TESTIMONY OF

Marten G. Mickos
Chief Executive Officer, HackerOne

BEFORE THE

**Commerce Subcommittee on Consumer Protection,
Product Safety, Insurance, and Data Security**

"Data Security and Bug Bounty Programs"

February 6, 2018

Introduction

Chairman Moran, Ranking Member Blumenthal, and Members of the Subcommittee, thank you for inviting me to testify today. I look forward to providing you with my perspective on Data Security and Bug Bounty Programs.

I am Chief Executive Officer of San Francisco-based HackerOne, the world's leading provider of hacker-powered security. I have spent my entire 30-year career in software, including as Senior Vice President at both Hewlett-Packard and Sun Microsystems, and prior to that as CEO of MySQL. In addition, I served on the Board of Directors of Nokia Corporation.

HackerOne operates bug bounty programs that connect companies and governments with the best white hat hackers in the world to find and fix vulnerabilities before malicious actors exploit them. As of January 2018, over 160,000 white hat hackers have registered with HackerOne to defend customers, among them the United States Department of Defense, removing over 60,000 vulnerabilities and preventing an untold number of breaches in the process.

The Threat of Weak Cybersecurity

Today's cybersecurity practices are severely outdated in contrast to the cyber threats that society faces. When exploited for criminal purposes, even just one single and relatively unremarkable security vulnerability can create havoc, as the Equifax data breach[1] grossly reminded us of in 2017.

Unfortunately it is only a question of time before cybercrime causes physical damage to structures or, worse, physical harm to humans. Citizens in general and consumers in particular are exposed to risks that they cannot possibly deal with themselves. Privacy is threatened. Consumer protection against faulty and vulnerable software-based products is presently inadequate.

The economic repercussions are enormous, and we are only now starting to see the true costs of lax cyber hygiene. When data breaches occur, corporations lose millions of

[1] https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do

dollars. These costs are often passed along to consumers who additionally face unquantifiable burdens associated with the breaches, including compromise of privacy.

It is an unfortunate fact that in the digital realm, society is currently failing to provide its citizens with what societies were established for: safety and security.

Hacker-Powered Security Offers a Solution

Whatever protections and defenses we build into our digital assets - and we should build a lot of them - there is one practice that covers every possible cause of cyber breach. There is an "immune system"[2] that will approach the digital assets from the same direction as adversaries and criminals do - from the outside. There is a mechanism that at scale has the opportunity to ultimately detect every hole, every weakness and every security vulnerability in a system or product built by humans.

This practice is often called "Hacker-Powered Security." It is a mechanism that turns the asymmetry that favors the attacker into an asymmetry that favors the collaborating defenders. It is a collective effort that relentlessly looks for more vulnerabilities. Its outstanding success metrics are a result of stochastic probability: the more attempts there are at finding vulnerabilities, the higher the likelihood that these will be found. Over time the result improves asymptotically towards 100%.

Hacker-powered security is a model that invites external and independent security researchers and ethical hackers - we will here simply call them "hackers" - to hunt for vulnerabilities in computerized systems. Today there are over one hundred thousand white hat hackers in the world. These are individual experts who have signed up to help corporations and organizations to detect and fix their security weaknesses. These hackers are motivated by the challenge, by the opportunity to do good and by peer recognition. They are rewarded for their finds with bounties. They are bug bounty hunters.

How Hacker-Powered Security Works

Hacker-Powered Security covers any cybersecurity-enhancing services and automations that are partially or wholly produced by independently operating security experts outside the company or organization in question.

[2] https://www.ted.com/talks/keren_elazari_hackers_the_internet_s_immune_system

The most fundamental function of hacker-powered security is a Vulnerability Disclosure Program, also called Responsible Disclosure or Coordinated Vulnerability Disclosure.

A vulnerability disclosure program is essentially a neighborhood watch for software. The motto is “If you see something, say something.” Concretely, if and when an ethical hacker finds a security vulnerability in and company or government organization’s website or mobile app or other computer system, this person will be invited to disclose the vulnerability found to the system’s owner.

Most human beings are ready to help their neighbor, so the impetus for vulnerability disclosure is enormous. Issues of legality and trust, however, make vulnerability disclosure more complicated than a regular neighborhood watch. To solve this issue, leading companies have created their own policy frameworks for the disclosure of vulnerabilities to them, and others turn to companies such as HackerOne to organize and coordinate such programs.

