Case Study:

A Safe Bet with Better Digital Security

April 17, 2018 / Cai Broughton. Account Manager SIRC.

Ontario Lottery and Gaming (OLG) Corporation is responsible for regulating lottery, casino and other gaming services in the province of Ontario, Canada; with $6.7B CAD in revenue (2012).

With such a vast amount of customers OLG were unfortunately targeted by a cyber-attack in 2016 at one of its Casino Resorts. But this heist didn't involve the taking of finances, it was raw data the attackers were after. Specifically the personal and private information of the customers of OLG.

"Overall we've seen a rise in attacks targeting gaming institutions like casinos," said J.Paul Haynes, CEO of eSentire, a Cambridge, Ont.-based managed security provider. "In cases like this where hackers have targeted and obtained sensitive personally identifiable information (PII) like social insurance numbers and credit card information, the effects of a breach can be felt for months and sometimes even years; usually the information ends up for sale on the dark web. With over 3 million customers per year and more than 2000 staff and a number of third party vendors, thousands of individuals could be impacted. All former and current customers and employees should remain vigilant and monitor their accounts for compromise."

It's a high price to pay for a lapse in security. And OLG have been implementing specific measures to heighten their security on premise, with tools like facial recognition software and a shared data base system for its multiple sites to draw resources from. Its' attention to detail and commitment to security, player safety and excellent service have earned OLG the highest possible recognition:

The Ontario Lottery and Gaming Corporation (OLG) has attained the highest level of recognition for its Responsible Gaming (RG) program from the World Lottery Association (WLA). OLG becomes just the fifth gaming operator in North America and one of only 22 in the world to achieve Level 4 accreditation from the WLA.

But despite all this, malicious hackers are finding a way to expose new exploits and holes in the security of lottery and gaming companies and they're doing it by hitting a previously un-suspected target. Breaches of data are now happening from areas previously unimaginable to even the most secure industry players.

Employee devices and external access are now an extremely exploitable hole in the networks of major companies.

This is all due to the changing way we now do business. With the advent of smart phones and computers and tablets becoming so affordable that…

The average number of connected devices per consumer is 3.64

…we're now living in a world where our private un-secured and under prepared personal electronics are increasingly becoming our medium to operate in our workplaces. The 'Bring Your Own Device' (BYOD) culture means we communicate, work, download, upload and report on a multitude of devices, from desktops, to laptops, to tablets and smartphones. It's an unavoidable change, since its effect on productivity is so high and these devices have become an indispensable asset in every other facet of life. There's no going against the grain for companies who want to operate as efficiently and optimally as they can. However the unfortunate downside to this is that when you increase the number of platforms you work from you increase the number of entrance points to be hacked from.

A survey completed by Ernst & Young (A Washington DC based Business Management Consultant) found:

- 57% of organizations consider the most likely source of an attack to be employees.
- 56% of enterprises believe they are unlikely to detect a sophisticated threat.
- On average, 2,000 or more unsafe, malicious apps are installed on large enterprise employees' mobile devices.
- 35% of employees store their work passwords on their smartphone.

The biggest concern most businesses have over adopting a BYOD strategy centers around security. According to a survey by Security Intelligence, the largest security issue is the risk of losing enterprise data.

These risks can take many forms, including:

- Lost, stolen or unauthorized access to devices
- Attacks and threats, such as malware, scams and fake apps
- Endpoint Security and compliance for personal devices that are accessing the company's network

The problem of security for BYOD becomes even more Relevant when you consider these statistics

It's a more relevant issue in today's technology landscape than ever, as 2016 experienced some of the worst cyber-attacks recorded so far.

With 4.2 billion records stolen in that year alone, which is an increase of 3.2 billion from hacks recorded in 2013, our concern about the dangers posed by hacking are unfortunately justified. But if you think 2017/2018 will come in dramatically safer, Thanks to an enormous Equifax breach that affected 143 million Americans (or 43.9% of everyone in the country) in 2017, the stats are still being counted but 2017 might possibly be worse than 2016.

It's a perfect combination of security vulnerability: The hackers are more present than ever before, because data is more informative than ever before and now thanks to a changing culture of BYOD, vulnerable data is more available than ever before.

With all this in mind the most highly rated and secure solution for digital file management is the only acceptable option.

So when it comes to secure solutions, look no further than Blackberry's highly rated and highly secure applications. Independent studies on a range of digital software producers found that Blackberry scored high across a range of features for its implementation of cross platform security implementation.

BlackBerry is the only vendor to receive highest scores in all six use cases of the Gartner Critical Capabilities for High-Security Mobility Management

1. **High-Security Government Grade**
2. **High-Security Commercial**
3. **Shared Data**
4. **Shared Devices**
5. **Nonemployee**
6. **Bring Your Own**

As well as testimony from the research groups, Blackberry also brought a personal touch to the security architecture of an online gaming company after they faced exploits after outsourcing their work to third party developers.

"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?"…

All vital questions to be answered when it came to finding the exploits in the system for this Gaming Company. The adaptive approach taken as well as the more unconventional and creative methods led to a more secure and profitable environment for OLG.

Whether it's the excellent features already built in to their file management software or the extra level of attention they pay to each customer based on the unique aspects of their industry, **Blackberry brings it to the table when it comes to securing vulnerable data.**

Within these features and options lies the solution to your ongoing data management needs. And SIRC is here to help provide the architecture to those building blocks and construct the fortified response your business or organization is looking for. Our expertise in the specialization of data solutions will be at your disposal in the design, implementation and support of your new security and file sharing structures. Working with your current system or introducing a fresh approach to provide the solution that best adapts to your needs.

We are here to help you secure your data and provide informative reports on just where and to whom your data is being shared.

Our methodology is as simple to understand as it is impossible to disagree with; it's your information, so you should know where it's going.