Friend or Foe?
Community Engagement

Justin Williams
Exec: Group Information Security
MTN
There are many reported instances of white hat hackers being arrested for trying to disclose information security flaws in publicly accessible systems. There are examples of organisations reacting negatively to public disclosure. A number of south african governmental organisation rank amongst these.

On the other side of the fence are those organisations who actively encourage positive engagement with the community through the implementation of bug bounty programmes.

While many security professionals would welcome the implementation of such programmes in their organisations they also dont want to become a target and actively encourage many hackers to start probing their perimeter and systems as this could have an impact on live systems and affect customer service.

The provision of easily accessible security contact details to allow for responsible disclosure can improve the proactive contacts with the community. Further, the implementation of a bug bounty programme can provide a set of ground rules for engagement and responsible disclosure.

This presentation explores some thoughts around the pros and cons of community engagement and the implementation of such a programme.
Contents

1 Introduction
Examples of engagement gone wrong, both in SA and internationally

2 Bug bounties
Discussion on bug bounty programmes and vulnerability disclosure

3 Concluding thoughts
Some final (conflicted) thoughts on community engagement and bug bounties
Introduction

Community engagement
**Introduction**

Belief that people are inherently good, want to assist and do the right thing. We don’t want to drive them down a path that is detrimental to us.

If people try to engage and are blocked it leads to frustration and potentially undesirable behaviour.

Unlike the bad world of cyber criminals, the research community or good hackers, hack into a system for the kick of it and it is a good cyber-citizen behavior for them to act responsibly and not cause harm to the parties involved.
Streisand effect (Butterfly effect)

“It happens when a person or company tries to suppress a piece of information and, in so doing, unintentionally popularizes it.”

• A web site hosted picture of the house of Barbara Streisand – nobody really cared (6 views)
• She unsuccessfully sued for removal
• The publicity drew many more people to the pictures than ever would have happened (420,000 views in the following month)

Source: Bloomberg Business Week
Wikipedia
Mr George Hotz (GeoHot)
A quick synopsis

- Geohot hacked the iphone when he was 17
  - Apple and hackers been in cat and mouse game ever since with each new release of iOS
- PS3 was unhackable, Sony was arrogant
- GeoHot hacked the PS3, met with disbelief
- Sony responds by removing OtherOS (Linux) from the PS3, prompting global outrage and lawsuits
- GeoHot found other vulnerabilities, published them online
  - Sony sued him to take down
  - Seized his computers, twitter account, PayPal records
A quick synopsis …

- German police raid apartment of Alexander Egorenkov, another hacker who distributed software that let PlayStation consoles run homemade games
- Other tech companies found ways to channel hackers
- Sony wasn’t very good at listening about flaws in it’s systems
- Sony settled with GeoHot on 31 March 2011, very biased settlement against Geohot
- Anonymous retaliated April 2011 100 million accounts hacked
- "Trying to sue a member in good standing out of existence didn't do them any favours" says Dave Aitel, white-hat hacker.
Impact of the Sony hack

- Largest cloud service outage in history
- Sony development partners lost money
- Customers couldn’t use paid services
- 250 000 pound fine from UK Information Commissioners Office
- Regulators kept them offline
- Sony had to compensate users
- Free cyber insurance (up to $1m)
- Free games
- Class action settlement re removal of others
- President & CEO apologises

Source: PC World

Sony has a responsible disclosure programme running at https://secure.sony.net
• Around the same time
• Microsoft releases Kinect
• Hours later Hackers reverse engineer protocol
• Lawyers threaten
• Microsoft retreats, praises hackers, offers to release API

• "Microsoft lawyers recognised that it has no legal case against Martin, who made no changes to the hardware [and] Microsoft marketers realised that the drivers might, in the end, be a gold mine for Microsoft.” ZD Net
• MedSec researchers find vulnerabilities in St Jude Medical pacemakers & defibrillators
• Connect to devices & cause fatal interruptions
• Partner with Muddy Waters Capital LLC (May 2016)
• Short the stock
• Shares decline 4.4% after disclosure with 25 million traded
• $89m movement in value
• St Jude was investigated in 2014 by Homeland Security
• Medsec claims St Jude had warning & did nothing
• Likely to sue them for disclosure, so had no choice
What about in South Africa? City of Jhb

• Gerd Naschenweng discovers bug in COJ website
• Altering account parameter allowed view of other customer statements, account numbers, PINs etc
• Phoned COJ call centre, agent didn’t understand, refused to put through to IT or a supervisor
• Email to COJ ignored
• Disclosed on MyBroadband forum and became story

• COJ discredits Gerd as hacker and criminal
• Claims to have laid charges

Source: www.businesstech.co.za
What about in South Africa? SAPS

- @DomainerAnon hacks SAPS and releases sensitive information
- 16 000 whistleblower reports, hundreds of police officers details
- Simple SQL injection attack

- “Back in late 2012 I tweeted the fact that I believed the SAP servers were vulnerable to attack” @DomainerAnon

Could this have been prevented if SAPS monitored twitter?

