Bug Bounties; Working Towards a Fairer and Safer Marketplace

Bug Bounties: Key Statistics

(Data taken from the BugCrowd 2017 State of Bug Bounty Report)

Total pay out to BugCrowd community: **$6,392,992** (up **211%** since 2016)

Average pay out on Critical (P1) vulnerabilities: **$1,776**

Industry with the top average pay-outs is auto at **$1,514** and the lowest is Retail/ E-commerce at **$403**

Highest average pay-outs are on hardware/ IoT targets such as routers, webcams, and wearables at **$742**

Lowest average pay-outs are mobile applications at **$385**. However, some programmes offer only t-shirts or achievement points.

As of March 2017, the community had nearly doubled year over year (**53,332**, up from **26,782** in 2016)

As of March 2017, the total number of valid vulnerabilities is an industry-leading **52,045**

The top 5 industries in terms of adoption are: Computer Software, Internet, Information Technology and Services, Financial Services and Banking, and Computer and Network Security

Bug Bounties; Working Towards a Fairer and Safer Marketplace

In the field of cybersecurity, independent researchers often find flaws in software that can be abused to cause harm. These flaws are known as vulnerabilities. Once these vulnerabilities have been detected, the researcher has a decision to make about how, when and where to disclose the vulnerability. The lack of formality in this process has led to some significant problems regarding the legality of 'researching' a product or service without permission and what ethical or responsible disclosure really means. The concept of crowdsourcing the search for vulnerabilities is attractive to some organisations, however, which has led to the development of in-house or externally managed bug bounty programmes.

A bug bounty programme is something that an increasing amount of websites and software developers offer: giving recognition and compensation to researchers for reporting bugs, exploits and vulnerabilities.

The area of responsible reporting is far from resolved, yet despite the challenges that remain, bug bounty programmes are being launched at a remarkable pace, facing many of the same ethical reporting challenges. There is evidence of both good and bad practice in the bug bounty marketplace and the intention of this research paper, commissioned by CREST, is to explore both further.

CREST is a not-for-profit accreditation and certification body that represents and supports the technical information security market.

In September 2017, representatives from CREST member companies and industry assembled at a workshop to discuss how to better understand bug bounty programmes, consider how such programmes sit in wider technical assurance frameworks, provide advice to the buyers of such services, protect the interests of those participating in programmes and finally, where appropriate, improve the bug bounty landscape. Attendees included researchers, penetration testers, CISOs, representatives from bug bounty platforms and end users from organisations who have launched, or are intending to launch, a bug bounty programme.

Ahead of the workshop, attendees and other relevant people were interviewed by Eleanor Dallaway, author of this report. The workshop was held under Chatham House rules so whilst this report includes many direct quotes, they are not attributed to participants or interviewees by name. There are many terms used to describe bug bounty hunters, including hackers, researchers and hunters. For the purpose of this report, we shall refer to them as researchers unless directly quoting a source that uses a different term.

Humble Beginnings

The first bug bounty programme was launched in 1995 by Netscape and ever since, bug bounty programmes have become increasingly popular, with most technology giants now running their own programmes.

Given the cybersecurity landscape, with attacks more frequent and more complex, many organisations are adopting a crowdsourcing model for their cybersecurity, turning to 'the crowd' for support, including the hacker community they traditionally distrusted.

Today, organisations of all sizes run bug bounty programmes, with reward size for uniquely identified vulnerabilities increasing with the popularity and legitimacy of bug bounties.

An organisation may choose to run its own programme in-house or it may choose to outsource the task to a third-party bug bounty platform. However, rules published publicly around security research can carry significant legal weight in the rare instance of inappropriate behaviour by a bug bounty researcher.

> ***"It's in the bug bounty company's interest to make its community look bigger than it actually is"***

Outsourcing a bug bounty programme to a specialist platform has become an increasingly popular and useful tool for organisations. Even some of the large technology leaders are now working with third-party programmes. Google, for example, recently announced its partnership with HackerOne to launch a programme that pays out bonus rewards to researchers who report vulnerabilities on eligible apps on Google Play. However, this is just a supplemented part of Google's bug bounty programme. The rest of its bug bounty programme – like many other major corporations – is handled in-house.

"Running bug bounties without outside service providers is the norm for major corporations like Microsoft, Apple, and Google for most of its bug bounties. The reason is simple: nobody at that scale, with complex bugs to triage, can rely on the security of a third party cloud provider whose bug triage staff likely lack the technical knowledge of the software at hand to really be of any use to those companies", explained one of the world's most renowned bug bounty experts. "This isn't your grandpa's web vulnerability bug bounty programme. These programmes are for bugs that command six figures or more, and only a tiny set of the population can find these types of bugs, let alone assess their severity properly".

In contrast, one expert said that the majority of bug bounty programs outsource initial triage, even independently run ones.

Outsourcing a Bug Bounty Programme

Bug bounty platforms offer anything from a fairly simple listing and facilitation of an introduction between hunter and organisation, to a full managed service, including the triage process.

Some of the bigger bug bounty companies boast large communities of hunters (at the time of writing, HackerOne claims 140,000 and Bugcrowd claims 60,000) but workshop attendees urged that those numbers should be qualified with active users, otherwise it can be misleading. "How can you validate active or non-active members of third party bug bounty services?" asked one workshop attendee. "It's in the bug bounty company's interest to make its community look bigger than it actually is."

HackerOne powers 900 organisations' bug bounty programmes, including the U.S. Department of Defense, Uber, Nintendo and Starbucks. "Third-party bug bounty services allow companies to focus security teams on resolving the bugs that are found by hackers, while the bug bounty vendor provides support of the platform and identifying bugs. Security teams are commonly small and nimble, and third-party platforms provide the extra support they need to price vulnerabilities or manage the triage process", said a spokesperson from one of the leading third-party bug bounty organisations.

Third-party bug bounty platforms received exclusively positive reviews from all researchers interviewed, with many claiming they offer support, ease of use and good insight.

For an organisation choosing to use a third-party bug bounty platform, it can shift some of the liability around who they are paying out to if there are internal concerns around potentially endorsing and unwittingly funding criminality.

The scale of third-party bug bounty sites is evolving fast, with HackerOne aiming to generate $100m in payments to ethical hackers by 2020. To date, 56,000 bugs have been resolved and $21.7m has been paid out in bug bounties through the HackerOne platform.

It can be argued, however, that bug bounty platforms unsurprisingly play up the money that has been paid out through their programmes to encourage take up. Those choosing to participate, however, should dig deeper before committing significant time and manage their expectation of income. "On the surface, the statistics look impressive, but when you drill down into the numbers you see that there are either a lot of researchers participating and earning very little, or a few successful researchers are making a lot."

