# U.S. Senate Subcommittee on Data Security and Bug Bounties:

**SUMMARY OF WRITTEN TESTIMONY AND HACKERONE STATEMENTS**

In February 2018, HackerOne was invited to testify in front of the U.S. Senate Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security for their "Data Security and Bug Bounty Programs: Lessons Learned from the Uber Breach and Security Researchers" hearing. HackerOne was honored to join the Senate and leaders in the hacker-powered security industry to discuss the role white-hat hackers can play—and are already playing—in strengthening the security of technology in general.

Following is HackerOne Co-Founder and CTO Alex Rice's summary of the hearing testimony, a full transcript of the hearing testimony of HackerOne CEO, Mårten Mickos, and finally Mårten's responses to follow up questions from U.S. Senator Jerry Moran of Kansas.

# U.S. Senate Hearing - Data Security and Bug Bounty Programs: Lessons Learned

**AUTHOR: ALEX RICE, CO-FOUNDER AND CTO, HACKERONE**

**DATE PUBLISHED: FEBRUARY 6, 2018**
Original publication: https://www.hackerone.com/blog/US-Senate-Hearing-Bug-Bounty-Lessons-Learned

Today, HackerOne was invited to testify in front of the U.S. Senate Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security. We are honored to join the Senate and leaders in our industry to discuss the role hackers can play in strengthening security.

The fallout from past breaches has done lasting damage to our trust in technology. This hearing[1] and others like it are necessary if we are to learn from past incidents and work better together to protect consumers and their data.

[1] https://www.commerce.senate.gov/public/index.cfm/2018/2/data-security-and-bug-bounty-programs-lessons-learned-from-the-uber-breach-and-security-researchers

For the first time in my life, an entire room of lawmakers were in awe of the valuable role hackers play in protecting us. Hackers have continually risen to this challenge despite obstacles and considerable personal risk. That tenacity speaks to their strength. The world is finally beginning to embrace an important truth:
**we need hackers.**

In the hearing itself, the committee and a group of invited security experts shared insights on the value hackers provide alongside the differences between legitimate bug bounty programs and criminal breaches. I've summarized the key points from the experts below, but those with an interest in this area will find their full statements are absolutely worthy of your time.

## FROM THE SENATE HEARING

### Justin Brookman - Director, Privacy and Technology Policy - Consumers Union[2]

Justin pointed to the commitment by Consumers Union to provide more information to consumers about which companies have the best data security practices, such as through their work on the open source Digital Standard[3]. This standard articulates the importance of hackers as a data security best practice:

> *"Consumers Union is a strong proponent of bug bounty programs, and believes that they play a crucial role in a data security ecosystem that has failed consumers far too often."*

The statement pointed to the counterproductive tendency for companies to report security researchers to law enforcement. Absent a strong indicator of malicious intent in this incident, Justin complimented Uber for their restraint in not immediately escalating the hacker to law enforcement, but criticized Uber's decision to not provide timely notification to its users.

Ultimately, the recommendation focused on (1) additional resources and authority for the FTC to challenge shoddy data security practices and (2) stronger, clarified, and unified breach notification standard enacted at the federal level. We wholeheartedly agree.

[2] https://www.commerce.senate.gov/public/?a=Files.Serve&File_id=53EBF526-F9A1-467D-911D-70A54C9CF9FA
[3] https://www.thedigitalstandard.org/the-standard

## Katie Moussouris - Chief Executive Officer - Luta Security[4]

Katie opened her statement with a reminder of the chilling effect existing laws have had on on security research for defensive purposes.

> *"In 2015, 94% of the Forbes Global 2000 had no published way to report a security hole to them. If you saw something, it was difficult to say something. It was even a risk to your freedom if the organization chose to pursue legal action against you."*

Katie explores the importance of a thoughtfully crafted vulnerability disclosure policy, highlighting the Department of Justice's recent Vulnerability Disclosure Framework[5] as a best practice for protecting both consumers and well-intentioned researchers.

Katie closed her statement highlighting the powerful role the defense market can play in bolstering the cybersecurity workforce and encouraged the subcommittee members to support investments into security defense training and education.

