A Safe Bet with Better Digital Security

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

Employee devices and external access are now an extremely exploitable hole in the networks of major companies and with customer data on the line, the stakes couldn't be higher.

The way we now do business has changed. With the advent of smart phones and computers and tablets becoming so affordable, 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 the medium we use 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

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:

High-Security Government Grade, High-Security Commercial, Shared Data, Shared Devices, Nonemployee and Bring Your Own

As well as testimony from the research groups, Blackberry also bought a personal touch to the security architecture of an online gaming company when they noticed several weak spots in their system 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. Blackberry's adaptive approach to finding exploits meant no method was off the table. Customized code for their websites digital security solution provided means to search commonly used methods to test their vulnerability were integrated seamlessly. And even more unconventional and creative methods…

In addition to testing their systems and processes, BlackBerry probed the organization'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 organization 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.

Blackberry's experience in re-orienting employees to provide their own security methodology when handling vulnerable and sensitive information is where their level of expertise reaches beyond the normal digital security architecture. 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.