Policy Analysis: Tapping into the Wisdom of the Cybersecurity Crowd

In May 2017, Warren Buffet called cyberattacks "the number one problem with mankind".[1] Cyberattacks are occurring with alarming frequency, sophistication, and scale. The credit reporting company Equifax disclosed in September 2017 that hackers had stolen the personal information of about 143 million United States consumers by exploiting a website vulnerability. Earlier that year, the WannaCry and NotPetya ransomware used a tool stolen from the NSA to attack hundreds of thousands of vulnerable machines and hold them hostage.

These attacks had in common the exploitation of software vulnerabilities by cybercriminals. According to the CERT Coordination Center (CERT/CC) of Carnegie Mellon University's Software Engineering Institute (SEI), over 90 percent of reported security incidents are the result of exploits against software design or coding defects.[2] Determining the best way to tackle software vulnerabilities is an ongoing challenge. I argue in this policy analysis that a focus on eliminating or reducing software vulnerabilities is a key pillar in the fight against cybercrime, and that engaging the community of independent white hats[3] in this undertaking provides the highest chance of success.

Software vulnerabilities and security

There are a number of key reasons to focus on software vulnerabilities in the fight against cyberattacks.

1. Prices of zero-day vulnerabilities are increasing

   Exploit acquisition firms often buy and sell zero-day vulnerabilities to government intelligence and law enforcement agencies.[4] In September 2016, the U.S.-based exploit acquisition firm Zerodium announced that it would pay

[1] Akin Oyedele, "Warren Buffett Says Cybersecurity Is the Number One Problem with Mankind at Berkshire Hathaway Meeting - Business Insider," *Business Insider*, May 6, 2017, http://www.businessinsider.com/warren-buffett-cybersecurity-berkshire-hathaway-meeting-2017-5/?r=US&IR=T.
[2] N.R. Mead and G. McGraw, "A Portal for Software Security," *IEEE Security and Privacy Magazine* 3, no. 4 (July 2005): 75–79, doi:10.1109/MSP.2005.88.
[3] White hats are hackers who perform security research and tests on information systems to find software defects and vulnerabilities.
[4] A zero-day vulnerability is a software security flaw discovered by someone such as a security researcher, malicious attacker, or general user that neither the software vendor nor the public knows about.

This policy analysis has been written by Lim Wei Chieh and has been funded by the Lee Kuan Yew School of Public Policy (LKY School), National University of Singapore. The case does not reflect the views of the sponsoring organization nor is it intended to suggest correct or incorrect handling of the situation depicted. The case is not intended to serve as a primary source of data and is meant solely for class discussion.

US$1.5 million[5] for an iPhone zero-day vulnerability that would allow a hacker to remotely take control of the device without any required user interaction. This was triple the previous rate of US$500,000. Zerodium would also now offer zero-day prices of US$500,000 for WhatsApp, WeChat, Telegram, Facebook Messenger and other messaging apps. The escalating prices reflect increasing demand for these software vulnerabilities, which can then be on-sold at much higher prices.

2. Ransomware targets vulnerable systems

   Ransomware is a type of malicious software (malware) that blocks access to a computer until the owner pays the attacker a sum of money. Such malware gain access and control of their targets by using zero-day vulnerabilities or exploiting the vulnerabilities of computers with outdated software. The WannaCry and NotPetya ransomware attacks in May and June 2017, which infected hundreds of thousands of computers in more than 150 countries,[6] both made use of the zero-day exploit named EternalBlue, for example.

3. Hacking or malware caused most data breaches between 2013 and 2017

   Data from the Privacy Rights Clearinghouse[7] suggests that data breaches – security events or incidents in which data is stolen from an organisation – caused by hacking or malware increased steadily between 2012 and 2017 (Figure 1).[8] Data breaches can result in the loss of data records such as credit card information, medical records, and other personal information, and indeed over 9 billion records were lost or stolen globally between 2013 and 2017 according to the security company Gemalto's Breach Level Index.[9] Hacking and malware contributed to the majority of stolen data records between 2013 and 2017, being responsible for over four fifths of such thefts each year with the exception of 2016.[10]

---

[5] "Our Exploit Acquisition Program," *ZERODIUM*, accessed September 6, 2017, https://zerodium.com/program.html.
[6] Irene Tham, "Comparing NotPetya and WannaCry and Tips on How to Stay Safe from Ransomware," *The Straits Times*, June 28, 2017, http://www.straitstimes.com/tech/comparing-petya-wannacry-how-to-stay-safe.
[7] The Privacy Rights Clearinghouse is a non-profit organisation involved in educating consumers on and advocating for privacy rights. The organisation has maintained a database of data breaches reported in the U.S. since 2005. The 2017 data goes up to August 30, and the data presented in Table 2 is based on substantiated public disclosures.
[8] "Data Breaches," *Privacy Rights Clearinghouse*, accessed September 6, 2017, https://www.privacyrights.org/data-breaches.
[9] "The Breach Level Index," *Gemalto* (Gemalto), accessed September 6, 2017, http://breachlevelindex.com/.
[10] According to the data breach statistics provided by Privacy Rights Clearinghouse (https://www.privacyrights.org/data-breaches), a single laptop containing five million records was stolen in 2016. This data breach was thus attributed to a physical loss rather than hacking or malware.