When an entity decides to offer financial rewards to finders of vulnerabilities, the vulnerability disclosure program is called a Bug Bounty Program. Bug bounty programs have existed at least since 1983.[3] The practice was perfected by Google, Facebook and Microsoft over the past half-dozen years. Around the same time, companies such as HackerOne emerged for the purpose of bringing this powerful method within reach of any organization that owns and operates a digital asset (meaning a computer system, a website, a mobile application, an Internet-of-Things device, or some other digital product).

Proven Effectiveness

Hacker-powered security programs have demonstrated their effectiveness compared to other methods for vulnerability detection. Hiring full-time employees or external service or product vendors to test for vulnerabilities is more expensive. Through HackerOne’s service alone, over 63,000 security vulnerabilities have been found and fixed. The current maximum bounty listed on HackerOne is $250,000. No other method for validating software or manufactured products that are in use by consumers has been shown to produce similar results at such a favorable economic unit price.

[3] Hunter & Ready ran a campaign in 1983 called “Get a bug if you find a bug”, offering a VW beetle as reward for bugs found in their real-time operating system. Netscape launched a bug bounty program in 1995.

Hacker-powered security is a model that scales. Today there are over 160,000 registered ethical hackers, and over the coming years this number is likely to grow to over a million. This army of hackers will be able to take on the work of the entire digital realm of our society.

Thanks to the diversity and scale of the hacker community, hacker-powered security finds vulnerabilities that automated scanners or permanent penetration testing teams do not find. Existing models are good at finding predictable security vulnerabilities, but even more important is to find the unpredictable ones - the unknown unknowns. Given a large enough hacker community and enough time, such vulnerabilities will be identified.

Vast and Diverse Clientele

Hacker-powered security emanated over the past decade as a best practice among Silicon Valley tech companies. Today, the model has matured and became applicable to all types of businesses. Any company, corporation, association or public sector agency that develops and deploys software (in whatever form, such as embedded in hardware) can benefit from hacker-powered security.

The vendors providing hacker-powered services have established communities of ethical hackers for whom they keep track of skill profiles and performance metrics. Bug bounty programs may be self-managed by the customer, or fully managed by the vendor. In the latter scenario, customers save both time and money while being presented with valid security vulnerabilities on a continuous basis. In either scenario, it is up to the customer to remediate the vulnerability once found.

Entities that operate such vulnerability disclosure and/or bug bounty programs include: Adobe, AT&T, CERT Coordination Center, U.S. Department of Defense, Dropbox, Facebook, Fiat Chrysler, U.S. General Service Administration, General Motors, GitHub, Google, LendingClub, Microsoft, Nintendo, Panasonic Avionics, Qualcomm, Snapchat, Starbucks, Spotify, Twitter, and United Airlines. Hacker-powered security is useful and accessible for organizations both large and small, technology-focused or not, in the private or public sector. The model is suitable for all entities that develop and deploy software.

Who are the Hackers?

The original experts at the Massachusetts Institute of Technology (MIT) defined themselves as *"one who enjoys the intellectual challenge of creatively overcoming limitations."*

Security experts may be described using a variety of titles including “ethical hacker”, “white hat”, “security researcher”, “bug hunter”, and “finder.” One title is conspicuously absent: Criminal. Hackers are not criminals. Specifically, bug bounty platforms offer no benefit to someone with criminal intent. On the contrary, HackerOne will record data about every hacker on the platform and only reward actions that follow the rules. For these reasons, criminals go elsewhere.

Hackers are driven by a variety of motivations, many of which altruistic. The security advocacy organization *I Am The Calvary* summarizes these motivations[4] as: **Protect** (make the world a safer place), **Puzzle** (tinker out of curiosity), **Prestige** (seek pride and notability), **Profit** (to earn money), and **Protest/Patriotism** (ideological and principled).

The HackerOne 2018 Hacker Report[5] - a survey of over 1,000 hackers - revealed that profit was only the fourth most common motivation for why hackers do their work. Before that came the desire to learn, be challenged, and have fun. To protect and defend is also a central motivation for hackers. A 2016 study by the National Telecommunications and Information Administration (NTIA) within the Department of Commerce found that only 15% of security researchers expect financial compensation in response to a vulnerability disclosure.[6]

Hacker-powered security does not only improve security. The model democratizes opportunity and offers meaningful work to anyone with the inclination and drive to be a useful ethical hacker. Many hackers are young adults. They can do their work from anywhere. The money hackers make is used to support their families, pay for education, and catapult them into successful professional careers. Hacking brings meaning and mandate to enterprising people irrespective of their location. Hacking brings positive societal impact across the nation.

