Global Data Privacy and Security Team

Data Security At A Glance:
Crowdsourcing Security With Bounty Programs

Data security officers keep their eyes open for risks. Usually this means monitoring reports from automated security systems that flag potential security events and listening to employees' reports of security issues. There is a great deal of debate, however, about the merits of listening to the security concerns of people outside of an organization. On one end of the spectrum companies refuse to discuss any aspect of their security with the public. On the other end of the spectrum companies proactively encourage the public to report security vulnerabilities by paying well meaning hackers (usually called "white hat" hackers) to report problems. While these companies view "bounty" programs as commonsense crowdsourcing, others view the concept as promoting corporate extortion.

The following provides a snapshot of information on bounty programs as well as a checklist for organizations that are starting a program, or evaluating an existing program.

The number of organizations that have established data security bounty programs[1]	The percentage of Bounty Programs that actually pay a cash bounty.	The percentage of Bounty Programs that offer nothing other than acknowledgment and credit to successful hackers
376	**27%**	**53%**

$100 to $25,000

Typical range of rewards offered for programs that pay monetary compensation

[1]Statistics from http://vulnerability-lab.com/list-of-bug-bounty-programs.php (last viewed Nov. 2014).

Bryan Cave's Global Data Privacy and Security Team has responded to hundreds of data security breaches and routinely helps clients, before a breach happens, analyze and improve upon their ability to respond to a breach if (or when) one occurs.

For more Information Contact:

David A. Zetoony
Partner
david.zetoony@bryancave.com
1155 F Street, N.W.
Washington, D.C. 20004
phone: 202 508 6000

Jason D. Haislmaier
Partner
jason.haislmaier@bryancave.com
One Boulder Plaza
1801 13th Street, Suite 300
Boulder, CO 80302
phone: 303 444 5955

BRYAN CAVE

What to think about when considering a bounty program:

If you do not enact a bounty program…

- ✓ What are the practical implications if the company views any hack as "unauthorized?"
- ✓ What are the practical implications if a "white hat" hacker tries to breach your security with no guidelines on how they should act?
- ✓ Is there a risk that individuals who know of a security vulnerability may provide that information to bad actors instead of providing it, first, to you?
- ✓ Is there a risk that individuals who know of a security vulnerability may provide that information to the media or to regulators instead of providing it, first, to you?
- ✓ How would the company view an unsolicited request for payment by a hacker?

If you do enact a bounty program…

- ✓ Do you have confidence that you can track / monitor successful participants?
- ✓ Will all of your systems be "in scope"?
- ✓ Should certain forms of attack be prohibited?
- ✓ Will employees be eligible to participate?
- ✓ Will you be encouraging attacks that might disrupt business activities?
- ✓ Will the program be focused on weaknesses to the security of sensitive personal information, to performance, or to both?
- ✓ Will you proactively disclose the level of compensation that a hacker should expect?
- ✓ What conditions of confidentiality will you impose on the hacker?
- ✓ Will you permit anonymous reporting?
- ✓ How can you avoid the unintentional access or acquisition of sensitive personal information?
- ✓ Will the program comply with international law?
- ✓ How will you receive and document security vulnerabilities?