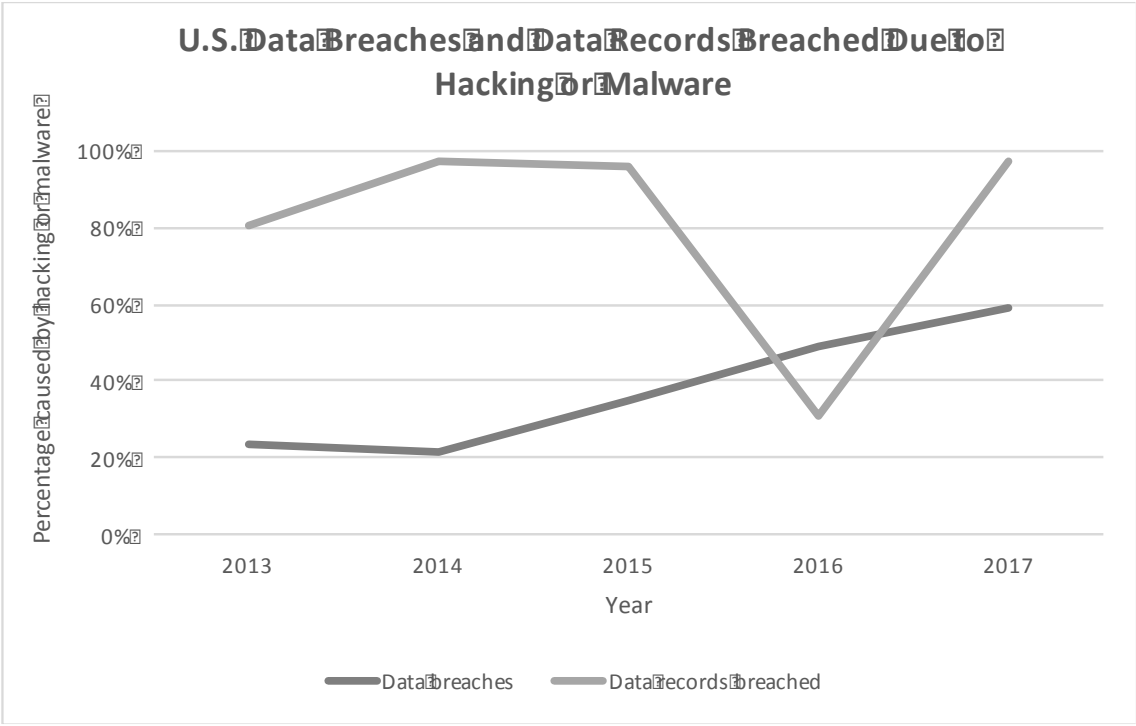
Table 1. Number of data breaches due to hacking or malware

	2013	2014	2015	2016	2017
Hacking or malware	209	184	184	394	215
Others	676	677	347	412	151
Total	**885**	**861**	**531**	**806**	**366**
Percentage of U.S. Data Breaches	**24%**	**21%**	**35%**	**49%**	**59%**

Table 2. Number of data records breached due to hacking or malware

	2013	2014	2015	2016	2017
Hacking or malware	48,805,382	67,092,537	153,091,160	3,427,360	10,092,786
Others	12,135,551	1,878,878	6,926,816	7,601,653	322,000
Total	**60,940,933**	**68,971,415**	**160,017,976**	**11,029,013**	**10,414,786**
Percentage of U.S. Data Breaches	**80%**	**97%**	**96%**	**31%**	**97%**

Figure 1. Data breach due to hacking or malware



It may seem like the obvious solution to vulnerabilities in software code is to ensure that software developers produce secure code. Developers, however, are not hackers. Fundamentally, software developers are trained to “build things”, while hackers “break things”. Software developers cannot necessarily be expected to examine code from a malicious hacker’s point of view and understand how their software might be abused, thus making it difficult for them to develop code that is resilient to cyberattacks. It is

therefore important to focus on detecting vulnerabilities both at the development stage and when the software is already in the live environment.

