SECURITY INNOVATION

# THE BUCK STOPS HERE:

# DIGITALX'S DIGITAL PAYMENTS SOFTWARE SECURED FOR RELEASE

Security Innovation Detects Vulnerabilities to Ensure Safe Beta Launch

"Security Innovation's deep security expertise and depth of domain knowledge allow us to be confident in the security of our software. They helped us to architect a secure system and validate our implementation."

**Alex Karis, CEO, digitalX**

## CYBER HACKERS ARE ALWAYS LOOKING

for new ways to exploit vulnerabilities in Web-facing software applications so they can access credit card numbers, social security IDs, bank account PIN numbers, and even customer funds. Verizon's 2015 Data Breach Investigations Report shows just how bad the problem is, analyzing nearly 80,000 security incidents, including 2,122 confirmed security breaches in 61 countries. Not surprisingly, software security is the top concern for most businesses, including digitalX (ASX: DCC), a digital payments company.

When digitalX began closed beta testing on its latest transaction software, AirPocket™ in the fall of 2014, it called upon leading independent U.S. security firm, Security Innovation, to provide risk assessments and penetration testing services. Security Innovation previously provided similar services for digitalBTC's leading digitalX Direct™ software.

AirPocket enables money to be sent anywhere in the world. Taking advantage of the sharing economy paradigm pioneered by Uber and Airbnb, users can send money to each other through the use of an AirAgent™. They can also send funds and payments directly through the mobile app, without an agent, in peer-to-peer transactions. AirPocket makes novel use of the bitcoin blockchain as a record ledger for an internal remittance network to facilitate lower cost transactions and create transparency.

*"With our specialized digital transaction products it is important to work with a firm with proven expertise in testing for software security flaws efficiently and making recommendations on how to fix them,"* says Alex Karis, Chief Executive Officer of digitalX. *"Security Innovation was our choice from the beginning, because their technology team had the best understanding of the emerging blockchain technology, as well as deep experience in the banking and financial industries."*

## THE CHECKS AND BALANCES OF SECURITY FLAWS

In June 2015, Security Innovation began a **two-phased engagement** to analyze and test AirPocket for software flaws that could be used by hackers to compromise sensitive customer information.

1 **Security Innovation's team conducted a design and architecture review** of the software based on specifications and APIs built by digitalBTC. The focus was on AirPocket's infrastructure design and special consideration was placed on the application's authentication model; sensitive data crossing security boundaries; interactions with third-party components; and common threats regarding secure practices in crypto-currency operations, which is critical given the application's use of the secure blockchain technology.

2 **Security Innovation then developed a threat model** based on analysis to identify and seek out vulnerabilities to specific cyber threats during penetration testing. Any security flaws would be reported immediately, allowing digitalBTC to address them before releasing the open beta version to public users.

*"Security Innovation did a great job of translating AirPocket's specs into a threat model they could use to best determine what needed to be tested on our system," says Fabricio Rodriguez, Chief Technology Officer at digitalBTC. "We had a lot of confidence in them based on their analysis and reporting on the digitalX Direct product."*

During the final penetration testing phase, Security Innovation looked for security flaws in digitalBTC's software application, including common application vulnerabilities, such as authentication coding errors, that could introduce vulnerabilities. In this case, Security Innovation did not examine the code itself, but instead tried to exploit the business logic of the application as a means to access systems holding confidential customer and company information. *"As you develop software, a rigid schedule is tough to keep and Security Innovation has been very accommodating, which has been great,"* says Karis.

## SAFE AND SECURE FOR OPEN BETA RELEASE

As a result of its testing, Security Innovation found the AirPocket API to be resilient to many common web services threats. Some issues regarding the design and intended workflow were identified and addressed. digitalBTC was able to move forward with the public facing open beta testing on schedule and with confidence.

*"digitalX has taken a huge step toward ensuring their customers' data is safe and secure before AirPocket goes public and becomes a new financial target for cyber criminals," says Joe Basirico, Vice President of Security Services at Security Innovation. Clearly, digitalBTC recognizes the importance of application security to its customers and is dedicated to bringing products to market that meet high standards for security."*

"With our specialized digital transaction products it's important to work with a firm with proven expertise in testing for software security flaws efficiently and making recommendations on how to fix them."

**Alex Karis, CEO, digitalX**

**ABOUT SECURITY INNOVATION**

Since 2002, Security Innovation has been the trusted partner for cybersecurity risk analysis and mitigation for the world's leading companies, including Microsoft, Sony, GM, Disney, Google and Dell. Recognized as a Leader in the Gartner Magic Quadrant for Security Awareness Computer-Based Training for the second year in a row, Security Innovation is dedicated to securing and protecting sensitive data in the most challenging environments - automobiles, desktops, web applications, mobile devices and in the cloud. Security Innovation is privately held and headquartered in Wilmington, MA USA. For more information, visit us at www.securityinnovation.com.

SECURITY INNOVATION