

Monitoring Firm Communications

Most IT Policies allow a firm to monitor all communications including BlackBerry's.

It is always useful to be reminded that communications conducted on firm equipment can be monitored and used as evidence if needed.

Recently, CIBC filed suit against a groups of former employees who left the bank to start a new business. The bank alleges that the employees stole confidential information and attempted to recruit employees prior to their departure from the bank. CIBC submitted as evidence, email and PIN to PIN messages sent between the BlackBerry users. This is the first time that BlackBerry specific messages have been used as evidence.

BlackBerry

Contrary to popular opinion, PIN to PIN messages are not private if the firm uses a BlackBerry Enterprise Server (BES). In addition to PIN messages, the BES can also monitor BlackBerry Messenger and SMS messages. The BES server will create a log for each device and, in some cases, even has a facility for emailing the results to a given address at whatever time frequency is desired. Thus, complete BlackBerry activity can be monitored and reported on for a single user or for the entire firm. Firm's wishing to step up the monitoring of their communications can employ these features.

If the firm's BlackBerry's are integrated using a carrier's Web site (eg. Rogers, Bell, Telus), then the PIN messages are not monitored - at least not by the firm.

Web Sites

Firms can also monitor and log information on the Web site habits of its users. The firm's firewall typically monitors the web sites that have been visited. Additional software on the network can monitor and block sites on the Internet by user. Logs can be useful for tracing the source of malware which can then be blocked from entering the firm. They can also be useful for monitoring or blocking the use of time consuming web sites such as Facebook and My Space.

Email

Email can be monitored at the firewall or through an email content filtering system. Most email systems contain basic monitoring which shows who is sending a message to whom. This is useful for tracing message delivery. But with further software, the entire message content can be monitored or even altered before sending - for example, to remove inappropriate language. Many firms add a disclaimer before or after all messages sent by the firm. Depending on the sophistication, that software can do a lot more in terms of monitoring email communications.

It is also possible to access any employees email by configuring their profile on an alternate machine. In most cases, all that is required is the user's password. Thus, if a firm needs to locate email evidence it is fairly easy to access.

Conclusion

If communications monitoring is important to a firm, the technology tools exist to facilitate it for almost all electronic forms of communication. If you are an end user, assume that all communication through firm equipment is monitored.

Charles Bennett is the Principal Consultant of Triella, a technology consulting company specializing in providing technology audits, planning advice, project management and other CIO related services to small and medium sized firms. Triella is a BlackBerry Alliance Partner. Charles can be reached at cbennett@triella.com or 647.426.1004. For additional articles, go to <http://www.triella.com/publications.html>.

© 2008, by Triella Corp. All rights reserved. Reproduction with credit is permitted.