Case Studies

The U.S. Department of Defense (DoD) and HackerOne pioneered the first federal government bug bounty program. Since the program’s inception, more than 3,600 security vulnerabilities have been safely resolved in DoD critical assets with

[4] https://www.iamthecavalry.org/motivations
[5] https://www.hackerone.com/sites/default/files/2018-01/2018_Hacker_Report.pdf
[6] https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf

hacker-powered security. While the majority of the vulnerabilities reported through the DoD vulnerability disclosure policy were without financial compensation, hackers have been awarded hundreds of thousands of dollars in bug bounty payments by DoD.

“Hack the Pentagon” was initially launched as a pilot program under the leadership of Secretary of Defense Ash Carter. This pilot ran from April 18 to May 12, 2016. During that short time more than 250 vetted ethical hacker participants submitted vulnerability reports. A total of 138 valid vulnerabilities were found and remediated.

"We know that state-sponsored actors and black-hat hackers want to challenge and exploit our networks," said Secretary Carter of Hack the Pentagon[7]. "What we didn't fully appreciate before this pilot was how many white-hat hackers there are who want to make a difference - hackers who want to help keep our people and nation safer."

"It's not a small sum, but if we had gone through the normal process of hiring an outside firm to do a security audit and vulnerability assessment, which is what we usually do, it would have cost us more than $1 million,[8]" Carter said of the $150,000 pilot program.

The Pentagon announced it would continue Hack the Pentagon program and bring this successful model to other agencies.

Hack the Army

The “Hack the Army” Bug Bounty program[9] ran from November to December 2016 with 371 registered, vetted and eligible participants. Of those who participated 25 were government employees including 17 military personnel. Of the 416 vulnerability reports submitted by hackers, 118 were unique, valid and actionable. The first one was filed within 5 minutes of the launch of the program.

While bug bounties are a way for the DoD to tap into private sector talent, sometimes the cybersecurity talent is already within their ranks. One of the researchers that successfully hacked the U.S. Army was an Army Captain presently in school at the Army’s Cyber Center of Excellence at Fort Gordon, Georgia. In addition to having a

[7] https://www.defense.gov/News/News-Releases/News-Release-View/Article/802929/defense-secretary-ash-carter-releases-hack-the-pentagon-results/
[8] https://www.defense.gov/News/Article/Article/802828/carter-announces-hack-the-pentagon-program-results/
[9] https://www.hackerone.com/blog/Hack-The-Army-Results-Are-In

full-time job and family, this officer registered for Hack the Army to get real, operational hands-on training in addition to his extensive schooling.

Hack the Air Force

It took just under one minute for hackers to report the first security vulnerability to the U.S. Air Force. Within the first 24 hours, 70 reports were submitted, 23 of which were valid. During the "Hack the Air Force" bug bounty challenge, 207 valid vulnerabilities were discovered. Nearly 300 vetted individuals had registered to participate in the Hack the Air Force bug bounty challenge and more than 50 earned bounties.

"Adversaries are constantly attempting to attack our websites, so we welcome a second opinion — and in this case, hundreds of second opinions — on the health and security of our online infrastructure,[10]" said Peter Kim, the Air Force Chief Information Security Officer. "By engaging a global army of security researchers, we're better able to assess our vulnerabilities and protect the Air Force's efforts in the skies, on the ground and online."

Two of the Hack the Air Force participants were military personnel opting to help as an act of patriotism despite being ineligible for bounties, and 33 participants came from outside the U.S. Some of the top participating hackers were under 20 years old, including a 17 year-old from Chicago who earned the largest bounty sum for 30 separate discoveries.

The Hack the Air Force bug bounty challenge was so successful that the Air Force ran a second bug bounty challenge - Hack the Air Force 2.0 - in December 2017.

Consistency with Existing Laws & Best Practices

Federal regulatory agencies responsible for consumer safety have acknowledged and adopted vulnerability disclosure programs as a cybersecurity best practice. These agencies recognize the critical role that hackers play in securing technology and protecting consumers.

In June 2015, the Federal Trade Commission (FTC) published security guidance for businesses summarizing security best practices from the agency's 50+ data security

[10] http://www.af.mil/News/Article-Display/Article/1274518/hack-the-air-force-results-released/

settlements.[11] One common cause for complaint against an organization's security practices was the lack of a vulnerability disclosure process. For example: "FTC charged that the company didn't have a process for receiving and addressing reports about security vulnerabilities. HTC's alleged delay in responding to warnings meant that the vulnerabilities found their way onto even more devices across multiple operating system versions."

In later comments made by the FTC to the NTIA Safety Working Group,[12] the commission reaffirmed the importance of this practice: "[FTC] staff highlighted the important role that vulnerability reports play in ensuring product security, and recommended that businesses implement reasonable vulnerability disclosure processes to facilitate communication with the research community."

