Synack

Hacker-Powered Cybersecurity:

Thinking Like the Adversary

Congressional Briefing

June 2018

For more information:

government@synack.com

Protecting America Calls for a Crowd

Protecting the American way of life is the US Government's top job. In the era of the internet, big data, and connected devices, protection for Americans in the cybersphere is more critical than ever. According to a report published by the World Economic Forum this year, cyber attacks are one of the top 5 most pressing global risks most likely to happen.[1]

Cyber attacks aren't just likely to happen, they are already happening. Over 98% of organizations take only minutes to compromise, from Uber to the City of Atlanta.[2] In 2015, OPM suffered a colossal data breach that exposed 21 million federal and would-be federal employees' personal data including their social security numbers and, in some cases, sensitive information about their families and friends. We later learned that Chinese state-sponsored hackers had exploited a fixable "zero day" in the OPM's systems that left the US vulnerable.[3] It's not just government facing this challenge: in 2017, the WSJ broke the news that Equifax was breached and released records of 145.5 million people including important personal information.[4] After the fact, they "quadrupled" their security spending—highlighting the fact that private enterprises and government agencies alike are in desperate need of scaling their defenses.

Unfortunately, our traditional models of cyber defense are not working. While federal cyber investments increased 162% from 2006 to 2018, the number of federal cyber incidents were increasing at a rate of 1,512% from 2006 to 2016.[5] When cybersecurity solutions aren't doing what it takes to protect American people, the time is ripe for action.

Convening a Briefing on how Crowdsourced Security Protects the American Way

Synack, Domino's, the US Cyber Command, and the US Congress met in Washington D.C. this past month to speak about crowdsourced security as part of a closed, bipartisan briefing for congressional staffers on crowdsourced security. This approach is not new; it has been widely adapted by the Department of Defense, including the Air Force and Army, and its success in the Pentagon has provided a strong use case for civilian agencies. What sets Synack apart is a controlled, highly managed approach to security that mimics criminal adversaries and nation states and has proven its effectiveness and efficiency to the private and public sectors alike.

The briefing engaged public and private sector leaders in security:

- **Rep. Ted Lieu:** A panelist at the briefing, Congressman Lieu is a member of the U.S. House of Representatives representing California's 33rd District. Active in the crowdsourced security debate and a trusted authority on technology topics on the Hill, the Congressman proposed a recent bill entitled "Hack Your State Department" to introduce a crowdsourced security program at the US State Department. He is also former active duty officer in the US Air Force.

[1] "These are the biggest risks the world faces," World Economic Forum, January 17,2018.

[2] Verizon 2017 Data Breach Investigations Report.

[3] "Chinese Breach Data of 21 Million Federal Workers," Washington Post, June 9, 2015.

[4] "Equifax Hack Might Be Worse than you Think," Wall Street Journal, Feb 9, 2018.

[5] GAO Report on Information Security, FISMA Annual Report to Congress, Morgan Stanley Blue Paper on Cybersecurity, Synack Analysis.

- **Shawn Turskey:** Turskey had a 31-year-long career at the NSA. As Executive Director of U.S. Cyber Command, he drives the strategic and technical innovation that helps the nation's cyber warriors get their job done.
- **Ethan Steiger:** The deliverer of 2 million pizzas a day in the US and crowdsourced security advocate, Dominos' Pizza VP & CISO Ethan Steiger spoke about how he utilizes crowdsourced security daily to scale and secure the business.
- **Mark Kuhr:** Synack's Co-founder & CTO hosted the briefing. Mark started his career on the front lines working in cyber operations against adversaries at the NSA before founding the market leader in crowdsourced security.

Rep. Ted Lieu made the case for instituting crowdsourced security as the testing standard across agencies through bipartisan legislation such as Hack Your State Department Act. As security leaders, Turskey and Steiger highlighted how crowdsourced security improves security and ROI when done in the right way. The briefing answered the questions:

- What processes and technology should be put in place to garner maximum effectiveness from your crowdsourced security programs?
- What controls can I leverage so I can use crowdsourced security testing to reduce my security risk without introducing new risk into the system?
- How do I efficiently integrate crowdsourced security into my operations to augment and accelerate my security team's efforts?