Hunting down security bugs

Vulnerabilities can be identified using three main approaches:

1. Static Application Security Testing (SAST): This approach identifies vulnerabilities by reviewing the source code of the software using manual methods and/or testing tools, commonly referred to as static code analysers. SAST provides an "inside out" view of the software's security status.
2. Dynamic Application Security Testing (DAST): DAST refers to the use of a vulnerability scanning tool to test the software using a library of known vulnerabilities. This approach provides an "outside in" view of the software's security status.
3. Penetrating Testing: This approach involves the use of manual techniques to expose vulnerabilities by mimicking the tactics, techniques and procedures of cyber threats for hacking software.

Other approaches and tools for identifying vulnerabilities include binary analysis and Interactive Application Security Testing (IAST), among others. Organisations may also choose to adopt a reactive stance for vulnerability detection, either by waiting for a customer to report a security bug or by discovering the vulnerability during or after an actual attack.

Most industry regulations and security standards require or recommend at a minimum the use of Penetration Testing to assess software. Many industry experts consider penetration testing to be the preferred method for vulnerability discovery, as it is more cost effective than SAST and provides a more targeted analysis than DAST.

Approaches to penetration testing

Penetration testing is often performed by security professionals called penetration testers, ethical hackers or white hats (as opposed to black hats, who hack with malicious intent). The U.S. Department of Defence (DoD) first used penetration testing as a means to break a computer system to find security flaws in the late 1960s. Teams of "penetrators" were then called "Tiger Teams".

Computers soon became more widely used in the private sector, and organisations formed their own Tiger Teams. As such, in-house teams have long performed penetration testing for private companies. But as companies started outsourcing their IT operations, outsourcing of penetration testing soon followed. At the time of writing, public and private sector organisations routinely outsource penetration testing work to security service providers.

In 1995, Netscape engineer Jarrett Ridlinghafer created the first bug bounty program. Having observed how a community of Netscape enthusiasts were finding and fixing

bugs in the company's software, Ridlinghafer convinced Netscape executives to fund a program to engage and reward these "bug hunters". Netscape launched the program with the beta release of Netscape Navigator 2.0, which also included the pre-release version of Java.[11] Eric Schmidt, then Chief Technology Officer at Sun, said :[12] "This program, along with Sun's extensive beta testing program, will help us to quickly identify and fix any potential vulnerabilities in Java, ensuring a highly secure solution at the time of release." Users who reported significant security bugs received a cash prize, while those who found other security bugs received Netscape merchandise.

However, this new approach of engaging a community of independent white hats did not catch on in a big way with other software vendors. There may have been a number of reasons for this:

1. Security was still considered a sensitive task best handled in-house or by reputable outsourced companies.
2. The ROI for bug bounty programs was still unproven as there was limited public data available for such activities.
3. Many companies had low confidence in white hats and those with hacking skills who were not formally employed by a service provider.

Bug bounty programs only gained greater acceptance when Google and Facebook launched their programs in 2010 and 2011 respectively. In 2013, a new breed of companies emerged that offered "managed" bug bounty programs on behalf of other companies, which quickly propelled the model into the mainstream. A company using one of these "managed" bug bounty programs would not administer its own bug bounty program. Rather, it would rely on an outsourced service provider who would implement and run the program on its behalf. As of 2017, many major institutions and companies – not just those in the technology sector – have launched some variation of a bug bounty program, including the U.S. government.

The challenges of the pay-for-time penetration testing model

Most industry regulations and security standards recommend that organisations perform penetration testing on an annual basis at a minimum. This may not be sufficient. At the time of writing, organizations are releasing new and updated software at a much higher rate compared to previous decades,[13] leading to software vulnerabilities also being introduced at higher rates. Figure 2 suggests that annual penetration testing could lead to a given software's vulnerabilities being exposed for more than 300 days before being discovered – and software developers would then require some time to fix the vulnerabilities after discovering them before the exposure

[11] "Netscape Announces 'Netscape Bugs Bounty' with Release of Netscape Navigator 2.0 Beta," *Netscape*, October 10, 1995, https://web.archive.org/web/19970501041756/http://www101.netscape.com/newsref/pr/newsrelease48.html.
[12] Ibid.
[13] "What Is Agile Software Development?," *Agile Alliance*, accessed October 11, 2017, https://www.agilealliance.org/agile101/.

would be reduced. With the next software release, vulnerabilities would start to increase again. As such, though penetration testing can change a software's vulnerability curve, the software is still significantly exposed to threat for a long period of time.