Source
- www.iol.co.za
- Mybroadband.co.za
MTN example 1: Media disclosure

- Information disclosure issue
- Media contact, little time provided to comment
- Incident process initiated
- System taken offline to reduce any unnecessary exposure
- CIO tweeted to this effect
- Fixed issue
- Brought back on-line
- 160 people had excessive access
- Why media? Did they try contact MTN directly first?

---

**MTN exposing subscribers’ personal details online**

A bug in MTN’s web portal for subscribers is exposing the private data of customers.
By Staff Writer - May 30, 2016  
46 Comments

**MTN online bill platform back up after data leak**

MTN has restored its online bill system after taking it offline following reports of a data leak.
By Staff Writer - May 31, 2016  
2 Comments

---

**Benjamin Marais**
@benjaminmarais

Dear MTN customers I am aware of an issue relating to or billing platform wrt access to other customers details. We r investigating urgently.
MTN example 2: Direct contact

- Email received from unknown external party
  - Had to request a security contact via a service provider
- Notification of XSS bug on an MTN domain
- Flagged as being *maybe* important not urgent
- Requested PGP key
- Info exchanged
- Investigated, confirmed and resolved within 5 days
- Courteous exchanges, token thanks provided

---- Original Message-----
From: [redacted]@gmail.com
Sent: 27 May 2016 11:13 AM
To: Grant Thompson [MTN South Africa] <Grant.Thompson@mtn.com>
Subject: PGP Exchange

Hey Grant,

I got your details from [redacted] when I asked for a security contact @MTNza. I'd like to disclose a silly XSS bug on a website in the mtn.co.za zone which I think _may_ important (maybe not that urgent though).

Please can you give me a PGP key to use for the details? The pub key you can use for me is here: [redacted]

Thanks.

P.S. Bounty/ Swag plz haha ;)

--
L.
:wq!
Public disclosure platforms

Whether we set up a bounty programme, register with bounty sites, or not, disclosures will happen.
Tried:
Anglo, Old Mutual, a number of banks, other telcos

Only one positive result
So what do we do?

- Engage call centre agents & corporate communications
- Monitor social media
- Internal Incident Forums
- Policies and processes

- Encourage community engagement
  - Accessible & visible security email accounts
  - Bug Bounties
Bug bounties
And vulnerability disclosure
What is a bug bounty?

“Rewarding friendly hackers who contribute to a more secure internet.”

The Internet Bug Bounty

“A bug bounty program is a deal offered by many websites and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to exploits and vulnerabilities.”

Wikipedia

“... is a crowdsourcing initiative that rewards individuals for finding a software bug and reporting ...”

Techtarget
When did they start?

In Oct 1995 Netscape launched a bug bounty program for Netscape Navigator 2.0, probably the first documented bug bounty program. Rewards ranged from cash to goodies from the Netscape store. Netscape was crowdsourcing before it had a name.

Google search keyword trends from 2004 : Source Bugcrowd inc.
Who offers these Bug Bounties?

- Tesla
- Pinterest
- Dropbox
- Yahoo
- Facebook
- Mozilla
- Google
- Apple
- Uber
- Tor project

+many many more
## Types of disclosure program’s

<table>
<thead>
<tr>
<th>PROGRAM TYPE + GOAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Disclosure Programs: The primary objective of these programs is to ensure there is a single, public, well-defined channel for security issues.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VISIBILITY</th>
<th>INCENTIVE</th>
<th>SCOPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>Recognition (i.e. public leaderboard)</td>
<td>Generally broad, accepting anything that could be considered a security risk</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Program Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Bug Bounty Programs: The organization running the bounty typically interacts directly with researchers to incentivize them to submit vulnerabilities.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VISIBILITY</th>
<th>INCENTIVE</th>
<th>SCOPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>Cash, swag, misc. (i.e. airline miles)</td>
<td>Slightly less broad, anything that could be considered a security risk and requires a fix</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Program Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Programs: A more exclusive and more highly incentivized program, often run via a crowdsourcing platform vendor that provides submission vetting and program management.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VISIBILITY</th>
<th>INCENTIVE</th>
<th>SCOPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private</td>
<td>High cash incentive</td>
<td>Typically more specific scope or focus to encourage testing on a particular aspect of an attack surface - can be either time-boxed, or on an ongoing basis</td>
</tr>
</tbody>
</table>

Source: Bugcrowd: The state of Bug Bounty 2016
Public bounties are just the beginning
Organizations looking to reap the benefits of a traditional public bug bounty program are utilizing private, on-demand and ongoing, bounty programs more and more. 63% of all programs launched have been private.