The cost of setting up and managing an in-house bug bounty programme can be significant and must be factored in. Organisations need to factor that fee into the equation when considering the money necessary to fund a programme. Organisations must also consider the security of the platforms they are looking to outsource to. "Since their bugs are stored there and seen by an unknown number of people at those companies, they are gambling on the relative security of those platforms", said an expert. "Even programmes where the organisation is simply using the platform and not paying for additional bug triage services carry the risk of data warehousing and transport security. For companies with bugs that are complex or take a longer time to fix, this risk is often unacceptable." Even when an organisation outsources its bug bounty programme, they must carefully consider the costs associated with removing the vulnerabilities found within an acceptable time period.

An interviewee used the example of Microsoft and the nation-state level adversaries who have, in the past, compromised its own corporate networks and accessed Microsoft's own internal bug databases. "There is no reason for Microsoft or an organisation like it to trust a third party with that bug data in the cloud. It's a poor risk choice, and one that we should expect to see realised in a bug bounty database breach in the future".

Another interviewee said that the company is accountable to the researcher, at the risk of public disclosure and must accept the consequences of failing to fix the bug.

According to the BugCrowd ***2017 State of Bug Bounty Report***, the number of enterprise bug bounty programmes launched in the past year has tripled. The more exciting and well-incentivised bug bounty programmes that are launched, the more skilled and diverse researchers these programmes attract, the platform states. This is evident in the statistic that in the past year, the size of the bug bounty research community has doubled.

The Motivations of a Hunter

Vulnerability researchers come from many different areas. Some are independent researchers trying to make a living from these programmes and some come from technical security companies who would like to supplement their income and continue to refine their skills. Many come from education wanting to pay for educational fees, raise their profile within the technical security community, hone their skills and improve their prospect of gaining employment within the industry. Some simply like the challenge and use it as a form of gaming.

In order to truly explore the programmes, look for good and bad practice and suggest ways in which bug bounty programmes could be improved, it is important to consider what motivates bounty hunters. Of all the interviews carried out with hunters who either regularly submit bugs to bounty programmes, or have occasionally dabbled with bug bounties, the most popular response to the question about motivation was career development. Hunters explained that the experience and proof of skill that is attained through successful bug hunting is helpful in both launching and progressing a career. Whilst it could be argued that those willing to talk to CREST are by definition interested in entering the industry or furthering their careers, the statement was made so often it was viewed as being consistent.

> ***"Bug bounties are a way for me to do what I love doing legally, and help someone at the same time"***

For the hunter, bug bounty experience helps to sharpen skills and improve knowledge. From the employer's perspective, a candidate with bug bounty experience can prove talent, aptitude and passion. A talent recruiter who attended the workshop commented: "Bug bounty experience is a good indication of ability; but it doesn't necessarily mean it's the right person. It demonstrates interest and talent and if we feel that we could harness those skills in a way that works for us, we would value that experience over entry point qualifications."

Some hunters explained that they hunt for the kudos. Motivated by praise and gratitude, they are satisfied in the knowledge that they are improving the security landscape. Ranking leader board systems are becoming increasingly prevalent on third-party bug bounty platforms whereby hunters achieve points for valid submissions. This is a driver and motivator for hunters. A hunter's public profile, where they can list vulnerabilities they've submitted and the points earned, can be used as an extension of their CV. "Some hunters believe this entitles them to higher salaries in penetration testing roles", said one attendee.

Around half of the interviewees and workshop attendees stated that the financial rewards offered for bounty hunting are "just a bonus". While nobody dismissed it as an incentive entirely, very few listed it as the primary motivation. In fact, of all the researchers in attendance, very few had succeeded financially with any of their efforts. Interestingly, however, there was a strong correlation between the more experienced bounty hunters and financial motivation. The novices were more interested in career advancement and the more experienced hunters were more focused on the monetary pay-out. "The money in bug bounties isn't in pay-outs, it's in the higher paid job that your experience may get you", said one hunter.

One attendee declared their motivation "legal hackery," explaining "bug bounties are a way for me to do what I love doing legally, and help someone at the same time."

Interviewees agreed that bug hunting is almost exclusively an extra-curricular activity and that very few are able to make a career out of it. Most of the world's bugs are found by a very small group of highly-skilled researchers who react very quickly to the launch of a new programme, according to workshop attendees. Bug hunting as a career would also be fairly risky given the lack of guaranteed income and the constant 'race to the finish line'.

It is believed, but not proven, that in the non-Western world many hunters use the funds earned from bug bounty hunting to fund their education. There is an alternative theory that this could be marketing stories to entice more young people to join the programme. Bug bounty payments could indeed support the cost of living in some developing countries suggested one workshop attendee, but they would have to consistently identify new vulnerabilities faster than anyone else.

Interestingly, workshop attendees agreed that bug bounty hunting is an ideal vocation for some individuals with personality traits that makes them struggle with more traditional roles and requirements. Bug bounty programmes give researchers a way of using their skills on their own terms.

Demands of the Hunting Community

When questioned about what bug bounty participants want during the process of submitting bugs to bounty programmes, interviewees' responses were fairly unanimous; they want transparency, recognition, to be kept in the loop and faster fix times. "We rate programmes on their response times and their ability to fix the problem, not on the size of bounty" said one workshop attendee.

Only one or two interviewees mentioned they wanted more money. Most declared they would be happy with acknowledgment, good communication from the company running the programme

and acknowledgment of their work. Hunters like personal contact. "An ignored hunter is likely to turn into a black hat hacker" warned one workshop attendee. This is an important consideration for an organisation considering setting up their own programme.

However, one interviewee pointed out that, "The motivations and incentives of a whitehat hacker participating in bug bounty and a blackhat hacker selling vulnerabilities are completely different."

It was suggested by one of the workshop attendees that any organisation that runs a bug bounty programme – be it independently or via a third party bug bounty platform – should publish a "sort of SLA to the world – a declaration of the time they will take to respond to bug reports and the time it will take to remediate." Whilst response can be controlled, it is difficult to see how a guaranteed remediation time could be implemented. A leading third-party bug bounty company discussed how some

> ***"Even without a bug bounty programme, accepting 'responsible disclosure' builds better relationships with researchers"***

of their customers have fixed severe vulnerabilities in a number of hours, whilst other companies take weeks or months to resolve a vulnerability. "These timeframes are always different and hackers can get frustrated if they are left in the dark after submitting a vulnerability they've invested time in finding. This is why communication and expectation-setting with the hackers and your internal development teams up front is incredibly important".

Furthermore, it was pointed out that companies that do not run bug bounty programmes should still have a process for receipt and handling of security vulnerabilities. "Every organisation should have an email dropbox for bug submissions to stop them going to helpdesks and getting no response" said one hunter. If implemented, such a process must be carefully managed however, to ensure that this does not suggest, encourage or even support the concept of researchers illegally attacking systems to which they have no rights.

"Even without a bug bounty programme, accepting 'responsible disclosure' builds better relationships with researchers" another participant said. There was very limited contact with the legal profession, but it is clear that further work to clarify the legal position and any implied acceptance of unauthorised 'research' into their systems is required.

