services
- Alex Tosheff, VMware