

A woman with long dark hair, wearing a light blue blazer, is looking down at a tablet device she is holding. The background is a server room with rows of server racks and blue lighting.

BlackBerry Cybersecurity Consulting

Helping This Agency Secure,
Connect, and Protect its Data

Industry Government
Services BlackBerry®
Cybersecurity Services

At a Glance

Government organisations regularly manage vast quantities of critical data – and this agency is no exception. Having recently established a new data portal designed to foster better access to public sector information, the agency needed to be certain it was still secure. A recent cultural change that saw the agency externalise its IT services, further increased its threat surface, and further complicated matters.

It approached BlackBerry® Cybersecurity Consulting to help evaluate its security posture, identifying weaknesses and ensuring better compliance. 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

For the public sector, cybersecurity is absolutely crucial. Governmental organisations hold every single detail about the lives of their citizens, from health records to birth certificates to social security numbers – and they have a duty of care to keep that information safe. Should they fail in that duty, they can be struck with massive fines, particularly under new regulations such as the GDPR.

This government agency was well aware of that, and approached BlackBerry Cybersecurity Consulting to help ensure it was compliant and secure. At the time, it had recently established a new portal designed to provide easier access to public sector information. It was also dealing with the cultural shift that resulted from a recent decision to outsource its IT department, moving its internal staff to an external organisation.

“There’s a lot of privatisation happening in government,” explains James McDowell, Director of BlackBerry Cybersecurity Consulting. “Agencies do it in the interest of reducing their effective budget. Once outsourced, staff are no longer a core payroll cost.”

“This outsourcing, coupled with the agency’s infrastructure and a changing regulatory environment, caused decision makers to re-evaluate their security posture - and they soon needed help.”



The Challenge

The agency had four key challenges that it faced. First, it operated under considerable budget constraints. Governmental organisations are under constant pressure to do more with less, and to find new and innovative ways to reduce their overhead. As a result, it's rare for an organisation to build its infrastructure to specification.

"The networking hardware and devices the agency uses are much like what you'd expect to find in a commercial office," explains McDowell. "It's not purpose-built, which tends to result in an increased threat surface – one which is more challenging to secure."

In addition to budget constraints, the agency was subject to strict regulations around how their data must be accessed, stored, and secured. They cannot, for example, host any data outside the country. This means that if they were to migrate to the cloud, all the supporting third party infrastructure would have to be within their borders.

In addition to the current regulatory climate, future regulations present an additional challenge, greatly increasing both data protection requirements and the penalties for improper security. With May 2018's GDPR, for example, the penalty for even a minor breach could rise as high as 4% of an agency's annual turnover. It is, says McDowell, a sum that could have a serious impact.

The agency also had to contend with a cultural change that happened internally as a result of its decision to outsource and commercialise its internal IT department. The cohesion between the people responsible for IT security and the organisation they worked for was fractured by this move. The flow of data changed in such a way that the agency was uncertain how to respond. This was further exacerbated by the need for more extensive security training for the agency's workers.

"While breached infrastructure might be the biggest risk organisations such as this one face, the biggest threat are agency staff – outsourced and otherwise," explains McDowell. "People make mistakes. They misplace data, they fall for phishing scams, they use weak passwords and engage in unsafe practices." Decision makers at the agency quickly realised they needed to bring someone in to help them evaluate, review, and renew their security posture. They needed an external expert to help them understand what needed to be done in order to secure both their systems and people. After some discussion, the agency approached BlackBerry.

“Really, what we’ve done is help bring the culture of the people using IT services together. Everyone is a little more security aware, and everyone understands the challenges that everyone else faces.”

James McDowell,
Director, BlackBerry®
Cybersecurity Consulting

The Services

According to McDowell, it was BlackBerry’s long history of working with government agencies that drove the agency’s decision. BlackBerry has a deep understanding of governmental challenges and needs, and employs within its Cybersecurity Consulting team some of the world’s leading security experts. This allowed them to evaluate the agency’s biggest risks, most significant threats, and most critical threat surfaces.

First, the team observationally identified a number of weaknesses in the agency’s physical security. They performed several social engineering tasks where they sent people to agency offices to attempt to gain access to the agency’s network or data. From there, they highlighted the risks, explained how they went about obtaining unauthorized access, and walked the agency through what it needed to do to prevent such an attack in the future.

“In most cases, physical security tests are as simple as walking up to the front desk with a good story and getting access,” says McDowell. “They’re meant to highlight failures where procedures might exist but aren’t being adhered to.” The BlackBerry Cybersecurity Consulting team also examined the agency’s systems from a technical point of view, highlighting weaknesses in technical defenses and security processes like patching and updates. As with physical security, the team advised members of the agency on how best to protect its threat surface.



The Results

By identifying risks and assisting in developing mitigation strategies, BlackBerry has helped the agency enhance its overall security posture. This enhancement has taken several forms.

A Significant Reduction in Risk: The agency has made everyone it works with significantly more security aware. By fostering a mutual understanding between different departments, the agency has been able to develop a long-term plan to enhance their posture over a period of time. This has, in turn, allowed it to achieve a demonstrable reduction in risk, as data loss is no longer as significant a threat.

Easier Compliance with Government Regulations: Thanks to BlackBerry's help, the agency is now able to comply with the strict regulations surrounding protection of its data. More importantly, it's prepared for upcoming changes in its regulatory climate such as the GDPR.

Integrity of Information: Last but certainly not least, the agency can now say with certainty that its threat surface is smaller. Its systems are properly patched and monitored, the flow of data between the agency and its external partners is fully protected, and weaknesses in its infrastructure have been identified and mitigated.



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](#).