In the US, where the majority of bug bounty programs are operated, there is guidance from the US Dept. of Justice around security research based on anti-hacking laws (CFAA). Further, the US Federal Trade Commission has guidance strongly advising the use of bug bounty programs and takes the presence of one of these programs into consideration when investigating notable breaches.

Workshop attendees pulled together a list of things that any organisation could do in order to improve its handling of vulnerability submissions. These included:

- **Taking legal advice**
- **Setting up an email address that will accept bug reports**
- **Formalising a triage process**
- **Acknowledgment of any reports submitted**
- **Better reporting and improved transparency**
- **Ensure thorough compliance**
- **Offering rewards - or at the least, acknowledgments - for duplicates**

The issue of transparency was raised many times. Hunters get frustrated by a lack of transparency in the bug submission process. For example, many cite the example of bug submission cases being closed due to being a duplicate. This can cause issues for two reasons. Firstly, when organisations don't publish information about bugs that have been submitted and fixed, there is no proof of duplicates, and researchers worry that companies can claim duplicate in order to avoid paying the bounty. Secondly, when companies aren't transparent about the bugs that have been submitted and/or fixed, hunters can spend a huge amount of time working to report a bug that has already been reported, thus wasting their time.

Bug Bounty Benefits for Organisations

Workshop attendees and interviewees were generally extremely positive about bug bounty programmes, which one described as an "always-on way to continuously test live software."

One interviewee said: "If you're not running a bug bounty programme, you're only stopping the good guys, not the bad guys. You're missing out by restricting the white hats."

The advantages of bug bounty programmes are plentiful. Quite simply, a bug bounty programme opens the doors to a much wider pool of talent without restriction. In other words, it's hacker friendly. "Bug bounty programmes give you the opportunity to widen your talent pool, rotate talent and absorb more brain power", said one CISO. There is no time limit for how long a hunter can spend trying to find a bug, so some argue that this results in a more thorough test of security.

However, it's worth remembering that not all bug bounty programmes will receive the same level of interest from hunters. If an organisation is at the bottom of the list, for whatever reason, it is unlikely to have many eyes looking at the system.

Another perceived benefit of bug bounty programmes is the pay-as-you-go model, which many consider to be a cost-effective way of finding vulnerabilities. Organisations are paying for results, not time spent. There are both advantages and disadvantages associated with this, and greater consideration will be given to the economic model later in this paper.

Running a bug bounty programme also transmits a clear message to the public: that an organisation is serious about security, and that it has a publically stated level of confidence. "Companies that run bug bounty programmes are viewed as the 'good guys' by the hacking community" said one workshop attendee.

Bug Bounty Downsides: For the Researcher

While there are clearly many benefits to bug bounty programmes, there are also many challenges. These can be broken down into those that affect hunters and those that affect the organisations running the programmes.

From the researcher's perspective, most bug bounty programmes today are a race against others to claim bounties for issues that may be discovered by more than one security researcher. "Only the first to enter a bug gets paid the bounty. Many suffer from wasted effort in finding legitimate bugs in the initial rush, only to accept that someone else reported it first and claimed the reward", explained a leading expert in the field.

We previously covered transparency in the hunting community demands section. A big concern for researchers is not getting credit for the work they do. One interviewee suggested that even if a bug submission is closed due to being a duplicate, the researcher should still earn reputation points for their work.

Increasingly, many enterprises – particularly financial institutions – adopt 'invite only' bug bounty programmes, whereby they approve hunters rather than using a more open crowdsourcing approach. They allow only fixed IP addresses registered with them to participate in their programme. This is an unpopular approach with many researchers who consider this to be in conflict with the intended purpose of bug bounties. From a legal perspective, it is not clear how this could realistically be enforced.

"From a bug bounty hunter's perspective, it's often difficult to determine if a programme is truly being run by a third party bug bounty service provider, or merely hosted on one of the bug bounty cloud platforms, but really handled by an organisation's own internal team", said a bug bounty expert. Does it even matter?

> ***Putting prices on vulnerabilities encourages people to be mercenary and focus on money rather than actually improving security***

"Yes, because there is a level of consistency in how bugs are handled: from the time to acknowledge a report, to the bounty award amount they can expect that can factor into how much effort they put into a particular programme." In a study done with MIT and Harvard, due to be published in an MIT Press book, the highest earning bug bounty participants tend to invest a lot of time looking at one bug bounty programme over all others to gain the highest pay outs for the most complex bugs. "They will avoid bug bounty programmes with what they perceive to be delays and unfair pay outs in favour of those in which they have built a solid rapport with the response team receiving the bugs."

Bug Bounty Downsides: For the Organisation

For the organisations that choose to run bug bounty programmes, there are many considerations and challenges. One of the biggest challenges faced is fear of 'the crowd', with many apprehensive about letting outside researchers loose on software.

One concern voiced over and over is legitimising the hacking of your website. "Bug bounty programmes invite people to have a go at your security and offer pay-outs in return. Permitting, and indeed inviting, people to hack your website is a risky game," said one CISO. "There needs to be a recognition that other systems are being made vulnerable, as are third-party suppliers."

"There's no real way for companies to differentiate legitimate people trying to find vulnerabilities and the people that are trying to attack the application," added another participant. "This can cause huge problems for SOCs and knowing when to give permissions."

One interviewee pointed out this problem is not unique to bug bounty and that Bugcrowd and Synack have software solutions to address the problem.

Another frequently voiced concern is the ethics around the hunter receiving the bounty. There is no contractual relationship or protection between the organisation and hunter like there is in penetration testing. "What's to stop a hunter also taking the bug to the black market and receiving a double payment for their finding?" one interviewee asked. It is also plausible that a hacker could try to sell a vulnerability on the black market first, and resort to bug bounty submission if unsuccessful. "Some black hats try to legitimise what they are doing by submitting a few vulnerabilities through a bug bounty programme" warned one attendee.

But one interviewee added, "Just because a bug is eligible for a monetary award from a bug bounty program does not mean the bug automatically would be valuable on the black market."

"Putting prices on vulnerabilities encourages people to be mercenary, and focus on money rather than actually improving security", another interviewee lamented. There is no guarantee that the bug found will not be sold to the highest bidder.

Bug Bounty Legalities

Organisations running bug bounty programmes will likely have ethics challenges around who they are paying bounty money to and how that is justified internally. It's hard to prove that bounty payments aren't being paid to criminals, and some organisations – and some sectors – understandably object to that.

Some of the participants suggested that mandating identity checks would be a positive step in ensuring that the right people are receiving payments and that companies aren't blindly funding organised crime for example. "I have questions about how a company actually puts bug bounty payments through their books. What word do you use to explain what and who you're paying without ID checks? What are the tax implications if you're paying someone with whom you have no contract or even agreement? How do you budget for an open ended activity where you do not know how many payments will be made, how much resolution will cost, whether it is even possible, and you do not know how to turn the programme off if you run out of money or want to change the emphasis?" These were all questions raised by workshop attendees.