Crowdsourced Security Has Become Mainstream in Government

Rep. Lieu (D-CA) and Ted Yoho (R-FL) are furthering crowdsourced security as the government's testing standard through bipartisan legislation such as the Hack Your State Department Act. Rep. Ted Lieu (D) is one of only four members of Congress with a computer science degree, and, unsurprisingly, he is an outspoken advocate and thought leader for crowdsourced security. This bill draws upon past successes with bug bounty programs at the Pentagon's DDS.[6] In 2016, the Pentagon/DDS launched the first-ever crowdsourced security testing program in US Government called "Hack the Pentagon". Led by Synack on the private/critical systems side of the program, "Hack the Pentagon" is considered a helpful playbook for other agencies to follow suit.

The Crowd Can Fill Government's Cyber Talent Gaps

Our nation doesn't have the talent we need. According to Cybersecurity Ventures, 3.5M cyber positions will be unfilled by 2022.[7] Mr. Turskey, who helps lead the 133 Cyber Mission Force Teams at the US Cyber Command, highlighted the need for more talent: "Why does USCYBERCOM use crowdsourced security? Because this model leverages some of the best talent in the world that has some very specific skill sets. Our USCYBERCOM defenders are strong, but crowdsourced, bug bounty security programs offer unique perspectives through a unique talent pool and is well worth the investment."

[6] https://lieu.house.gov/sites/lieu.house.gov/files/LIEU_091_xml.pdf

[7] GAO Report on Information Security, FISMA Annual Report to Congress, Morgan Stanley Blue Paper on Cybersecurity, Synack Analysis.

The government can recruit security researchers, but it takes time and they can't match the exponential increase in attacks with quality talent. Enterprises are also struggling, as competition for the top talent in the security field heats up with the increased demand.

Steiger (Domino's) and Turskey (US Cyber Command) agreed engaging the private sector can help address the talent shortage. Crowdsourced security platforms help source and vet talent for customers. Synack's proprietary recruiting vetting methodology is based on the founders' NSA background. Partnering with Synack provides a speed and scale to operations that accelerates organizations' efforts to match the growing threat of cyber attacks.

Managing Risks in a Crowdsourced Security Approach

There are differences, and therefore trade-offs, between bug bounty programs and private, managed crowdsourced security testing. In an open system, providing a wide swath of individuals to come at a target may seem like an appealing concept. Traditional bug bounty programs emphasize not just the number of vulns they can find, but also the number, talent and diversity of researchers on their platform. However, more is not necessarily better. A high volume of researchers engaged in a program can introduce noise into the system and lower the quality of the output. This volume is accompanied by a lack of control and visibility into testing activity and can be difficult to stomach--especially for critical and sensitive systems.

Ethan, Domino's CISO and VP, highlighted that while he wouldn't trust the general population, he would trust the Synack Red Team, which is stringently vetted and includes just the top 10% of applicants. In the words of Ethan, "There are comforts with Synack. I know I'm not taking unnecessary risks."

Vetting is absolutely critical and it's a feature that will allow for government agencies to deploy crowdsourced testing across their systems. But one-time vetting is not enough on its own; we want physical proof that these hackers are doing what they said they would do. At Synack, all testing performed by our Synack Red Team is conducted through our controlled platform with a secure virtual private network (VPN) gateway with full packet capture. (A VPN is a way to extend the security and access of being on a private network in the office to those working remotely on shared or public networks.) In tracking and keeping a record of everything that happens on our platform, we offer our customers full transparency and control during the testing process.

Reducing Risk While Increasing ROI

As Ethan mentioned during the briefing, Domino's is the global leader in pizza with over $12 billion in global retail sales. Not only does the company make and deliver pizza, they've successfully spearheaded a new age of convenient digital food order and delivery. Today, you can order a Domino's pizza through a smartphone app or a tweet, and not coincidentally, 65% of Domino's pizza sales are now digital. To support beloved American businesses like Domino's that are critical to the economy and dependent on customers trusting them with their personal information, robust cyberdefenses are essential. The line of defense should start with the companies themselves, who need to invest in cybersecurity solutions that offer a high ROI for the business—like crowdsourced security.

For Ethan, being the Chief Information Security Officer means protecting the bottom line by preventing business downtime… and making sure customers' pizzas are delivered on time. To do this, he knew that he needed a proactive approach to cybersecurity—he would have to work with development teams to build secure apps and test them before they connect to the internet. Crowdsourced security provided an elastic security solution that was easy to integrate into the development cycle and would identify security weaknesses before they went online, helping to minimize risk to the business.

