Bug Bounties: Overcoming Fears, Finding Solutions

02 May 2018 By: Sean Sposito, Al Pascual

As financial institutions (FIs) increasingly focus on digital channels, industry leaders are coming to accept that any web or mobile application, piece infrastructure or network, or API open to the Internet will be scanned and pulled apart. More often than not, this dismantling is done voluntarily by independent security researchers who will expect the FI to have a mechanism by which they can report urgent issues they uncover, see software weaknesses fixed, and be rewarded for valid reports.

Indeed, retail banks, payment networks, and other FIs are coming to grips with the idea of outsiders poking at their publicly exposed systems. They’re dipping their toes in the water. They’re starting to embrace vulnerability disclosure as a strategy for lessening the risk that accompanies unknown or overlooked hardware and software vulnerabilities. However, many FIs still don’t see the upside of public bug bounty or vulnerability rewards programs (VRP). They’re fearful that rewarding vulnerability reports may result in unauthorized disclosure or regulatory consequences. This report examines the interest, trust, and doubts FIs have in bug bounty programs (initiatives that incentive vulnerability disclosure) and, more generally, vulnerability disclosure.

Key questions discussed in this report:

- What types of security skills and capabilities are FIs most interested in adding to their internal, security teams in the coming year?
- What types of crowd-sourced security models are FIs most comfortable with – if any?
- What are the attitudes of security professionals within FIs towards private and public bug bounty programs?
- What concerns do FI security leaders have when it comes to such security controls?

Companies Mentioned: Acorns Grow Inc., Bank of America, Card.com, Circle, Citibank, Coinbase, Dash Digital Cash, ING, JPMorgan Chase, LendingClub, Mastercard, PayPal, Simple, USAA, Western Union

Data in this report is based on information collected in a random-sample panel of 800 information technology security decision-makers, 200 of whom work in financial services. For questions answered by all 800 survey respondents, the maximum margin of sampling error is ±3.46 percentage points at the 95% confidence level. For questions answered by all 200 financial services respondents, the maximum margin of sampling error is ±6.93 percentage points at the 95% confidence level. The maximum margin of sampling error is higher for questions answered by segments of respondents."

Javelin conducted a series of interviews with industry executives, vendor executives, and other relevant stakeholders to gain an understanding of crowd-sourced security models. Interviewees represented a variety of types of organizations, including crowd-sourced security vendors, among others.