In the research for this paper, there was much evidence of many researchers being flippant, and arguably naïve, about the legalities around the difference between hunting on systems without permission and legitimate bug bounty hunting. It was suggested that universities need to actively educate students in relevant disciplines about the legalities of vulnerability disclosure and the challenges and dangers of participating in bug bounty programmes.

Generally speaking, there is also a lack of awareness that if a researcher is partaking in a legitimate bug bounty programme with the use of explicitly illegal tools – a ransomware toolkit downloaded to run against the system, for example – that is still illegal usage and would be viewed as unacceptable in many parts of the world. Clarification from law enforcement and support to the hunting community in terms of legal and illegal activity is clearly required.

Law enforcement is concerned that bug bounty programmes could encourage the use of illegal software. The purchase of illegal software in order to participate in a bug bounty programme is also, therefore, potentially aiding the funding and thus the ecosystem of illegal software.

There is also concern from law enforcement agencies that cyber-criminals could use bug bounty programmes as a way to identify talent and groom vulnerable young people. Cyber-criminals search for new impressionable talent to groom and turn to the life of cybercrime. With a great deal of bug bounty participants thought to be teenagers or certainly at the very beginning of their careers, this community are thought to be impressionable with a potentially vulnerable or flexible moral compass.

In the same way that cyber-criminals could use programmes to identify and groom the vulnerable, law enforcement could utilise bug bounty hunting as a way of identifying vulnerable individuals with talent and provide a positive intervention. "Intervention programmes don't currently work with bug bounty programmes, but we should find a way to collaborate", said an attendee. "Before we are able to do that though, we need confidence in the programmes."

Requirements for Running an Internal Bug Bounty Programme

Running a bug bounty programme requires a lot more work than many realise. Organisations can quickly become overwhelmed by running their own programme. Defining scope and disclosure inputs, identifying programme security owners, establishing a vulnerability management programme and even determining time-to-fix agreements within that programme require a great deal of time and resource. In addition to these considerations, organisations must address how to establish attractive pay-out ranges, how to set up an efficient triage and validation process, and ultimately attract a solid crowd of researchers to actively participate. Consideration must also be given to how to close down a programme.

"Even if an organisation has help with triage and setting bounty amounts, they are still responsible for fixing the bugs that are valid, and if they haven't done enough of their own bug hunting and fixing first, this will be a painful process", explained one expert.

It is also important that an organisation carefully considers how the programme will fit into the wider cybersecurity assurance programme and when it is introduced.

To ensure an organisation is ready and equipped to launch a bug bounty programme, many first begin with more traditional penetration testing programmes or limited private bug bounty programmes (inviting select researchers to participate) to train their security teams and solidify a vulnerability response process before evolving to an open, public programme.

There are several areas of maturity, not just in engineering, that must be tackled to run a bug bounty successfully. Some companies offer an assessment of the capabilities in vulnerability

coordination readiness based on the ISO standards 29147 and 30111 for vulnerability disclosure and vulnerability handling processes. It is possible to run a bug bounty without this step, "but organisations tend to run into operational surprises that are unpleasant and inefficient to address after a programme is already launched, and they tend to overpay over time for bugs that could have been found more efficiently through other lower-risk means."

A badly run programme will cause significant problems over a long period of time so it is essential to ensure that an organisation has the maturity and ability to comprehensively handle a bug bounty programme. In order to commit to a programme, an organisation must have the internal resource and budget to do so. It needs to have the staff and skills to be able to support the triage process and enough money to pay out when appropriate.

The more programmes an organisation runs, the more bugs that will be found, and any organisation needs to be prepared for that in terms of triage, fixes and financial rewards. Not all submissions are legitimate vulnerabilities however, and an organisation needs to be prepared for many false positives. No organisation wants to be left with unresolved vulnerabilities in the public domain.

Duplicate findings are a significant concern to researchers so the organisation must think very carefully about how they are going to be transparent to the researcher community whilst not publicising their vulnerabilities to a much wider audience.

"There are some questionable findings in penetration-testing exercises. There are many more questionable findings in bug bounty programmes" said one attendee. Furthermore, bounty prices for high-impact vulnerabilities are higher so researchers have a tendency to mark bugs as 'high-impact' too liberally, thus demanding immediate attention and misplacing resource.

One interviewee raised the topic of capping liability. "How do you cap your liability with a bug bounty programme? If you can't, how can a CISO get sign-off from the board without knowing a finite cost of the programme? Further, an organisation needs to consider that cancelling a bug bounty programme may be very difficult without annoying hunters who may have already invested a significant amount of time in the programme."

Another attendee added: "Can you ever officially close a bug bounty programme? Once you start, you need to be prepared and committed to making it continue. Once you have opened your environment to the crowd, what type of legal recourse will you have if hunters continue to attack the environment? You can cap the money, but that won't work because hunters will just go to the black market instead." This is explored further in the next section.

The Price of a Bug

What became very apparent in the research is that there is no 'normal' when it comes to the pricing of bugs. After all, many of the interviewees pointed out, a vulnerability is worth whatever someone is willing to pay for it. However, BugCrowd have aggregated data on the average price of a bug (Please see infographic on page 2). In theory, bugs can be worth anything from a t-shirt to $500,000 (An Exodus offering for an iOS bug).

Rarely will a legitimate bug bounty programme offer a greater reward than the black market would, but many argue that this is irrelevant; that hunters either have a moral compass or don't, and that those that do would never consider a black market pay-out, even if it was a greater amount. Whilst this may be the case, it can also be argued that those wishing to illegally attack systems will hide behind bug bounty programmes to legitimatise their activities. Eventually, this latter category of researcher would inevitably find themselves selling to the black market at some point.

One interviewee added, "If someone is inclined to participate in the black market, they will but bug bounty provides a legal avenue for these individuals to leverage their skills in a positive and be financially rewarded."

When questioned about whether bug bounty programmes should offer higher bounties, the majority of interviewees said no. "If bounties are increased, what's to say the black market wouldn't increase in line with it? This would result in a bidding war that wouldn't help anybody" said one interviewee.

One workshop attendee put forward the idea of bug bounty programmes offering education vouchers rather than cash for vulnerabilities. This idea was popular with around half of the bug bounty participants that attended the workshop. This could also deter black hat researchers from participating. It would, however, limit the crowd to those wanting educational vouchers.

> ***"The two are complimentary – neither should dispose of the other. Companies should still run penetration testing and bug bounty programmes should sit on top"***

The Effect of Bug Bounties on the Penetration Testing Industry

During the conversations that took place in the research for this paper, many discussions arouse surrounding the potential impact that bug bounty programmes could have on the penetration testing industry.

There are many similarities between the two disciplines and, many argue, the skills required to succeed at each are fundamentally the same. One attendee described bug bounty programmes as a "crowdsourcing approach to penetration testing." Another workshop attendee however pointed out that having the skills to find vulnerabilities doesn't necessarily prove that the individual also has the skills to suggest and implement corrective action.

There are some concerns that bug bounties could ultimately displace penetration testing, but digging deeper, these concerns are based entirely on perception and are not valid.