In October 2016, the National Highway Traffic Safety Administration (NHTSA) published *Cybersecurity Best Practices for Modern Vehicles.*[13] It states: "Automotive industry members should consider creating their own vulnerability reporting/disclosure policies, or adopting policies used in other sectors or in technical standards. Such policies would provide any external cybersecurity researcher with guidance on how to disclose vulnerabilities to organizations that manufacture and design vehicle systems." Major automakers, including General Motors[14] and Tesla[15], have adopted policies for encouraging hackers to identify and disclose vulnerabilities in their connected automobiles.

In December 2016, the Food and Drug Administration published *Postmarket Management of Cybersecurity in Medical Devices*[16], noting that "...cybersecurity information may originate from an array of sources including independent security researchers.." and described "Adopting a coordinated vulnerability disclosure policy and practice" as a critical component of any medical device manufacturer cybersecurity program.

In July 2017, the Department of Justice (DoJ) Criminal Division's Cybersecurity Unit published *"A Framework for a Vulnerability Disclosure Program".*[17] The DoJ observes

---

[11] https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business#current
[12] https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-national-telecommunications-information-administration-regarding-safety-working/170215ntiacomment.pdf
[13] https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf
[14] https://hackerone.com/gm
[15] https://www.tesla.com/about/security
[16] https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf
[17] https://www.justice.gov/criminal-ccips/page/file/983996/download

"[organizations are] adopting vulnerability disclosure programs to improve their ability to detect security issues on their networks that could lead to the compromise of sensitive data" and goes on to provide guidance for operating these programs in a manner consistent with existing cybercrime laws.

In October 2017, deputy attorney general Rod Rosenstein made this public statement:[18] “All companies should consider promulgating a vulnerability disclosure policy, that is, a public invitation for white hat security researchers to report vulnerabilities. The U.S. Department of Defense runs such a program. It has been very successful in finding and solving problems before they turn into crises.”

These federal agencies have recognized the critical role that ethical hackers play in enabling public and private sector organizations to provide secure services that are resilient to cybersecurity vulnerabilities.

Conclusion and recommendation

We need hackers. Our goal must be an internet that enables privacy and protects consumers. This is not achievable without ethical hackers taking an active role in safeguarding our collective security.

Hackers are truly the immune system of the internet. They are a positive power in society. We must enable and encourage them to make their best security contributions. This requires a safe legal environment encouraging all individuals to come forward with vulnerability information, no matter the circumstances.

I provide you with the following recommendations:

First, the Computer Fraud and Abuse Act (CFAA), enacted in 1984, contains vague wording that has not kept pace with the proliferation of the internet. The act is in need of modernization. I encourage the members of the committee to support CFAA reform[19] to remove imposed criminal penalties on actions that do no harm to consumers. Individuals that act in good faith to identify and report potential vulnerabilities should not be legally exposed.

[18] https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-global-cyber-security-summit
[19] https://www.eff.org/document/letter-def-con-cfaa-reform

Second, the patchwork of breach notification laws enacted primarily at the state level may create uncertainty and perverse incentives for those who safeguard consumer data. I encourage this subcommittee to support a harmonized and unambiguous breach notification law governing all U.S. companies and consumers. It is important that such a law provide clarity on the definition of a data breach to ensure that those who operate or participate in a good faith vulnerability disclosure policy are not legally exposed.

Third, I repeat the words of numerous experts that a ubiquitous "See something, Say something" practice for vulnerabilities is a vital and critical step towards improving cybersecurity for consumers. The absence of a formal channel to receive vulnerability reports reduces a vendor's security posture and introduces unnecessary risk. Corporations should welcome input from external parties regarding potential security vulnerabilities and Congress should encourage that behavior.

As Jeff Massimilla, Vice President for Vehicle Safety and Product Cybersecurity at General Motors, stated: "To improve the security of their connected systems, every corporation should have a vulnerability disclosure policy that allows them to receive security submissions from the outside world."[20]

Hacker-powered security has matured as a model to be ready to help society solve one of its most pressing problems: cyber threats.

Pioneering entities have perfected the practice of hacker-powered security. Hundreds of thousands of security vulnerabilities have already been found and remediated. The vast community of hackers stands ready. The hackers are not asking what society can do for them. They are asking what they can do for society. Ethical hacking may be the only force that can stop criminal hacking. The asymmetry of digital threats can be turned around with pooled defense. Together we hit harder against cybercrime.

Thank you for the opportunity to testify on this important issue.

[20] https://www.cnet.com/roadshow/news/general-motors-cybersecurity/