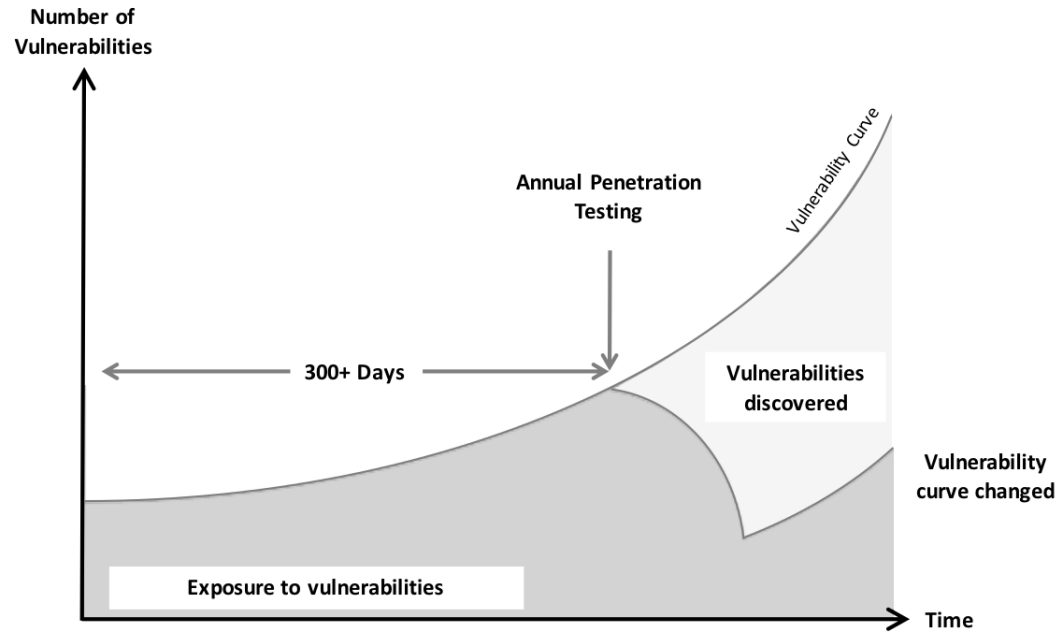


Figure 2. Effect of Annual Penetration Testing (Illustrative)

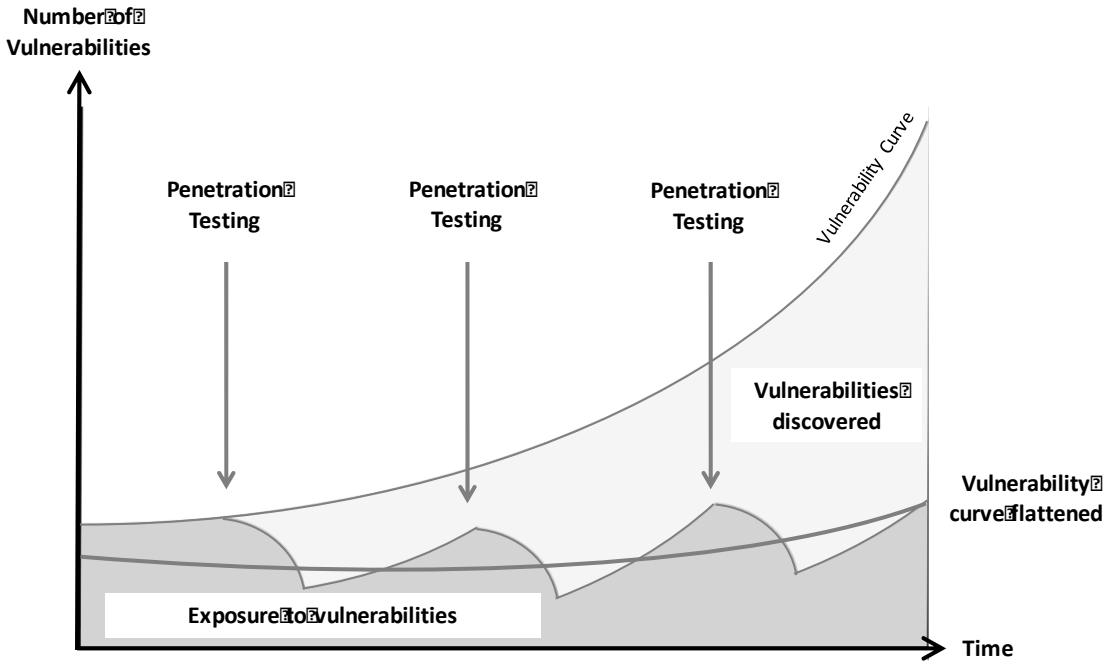


Figure 3. Effect of "Ongoing" Penetration Testing (Illustrative)

Performing penetration testing at a higher frequency can significantly reduce a software's exposure to threat (Figure 3), and approaching penetration testing on a "continuous" basis can help flatten the vulnerability curve. But the cost of a higher-frequency approach can often be prohibitive for an organisation, and can even exceed that of a data breach. Many organisations calculate the cost of penetration testing based on how much time the penetration tester needs to perform the work. To perform penetration testing multiple times a year, the organisation would have to pay multiples of a single annual test's cost.