## John "Four" Flynn - Chief Information Security Officer - Uber[6]

The Uber CISO covered the importance of bug bounty programs at length, describing them as "a critically important tool and widely used as part of comprehensive data security programs". Since its initial launch, the Uber program has resolved more than 800 unique vulnerabilities, before they had the opportunity to become breaches.

> *"Uber's bug bounty program unquestionably has increased the scale and speed at which we are able to identify and eliminate cybersecurity threats."*

The 2016 Uber Data Security Incident "unfolded in a way that is entirely different from the typical bug bounty program scenario". The key distinction? "The intruders not only found a weakness, they also exploited the vulnerability in a malicious fashion to access and download data."

[4] https://www.commerce.senate.gov/public/?a=Files.Serve&File_id=E162FD54-F858-44AE-B25F-64E331C628AE
[5] https://www.justice.gov/criminal-ccips/page/file/983996/download
[6] https://www.commerce.senate.gov/public/?a=Files.Serve&File_id=7D70E53E-73E9-4336-A100-67B233084F12

This statement grants the public some valuable transparency into Uber's response process to this incident. This response to this incident got a lot right: containment, attribution, etc. But, critically, it sheds light on everyone's main question: why wasn't there a breach notification?

The statement provides a public admission that Uber reflects upon that decision as wrong. John apologetically made no excuses for the lack of notification.

John shared several additional lessons learned. In particular, he highlights the importance of a multi-stakeholder process for security incidents and the early involvement of law enforcement. He concludes with strong support for a unified, national approach to data security and breach standards.

## Mårten Mickos - Chief Executive Officer - HackerOne[7]

Mårten provided three recommendations aimed at safe harbor for hackers while they work to improve security:

First, the Computer Fraud and Abuse Act (CFAA), enacted in 1984, contains vague wording that has not kept pace with the internet. CFAA reform is urgently needed to create safe harbor for individuals that act in good faith to identify and report potential vulnerabilities.

Second, unifying the patchwork of breach notification laws enacted primarily at the state level with a harmonized and unambiguous federal standard could strongly benefit both consumers and companies alike. Those who participate in a good faith vulnerability disclosure policy must never be pulled into misguided legal proceedings.

Third, security best practices remain woefully inadequate across the industry. Consumer protection agencies (primarily the FTC) should receive further resources and empowerment from Congress. For example, all organizations entrusted with the safeguard of consumer data could, at a minimum, implement a vulnerability disclosure policy.

[7] https://www.commerce.senate.gov/public/?a=Files.Serve&File_id=CF1E3C8C-1D90-4F85-9E11-78271A5776A6

# PRACTICAL LESSONS LEARNED

Today's hearing served as validation that working alongside hackers is a necessary security practice. It also reaffirmed several best practices that HackerOne has long recommended to our customers. Anyone who is considering or already operating a bug bounty program should weigh the following recommendations:

1. Define "authorized." Every disclosure policy should speak to which activities are considered authorized, steps to avoid sensitive information, and how individuals should handle an unlikely encounter with sensitive information. The DoJ's Vulnerability Disclosure Framework[8] provides a solid reference, and we recommend the following template policy language:

   *Make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of our service. Only interact with accounts you own or with explicit permission of the account holder.*

   *If you do encounter Personally Identifiable Information (PII) contact us immediately, do not proceed with access, and immediately purge any local information.*

2. Do not pay a bounty to a participant who has willfully violated program rules. On HackerOne, immediately "Request Mediation[9]" if you suspect a hacker is acting in bad faith.

3. All bounty amounts should adhere to clear, published policies. Never increase bounty amounts in response to demands, opening the door to dangerous quid pro quo negotiations.

4. Contact law enforcement and a legal specialist if you believe you are being extorted or discovered a strong indicator of criminal intent. HackerOne will never knowingly assist with an extortion payment, unless under explicit instruction from law enforcement.

We also learned an important lesson. HackerOne has traditionally viewed our services as specializing in preventing data breaches, not incident response. We recognize the need for us to be stronger partners in this area. Toward that goal, HackerOne will begin active steps toward helping our customers become incident-ready.

We **need** hackers. They are the immune system[10]. HackerOne will continue to fight for a safe environment that enables hackers to do their best work.

