#ForensicPerspectives

"Bug bounty" demands: *legal bane or information security boon?*

A "bug bounty" request occurs when a self-described security researcher contacts a company, claiming to have discovered an information security vulnerability, often in the company's public-facing website or applications, and requests a cash payment in exchange for details.

According to published reports, **the average bug bounty payment is $1,000,** and the **90th percentile payments for high and critical vulnerabilities is $12,000.**[1]

While these amounts may seem small, the risks associated with responding to – or ignoring – these payment requests can be significant.

Potential benefits

A well-designed "bug bounty" program can deliver a range of benefits, including:

1. **Early detection**
   Identifying vulnerabilities early allows for remediation efforts before threat actors can exploit them.
2. **Cost-effective security**
   By "crowdsourcing" security efforts, organizations can identify additional vulnerabilities more cost-effectively; payments should only be made when genuine vulnerabilities are confirmed, as well as clean hands on the part of the security researcher.
3. **Commitment to security**
   A published "bug bounty" program demonstrates a commitment to information security, privacy, and compliance with applicable standards.
4. **Encourages responsible disclosure**
   A formalized program can encourage third parties to report vulnerabilities directly to the company, potentially reducing the risk that such information is brought to a regulator (e.g., under government whistleblower programs), or sold on the dark web.

Potential risks

Implementing a "bug bounty" program comes with governance challenges, including:

1. **Veracity of claims**
   Not all claims are truthful. Can the claim be validated?
2. **Exploitation risk**
   Has the security researcher exploited the vulnerability, perhaps exfiltrating data, deploying ransomware, or publishing/ monetizing the opportunity on the dark web for malicious activity for malicious activity?
3. **Legal ambiguities**
   Is the request genuinely a "bug bounty" inquiry, or has it crossed into ransom territory? Will regulators agree with your assessment? As demonstrated in *USA v. Joseph Sullivan*, there are significant differences between a "bug bounty" and an extortion demand.
4. **Legal and reputational risks**
   What are the legal, regulatory, and reputational risks of ignoring a tipster or, conversely, making the requested payment?

[1] 7th Annual Hacker Powered Security Report (www.hackerone.com/reports/7th-annual-hacker-powered-security-report).

CRA Charles River Associates

Regulatory guidance

Recognizing that companies and government agencies may wish to establish a formal "bug bounty" program, various regulators have issued guidance. For example, the U.S. Department of Justice's Cybersecurity Unit has provided a four-step framework to guide the design of such a program.[2] Notably, the DOJ emphasizes that making "bug bounty" payments in the absence of a carefully designed, written program can increase an organization's risk of unintentional civil or criminal violations of law.

Evaluating and responding to "bug bounty" requests

Depending on the specific circumstances, clients will typically retain forensic experts to provide independent, objective advice on:

1 **Validating vulnerabilities**

Confirming the vulnerability, advising on remediation, validating the effectiveness of the remediation, determining if notification-triggering data has been accessed, and assessing whether the vulnerability has been exploited by the security researcher or others.

2 **Due diligence on researchers**

Conducting reputational and integrity due diligence on the security researcher to validate their intentions and reduce legal, reputational, and regulatory risks before making any "bug bounty" payment.[3]

3 **Incident response**

Investigating any indicia of exploitation, pursuant to the company's incident response policies, and assisting with disclosure and notification obligations.

4 **Malware neutralization**

Searching for and neutralizing malware.

We invite you to reach out to us or any other member of the CRA Forensic Services Practice to continue the conversation on these or other forensic matters.

CRA's Forensic Services experts advise on the prevention, detection, and correction of a broad range of waste, fraud, and abuse risks and allegations. Recent assignments have included leading complex cyber incident response engagements, conducting theft of trade secret investigations, providing expert witness testimony on both liability and damages, consulting on national security/technology/trade compliance, and delivering information security and privacy monitorship services.

Contacts

Bill Hardin, CPA, CFE, PMP
Vice President and Practice Leader, Forensic Services
+1-312-619-3309, bhardin@crai.com

David Cowen, CISSP, AWS SAA, GCFR, GCFE
Vice President, Forensic Services
+1-214-662-4478, dcowen@crai.com

[2] *A Framework for a Vulnerability Disclosure Program for Online Systems* (July 2017), U.S. Department of Justice Cybersecurity Unit (www.justice.gov/criminal/criminal-ccips/page/file/983996/dl?inline).

[3] CRA maintains private investigator licenses, as required under certain circumstances to furnish certain investigative services.