An expert points to the security and privacy advantages of penetration testing. "Penetration tests are under NDA and will remain private, and tend to employ higher-skilled bug finders, so that's still a valuable niche that is not going away anytime soon", she said. "Even the bug bounty programmes that purport to offer NDAs and higher-skilled hunters run out of fresh eyes very quickly and cannot serve as a full replacement. If penetration testing is to co-evolve with bug bounties, the companies offering them should offer a lower-cost, web-bug-only, pay-per-bug, hybrid service offering."

"There is a lot of overlap between what bug bounties do and what penetration testing is, but with penetration testing, you get that assurance that a thorough test has taken place", said one participant. "It's a guarantee of time spent and of expertise. Bug bounties will never negate the need for that assurance."

One workshop attendee did voice a concern that if a vulnerability was found through a bug bounty process after a penetration test was carried out and the penetration test did not detect the bug, that the discovery could be used against the penetration testing company. The argument could then be made that the penetration test carried out was insufficient given that it did not detect or remediate a vulnerability that was later detected through a bug bounty programme. The counter argument is that there is limited scope with a fixed amount of time available.

As previously mentioned, very few people make a career out of bug bounties and it was also suggested that this is no different to multiple pen test companies competing head-to-head, testing the same product. The lack of guaranteed income is too much of a risk for most researchers and penetration testers. Even for those participating from outside of the industry, the hourly rate is seen as being extremely low, if any income is to be derived at all.

Consequently, a portion of the bug bounty crowd is made up of a lot of young adults and researchers who have penetration testing day jobs and partake in bounty programmes as an extracurricular activity to hone skills and earn additional income.

Whilst there are benefits to the penetration tester's employer if they partake in these programmes as extra-curriculum - primarily that the researcher is honing their talents in their own time – there are also concerns.

Researchers are often not open with their employer about their participation in bug bounty programmes and employers are worried that their staff are hunting for bugs during work hours. There is also concern about researchers using their company's machines and toolsets and thus breaching intellectual property protection. Those unique toolsets are linked to the penetration company's name and thus its reputation, and any wrongdoing by a researcher could thus be traced back to their employer. For example, using a shrink-wrap product under the licensing agreement of their company to carry out independent bug bounty work is breaching the licensing agreement of the company. Although it was pointed out that software licensing issues are not unique to bug bounty.

There is also the issue of penetration testers participating in clients' bug bounty programmes under a hidden identity. A penetration tester could deliberately leave a vulnerability unreported in order to go and fraudulently report it through the company's bug bounty programme to make additional income. One well-known penetration company is vigilant about this and "have measures in place to make sure we do everything above board to ensure that our staff can't exploit our clients."

Employers should consider contracts that preclude competitive work where appropriate. Those that endorse or encourage

extracurricular bug bounty programmes could look to change their contracts of employment to include rules or best practice for any extracurricular work. One attendee argued that penetration testers should have to declare any additional bug bounty work they may be participating in, "in the same way that any industry would expect a declaration of potentially conflicting work or assignments." There is also a question as to whether a student at an educational institution should also make the same declaration, particularly if they are using the educational institution's facilities for the work.

Room for Both Disciplines

Third-party bug bounty services unsurprisingly argue that bug bounty programmes are a security measure every company should consider as a component of a larger security strategy. Interviewees and workshop participants agreed that a 'belt and braces' approach is recommended for any organisation that has the money and resource to invest in both penetration testing and bug bounty programmes. "The two are complimentary – neither should dispose of the other. Companies should still run penetration testing and bug bounty programmes should sit on top" advised one CISO. It's essential that we define how penetration testing and bug bounties can sit together in an eco-system including vulnerability assessment tools and services.

> ***"The penetration industry needs to have a view, academia needs to have a view and so does law enforcement"***

The risk that does face penetration testing as a discipline, according to workshop attendees, is if the communication around the two disciplines is not clear enough and consequently decision makers do not understand the advantages of the disciplines. "If the communication isn't right around the difference between the two disciplines and a distinction isn't made…then penetration testing could be at risk. It's important that organisations understand why both are necessary", said one participant.

There is also an argument that suggests bug bounties could actually be a great opportunity for penetration testing companies. "Penetration testing companies could provide a service to manage bug bounty programmes on behalf of a client", suggested one attendee. It transpires that many penetration testing companies are already offering this service. Workshop attendees suggested that vulnerability platforms could be something that CREST companies could look to offer.

It was noted that there is an appetite from some companies that are bug bounty orientated to become a CREST company in order to add credibility. "We either need to find a way to accredit them against best practice once it is defined or much less preferably find a way to say no", it was explained.

The Economic Model

Earlier in this report, the economic model for bug bounties was mentioned. Organisations of all sizes must consider the economic model when taking the decision to launch a bug bounty programme. Naturally, all businesses are looking for value for money. There is a perception that the cost of bug bounties to the buying community is low. On the surface, bug bounty programmes appear to offer great value for money, paying only for value (vulnerabilities) rather than effort (time). In penetration testing, the model is reversed.

However, the economic model is about more than just the cost of the bugs. The cost of setting up, triage, remediation and admin should not be ignored and needs to be factored in to the economic model. Once these costs are broken down, what is the return on investment? When one interviewee was asked whether penetration testing or bug bounty programmes offered better value for money, they answered "It's hard to quantify given the disparity in bounties offered."

Justifying the cost of a bug bounty programme to the Board can also be a challenge, suggested many interviewees. Firstly, it's hard to estimate the total cost as previously discussed. Secondly, unlike with penetration testing, when an organisation procures a service, you cannot dictate a prioritised list of things to do and test, making it harder to justify.

The Question of Regulation, Accreditation, and Self Administration

One of the main objectives of this report is to establish whether any form of control on the bug bounty industry is required. From the research conducted, it seems clear that there is a big difference between well-run third-party bug bounty services and those entering the market who simply do not understand the issues. It is also clear that the increasing size of the market will attract more, and often less mature, business into this area. Good quality bug bounty platforms are looking for ways to differentiate their services in the market.

Buyers are also seeing the potential benefits of bug bounty programmes but cannot easily identify quality service providers. They also do not have any clear guidance on how to set up

> ***"We must not take a domestic-only view. Any regulation that was put into place would need to work with US suppliers and those around the globe. This makes it immensely challenging"***

> ***It's hard to quantify give the disparity in bounties offered***

programmes of their own which can lead them into very difficult waters. A level of maturity is required from the buyers of bug bounty services that, at the moment, is difficult to quantify.

It has also emerged that researchers need some form of protection, in the form of clarity on what is legal and what is not, and in terms of the transparency of those running the programmes. As it stands, it is easy for unethical programmes to run, paying nothing for people's time and skills.

One interviewee did point out that that it's common for bug bounty programs not to offer monetary awards. Offering financial incentives is a competitive advantage but all pay-outs are issued at the discretion of the company.

The question is what this 'control and support' should look like?