**ALEX RICE, CO-FOUNDER AND CTO, HACKERONE**

[8] https://www.justice.gov/criminal-ccips/page/file/983996/download
[9] https://support.hackerone.com/hc/en-us/articles/208475476-What-are-examples-of-bad-behavior-
[10] https://www.ted.com/talks/keren_elazari_hackers_the_internet_s_immune_system

# Full Testimony of Mårten Mickos Before the Commerce Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security

**AUTHOR: MÅRTEN MICKOS, CHIEF EXECUTIVE OFFICER, HACKERONE**

**DATE PUBLISHED: FEBRUARY 6, 2018**

Original publication: https://www.commerce.senate.gov/public/_cache/files/cf1e3c8c-1d90-4f85-9e11-78271a5776a6/627FACFBD6AA202FAAA9976EF0733722.marten-mickos---hackerone---testimony.pdf

## 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.

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

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 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

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

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.

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).

[3] Hunter and 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.

## 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.

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 become 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 are 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

[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

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 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.

[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

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 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.

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

# CONSISTENCY WITH EXISTING LAWS AND 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 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.

[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

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 "[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.

[17] https://www.justice.gov/criminal-ccips/page/file/983996/download

[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/

# Answers to Questions for the Record From Mårten Mickos

**AUTHOR: MARTEN MICKOS, CHIEF EXECUTIVE OFFICER, HACKERONE**
**DATE SUBMITTED: MARCH 6, 2018**

In connection with the hearing "Data Security and Bug Bounty Programs: Lessons Learned from the Uber Breach and Security Researchers" Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security U.S. Senate Committee on Commerce, Science and Transportation. Written questions submitted by the Honorable Jerry Moran to Mårten Mickos.

## QUESTION 1

**What separates a good faith researcher from a malicious actor? What's to stop a criminal from posing as a researcher? How can companies or vendors tell the difference?**

## ANSWER

Intent is what separates a good faith security researcher from a malicious actor. Researchers that are reporting vulnerabilities through lawful channels are doing so with the intent that the vulnerability report be delivered to the owner of the system for the bug to be resolved.

Vulnerability disclosure and bug bounty programs are so designed that they provide no particular benefit or special access to the participants. On the contrary, the programs generate additional work for the participant while collecting various pieces of information about them. For these reasons, a malicious actor has something to lose and nothing to gain in such a program. It is more rational for the malicious actor to engage in their unauthorized activity outside of the program.

Like in most professional endeavors, it is at least in theory possible for a criminal to pose as a legitimate participant. But given that there are no benefits but only obligations in a program, this would not be rational behavior. The only way to receive a benefit from a vulnerability disclosure or bug bounty program is by reporting a valid vulnerability to the owner of the system. When that happens, a vulnerability can be removed and rendered unusable by criminals.

Criminals, for the above mentioned reasons, do not wait for vulnerability disclosure or bug bounty programs to start, and they obtain no benefit from joining such programs if they exist. Criminals engage in their unauthorized activity at any time and outside any formal program.

When researchers bring security vulnerabilities to the attention of companies and organizations, they should assume good faith until proven otherwise.

The question of whether an entity operating a program can tell the difference between a well-intended researcher and a criminal becomes philosophical or even irrelevant. Outside of the program, any criminal activity is possible and often likely. Inside the program, only good and non-criminal deeds are rewarded.

The above text describes the general case. Additionally, there can be a special case of a bug bounty program in which the program-operating entity indeed does offer special access or benefits to the participants. For instance, a company may provide test accounts or other credentials to participating researchers so that they may venture deeper into the computer system in their hunt for vulnerabilities to report and be rewarded for. In such programs, the participating researchers go through additional vetting and screening. The exact nature of the screening depends on the company's or organization's preferences and may include verification of identity and tax ID, verification of home address, criminal background check, and so on. With these additional screening requirements, the operator of the bug bounty program guards itself against malicious actors gaining access to the program in question.

For an overview of the motivations of ethical hackers and for personal profiles of a number of them, we recommend reading the 2018 Hacker Report that is available from HackerOne, Inc., on our website www.hackerone.com and by contacting us by email at info@hackerone.com.