Besides the cost, there are several other key issues for a 'pay-for-time' penetration testing model:

1. Spend not necessarily correlated to returns

   Due to the nature of such work, service providers are unable to guarantee that they will find any or all vulnerabilities. One cannot find something that is not there, and if a vulnerability does exist, the penetration testers assigned to the job may either lack the capability to find it or be unable to do so within the timeframe of the testing period. And even if vulnerabilities are found, they may not be the critical ones that attackers choose to exploit. The only guaranteed return for an organisation is the "assurance" that the organisation has a process in place for vulnerability detection.

2. Challenging vendor selection

   The "traditional" approach to outsourced penetration testing relies on an organisation selecting the right vendor for their penetration testing needs. This can be a challenge when many vendors have similar testing methodologies, well-credentialed consultants, and previous experience with high-profile clients. It is difficult to differentiate one from the other and to prove authentic expertise. In certain cases where the testing is not performed onsite, the organisation cannot even be sure which individuals are performing the actual work.

3. Motivation issues

   Penetration testers assigned to the job are not necessarily incentivized or motivated to go above and beyond what is minimally required in their work. They do not get paid more for discovering more vulnerabilities. Meanwhile, hackers take home a "pay cheque" only if they find and exploit vulnerabilities for financial gain. This misalignment in motivation tilts the scales in favour of the attackers rather than the defenders.

The sometimes lacklustre results of penetration testing have led some organisations and professionals to adopt a checkbox compliance attitude. This attitude encourages approaching established vendors, selecting the ones who offer the lowest prices, and paying them the bare minimum to perform penetration testing – thus ticking the

compliance checkbox. If an incident occurs due to an exploited vulnerability, the organisation can then blame the service provider, which can then point to its disclaimer asserting that the service provider offers no guarantees. The situation is not helped by some cybersecurity vendors and even government officials taking a "Not if, but when" and "resistance is futile" attitude towards cyberattacks. Thus, such organisations may limit continued investment in better preventive measures to find and fix vulnerabilities since the bad guys will get in eventually.

Engaging the white hat community

The bug bounty model may be a viable alternative to the "pay-for-time" approach to penetration testing in the current digital landscape. Bug bounties encourage communities of independent white hats to uncover software vulnerabilities. If a reported vulnerability is valid, the white hat is compensated for the discovery. Only the first person to find the vulnerability is rewarded – there are no prizes for second place.

This model performs well for a number of reasons.

1. Pay for results, not for time

   In the "pay-for-results" model, the organisation pays for each validated vulnerability instead of paying for time spent looking for a vulnerability. The organisation thus gets better value for their money.

   This approach also makes vendor selection less consequential because the organisation only pays for the validated results that they receive. If the community finds nothing, the organisation pays nothing apart from the cost of administering the program.

2. Diversity of expertise

   In the "pay-for-time" model, only a limited number of penetration testers – typically between one and three – perform the penetration test. The results are thus dependent on the knowledge, expertise, experience and motivation of the penetration tester(s) performing the work. Engaging the white hat community, on the other hand, provides an organisation with the expertise of a group of white hats who can operate independently from each other, in geographically diverse regions, with their own local influences and perspectives.

3. Built-in motivation

   Only the first person who finds and reports a vulnerability receives a reward – no one is paid for "effort". As such, there is a strong incentive for white hats to work quickly and deliver results.

Addressing the challenges of the bug bounty model

The bug bounty model is not without its challenges. A successful bug bounty program requires the following:

1. Resources to manage the program

   Administering a bug bounty program has costs, mostly due to the human resources needed to manage the vulnerability submission and resolution process. Depending on the scale and success of the program, white hats may be submitting hundreds of reports to the organisation every month. A well-managed program requires a team to both ensure a smooth and efficient submission and resolution process and to interpret and understand the problems being submitted.

2. An understanding of the community

   An organisation that hopes to meaningfully engage the white hat community and ensure the success of their bug bounty program has to understand and work with the white hat working culture. Good practices in this regard include ensuring clarity and specificity in the terms and scope of the program as well as being responsive in communications with the community. If an organisation is slow to respond, there is a risk of a white hat disclosing a vulnerability to the public.