Ethan uses his crowdsourced security program to gamify the development process. He informs developers that their work will eventually be tested by a third party for vulnerabilities: "Developers now measure the time it takes Synack to find vulnerabilities in their code." This has transformed the way the development team works with their security team; Synack's testing meant "more ownership of the code" and a "greater inclination to fix things" from the development end. Ethan also observed that "a system that is 'bug bountied' will strengthen other systems."

Crowdsourced models depend on having the right number of skilled, trusted researchers on your project. Statistics across open and private bug bounty programs indicate between 30 and 100 hackers may be the optimal number per project. Much of the value of crowdsourced security should come not just from finding vulnerabilities, but from the peace of mind that comes with knowing that testing coverage is robust and the security team is focusing on the most important issues. The crowdsourced security model incentivizes researchers to find vulnerabilities for paying them for what they find, rather than paying them on a time and materials basis like a traditional pen test. This helps accelerate the vulnerability discovery process and guarantee thorough coverage of a target. As Mr. Turskey highlighted, "Bug bounty has turned around critical vulns in days." Critical to finding, however, is prioritizing to focus security team attention on the issues that matter most. Mr. Turskey went on to say, "USCYBERCOM knows that the money we spend to resolve vulnerabilities found from crowdsourced security is being spent on the highest priority issues."

In some ways, Synack is like a safety in football, the last form of defense before bringing sensitive systems online. In the words of Ethan, "Synack is our last chance to find something before we move it to the internet." By taking a proactive approach to hardening assets against attack, the business is able to minimize its security risk and improve the ROI of its security program.

Building More Secure Systems After the Vulnerabilities are Exposed

No crowdsourced security program should be complete without remediation. Talent-strapped security teams require help not just with finding, but also fixing security issues. A common concern of new adopters of crowdsourced security is that their teams will be overwhelmed with findings without the resources to fix them. Synack and Rep. Lieu helped allay these concerns.

Synack helps build remediation support into their programs to remove operational burden from security and remediation teams. The Synack Red Team provides detailed reports of every vulnerability found. These include steps to reproduce, as well as suggested fixes. These reports should be detailed enough to send directly to development teams for a speedy response. Once the patch is implemented, Synack provides patch verification, a critical step that involves the researcher that found the original vulnerability re-testing the patch to ensure that it was truly effective.

With skilled hackers providing expert insights and intelligence, remediation can be much more efficient but for those that do run into the need for additional resources to address the vulnerabilities they find, there is an answer. Rep. Lieu discussed a revolving fund that he, Rep. Will Hurd, and other members of Congress are in the process of setting up. The fund allows agencies to borrow money to fund remediation activities and pay it back so that security is not sacrificed out of budgetary constraints.

A Call to Action to Keep Americans Safe in the Digital Age

Ultimately, crowdsourced security done right is the most efficient, impactful method of strengthening our nation's assets against the adversary. As Shawn Turskey put it, "USCYBERCOM learns from these tests. They make us stronger."

While crowdsourced security requires a propensity for change, the panelists agreed that the ROI is well worth it. Done right, a crowdsourced security program should offer the right control and visibility to put the agency in the driver's seat. While it may feel more comfortable to start with a lower-value asset, Shawn Turskey's comments highlighted the need for a more aggressive approach.

"The crowdsourced security legislation we see today often excludes high-value assets from this kind of opportunity because they are too sensitive," he shared at the briefing. "Congressman, high-value assets are exactly the systems that the crowdsourced model should be testing first. They are too valuable to ignore."

Below we have highlighted what you can expect from a crowdsourced security program.

What Does Success Look Like for Your Agency?

A crowdsourced security program should increase Attacker Resistance. This means:

Increased effectiveness

Are you finding issues earlier?

Are you finding vulnerabilities you didn't find before?

Are you better equipped to prioritize your vulnerabilities for remediation?

Increased efficiency

Do you have more testing coverage across your attack surface?

Are you able to deploy tests rapidly?

Is your testing solution unburdening your security team and accelerating their activities?

Are insights making remediation easier than it was before?

Increased insight

Do you have a full audit trail of testing activity?

Are you seeing your results in real-time?

Are you identifying which of your assets are more vulnerable to attack, from a researcher's perspective?

Do you have metrics with which you can benchmark across assets or against other organizations?

Synack, Inc.

855.796.2251 | www.synack.com | government@synack.com