## QUESTION 2

**What is the role of bug bounty programs when faced with extortion attempts?**

## ANSWER

Extortion has absolutely no role in bug bounty programs.

Whenever a situation develops that may indicate an extortion attempt, HackerOne advises the sponsor of the program (its customer) to notify and work with law enforcement for guidance and instructions. It is always the entity with the bug bounty (or vulnerability coordination) program that determines whether conduct by a hacker or hackers is authorized or unauthorized. Bug bounty platform providers such as HackerOne act as a preventative service.

There are situations where immature researchers may ask for a bounty in an impolite or even threatening way. Often, such situations can be de-escalated with the help of mediation and diplomacy. Hackers do commonly suggest or ask for specific bounty amounts from the vendor.

The size of the bounty is largely determined by the severity of the vulnerability, and severity can be properly assessed only by the customer. So the finder is in a position of no control at all over the payment outcome. To balance this, they often make suggestions, requests and claims for specific bounties in the hope that the customer will be open to suggestions. As many hackers are young and all of them are impatient, the language of such requests may not seem proper to someone not familiar with the trade, even though the hacker has the best of intentions.

## QUESTION 3

**According to your testimony, the diversity and scale of the hacker community allows the "hacker-powered security" model to identify vulnerabilities that automated scanners and permanent penetration testing teams will not. Can you please further explain this sentiment? Are there any metrics or numbers that are able to cite to quantify the effectiveness of the model over other approaches?**

## ANSWER

Customers on HackerOne have resolved more than 65,000 unique security vulnerabilities to date by working with the hacker community. A good portion of these customers have reported back to HackerOne that they are finding vulnerabilities that they could not otherwise detect with scanners or penetration testing (also called pentesting). The strongest metric in support of hacker-powered security is the fact that even after deploying scanners and pentests there are innumerable security vulnerabilities that bug bounty and vulnerability disclosure programs identify.

There are a number of reasons for this. A key reason is that scanners and penetration testing are limited in scope whereas hacker-powered security is broad and diverse.

A scanner has been programmed by engineers to detect specific previously known vulnerability types, but it is limited in its ability to modify its search or "think outside the box." Though useful, scanners cannot find what humans can. Penetration tests are conducted by humans and therefore represent more intellectual variety and creativity than scanners. But they cannot measure up against a broad and creative collection of external researchers. Penetration tests follow pre-defined guidelines and are designed to test for a specific set of vulnerabilities. Often, customers are more eager to get a clean report than to find all possible vulnerabilities.

In both the case of scanners and of penetration testing, the customer is paying a fixed price for effort. But in the case of hacker-powered security, the customer pays for result. Hackers do not get paid unless they find something of value to the customer. This leads the hackers to try harder and think more creatively, and that in turn leads to superior results.

## QUESTION 4

**Your testimony described vulnerability disclosure programs with the motto of "If you see something, say something," and further elaborates how the outside hacker will be invited to disclose the vulnerability to the system's owner. During the disclosure process, is it a common practice for the hacker to actually take exposed data in order to demonstrate proof of vulnerability to the company? If so, is there a standard type or amount of data that these [sic] is needed for the hacker to demonstrate authenticity?**

## ANSWER

The amount of evidence that it is prudent to collect when discovering a security vulnerability is a topic of great interest to the security community. On the one hand, the hacker is bound and committed by the program rules not to cause harm or obtain any data that is not needed for the work. On the other hand, there are situations where perhaps the only way of demonstrating that a breach could be possible is to actually exfiltrate some data.

Entities that operate bug bounty programs declare on their program page the rules for the hackers. Typically, they will prohibit data exfiltration, as this example from a prominent bug bounty program shows: "Findings not eligible for bounty:... Internal pivoting, scanning, exploiting, or exfiltrating data from internal [company name] systems."

It should be noted that a hacker may not initially know what is inside a data file found. In order to determine the nature of the file, the hacker may have to open it, which for practical purposes may mean downloading it, which amounts to exfiltration. If the contents are irrelevant, then no harm was done. If the file contains pointers to other data sources, or perhaps credentials to another system, then this is valuable information for resolving the security problem. But if the contents turn out to be customer or personal information, then the hacker must immediately erase any such copies of the file and refrain from opening it or using it again. The determination of whether it is permissible to open the file or not can be made only after the file has been opened.

