# Why This Global Bank Trusted BlackBerry to Evaluate Its Security Vendor
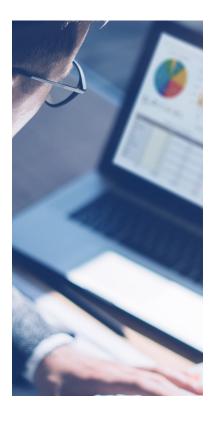
**Industry:** Financial Services
**Services:** BlackBerry®
Cybersecurity Consulting

## At a Glance

Staff at this global bank use mobile devices and applications extensively to stay connected and productive. To better protect the large threat surface created by such significant use, the bank reached out to a third-party security vendor for a mobile antimalware app. To ensure the app was up to its exacting security standards, the bank then approached the BlackBerry® Cybersecurity Consulting division.

A full-service cyber consultancy practice, BlackBerry Cybersecurity Consulting leverages BlackBerry's proven leadership in high-security organisations and use cases. Through extensive investigative experience and in-depth knowledge, BlackBerry's cybersecurity professionals assess the unique threat landscape and security challenges of each organisation they work with.

**BlackBerry**

# The Organisation

A global retail and investment bank with offices all around the world, this organisation is a heavy user of mobile devices and applications – as is common in the financial sector. Its staff frequently works remotely via mobile apps. Aware of the significant risks this presents, the bank has implemented multiple security measures designed to protect client and financial data.

One such security feature was a mobile antimalware solution developed by a third-party security vendor. "Effectively, every device used to conduct business at the bank would have this app installed on it," explains BlackBerry Cybersecurity Consulting Director James McDowell. "If someone clicks a link they shouldn't, for example, the app would alert them. For the client, it was a necessary step in protecting their mobile infrastructure."

# The Challenge

The bank was aware that even security software can contain vulnerabilities. Given the size of their planned deployment, decision makers didn't want to take any chances. They knew that even though the app itself would not manage sensitive data, it could be used by hackers to gain a foothold in the bank's network.

"Applications present a significant threat surface to any business, for a number of reasons," notes McDowell. "The client understood this, as well – there's been a real shift in the understanding of threat surfaces of late. Historically, all we've had to worry about is ourselves and our businesses."

Hackers will always seek the path of least resistance. And with large businesses spending more and more on security, direct attacks on networks have become far more challenging. It's more economical for criminals to search for weaknesses in other areas of an organisation's ecosystem, such as suppliers, applications, or employees.

"One company we've worked with in the past has invested millions into cybersecurity to protect their intellectual property," he continues. "When they were breached a few years ago, we found that hackers had been monitoring the organisation for a while. They ultimately breached the company by exploiting a vulnerability in a minor third-party it did business with."

**BlackBerry**

The bank needed to validate the mobile antimalware app's code, both to ensure that it did what it claimed to do and to address any potential security risks. Unfortunately, code review is a complex, time-consuming process, one which the bank lacked the in-house expertise to manage on its own. They knew they needed to bring in help, and after a brief discussion, they brought in BlackBerry.

"BlackBerry was already well-entrenched within the organisation from a licensing perspective," explains McDowell. "They knew about the expertise of our Cybersecurity Consulting division. More importantly, they knew that we would be objective – that we would not attempt to use our evaluation to open up a sales opportunity."

# The Services

Over the course of three weeks, McDowell and his team carried out a thorough, manual review of the application, examining each line of code. They found a large volume of serious vulnerabilities, and in the process discovered something odd. The vendor had not developed the application internally - it had been purchased from a third- party vendor and repackaged.

"We found a lot of random, inert snippets of code referencing another company," McDowell explains. "The code hadn't been sanitized at all. With that in mind, the vulnerabilities we found were not especially surprising."

McDowell and his team examined more than the application, as well. They also took a close look at the service-level agreement, where they found another serious issue. One of the SLA's strictures was that the vendor was responsible for notifying the bank of new malware within twenty-four hours.

"From our position as security experts, we were advising on more than technology," says McDowell. "We were also looking at the service side of things. Given how much damage a virus can do in a day, a notification period that long was unacceptable."

**BlackBerry**

# The Results

By relying on BlackBerry's expertise, the bank was able to establish a strong position for negotiation with their vendor. In addition to remediating the vulnerabilities BlackBerry uncovered, they were able to demand a better service-level agreement. More importantly, the bank can now turn to BlackBerry in the future for rigorous testing on any other apps it decides to deploy.

**Efficient, Effective Application Review:** Because of the time and effort required, many organisations don't bother with app validation on smaller deployments. Thanks to BlackBerry Cybersecurity Consulting, the bank no longer needs to make such a sacrifice. Review of the antimalware app only took a few weeks.

"One of the opportunities we saw here was to create what we call an app validation factory," explains McDowell. "This allows us to put anything a client deploys through rigorous testing over a short timeframe, highlighting the potential risks we uncover. The client can then decide which risks are worth remediation based on our advice."

**A Better, More Secure Deployment:** Aside from the security issues and SLA, the bank was satisfied with its third-party vendor. Through BlackBerry's evaluation, it was able to negotiate a better SLA with its vendor. More importantly, it was able to deploy the app as it had originally planned.

"The bank highlighted the vulnerabilities we found and demanded remediation before moving forward," explains McDowell. "The product was a good fit for them – and they're now able to use it without worrying about compromising their security."

**An Improved Outlook on Security:** By working with BlackBerry, the bank has a greater understanding of the potential risks an app deployment might represent. McDowell expects that this will serve the organisation well, both in future deployments and future vendor negotiations.

"I got the sense that what we did wasn't a standard process for the bank," says McDowell. "We just happened to be available at the time, and they had the idea to have us run the validation. I don't think they expected us to find the vulnerabilities we did.

**BlackBerry.**

## About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) is a trusted security software and services company that provides enterprises and governments with the technology they need to secure the Internet of Things. Based in Waterloo, Ontario, the company is unwavering in its commitment to safety, cybersecurity, and data privacy, and leads in key areas such as artificial intelligence, endpoint security and management, encryption, and embedded systems. For more information, visit BlackBerry.com and follow @BlackBerry.