Bug bounties move beyond just technology companies
In nearly 300 programs run, our customer base has diversified from mostly tech companies, to now over 25% of programs launched by more traditional verticals such as Financial Services + Banking.

Average priority of submissions increases across all programs
We saw an overall increase in average priority per vulnerability, up from what we reported in our last report, with regional differences in average priority.

XSS continues to dominate
The most commonly discovered vulnerability is still Cross-site Scripting (XSS), which represents over 66% of categorized vulnerabilities disclosed, followed by Cross-site Request Forgery (CSRF).

Payouts are on the rise
Related to the increased severity of vulnerability submissions, the all time average bug reward on Bugcrowd’s platform has risen from $200.81 in our first annual report, to $294.70, an increase of 47%.

“Super hunters” emerge
Earning hundreds of thousands of dollars from bug bounties alone, a tier of ‘super hunters’ is emerging, often getting attention from organizations’ security team recruiting efforts.
**Starting a bug bounty programme**

- You need people
  - Defined process
  - Meet SLA’s for logging, responding & fixing
- You need internal visibility and buy-in
  - Cross functional policies
  - Infrastructure, Development, Incident response, legal etc
- Know your attack surface
  - Risk assessments
  - Break down of components
  - Define in and out of scope
  - Ongoing list of False positives
- Rewards
  - HOF vs Swag vs Bounty
Starting a bug bounty…

• Run it yourself vs use an existing managed platform

• Benefits of using a managed platform
  • Defined processes (ISO compliant)
  • Existing community (Hacker ratings)
  • De-duplication
  • Validation of bugs
  • Sandboxed testing
  • Hackbot learning machines
  • Handling of payments

• Cost?
  • No cash changing hands can be free
  • Typically around 20% of the bounty

Managed platforms

HackerOne
Bug Sheet
Cobalt
Bugcrowd
CrowdCurity
Synack
ISO 29147:2014 Vulnerability disclosure
• First proposed in 2005
• Published in final form February 2014
• Available for free download

ISO 30111 Vulnerability handling
• Published in final form in 2013
• Interfaces with ISO 29147
Vulnerability disclosure policy

Minimum policy aspects (ISO 29147)
- How to contact vendor
- Secure communications
- Setting communications expectations
  - Acknowledgement (7 days) & updates
- Out-of-scope services
- Report tracking

Optional aspects
- Credit to finder
- Synchronised public disclosure
- Distribution
Vulnerability handling

• Have a process and organisation structure to support investigation & remediation
• Perform root cause analysis
• Weigh various remediation options
  • Adjust for real world risk factors
  • Balance speed with thoroughness
• Try to co-ordinate with other vendors (if appropriate)
  • Multi-vendor issues
  • Supply chain issues
Vulnerability handling: response capability

• Policy
  • Why response?

• Organisational capability
  • Who is in charge of response?

• Engineering capability
  • How quickly, effectively and thoroughly do we respond?

• Communication
  • How clear and timely is our guidance?

• Analysis capability
  • How can we learn from this to prevent additional vulnerabilities? Can we predict trends to aid in investment of resource?
Rewards for disclosure

• Analysis of BugCrowd list of bounties (18/8/2016)
  • https://bugcrowd.com/list-of-bug-bounty-programs
  • Sample of 489 programmes

• Rewards
  • 65% Hall of fame (32% HOF only)
  • 41% Reward
  • 22% Responsible disclosure
  • 7% Swag (2% Swag only)

• 59% offer no monetary reward
Apple Web Server notifications

This article provides credit to people who have reported security issues in Apple's web servers.

Credits

2016-06-20 beatsbydre.com
A cross-site request forgery issue was addressed. We would like to acknowledge Aadli (@aadlitya_puran) for reporting this issue.

2016-05-11 icloud.com
A server configuration issue was addressed. We would like to acknowledge Gary O'Lea and Graham Bacon of appcheck-ng.com for reporting this issue.

2016-05-05 itunes.apple.com
A server configuration issue was addressed. We would like to acknowledge Akshay Jain (facebook.com/akshayjain011) for reporting this issue.

2016-04-22 apple.com
A server configuration issue was addressed. We would like to acknowledge SafiAllah I Security GmbH - Government Laboratory (facebook.com/WhiteHatSecuri) for reporting this issue.

2016-04-20 trailers.apple.com
A cross-site scripting issue was addressed. We would like to acknowledge Edwin Foux for reporting this issue.

