Input to the Commission on Enhancing National Cybersecurity

Cybersecurity Workforce

Internet of Things

Public Awareness and Education

Identity and Access Management

Cyber-security is a much bigger problem than the average American is aware of. While our digital economy is at significant risk due to cyber-attacks, we all are at risk in our daily lives. The loss of services, exposure of private information, and the degradation of digital trust will affect our productivity and well-being going forward. Significant steps must be taken to put us on a better path, especially with the increasingly connected world. Every day more and more critical systems -- life support, power grids, water supplies, all are vulnerable to a kid with a mouse and a keyboard. The Internet has become the leveler of the global battlefield, and we keep connecting more and more devices without much thought. This new reality must be addressed with leadership, innovation, and perseverance.

Fundamentally, our nation will only make progress when we improve our people's understanding of cyber risk and how to go about mitigating that risk. This applies to not just the actual cyber practitioners, but to all users of devices that are connected to the Internet or to other systems.

The first thing that has to be done is the creation and maintenance of stronger leadership. Too often organizations have CEOs, CIOs, or CISOs, who don't actually understand technology and certainly don't understand the cyber risks for exploitation, attack, and the subsequent best ways to approach cyber defense. When there's a failure in leadership, there is little hope "among the ranks" of having any cyber resiliency, not to mention getting close to feeling "secure". Furthermore, good security practitioners follow good security leaders, so attracting, empowering, and retaining those leaders must be a priority in order to maintain a solid team.

As for the overall talent deficit – it is completely real. I've spoken to 600 organizations globally, including four of the Fortune 5 down to start-ups with fifty people. From Singapore to Dubai to London to San Francisco, there's a huge shortage of qualified candidates. When a new job opening is announced for a security analyst, cyber intelligence officer or anything similar, there are many applicants but very few who are worthy of even a second round look. Teams and organizations are getting desperate. If we do not address this problem, we do not make any progress with cyber security.

Aside from people, there's security technology. And there's plenty of technology. Unfortunately most deployed technology is largely ineffective, and there are two reasons for it. First, often the approach or the defensive mechanism is outdated or just no longer as effective because the adversaries have adjusted or the infrastructure has changed. So what used to work no longer does. Secondly, there's a huge "deploy-and-decay" problem where tools are deployed and unless they are given the care and feeding that they require (which they aren't given), they become rusty and get worse and worse. This then leads to worse use of human time and an overall decrease in morale because now the environment is getting worse and there are no people coming to save the day.

Looking forward, current information technology trends do give us some hope. With most of IT focused on two areas, it decreases (or at least has the potential to decrease) the complexity and entropy within our environments. This is largely looking at the private sector, but there are hints of this in the public sector as well. Technology is moving into cloud-based servers and services, and mobile employee devices. This means that a lot of security teams are focused on cloud providers and on employee laptops and phones. While these areas have plenty of cyber risk, approaching the problem has always been the same – whether you are home, in an airport or at work, having the same security controls creates consistency for the security team. It also allows for fewer pieces of technology to both manage and defend, which should be a good thing.

The downside of centralizing on backend services is that it creates a huge area of risk – one major compromise of a webmail or virtual-hosting service provider and there are thousands or millions affected. Still, we as a nation (and as private companies) can focus heavily on securing these popular services and forcing best-practice security controls in (like multi-factor authentication). The roaming abilities of these employee owned devices also creates a lot of risk, as now they're in potentially hostile environments all the time. The upside is that rather than assuming they're in the relative safety inside the perimeter (which doesn't really exist anymore), security teams can truly approach the problem knowing there is risk and making sure there are proper controls and a sufficient level of visibility for them to prevent, detect, respond, and remediate against threats.

In waging this fight, there are attempts to wage it together. With more and more sharing, there is the feeling that one is no longer alone against both criminal and state sponsored opponents. This is a good thing. There are a couple missing pieces however, and I'm not sure they're recognized enough. First, "threat intelligence", as the term is often used, is mostly referring to threat data. Logs are collected, some information is gathered, and then it is all pushed to a central clearinghouse of sorts and received by hundreds or even thousands of other practitioners and organizations. But it's not processed enough on the front-end, and there's often not enough context to make it useful. Context is king and yet often an ip-address or a hash shows up with little reason as to why it showed up or what other information needs to be seen along-side it in order for action to be taken (or an alert to be fired). So threat data must eventually become threat intelligence in more than just the name. Secondly, what's missing is the sharing of the what, how, and why of our security programs. What did a successful organization build for a security program, how did they build it, and why did they build it that way. Those pieces of insight,

those building blocks are so much more valuable than pieces of intelligence who have a half-life often in hours or days, shorter than the time it takes to consume and apply those into an environment. So we must encourage the sharing of the building blocks of programs, especially why the program was built that way. From here teams actually start to have a formula for creating more robust security practices.

Taking all this into account, one fundamental shift that would be beneficial is to take a people-first approach. The idea is that you look at technology trends in your environment, you look at the risk around those trends, then you take into account the skills your team has (or you can hire for), and then finally you get security technology to fill in remaining gaps or to enhance those existing skills. This is not how security is done today. Security today is that someone decides to buy a bunch of security products and then tries to find people to manage those products – it's backward because security is still about people.

There's plenty more to write about, but let's talk about what the government's role in all this should be. The government should be focused on a few items, and most of them revolve around guidance.

Encouraging more individuals to join the cyber ranks

Providing economic incentives, like stipends, to obtain cyber security skills and credentials

Increasing the compensation offered to public servants in the areas of cyber defense, forensics, incident response, security architecture, and security leadership. The compensation in the private sector dwarfs the public.

Creating public awareness around cyber security – Grandma's computer might be the one sending phishing attacks to Fortune 100 companies that ultimately leads to a ransomware or credential theft

Establishing best-practices for building cyber security programs

Providing guidance to organizations for how to evaluate security technologies

Providing guidance to organization for hiring and retaining talent

Sharing lessons learned and intelligence from the Government side to the private side helps fill the trust-deficit between Washington and Silicon Valley

Helping consumers increase their understanding of cyber risks and how to mitigate those risks – we need public service announcements around multi-factor authentication, good password creation, and similar "low-hanging fruit"

Provide security education earlier -- when students are exposed to computers or tablets, make sure they have a "device health" education class, or something similar; kids should not talk to strangers, and this includes online (and visiting unfamiliar links and websites)

Establishing committees that are not just former generals and lawyers, but who are still “in the trenches” getting their hands dirty against malware, exploits, and creating detection rules

Thank you for considering this feedback.

Ben Johnson

Co-Founder & Chief Security Strategist, Carbon Black

Lecturer, Entrepreneurship in Technology, University of Chicago

Former NSA Computer Scientist