## QUESTION 5

**HackerOne's 2018 Hacker Report and a 2016 study conducted by the National Telecommunications and Information Administration (NTIA) both indicated that profit is a relatively limited motivation among hackers participating in coordinated vulnerability disclosure programs.  Given the panel's experience with professionals in this field, could you please further describe the predominant motivators?**

## ANSWER

In the course of its business, HackerOne has enabled tens of thousands of hackers to find and help fix over 65,000 security vulnerabilities. The motivations behind the hackers' work are as diverse as the group. In the hacker surveys we have conducted, we consistently see hackers operating under multiple motivations.

Financial rewards are essential and important, but they are far from the only motivation. The presence and success of numerous vulnerability disclosure programs (i.e., programs that pay no financial rewards) serve as a clear indicator that there are plenty of hackers ready to hunt for security vulnerabilities for other than pecuniary reasons. For instance, in the various programs by the Department of Defense, about 3,000 vulnerabilities have been reported into the vulnerability disclosure program and 600 within the bug bounty programs.

Many hackers hack for the intellectual challenge. They want to learn more and they are eager to know that they have the skill to find a hole in the armor of a famous company or government entity. Being thanked or acknowledged by a prestigious vulnerability disclosure program is a great motivation.

Often, hackers hack in order to find like-minded people and be able to collaborate with them. It is a reward in itself to be able to interact with someone with unusual skill or intellect.

Others hack for the pragmatic reason of advancing their careers. The list of vulnerabilities found that each hacker has on their individual HackerOne page serves as evidence of their skills. It helps them gain entry to colleges and universities or to land a security job at a company or other organization.

For many, there is an altruistic motive in hacking. They want to make the world a more secure place. They want to contribute to society. They have a sense of duty and feel that if they know how to detect vulnerabilities, it is their mandate to report them to the owners of the various systems.

## QUESTION 6

**Would you agree that it is absolutely critical for companies to administer any vulnerability disclosure program responsibly based on sound principles (such as those included in DOJ's 2017 guidelines) as it has obvious impacts on industry-wide use of these types of programs that are proven to protect consumers?**

## ANSWER

Yes, HackerOne applauded the U.S. Department of Justice for its 2017 guidelines for vulnerability disclosure programs (VDP). The DoJ's guidance reflects best-practices across the industry and is a critical document for any organization. Indeed, in many ways, HackerOne is dedicated to facilitating the responsible implementation of VDPs across the broad spectrum of vulnerable entities in line with the DoJ's guidance.

## QUESTION 7

**Given the unique national security aspects of working with DOD, I am interested to hear more about HackerOne's involvement in the vulnerability disclosure programs aiding our Armed Services, starting with the "Hack the Pentagon" program and followed by the "Hack the Army" and "Hack the Air Force 1.0 and 2.0."**

## ANSWER

The Department of Defense's Defense Digital Services pioneered the first ever Federal bug bounty challenge, "Hack the Pentagon," in 2016. The DoD is continuing to do so by engaging with the global hacker community through its ongoing vulnerability disclosure policy.

Since the Hack the Pentagon program launched in 2016, over 3,600 vulnerabilities have been resolved in government systems through the bug bounty and vulnerability disclosure challenges on HackerOne. Working with the ethical hacker community supplements the useful work the DoD's internal security teams are already doing.

## HACK THE ARMY

The Hack the Army Bug Bounty program ran from Wednesday, November 30, 2016 to Wednesday, December 21, 2016. Hackers reported more than 118 valid unique security issues.

Through this program, the Army was able to tap into the reservoir of diverse hackers on HackerOne, many of whom would otherwise not work with the Army, augment the work the Army red teams are already doing to help secure their systems and networks, and increase the security of mission critical systems and networks that house information critical to military recruiting.

The Army chose as its target digital assets that might have been used as a stepping stone for reaching personally identifying information about Army recruits - colloquially referred to as "the crown jewels." Ensuring this data was secure was a high priority for DoD because of the sensitivity of the information for America's potential war fighters.

The most significant vulnerability found was due to a series of chained vulnerabilities.

