



This Online Gaming Company Didn't Want to Roll the Dice on Security - That's Why it Worked with BlackBerry

At a Glance

Industry Online Gaming
Services BlackBerry®
Cybersecurity Services

With offices across the United Kingdom, this gaming company has been in operation for decades. In recent years, it has expanded its business online. Concerned that some customers might use its new line of business to cheat for financial gain, the company approached BlackBerry® Cybersecurity Consulting for help securing its gaming applications.

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.



The Organisation

With a history that spans decades, this UK gaming company brings in several billion pounds a year. Recently, the owner decided to bring the business online. Though this greatly increased its customer base, it also opened the organisation up to an unexpected problem: cyber criminals.

"When you're face-to-face in a betting shop, it's difficult to try to cheat them out of their money," explains James McDowell, Director of BlackBerry Cybersecurity Consulting. "The Internet is a completely different ball game, and the owner of the company realised that. They approached us with the concern that people might be able to cheat them online."

As it turns out, they were right – and BlackBerry helped them address their concern.

The Challenge

Although it's certainly possible to steal from a business's physical office, it's far easier to defraud them online. Gaming companies are a prime target for this particular brand of attack, given the large volumes of money they frequently handle. This organisation was no different – its website features a large selection of different gaming applications, all purchased from external vendors.

"A lot of the games on these online platforms are not developed by the company themselves – they're brought in from a third party," says McDowell. "Given the number of different apps used by the organisation, there was almost certain to be at least a few vulnerabilities. And each of those vulnerabilities could be used to commit fraud."

What's more, because these apps are purchased and not developed internally, they carry additional risk. A hacker could examine the games on a website and research them online to uncover and exploit common vulnerabilities. And the victim would likely be none the wiser.

"There are a lot of unanswered questions where application vendors are concerned," McDowell continues. "What validation are their applications going through before being distributed? What kind of code have they shipped to their clients? What are they doing about security?"

These were questions the firm's leadership recognised their cybersecurity posture as being too immature to answer. They knew they needed to bring in an expert, and BlackBerry fit the bill.

“Whenever we approach security, we ask the question of how a company makes money. That’s how we formulate our security assessment – and it’s how we patched several major vulnerabilities that would have cost our client a great deal of money.”

James McDowell,
Director, BlackBerry®
Cybersecurity Consulting

The Services

The organisation gave BlackBerry full rights to perform any tests necessary to evaluate its security posture, including probing its website for vulnerabilities and evaluating the physical security of its retail outlets. BlackBerry then carried out a full assessment of the organisation’s infrastructure – both online and off.

The Cybersecurity Consulting team examined the code of the company’s applications for vulnerabilities, and attempted to test if those vulnerabilities could be used to commit fraud. The assessment revealed several major gaps in the company’s security.

“One of the applications we tested was a trivia game hosted on the company’s website,” says McDowell. “After analyzing the app, we discovered a flaw in how the questions were transmitted from the server to the user – they were encrypted until the moment before they reached the user’s computer. This allowed for a window of opportunity to intercept each question.”

BlackBerry’s team developed code that would take the question in plaintext, search it on Google, and automatically input the search results into the game. They then used the code to win 50,000 pounds in less than an hour. After returning the money to the gaming company, they walked the company through the exploit – including how to defend against it.

They did this for several applications on the company’s website, but also tested its overall security posture.

“We weren’t just looking for technical vulnerabilities in the apps,” explains McDowell. “We were looking for exploitable, vulnerable business processes. For example, were we able to open an account without address verification? Are there measures in place to detect and mitigate unusual activity?”

“Our tests were about showing our client where their blind spots were, and helping eliminate them,” he adds.



The team also carried out a test phishing campaign. They created an email address that looked like that of the IT Director, and used it to send an email with a link to a dummy program meant to represent malware. They then chose the emails of one hundred people at random to receive that email.

In addition to testing their systems and processes, BlackBerry probed the organisation's retail outlets to determine defenses against social engineering attacks. In one test, the team printed off false lanyards and polo shirts embroidered with the company's logo. They then walked into an outlet and informed the staff they were from central IT and had an update that needed to be installed on the till system.

"A lot of what we did is what's called open-source intelligence," says McDowell. "We looked around the web to see if anyone was talking about the company, to see if anyone had highlighted vulnerabilities within the organisation or its game – it was really an extension of the original groundwork we did."

After locating the gaming company's vulnerabilities, BlackBerry then took it through the processes necessary to fix potential exploits. Finally, the team walked the business through other steps it could take to improve its security posture.

The Results

Working with BlackBerry Cybersecurity Consulting, the company has made itself more secure in two core areas.

Improved Security Awareness: Assessment of the organisation's physical outlets and staff behavior allowed it to develop better security awareness programs for its employees. Workers now understand the different ways a criminal might attempt to use them to defraud the organisation. There are also concrete security processes for the workers to follow in the event of an incident.

Elimination of Vulnerabilities and a Better Response Plan: With BlackBerry's help, the organisation now has a better incident response plan. It has also implemented monitoring solutions to detect behavior that might indicate fraud. Lastly, by taking the organisation through the vulnerabilities in its applications, BlackBerry was able to help it eliminate them, fostering a better organisational understanding of security in the process.

About BlackBerry Limited

BlackBerry Limited is an enterprise software and services company focused on securing and managing IoT endpoints. The company does this with BlackBerry® Secure™, an end-to-end Enterprise of Things platform, comprised of its enterprise communication and collaboration software and safety-certified embedded solutions.

Based in Waterloo, Ontario, BlackBerry Limited was founded in 1984 and operates in North America, Europe, Asia, Australia, Middle East, Latin America and Africa. The Company trades under the ticker symbol "BB" on the Toronto Stock Exchange and the New York Stock Exchange. For more information visit [BlackBerry.com](https://www.blackberry.com), and follow the company on [LinkedIn](#), [Twitter](#) and [Facebook](#).