State-regulation

There was a great deal of debate on the need for regulation. It was however clear that there were differences in the interpretation of what regulation means. The most formal is primary legislation. In government, a regulation specifically means a piece of delegated legislation drafted by subject matter experts to enforce a statutory instrument. State mandated regulation is government intervention in the private market in an attempt to implement policy and produce outcomes, which might not otherwise occur, ranging from consumer protection to faster growth or technological advancement.

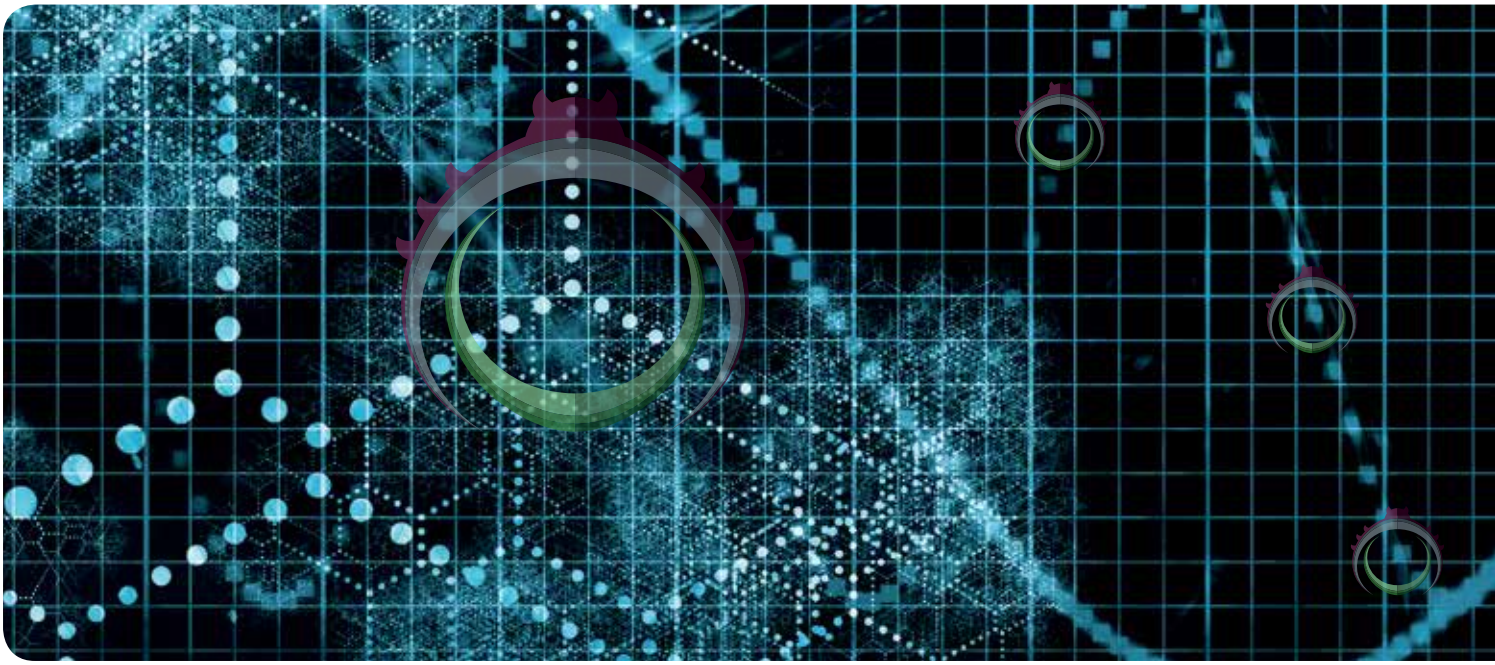
There are currently two bills proposed in the US that, according to one expert, attempt to "galvanise bug bounties for DHS and the Treasury. This is cart-before-horse thinking. They are looking at the success of the DOD Hack the Pentagon bug bounty, and missing the key aspect that there were a couple years of preparation for the response and legal teams that went into that success."

There was a huge amount of hesitancy around the concept of regulation by both interviewees and workshop attendees. "State-driven regulation would completely kill bug bounties", declared one attendee. It is also difficult to see how regulation in this area could keep up with the changes in this fast-moving and dynamic environment when even traditional industries are failing to regulate disruptive approaches to business. Governments and Regulators are, however, going to have to have a view based on informed research on bug bounty programmes as the question about their suitability for use on government systems and regulated environments will undoubtedly be asked.

One of the most cited reasons for objection to regulation was the international stage on which bug bounties take place – bug bounty programmes have no geographical restriction - and the challenges around any regulation being applicable and recognised worldwide.

"No country can take a domestic-only view. Any regulation that was put into place would need to work with US suppliers and those around the globe. This makes it immensely challenging" said a workshop participant.

In penetration testing, the firm carrying out the service understands the laws under which those types of programme operate. Legal protection disappears when programmes are opened up to areas where legislation and laws do not apply. We can't formally regulate something when we don't know where it's coming from.



One interviewee, however, argued that there is a need for regulation in the bug bounty space and had a different view of what that should look like. In their opinion, regulation is all about protecting the researcher. "At a minimum, regulation should make it mandatory for organisations to have a way for hunters to report vulnerabilities they discover. Society is at a disadvantage when ethical hackers are not encouraged to explore technologies freely and creatively." One interviewee suggested that government mandates like this can be pretty dangerous if done incorrectly.

"Often, the fear of prosecution keeps ethical hackers from reporting a vulnerability they have found. By leaving it unreported, malicious cyber-attackers have the opportunity to discover it on their own and exploit the bug for their gain." However, another interviewee questioned whether ethical hackers have been prosecuted.

Whilst the debate regarding ethical disclosure and the legality of 'exploring technologies' is valid, interesting and challenging, it relates more to the disclosure of vulnerabilities found through more general research activities rather than bug bounty programmes.

The industry should closely monitor standards such as the ISO 29147 and any decision on ethical disclosure should be incorporated into the debate on bug bounty.

Self-regulation

Self-regulation is the process whereby an organisation monitors its own adherence to legal, ethical, or safety standards, rather than have an outside, independent agency such as a third-party entity monitor and enforce those standards. Self-regulation of any group can be a conflict of interest, due to the inherent issues in asking any organisation to police itself. In such a fast-evolving industry as cyber security, it is difficult to perceive how self-regulation would provide confidence to the buying community, governments and regulators.

Industry Self-regulation

In business, industry self-regulation occurs through self-regulatory organisations and trade associations that allow industries to set rules with less government involvement. In other areas of the technical security industry that fall under the mandate of CREST, the requirements for membership and the rules to which they must adhere are set by the industry itself and CREST fulfils its mandate through company accreditation and enforceable codes of conduct.

Whilst there was little appetite for formal government regulation, there was general support from both buyers and service suppliers to the concept of industry self-regulation.