3. Sufficient budget for the program

   The bug bounty model requires work to be delivered before the white hats are compensated. Organisations must always ensure they have enough in their budgets to pay for a given vulnerability.

Though the bug bounty model is over 20 years old, and has now been adopted in various forms by Fortune 500 firms and government agencies, many organisations still do not fully trust the white hat community. Common concerns include:

1. If they are so good, why aren't they employed by a service provider?

   Some white hats have full-time jobs and are participating in bug bounty programs merely out of interest. Others may not want to work for service providers or large enterprises. A study conducted by BugCrowd[14] found that only 15% of white hats participating in bug bounty programs are full-time "bug hunters".

2. If the black market offers a higher price, won't the white hats find a vulnerability and sell it to the highest bidder?

[14] "2017 State of Bug Bounty Report" (BugCrowd, 2017), https://pages.bugcrowd.com/hubfs/Bugcrowd-2017-State-of-Bug-Bounty-Report.pdf.

Even without a bug bounty program, black hats or white hats gone rogue are already finding and selling zero-day vulnerabilities. Having a bug bounty program has no effect on the zero-day market. Also, a zero-day vulnerability commands a price only if the buyer believes that there is an extremely low possibility that the vulnerability will be discovered by the software owner or other white hats. Once discovered, the value of the zero-day vulnerability drops to zero. A bug bounty program increases the likelihood that vulnerabilities will be found, and hence reduces the vulnerability market size.

3. Won't an organization's bug bounty program put the organisation on the radar of malicious hackers?

   An organisation with assets of value will be targeted by malicious hackers with or without a bug bounty program. There is no basis for assuming that having a bug bounty program increases an organisation's attractiveness to attackers.

It is worth noting that bounty programs need not necessarily be a "free-for-all" in which anyone can participate. Many of the challenges that might accompany such programs could be addressed by designing a program that suits an organisation's needs and risk appetite. There are several ways that organisations could customise their programmes.

1. Public vs. private: Programs need not necessarily be advertised to the public, and organisations could offer private programs that limit the number of participants. Both approaches offer their own advantages and disadvantages. For example, a public program could provide a diverse range of expertise while a private program could ensure that only vetted white hats with specific skillsets participate.

2. Broad vs. narrow: An organisation could define its program's scope broadly, making any of its assets fair game, or narrowly, including only certain critical assets. A broad scope might offer better coverage, but could require a higher budget. A narrow scope could help the organisation get a better return on spend by focusing on what's important.

3. Curated crowd: Organisations or managed "bug bounty" service providers could validate the capabilities of participants and perform background screening through third party background check companies. This could help allay the concern that white hats may not have the desired capabilities for the job.

4. Monitored traffic: Organisations or managed "bug bounty" service providers could require participants to perform testing through specific systems which could then capture and monitor the test traffic for anomalies. If potentially harmful activities are detected, the organisation could then respond in an appropriate manner to defuse the risk. This also would offer better control for the organisation as only network traffic originating from a defined source would be considered "bug bounty" traffic, and anything else would be open for investigations.

Bug bounty adoption

BugCrowd, a service provider that manages more than 600 bug bounty programs, noted in its 2017 annual report[15] that the number of bug bounty programs has tripled since 2016. 16% of programs are run by companies with more than 5,000 employees, and 11% of programs are adopted by the highly regulated financial services and banking sector. Several examples suggest that the programs are effective.

1. Facebook: In a post shared in October 2016, Facebook reported[16] that US$5M had been awarded to more than 900 security researchers since July 2011. White hats reported over 500 valid vulnerabilities[17] in 2015, and submitted 9,000 reports for validation in the first half of 2016.

2. Google: In a January 2017 blog post, the company reported[18] that US$9M had been paid out to more than 350 white hats for more than 1,000 discovered security vulnerabilities since 2010.

3. LinkedIn: In a presentation[19] at Blackhat USA 2015, Linkedin shared that 27% of critical security bugs handled in 2014 were discovered externally rather than by the internal team.

Though the technology sector still accounts for the most adopters of bug bounty programs, the last few years have seen non-technology companies from a variety of industries jumping on the bug bounty bandwagon.

- Technology: Apple, Samsung, Google, Facebook, LinkedIn, Twitter, Microsoft, Amazon, SAP
- Finance: Mastercard, Western Union, ING, Paypal
- Transport: United Airlines, General Motors, Fiat Chrysler, Tesla, Uber
- Retail: Starbucks, Walmart, Bosch
- Education: Massachusetts Institute of Technology (MIT), Pennsylvania State University (PSU)
- Government: U.S. Department of Defense

It should be noted that the common use case for the bug bounty model is to provide an additional layer of cyber defence rather than a replacement for all security testing programs. Cybersecurity is only effective with layered defence.

