Seven Basic Cyber Security Measures as Revealed by Wisdom of the Crowds

Individual experts offer good advice, but the aggregate of their guidance is wisdom – at least according to the no longer faddish "wisdom of the crowds" approach.

Regardless, what many people say are necessary and practical steps for better cybersecurity probably carries more weight than what just one person says, at least so long as cybersecurity lacks outcome-based, objective metrics.

Accordingly, here are the seven most important things small and medium-sized organizations should do, according to a survey the Internet Security Alliance did of five publications that prioritize cybersecurity controls.

These are controls for which there's unanimous agreement among the five:

- Have an information security policy;
- Patch your systems and applications, and probably do it automatically;
- Require multi-factor authentication;
- Restrict employee's ability to surf the web on company computers;
- Train employees on cybersecurity practices;
- Scan and filter email and web traffic;
- Set up logging and store the data for the long-term.

The publications we consulted are the NIST Cybersecurity Framework; NISTIR 7621 R1, Small Business Information Security: The Fundamentals (pdf); the Internet Security Alliance's The Advanced Persistent Threat: Practical Controls That Small and Medium-Sized Business Leaders Should Consider Implementing (pdf); the Center for Internet Security's Critical Security Controls; the Australian Signals Directorate's Strategies to Mitigate Targeted Cyber Intrusions.

You can download the full spreadsheet we used to map the publications (.xlsx), which also notes areas of lesser agreement on cybersecurity controls.

Of course, what cybersecurity really needs is a set of empirically-generated set of prioritized controls that can be shown to have a demonstrable effect on security outcome and whose costs can be measured. It's not just us who say so: Metrics feature prominently in the presidential cybersecurity commission's newly-released report through a recommendation for a working group to develop "industry-led, consensus-based metrics" for the purposes of "better understanding and quantifying the benefits" of the NIST framework.

Some fear such work would be a first-step toward regulation. We believe the opposite. Cybersecurity measures with demonstrable cost-effective improvements don't have to be legislated or regulated into the economy; the private sector will naturally implement these controls. Measures that are effective but not economically sustainable are a natural fit for targeted incentives that close that gap.

RATIONALE

We did this because a list of empirically selected, prioritized measures that small- and medium-sized businesses should implement is a long-standing goal of the Internet Security Alliance.

For a while, the expectation was that such a thing would develop naturally through the National Institute of Standards and Technology Cybersecurity Framework. After all, the executive order that created the NIST CSF said the framework meant to provide "a prioritized, flexible, repeatable, performance-based, and cost-effective approach" toward cybersecurity.

Unfortunately, while the framework provides the structure for prioritization, its universe of cybersecurity controls comprises the totality of an extremely-well managed cybersecurity program. It's too encompassing, by itself, to offer a truly prioritized set of cybersecurity controls.

That's especially the case for small- and medium-sized businesses, which typically lack the resources to implement the full suite of framework subcategories. Or for that matter, to trace the progression from Function to Informative Reference and turn that information into an actionable item. For non-experts who lack the willingness or time to plunge its depths, the framework is as a conceptual document rather than a useful one. And its non-experts who are the framework's most important audience – it's in their organizations where the weak spots lie.

The framework is a useful starting point, but it's apparent the conversation about prioritization has stalled. As one administration replaces the next, we're attempting to give this important topic impetus by looking for agreement about cybersecurity controls among publications written from the start with a utilitarian aim. These publications aim to tell readers *this is what you must do* rather than give cybersecurity a conceptual framework.

In the aggregate, their measures represent the consensus about basic cybersecurity and present a basis for having a larger discussion about prioritizing controls, and how to measure their outcomes and cost.

METHODOLOGY AND LIMITATIONS

We began with two publications. The ISA's own The Advanced Persistent Threat: Practical Controls That Small and Medium-Sized Business Leaders Should Consider Implementing (pdf) and NIST's newly revised publication (pdf) with recommendations for small business cybersecurity.

It turns out the two contain common advice, and their touchpoints became more visible when mapping each publication's full set of controls to the Informative References in the NIST Cybersecurity Framework and the corresponding framework Function, Category and Subcategory. (We used NIST SP 800-53 Rev. 4 as the sole informative reference.)

Thereafter, we looked for additional agreement between those two publications and the Center for Internet Security's Critical Security Controls (once known as the "SANS Top 20") and the Australian Signals Directorate's "Strategies to Mitigate Targeted Cyber Intrusions" (informally known as the Australian Top 35). We didn't undertake a full mapping of the CIS or ASD controls to the NIST Cybersecurity Framework, and nor to each other. For the purposes of

establishing areas of unanimous or very high agreement, it was an unnecessary task, even if there may be future value in finding where these two very technically-minded documents agree.

Some caveats: the mapping by necessity is rough and it's possible, especially with the CIS and Australian Signals Directorate controls, that someone might object to an equivalency we've made. Our objective was to look for rough areas of agreement, not areas of exact duplication. If you see an equivalency that's mistaken, please get in touch.

Also, some of these publications are dated. Our publication came out in 2012. The Australian Signals Directorate hasn't (to our knowledge) updated its list of controls since 2014. In addition, each of these publications have a different focus. The CIS controls seem slightly biased to network administrators.

CONCEPTUAL CONCLUSIONS

The practical outcomes of our work are at the top of this blog post: Seven controls that have unanimous or nearly unanimous agreement among multiple, independent publications.

Still, there's one interesting outcome at the conceptual level worth noting. And that's the relative dominance of the "Protect" function of the NIST Cybersecurity Framework in the seven controls. About 43 percent of the commonly-agreed on controls come under that heading, with 29 percent each for "Identify" and "Detect." "Respond" and "Recover" don't figure in the total, at all.

Cybersecurity has come under criticism for being too defensive in nature, for relying on digital moats and walls. "Cyber resilience," under which organizations continue to function even when under active attack, is often described as the state organizations should aim for. If that's the case, then it has yet to be reflected in collective wisdom – at least as we've found it.

Of course, our sample of controls has a known bias toward small businesses and in the methodology section we've also noted that part of our sample is a little old. Regardless, it's probably not far off the mark to say that there's a gap between talk of cyber resilience and the things that most cybersecurity practitioners do on a daily basis.

NEXT STEPS

Wisdom of the crowds is great. Any organization not doing most or all of the seven controls shown by our survey probably is unnecessarily vulnerable.

But with cybersecurity becoming a problem of greater magnitude, not less, the hand-wringing about prioritization, measurement and incentives seems misplaced.

We know establishing these things this isn't an easy task. Cybersecurity resists pat measures, such as "number of blocked incidents." Choosing the wrong metrics might incentivize the wrong behavior among practitioners or vendors. And even with the right set of metrics, isolating the impact of a particular input – and just as importantly, the cost of that input – can be difficult.

Important things are rarely easy. And the time available to improve cybersecurity isn't unlimited. The prospect of the Internet of Things, a possible era of destabilized international relations plus our recent experience with Russian information war and the potential of voting machine hacking to destabilize our country add up to an urgent call to action.

To that end, we call on Congress and the next administration to fund studies that take the NIST Cybersecurity Framework and test its implementation until we know the priority of controls within it and their associated costs. Simultaneous with that, the public- and private-sectors in a process similar to the one that underpinned formation of the framework itself should convene to discuss incentives. The clock is ticking.

Written by Dave Perera, ISA Assistant Vice-President for Government and Policy