A researcher could move from a public-facing website, goarmy.com, and get to an internal DoD website that requires special credentials to access. The researchers got there through an open proxy, meaning the routing was not shut down the way it should have been. The researcher, without even knowing it, was able to get to this internal network because there was a vulnerability with the proxy and with the actual system. On its own, neither vulnerability is particularly interesting. Paired together, they become critical.

Automated testing tools are not capable of such leaps of logic. It requires a highly skilled and creative researcher (or team of researchers) to chain together a number of independent flaws in order to create a path to the critical inside of the system.

The Army remediation team that owns and operates the websites, as well as the Army Cyber Protection Brigade, acted quickly. Once the report was submitted, they were able to block any further attacks, and ensure there was no way to exploit this chain of vulnerabilities.

## HACK THE AIR FORCE

The Hack the Air Force Bug Bounty program ran from May 30, 2017 to June 23, 2017, with nearly 300 individual hackers participating in the bug bounty challenge. More than 50 hackers earned bounties for reporting more than 207 valid unique security vulnerabilities, the first of which was reported in less than a minute from the start of the program.

Some of the vulnerability reports received an initial response time of less than a minute by the Air Force security teams. The average time to resolution during the challenge was 4 days. What this means is that the Air Force's security team was extremely fast at processing reports, verifying them and resolving bugs, making the systems more secure faster.

## HACK THE AIR FORCE 2.0

On December 9, 2017, the first day of the challenge, 24 hackers met in New York City and participated in a live hacking event—the first ever to include federal government participation on- site. DoD and U.S. Air Force personnel worked alongside the vetted and pre-selected hackers to simultaneously report security flaws and remediate them in real-time. Together, they collaborated to find 55 of the 106 total vulnerabilities during this nine-hour hacking event.

Twenty-seven trusted hackers successfully participated in the Hack the Air Force bug bounty challenge—reporting 106 valid vulnerabilities and earning a total of $103,883. Hackers from the U.S., Canada, United Kingdom, Sweden, Netherlands, Belgium and Latvia participated in the challenge. In this event, the highest single bounty of any Federal program—$12,500—was awarded.

## QUESTION 8

**More specifically, were there lessons learned from the earlier programs that your company addressed and implemented in the more recent programs?**

## ANSWER

Working with its DoD counterparts, HackerOne and the security research community continue to improve its programs. We regularly revise and improve our internal process descriptions and our external program guidelines in order to reduce the risk of failure in a program and to increase the overall productivity and effectiveness of hacker-powered security. We also continually learn more about the digital assets of our customers so that we can provide better advice on which assets to include in a program, and at what phase of the program.

As our customers develop a thorough expertise in operating a bug bounty program, we may recommend events where hackers and the security team of the customer are brought together for a live hacking event. We did so during "Hack the Air Force 2.0" and the results exceeded expectations.

Hack the Air Force targeted operationally significant websites and online services. The goal of the program was to explore new approaches to its security, and to adopt the best practices used by the most successful and secure software companies in the world. The preliminary results indicate nearly doubling the results of the first Hack the Pentagon program a year earlier.

With every DoD bug bounty the pool of invited participants has grown, with the intent of opening it wider to continue to include all qualified participants. By now, every person on HackerOne is legally permitted to participate in the DoD's vulnerability disclosure program (VDP). To date, the DoD's VDP has resolved more than 3,000 security vulnerabilities.

## QUESTION 9

**How did your company account for the specific capabilities and functions of the different services your company worked with?**

## ANSWER

The key to success in a bug bounty or vulnerability disclosure program lies in diversity of approach and specificity of skill among the hackers. That is why HackerOne has established the world's largest community of security researchers, also known as white hat hackers. By having an enormous pool to draw from, we ensure that for each particular program there is a large enough group of hackers with the particular skills needed. We record and keep track of skill profiles in our hacker database. When a new program launches, we can find the hackers most likely to have the required skills.

As new customers launch programs on HackerOne, a useful cross-pollination of skills often happens. The new customer typically brings along hackers with deep skills in their particular digital asset. These hackers can then find other programs with similar profiles. And from those other programs, existing hackers may engage in the new program. In this way, over time, individual hacker skills are strengthened, and the overall skill profiles in the HackerOne community become more complete.

