Luta Security

Statement of Katie Moussouris for the hearing entitled, “Data Security and Bug Bounty Programs: Lessons Learned from the Uber Breach and Security Researchers” for the Senate Committee on Commerce, Science, and Transportation’s Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security[1] on Tuesday, February 6, 2018

Chairman Moran, Ranking Member Blumenthal, and distinguished members of the Committee, thank you for the opportunity to testify at this hearing on behalf of Luta Security and the security research community.

We commend the Committee for holding this open hearing to help understand, clarify, and differentiate between defensive security research and vulnerability disclosure activities, which may or may not include bug bounties, versus Internet-enabled crimes, which may include extortion for unauthorized access to consumer data.

I am the founder and CEO of Luta Security, working with governments and complex organizations on multi-party supply chain vulnerability coordination to create mature, robust, sustainable vulnerability coordination and disclosure programs. We base these programs on the industry international standards ISO/IEC 29147 Vulnerability disclosure[2], ISO/IEC 30111 Vulnerability handling processes[3], and our Vulnerability Coordination Maturity Model.

I am the co-author & co-editor of these international standards, was co-chair of the NTIA’s multi-stakeholder vulnerability disclosure working group subcommittee of multi-party vulnerability coordination[4], with over 20 years of professional technical and strategic work in technology and information security, as a former penetration tester at @stake[5], to creating Microsoft Vulnerability Research, the first Microsoft bug bounties, and advising the US Department of Defense for years, resulting in the launch of the Hack-the-Pentagon program. I am also one of two private industry official delegates of the US technical experts working group to renegotiate the Wassenaar Arrangement[6], successfully helping clarify exemptions for vulnerability disclosure and incident response in export controls.[7] I served as an expert witness for European Parliament's consideration of dual-use export control reform in the context of vulnerability disclosure and bug bounty programs.[8]

[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
[2] http://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147
[3] https://www.iso.org/standard/53231.html
[4] https://www.first.org/global/sigs/vulnerability-coordination/multiparty/FIRST-Multiparty-Vulnerability-Coordination-draft.pdf
[5] https://en.wikipedia.org/wiki/@stake
[6] https://langevin.house.gov/press-release/langevin-statement-wassenaar-arrangement-plenary-session
[7] http://thehill.com/opinion/cybersecurity/365352-serious-progress-made-on-the-wassenaar-arrangement-for-global
[8] https://www.youtube.com/watch?v=kDJxAm-AVNA&feature=youtu.be

Today, I'm here as a witness to talk about the defense market for bugs, the role of bug bounties and other security research, and the role of the defensive ecosystem to shape these new markets.

When I was a teen learning to hack in the late '80s, there was no broadly-recognized and accessible defensive market for hacking skills, no online banks or e-commerce sites to hire us to test their Internet-facing systems for holes, no bug bounty programs, and even the United States government had only a few years earlier become aware of threats to national security across the burgeoning early Internet - through Hollywood films such as War Games.

This awareness of the power of hackers had prompted not job offers or viable legal career paths, but legislation that made hacking a criminal offense.[9] This law not only gave prosecutors the necessary legal tools to go after nation state actors and criminals, but to this day has caused a chilling effect on security research for defensive purposes. This chilling effect on researchers has also been reflected in the reluctance of governments and organizations to engage with hackers, further complicated by recent data breaches under the mis-applied term "bug bounty".

Only in the past 5 to 8 years have we seen any major acceptance by governments and companies working cooperatively and openly with hackers. However, there is still a great fear among many organizations that opening a front door for hackers to report security holes will cause damage from disruption of operations, intellectual property theft, fraud, reputational damage, and data breaches.

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 under the Computer Fraud and Abuse Act (CFAA).

While the CFAA hasn't materially changed over the past 34 years to grant security researchers safe harbor for helping to point out security bugs, in July of 2017, the Department of Justice issued "A Framework for a Vulnerability Disclosure Program for Online Systems."[10] This guide is meant as a way to help organizations think through important scoping issues around protected classes of data and systems when creating vulnerability disclosure programs, with or without cash incentives or bug bounties.

The main premises to help create robust vulnerability disclosure or bug bounty programs are straightforward in the DoJ framework, with a summary of the key aspects as follows:

1. Decide whether sensitive systems and data are in scope for discovery and reporting by external helpful hackers.
2. Encourage the use of test accounts whenever possible to avoid the unnecessary compromise of other users' privacy and data without their permission.
3. Make it clear that only the minimum necessary proof is required to prove that a vulnerability exists, and that no further access or exploitation past that point is authorized.

[9] https://www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html
[10] https://www.justice.gov/criminal-ccips/page/file/983996/download

4. Further define how any deliberately or accidentally accessed private data should be stored and transmitted.
5. Specify the manner in which proof of the hack is conveyed, perhaps using a screen capture to avoid further transmitting the protected data.
6. Decide whether to include the requirement to destroy any copies of data once the report is delivered.

