Link to Article on website

Bug-Bounty Programs: lessons learned for Asia from the U.S. experience

A Bug-Bounty Program invites ethical hackers to explore a company's systems and then to report back.

BY:
Daniel P. Levison, Partner, Morrison & Foerster, Singapore
Jake M. Robson, Partner, Morrison & Foerster, Singapore
David A. Newman, Of Counsel, Morrison & Foerster, Washington DC
David Hambrick, Associate, Morrison & Foerster, Singapore
Nick Davies, Associate, Morrison & Foerster, Singapore

Morrison & Foerster LLP is an international law firm with 16 offices located throughout the United States, Asia, and Europe. The firm has over 1,000 lawyers who advise clients across a range of industries and practices, including corporate/M&A, private equity and fund formation, banking and finance, data privacy and security, intellectual property, litigation, anti-corruption and compliance.

ACROSS THE GLOBE AND IN AN INCREASING NUMBER OF INDUSTRIES, companies are considering adopting so-called "bug-bounty programs" (BBPs) to augment their cyber security efforts. A BBP invites ethical hackers to explore a company's

systems and then to report back about any discovered weaknesses in exchange for a reward. A broad range of U.S. companies in the tech sector have adopted these programs, and their use is increasingly spreading to other industries and geographic areas as well. The U.S. experience with these programs underscores their value but also highlights best practices and potential pitfalls in their design and execution.

BBPs: on the rise in the United States and beginning to gain favour in Asia

BBPs have come into favour in the United States and elsewhere because they can act as cost-effective ways to supplement existing efforts to identify and remediate system vulnerabilities. The prospect of paying USD 500 (the approximate average reward for a discovered bug of any severity in the U.S.-headquartered platform HackerOne) as an alternative to enduring an incident that could ultimately cost millions of dollars is understandably an attractive one to companies that increasingly view cyber security as a major area of risk.

Some U.S. companies see such programs as a lower-cost complement to increasing investment in internal security measures. Even large institutions that make substantial investments in internal security and those in highly regulated industries have found value in enlisting outside actors with a new perspective to stress test and supplement their cybersecurity efforts, including high profile companies in the financial sector such as Western Union, ING, and PayPal, all of which have launched BBPs.

BBPs are beginning to gain favour in Asia, as well, even as the practice is less pervasive. In Japan, Sprout hosts a bug-bounty platform for over 100 Japanese companies. Additionally, HackerOne, a U.S.-headquartered company that hosts BBPs for many U.S. companies, has partnered with Grab, one of Southeast Asia's largest ride-sharing platforms, to announce the adoption of Grab's BBP. This expansion has now spread to institutions and industries that are typically slower to experiment in new cyber security approaches. For example, Singapore's Ministry of Defence recently hosted its first BBP, which ran from January to February 2018.

Lessons learned from the U.S. experience

As these programs begin to expand in Asia, it is important for in-house counsel and privacy officers to consider valuable lessons learned from the U.S. experience. Among them:

- **When designing a BBP, think carefully about what network components and data to include and consider making sensitive information off limits.** Organisations should consider a number of factors when deciding what should be included within the scope of a BBP, including the sensitivity of the information, the safeguards in place, and any applicable regulatory or contractual restrictions. These were among the key takeaways from advisory U.S. Department of Justice guidance issued last year addressing BBPs.

- **When drafting the publicly available policy for the program, be clear and specific about the scope of authorised conduct.** It may be useful, for instance, to prohibit participants from engaging in any intentional

conduct that changes user-generated data, impairs or disables systems, or that otherwise makes data inaccessible or includes the downloading of any company information.

- **Assign a central point-of-contact to receive vulnerability disclosure reports and be clear about which personnel are authorised to answer questions about the program.** It is easier to respond to unusual reports and difficult questions if there is a clear point of reference for report processing. Questions that raise new and unanticipated legal issues should be handled carefully.

- **Be transparent about whether and how you will pay a bounty, and only pay a bounty if it is for an activity that is specifically authorised by your policy.** It is important to create rules and to follow them closely. Otherwise, a company might put itself into an unfavourable negotiating position with participants. This includes setting different reward amounts for different discoveries.

- **Consider using test accounts and a third-party system to host.** The use of test accounts will help to ensure that customer data is not unnecessarily compromised. Depending on the organisation, there may be value and efficiencies to using a third-party platform to host the program.

- **Consult with specialist counsel to make sure that your program complies with applicable regulations.** Regulators in certain highly regulated sectors, like the financial services industry, may require regular vulnerability assessment and penetration testing. It is important, however, that such efforts are made in compliance with local regulations.

Conclusion/Takeaways:

A BBP is a valuable tool that should be carefully tailored to each organisation and the regulatory regime to which it is subject. Even though financial services companies have been slower to adopt them, if designed appropriately, they could serve as a valuable tool for banks and other companies to enhance their security.

Regulatory guidelines in Singapore, for example, recommend that financial institutions in Singapore conduct vulnerability assessments and stress test their systems, but our experience is that currently this is often done with the assistance of specialist firms rather than through BBPs.

At the same time, it is important for companies to consider their specific regulatory context and any applicable requirements – to understand potential risks but also to determine whether BBPs can assist in meeting applicable standards. ■