In the context of bug bounty this would mean that the company providing the bug bounty platform would have been assessed against 'best practice' by an independent third-party. Industry self-regulation could:

- Provide clear water between the quality service providers and those who have not got appropriate policies, processes and procedures in place to protect their clients (clients could still use the services of unaccredited companies but with less protection)
- Provide access to arbitration services to handle complaints
- Help mature the market
- Allow governments and regulators to direct buyers to a register rather than a specific company
- Provide agility to refine the processes in line with the maturing delivery model
- Make the buyers of such services much more confident in the level of service being provided

This form of industry self-regulation would also provide protection and confidence to the researchers who are participating in the scheme, ensuring that the transparency requested is in place. Accreditation could:

- Allow escalation regarding concerns from researchers should they believe a programme is not being run appropriately or a vulnerability is not being taken seriously by the company
- Provide confidence that controls are in place to manage the risk of rogue researchers

For educational institutes, industry self-regulation could:

- Allow university faculties and students to direct students to 'ethically run' programmes
- Allow the university to reinforce best practice and not encourage potentially illegal activities
- Provide students with confidence that the programmes that they are participating in are ethically run

For law enforcement, industry self-regulation could:

- Support steps to control potential grooming activities
- Allow structured access to positive intervention activities
- Provide the ability to point to a register rather than an individual company
- Offer a potential route for them to access the 'crowd' to help with law enforcement activities

Workshop attendees were keen on the idea of good practice codes that could be self-regulated by the industry. "We need to look at existing best practice and take it further," said one workshop attendee. "There is a lot of good practice coming out of penetration testing already. So, let's analyse this and see whether we can work up a best practice guide that gives the best of both worlds; the structure and control from penetration testing and the freedom and creativity of bug bounties."

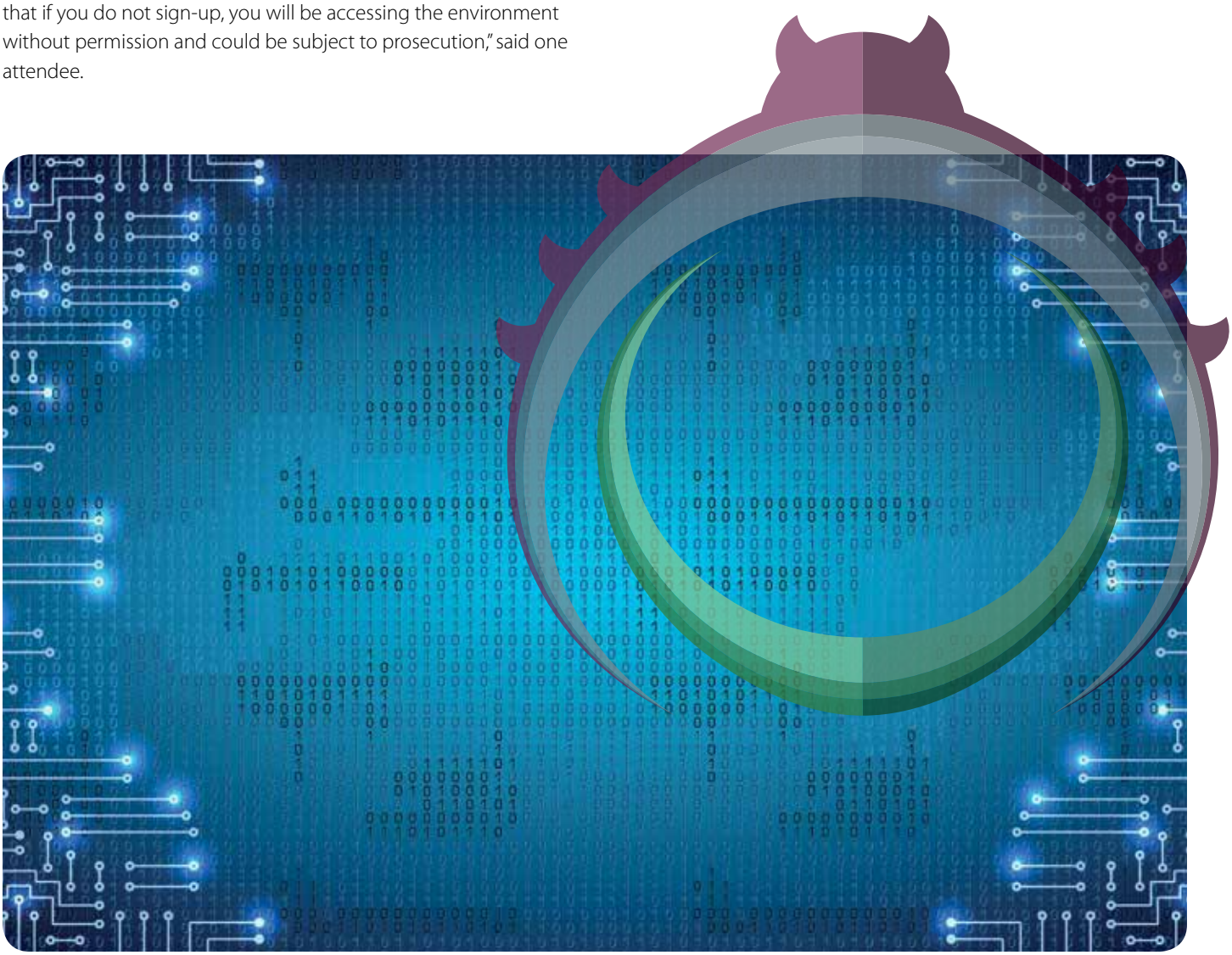
Formal sign-up processes for bug bounty programmes would allow ethics to be re-enforced as part of the sign-up process. In the case of third-party programmes, ethical elements and responsible disclosure guidelines can be written into the contracts.

The workshop group suggested that the formal sign-up process should create a contract with 'the crowd'. "There is nothing to stop those who have not signed up from attacking the environment, however there should be statements on the system that state that if you do not sign-up, you will be accessing the environment without permission and could be subject to prosecution," said one attendee.

In-House Established Programmes

There are still going to be companies that have achieved a level of maturity that would allow them to run their own bug bounty programmes. These would fall into two categories; those who take third-party advice on setting up a programme and those that do all the set up themselves.

Whichever approach is taken, the ability to build a programme against defined 'good practice' would be very helpful. It would provide assurance that the third-party fully understands what is required and advises their clients appropriately. For an in-house designed and developed service, it would allow the internal team to build their programmes in line with industry best practice. If they choose to do so, they could also have their programme independently assessed prior to launch.



Certifying Researchers

The concept of certifying bug bounty researchers at an industry level was raised at the workshop. Participants had mixed opinions on this topic.

One side of the argument is that one of the main benefits of a public bug bounty programme is the volume of diverse eyes on a piece of technology. "By restricting certain researchers, organisations are decreasing the number of watchdogs monitoring their technology for vulnerabilities," argued one supplier, adding that bug bounty hunters can be any age with varying degrees of experience and expertise.