To protect both well-intentioned researchers from ambiguity and accidental overstepping the intended scope, as well as to protect consumers whose data may be subject to access, transmission, and storage without their consent, it is important to define these parameters as clearly as possible. This applies in vulnerability disclosure programs as well as bug bounties.

Finally, as a creator and advisor of some of the major new bug bounty programs in the past several years, I want to point out that the ecosystem for rewarding bug hunting is skewing the markets toward more bug hunters, but not necessarily more bug fixers. This imbalance that is being created in these markets may very well shift the ecosystem towards rewarding more data theft than bug hunting.

There is a difference between paying $10,000 for a bug and paying $100,000 for a breach. If the legal market for bugs becomes muddied with extortion payments that are exponentially higher, we will be building the wrong kind of market, and consumers will be the victims instead of the beneficiaries of enhanced work with hackers.

Already, we are facing a global shortage of talent in cyber security, and while more legal ways to report bugs is good, the creation of an overall defense workforce is necessary, in the United States and worldwide.

“In 2017, the U.S. employs nearly 780,000 people in cybersecurity positions, with approximately 350,000 current cybersecurity openings…”

““With more than 200,000 open cybersecurity jobs in 2015 in the U.S. alone and the number of threat surfaces exponentially increasing, there’s a growing skills gap between the bad actors and the good guys. One way to close the gap is through automation, but we also need to train developers, at the very earliest stage of their education, to bake security into all new code. It’s not good enough to tack cybersecurity on as an afterthought anymore. This is especially true as more smart devices become Internet accessible and therefore potential avenues for threats.”

According to a 2016 study, “none of the top 10 U.S. computer science programs required a cybersecurity course for graduation, and 3 of the top 10 university programs don’t even offer an elective course in cybersecurity.”[11]

[11] https://www.cloudpassage.com/company/press-releases/cloudpassage-study-finds-u-s-universities-failing-cybersecurity-education/

Much like in Star Wars, The Force for finding vulnerabilities has a dark side as well as a light side, but they are two sides of the same coin, representing indistinguishable skill sets. We are creating more of an imbalance in The Force, weighted against defenders.

As a visiting scholar with MIT Sloan School helping to study the vulnerability economy and exploit markets, I helped clarify the differences in the offense and defense markets for bugs. The offense market is characterized by nation states and criminals buying bugs and exploits at high prices to keep them from being fixed as long as possible to prolong their use in attacks.

The defense market is typically paying lower amounts than the offense market, but doesn't traditionally require the bug hunter to stay silent about their find, once it is fixed, providing the finder with recognition and further opportunities for their career in other ways.

The defense market for bugs cannot compete directly with the offense market on price.

Very quickly, we would run out of willing software developers and testers, and the markets are already taking that direction in the way that bug bounties are being used today. Bug bounty hunters worldwide are on average able to make more than being a software developer in many countries. Perverse incentives include overpaying for bugs on the defense market, as well as the rewarding of data theft with much higher prices than an honest bug hunter would get for adhering to the rules.

The entire defensive bug hunting ecosystem has a responsibility to help uphold the law & guide the creation of programs that will not breach ethical or legal standards. We have a responsibility to the current and next generation of hackers to demonstrate best practices in bug bounties as well as the broader vulnerability disclosure picture.

"Focusing on the labor market opens new productive avenues for conversation and future research: It suggests linkages between research on vulnerability markets and a larger body of work rooted in the tradition of economic sociology. These efforts consider markets not only or, at times, not even primarily—as engines of efficient resource allocation, but move to address pressing descriptive questions related to the contingent and historical specificity of the construction of markets.

Markets are not inevitable. They are always actively created."[12]

If Congress were to act to help clarify the role of defensive security research, and encourage the growth of the defense market for bugs, as well as the United States labor workforce in cybersecuritydefender roles, I would ask that:

[12] Ryan Ellis, Keman Huang, Michael Siegel, Katie Moussouris, and James Houghton. "Fixing a Hole: The Labor Market for Bugs." New Solutions for Cybersecurity. Howard Shrobe, David L. Shrier, and Alex Pentland, eds. Cambridge: MIT Press. In Press. ISBN: 9780262535373 https://mitpress.mit.edu/books/new-solutions-cybersecurity

1. Funding for increased education in security be set for all grades (K-12), to begin finding early security talent and recruiting for defense
2. Setting forth requirements that all college majors in computer science understand secure coding and organizational cyber risk management
3. Fewer “Hack the x” bills be introduced without proper assessment of sustainable defensive capabilities in each government agency considering launching a bug bounty.

Again, I’d like to thank you for the opportunity of testifying today. I welcome your questions and comments.