Additionally, both HackerOne and its clients may arrange for additional education, training and briefing of hackers in specific areas of technology. The more information there is available, the sharper the skills and the better the results of bug bounty programs.

Arguably the best source of learning for ethical hackers is the Hacktivity feed where vulnerability reports are being published by various companies and government agencies for others to learn from once the vulnerability has been fixed and removed.

## QUESTION 10

**Please explain the utility of a combined pool of federal employee and outside participants.**

## ANSWER

The success of cyber security is measured not by how many good events there are but by how many bad events can be avoided. The best results are achieved by multiple layers of security. Even if one layer occasionally fails, there is another layer that will catch the deviation from the norm.

Cyber security starts with the design of the digital system. This is the first layer of security. Later in the software lifecycle comes quality assurance, which also removes weaknesses. When a digital asset is ready for production use, it still needs testing and validation. This is where internal and external bug hunting teams come into the picture. Internal teams of employees have the benefit of inside knowledge of the system. External teams of hackers have the benefit of lack of bias. These and other, more technical, layers of security are needed for the best outcome.

A theme we heard over and over again while working with the DoD is that military and civilian personnel need hands-on training whenever possible. This keeps their skills sharp and allows them opportunities to see unique tactics from a highly skilled researcher community. Allowing employees to participate in bug bounty programs provides realistic training experiences in a controlled environment, at a low cost.

## QUESTION 11

**Your testimony states that $250,000 is the current maximum bounty listed across all programs that the company administers for its clients.  Are the maximum bounty amounts pre-determined in agreements with your client companies?**

## ANSWER

On HackerOne's platform, it is the customer that sets the bounty criteria, often based on a recommendation from HackerOne. HackerOne maintains a set of recommended bounty amounts that we derive from historical bounty payment data, adjusting for size and ambition level of the program in question. The bounty amount is typically a function of the severity of the vulnerability and the value of the digital asset in which the vulnerability was found.

The client company has the full right to deviate from their own criteria and pay out higher bounties than advertised. As a matter of fact, many programs do not publish or advertise any maximum bounty.

In addition to bounties, customers can choose to pay individual bonuses to hackers. For instance, if a hacker has prepared an unusually well-researched and well-written vulnerability report to the customer, the entity may choose to reward the hacker with a bonus on top of the bounty. The bonus amounts are typically small. In 2017, less than 5% of all hacker rewards were bonuses.

## QUESTION 12

**Your testimony stated that the Computer Fraud and Abuse Act is in need of modernization to prevent liability of hackers acting in good faith in identifying vulnerabilities to protect consumers.  Do you have any specific recommendations related to modernizing the law?**

## ANSWER

Current law, particularly the Computer Fraud and Abuse Act (CFAA), does a disservice to the internet and its citizens. Congress should amend it to reflect the modern-day needs of the country's cybersecurity community, including the value and necessity of voluntary disclosure programs.

The CFAA fails to define the terms "without authorization" or "exceeding authorized access," which are key elements of the law. This broad undefined language has resulted in the CFAA being called one of the most controversial, confusing, and inconsistently interpreted laws in the country. We suggest that the law should clarify "without authorization" and distinguish between bad intent on the one hand, and good intent or innocent lack of intent on the other.

While intended as a criminal law preventing malicious hacking, a 1994 amendment to the bill allows for civil actions. We suggest that the CFAA focus on criminal liability rather than civil liability. Much of the chilling effect created by the law originates from its broad interpretation in civil cases, where the burden of proof is reduced.

HackerOne also suggests that violations of contractual obligations, such as a website's terms of service, must not form a basis for criminal charges. Further, it should be clarified in the law that if access to data is already authorized, gaining that access in a novel or automated way is not a crime (i.e., changing IP addresses, MAC addresses, or browser User Agent headers). Finally, minor violations of the CFAA should be punishable with minor penalties, ensuring the punishment fits the violation.

HackerOne urges Congress to modernize the CFAA and related laws to reflect the necessity to fight cybercrime with modern-day tools and processes, including particularly voluntary disclosure programs.

# MAKE THE INTERNET SAFER