---

[15] Ibid.
[16] "Facebook Bug Bounty: $5 Million Paid in 5 Years," *Facebook*, October 12, 2016, https://www.facebook.com/notes/facebook-bug-bounty/facebook-bug-bounty-5-million-paid-in-5-years/1419385021409053/.
[17] "2015 Highlights: Less Low-Hanging Fruit," *Facebook*, February 9, 2016, https://www.facebook.com/notes/facebook-bug-bounty/2015-highlights-less-low-hanging-fruit/1225168744164016/.
[18] "Vulnerability Rewards Program: 2016 Year in Review," *Google Online Security Blog*, January 30, 2017, https://security.googleblog.com/2017/01/vulnerability-rewards-program-2016-year.html.
[19] Cory Scott and David Cintz, "The Tactical Application Security Program: Getting Stuff Done," in *Blackhat USA 2015*, 2015, https://www.blackhat.com/docs/us-15/materials/us-15-Scott-The-Tactical-Application-Security-Program-Getting-Stuff-Done.pdf.

U.S. Department of Defense leads the way

In 2016, the United States Department of Defense (DoD) gave the bug bounty model a try with a pilot program: "Hack the Pentagon". For 25 days in April and May 2016, the U.S. DoD ran a bug bounty program[20] in which 1,410 white hats hacked five public-facing websites. By the end of the program, the white hats had discovered 138 vulnerabilities and had received US$150,000. The first vulnerability report was submitted just 13 minutes after the opening bell.[21]

Then U.S. Defense Secretary, Ash Carter said:[22] "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."

The program showed how the bug bounty model could work for a government agency. Some of the key parameters put in place included the following[23]:

1. Restricted eligibility: "Participants must be U.S. citizens and must not be on the U.S. Treasury Department's Specially Designated Nationals list of people and organisations engaged in terrorism, drug trafficking and other crimes. U.S. citizens and companies are prohibited from doing business with listed entities."[24]

2. Background checks: "Successful participants who submit qualifying vulnerability reports will undergo a basic criminal background screening."[25]

3. Defined budget: US$150,000 in funding was allocated for the program.

The U.S. DoD then launched a Vulnerability Disclosure Policy that allowed anyone to report vulnerabilities on any public-facing website owned, operated, or controlled by the U.S. DoD. Security researchers following the guidelines would not be subjected to law enforcement or civil action.

At the end of 2016, the U.S. DoD ran its 'Hack the Army' program. [26] This time, white hats found 118 valid vulnerabilities. Most significantly, a white hat who found a vulnerability on the DoD's public-facing recruitment website also found his way into

---

[20] Lisa Ferdinando, "Carter Announces 'Hack the Pentagon' Program Results," *U.S. Department of Defense*, June 17, 2016, https://www.defense.gov/News/Article/Article/802828/carter-announces-hack-the-pentagon-program-results/.
[21] "'Hack the Pentagon' Fact Sheet," June 17, 2016, https://www.defense.gov/Portals/1/Documents/Fact_Sheet_Hack_the_Pentagon.pdf.
[22] Ibid.
[23] "'Hack the Pentagon' Pilot Program Opens for Registration," *U.S Department of Defense*, March 31, 2016, https://www.defense.gov/News/Article/Article/710033/hack-the-pentagon-pilot-program-opens-for-registration/.
[24] Ibid.
[25] Ibid.
[26] "Hack The Army Results Are In," *HackerOne*, January 19, 2017, https://www.hackerone.com/blog/Hack-The-Army-Results-Are-In.

the internal DoD network.[27] This was followed by the 'Hack the Air Force' program in June 2017, which unearthed 207 vulnerabilities. At the time of writing, the U.S. DoD was not the only one embarking on bug bounty programs: the General Services Administration announced its program in May 2017,[28] and the Hack Department of Homeland Security (DHS) Act was introduced to the Senate in the same month.[29]

Roadmap for the Singapore government

At the time of writing, Singapore's private and public sectors have yet to engage the independent white hat community in a meaningful way. The U.S. approach offers a roadmap for the Singapore government to adopt the bug bounty model and engage the white hat community.

1. Start with a pilot program

   A pilot program similar to the U.S. DoD's "Hack the Pentagon" program would allow the Singapore government to test the white hat model and program parameters on less sensitive assets. In the program's early stages, the program could limit participation to citizens and permanent residents to reduce the risk of hostile state-sponsored attackers. The number of participants may be limited by the resources available within Singapore, however.