2016-04-20 jobs.apple.com

Author: Justin Williams (Executive : Group Information Security) @JJZA Justin.Williams@mtn.com
## What is a bug worth?

<table>
<thead>
<tr>
<th>Security Maturity Model</th>
<th>Basic</th>
<th>Progressing</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Payout Range</strong></td>
<td>$100 - $1,500</td>
<td>$200 - $5,000</td>
<td>$300 - $15,000</td>
</tr>
<tr>
<td><strong>Average Bug Payout</strong></td>
<td>$300</td>
<td>$600</td>
<td>$1,000</td>
</tr>
<tr>
<td>P1</td>
<td>$1,500</td>
<td>$5,000</td>
<td>$15,000</td>
</tr>
<tr>
<td>P2</td>
<td>$900</td>
<td>$1,800</td>
<td>$2,500</td>
</tr>
<tr>
<td>P3</td>
<td>$300</td>
<td>$600</td>
<td>$900</td>
</tr>
<tr>
<td>P4</td>
<td>$100</td>
<td>$200</td>
<td>$300</td>
</tr>
</tbody>
</table>

*Baseline vulnerability budget*

Source: Bugcrowd : Defensive Vulnerability Pricing Model
Downsides of bug bounty?

• Don’t expect Researchers to take into consideration your risk strategy
• Few researchers will carefully read your Bug Bounty Guidelines and Conditions
• Bug Bounty Requires Very Serious Technical, Human and Thus Financial Resources
• You WillHardly Distinguish Black Hats and Legitimate Researchers in Your Logs
• Unexpected Testing Methodologies and Techniques Will Regularly Appear on Your Horizon

Source: Ilia Kolochenko : ITProPortal.com
So I’m the guy who sent the t-shirt out as a thank you.

By Ramses Martinez, Director, Yahoo Paranoids

So, I am the guy who started sending t-shirts as a thanks to people when they sent us a potential vulnerability issue. What an interesting 36 hours it has been :)

Here’s the story. When I first took over the team that works with the security community on issues and vulnerabilities, we didn’t have a formal process to recognize and reward people who sent issues to us. We were
Apple bug bounties outbid

Apple’s bug bounty program favors quality over quantity

The company will pay between $25,000 and $200,000 for exploits

Exodus Intelligence bounties

<table>
<thead>
<tr>
<th>Target</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS 9.3+</td>
<td>$500,000</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>$150,000</td>
</tr>
<tr>
<td>Microsoft EDGE</td>
<td>$125,000</td>
</tr>
<tr>
<td>Firefox</td>
<td>$80,000</td>
</tr>
<tr>
<td>Windows 10 LPE</td>
<td>$75,000</td>
</tr>
<tr>
<td>Adobe Reader</td>
<td>$60,000</td>
</tr>
<tr>
<td>Adobe Flash</td>
<td>$60,000</td>
</tr>
</tbody>
</table>

Zerodium also offers $500,000 rewards for zero-day vulnerabilities in iOS

Ivan Krstić, the head of Apple Security Engineering and Architecture, on stage at the Black Hat USA 2016 security conference on Aug. 4, 2016. Credit: Lucian Constantin
Concluding thoughts
And some enterprise challenges
Some Enterprise challenges

- Scope & attack surface
- Language
- Time Zones (marginal)
- Culture
- Silos
- Integrated enterprise systems
  - CMDB
    - Issues tracking
- Forex restrictions (pay bounties)
Competing concluding thoughts

A bounty program definitely helps manage responsible disclosures better since the efforts/rewards are balanced, and outsourcing it to companies who might have more expertise in managing such programs makes a lot of sense from a planning & execution perspective.

It is definitely better than asking people to make submissions at security@xyz.com email address.

Anupam Bonanthaya : Aujus

“... you’d be better off concentrating on the main risks to web applications, and spending your security budget on traditional web security solutions and services that are more suitable to your business needs and technical requirements.

Bug bounty is like hitchhiking: a great way to travel when you are on holidays or have plenty on time, but totally unsuitable for the majority of business trips, which require assurance, quality and accuracy.”

Ilia Kolochenko, CEO of High-Tech Bridge.
Conclusion

1. No single answer
   Do your homework, understand the pros and cons before initiating the program

2. It's a journey
   Have a plan for engagement with the community and don't go to full bug bounty until you are ready

3. You aren't in control
   People are assessing you and reporting regardless of your state of readiness

4. Disclosure policy
   Define the rules of engagement and scope, let the community know it's safe to engage

5. Stay alert
   Include open disclosure platforms and social media in your list of sources monitored

6. Be ready to respond
   Disclosures will happen and you can't control when. Be ready.