Various bug bounty platforms have selection systems of their own. One maintains a "community of credible hackers" and rewards talent through its reputation programme, which has a publicly visible leader board giving researchers a reputation score dependent on how vulnerability reports are closed. A high reputation score gives a researcher various benefits, including access to exclusive private bug bounty programmes.

Another evaluates researcher performance in four key areas: quality, activity, impact and trust. "In order to be invited to private programmes, researchers must prove both their skills and their trustworthiness via public programmes. They also conduct background-checks and provide ID-verified researchers based on customer needs. This maybe a difficult approach to scale.

One interviewee stated that." "Formal registration for bug bounty researchers would be a mistake, not only because the majority of bug bounty hunters are in various countries around the world, but also because a huge proportion of them are minors."

Whilst the certification of all researchers would be difficult, looking for certification of those who participate in private bug bounty programmes is worthy of further investigation.

In addition, consideration should be given to those individuals who set up the programmes and triage the results. This would provide greater assurance to the buying community and would give confidence to the community of researchers that the scheme is being administered fairly by skilled, knowledgeable and competent individuals.

Who Should Take the Lead?

Workshop attendees considered who could lead an initiative to improve best practice in the bug bounty space. Governments were dismissed because they are not engaged enough in the industry and are not currently close enough to the bug bounty community. It is also difficult to envisage how governments could collaborate and agree fast enough to implement a common view that would be accepted by the industry and the researchers. The concerns regarding formal regulation would also be magnified.

"It needs to be led by a body which represents the bug bounty industry," suggested a workshop participant. CREST, it was proposed, could look to take a lead on this role in regions where it is established; and where possible collaborate with other industry bodies around the world who may be looking at this area of the cyber security industry. But as the workshop attendees countered, "It must not dilute the value of the CREST brand."

One interviewee stated strongly that, "Most bug bounty companies are not seeking any form of industry self-regulation administered by a third-party."

Conclusion: A Vision for an Improved Bug Bounty Space

Bug bounties are becoming better understood and more deeply embedded into the information security industry.

The number of enterprise organisations, researchers, and bounty pay-outs are on the rise and there is also a notable increase in the criticality of submissions. Adoption is increasing remarkably fast and expectations are that it will continue to do so for the foreseeable future.

"The explosion of the bug bounty market is already here, and it's here to stay. This is OK, but we need to put controls around it so we know what good looks like in order to protect researchers, organisations and the bounty platforms", said one participant, who argued that the entire eco-system needs to be mapped and defined, including penetration testing and bug bounty programmes.

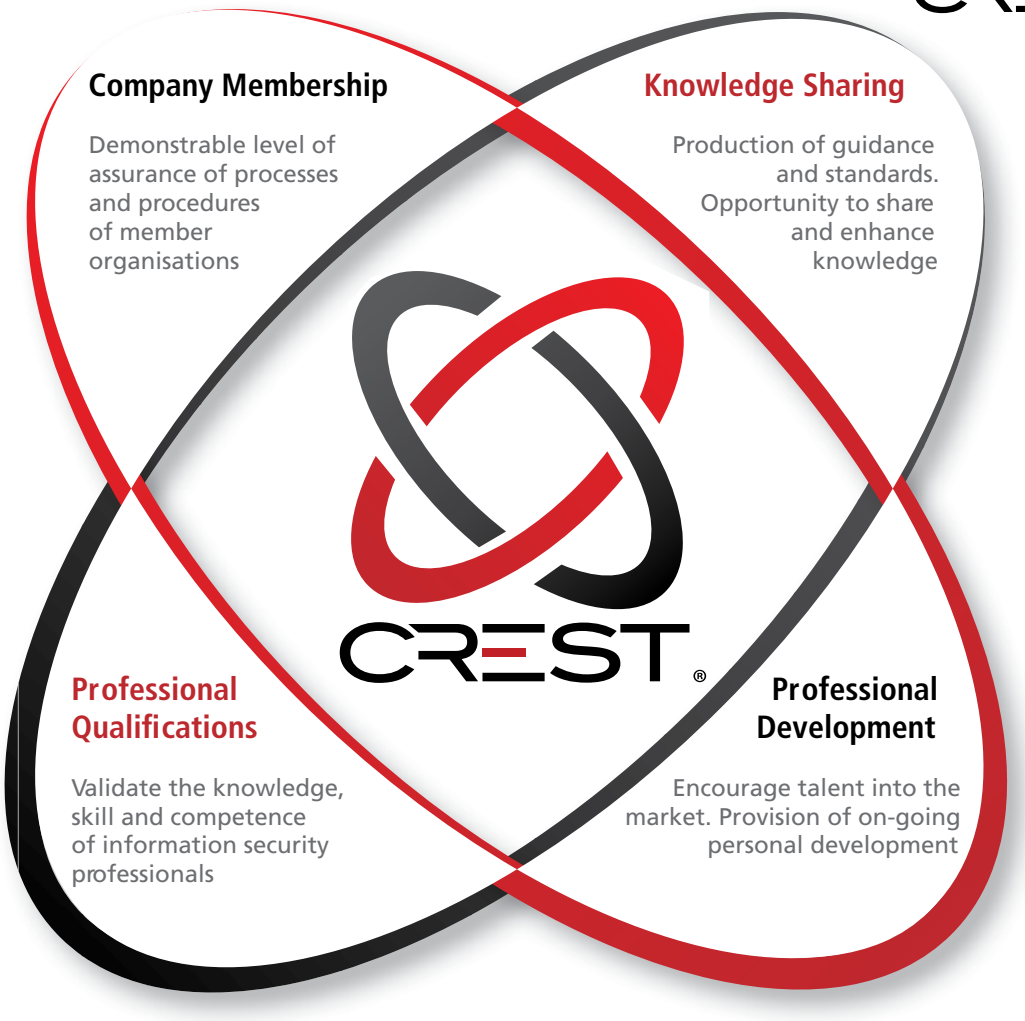
"The logic for penetration testing is absolutely there, it sounds like a great disruptive system. But we need to be vigilant about the challenges and the risks," the participant continued. The numbers around vulnerabilities found are actually low, he argued, and happen in spikes. "Once the low-hanging fruit has been found, researchers will drop out of the programme".

Organisations must carefully consider whether they are ready to run a bug bounty programme, and give further consideration to how they run it, be it internally or with the help of a specialist platform. The maturity required to run a successful programme should not be underestimated.

Whilst it has been agreed that regulation would be incredibly difficult, there is a definite need to define best practice and reconsider codes of conducts.

Finally, it is a paramount that we find a way to protect young individuals, experimenting with vulnerability programmes, from the potential grooming of the dark web. It's important to educate them about best practice, about legalities and about what's right and wrong. "The penetration industry needs to have a view, academia needs to have a view and so does law enforcement", said a participant.

CREST is committed to taking the suggestions and ideas shared at the bug bounty workshop to work towards an improved future for bug bounty hunters and programmes.



For further information contact CREST at
http://www.crest-approved.org

Warning

This Guide has been produced with care and to the best of our ability.
However, CREST accepts no responsibility for any problems or incidents arising from its use.