2. Implement a broader plan

   The lessons learned from the pilot program could be used to further adjust the model and program parameters to expand the program across government agencies. The program could be tiered with different requirements and restrictions based on the nature of the agencies.

3. Build greater capacity

   To increase its white hat resources, Singapore could explore international cooperation with ASEAN nations. One of the pillars of Singapore's Cybersecurity Strategy[30] is to strengthen international partnerships and collaboration, including cyber capacity building initiatives. A cooperative model within the ASEAN nations could enable the sharing of white hat resources across the region.

---

[27] Kate Conger, "Hacking the Army," *TechCrunch*, January 19, 2017, https://techcrunch.com/2017/01/19/hacking-the-army/.
[28] Omid Ghaffari-Tabrizi, Waldo Jaquith, and Eric Mill, "The next Step towards a Bug Bounty Program for the Technology Transformation Service," *18F*, May 11, 2017, https://18f.gsa.gov/2017/05/11/the-next-steps-towards-bug-bounty-program-for-technology-transformation-service/.
[29] Selena Larson, "Senators Introduce a Bill to Hack the Department of Homeland Security," *CNN*, May 26, 2017, http://money.cnn.com/2017/05/26/technology/hack-the-dhs-act-bug-bounty/index.html.
[30] *Singapore's Cybersecurity Strategy* (Cyber Security Agency of Singapore, 2016), https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf?la=en.

At the time of writing, the Singapore government has opted for stronger regulations and requirements for accreditations and certifications for penetration testing service providers and professionals. In July 2017, the Ministry of Communications and Information (MCI) and the Cyber Security Agency of Singapore (CSA) released the Cybersecurity Bill for public consultation. The proposed bill included a licensing framework for the regulation of cybersecurity service providers and specifically licensing penetration testing services, among other things.

A year earlier, the CSA issued a directive (CSA Directive No. CSA-D02/2016) requiring Critical Information Infrastructure Owners/Operators to "ensure that both professionals and service providers engaged for penetration tests on CIIs possess industry-recognised certifications and accreditations respectively (e.g. CREST or equivalent accreditations & certifications)." According to the CSA, this directive was aimed at ensuring the quality and competency of service providers. To obtain CREST certification, service providers pay a fee of £5,000 – £25,000 and submit an application form with required documentation.

Regulating the cybersecurity industry through licensing, accreditation and certification may provide greater control on service quality based on accepted standards and benchmarks. This approach may not be effective if almost everyone can qualify under the "lighter-touch framework", however, and may also shut out significant expertise in penetration testing. Many white hats do not believe in certifications and are unwilling to pay for paper qualifications pertaining to the industry.

Conclusion

There has been much discussion on the shortage of cybersecurity professionals in the market. In his opening speech at the inaugural Singapore International Cyber Week, Prime Minister Lee Hsien Loong expressed his concern that "we face a severe shortage of talent and skilled expertise, as do many countries."[31] In a 2016 speech, Dr. Yaacob Ibrahim, Minister for Communications and Information, said that "there may be as many as 30,000 new jobs to be filled" for the infocomm workforce by 2020.[32]

Organisations have an opportunity to tap into the "cognitive surplus"[33] of the cybersecurity crowd by sourcing for expertise in the white hat community. Today, the white hat community is securing many of the technology products and services we use as individuals and in business. Singapore's public sector should take the lead and conduct an extensive study of the white hat model to address the cybersecurity problems presented by growing software vulnerabilities.

---

[31] "Prime Minister Lee Hsien Loong Delivered This Speech at the Inaugural Singapore International Cyber Week.," n.d., http://www.pmo.gov.sg/newsroom/pm-lee-hsien-loong-singapore-international-cyber-week-opening-ceremony.

[32] "Speech by Dr Yaacob Ibrahim, Minister for Communications and Information, at the Singapore Computer Society Gala Dinner and IT Leader Awards 2016 on 4 March 2016, 8.15PM at Shangri-La Hotel," in *Singapore Computer Society Gala Dinner and IT Leader Awards 2016* (Ministry of Communications and Information, 2016), http://www.nas.gov.sg/archivesonline/data/pdfdoc/20160304002/Speech by Min(CI) Dr Yaacob Ibrahim at SCS Gala Dinner and IT Leader Awards (4 Mar 2016)_Final.pdf.

[33] Clay. Shirky, *Cognitive Surplus : Creativity and Generosity in a Connected Age* (Penguin Press, 2010).

Chris Lynch, who heads the U.S. DoD's Digital Defense Service, puts it best when he said. "We cannot hire every amazing hacker and have them come work for us, but we can do these crowdsourced bug bounties. I'm done with being afraid to know what our vulnerabilities are. That's not okay." [34]

[34] Conger, "Hacking the Army."