Sunshine Technology Team

Meeting 10/14/09

1:44 pm

- Deputy Attorney General Joe Jacquot introduced himself and thanked everyone for their interest. He emphasized that the AG is "both pro- technology and pro open government."
- This "fact finding mission" is to learn how to use the tools of technology in order to do what the taxpayers want and do it in the open.
- Today's presentation is from Research in Motion.
- The next (date TBA) will be voice over IP and instant messaging.
- The third will cover social networking.
- Florida's public records laws are sound and strong.
- This is an open meeting. We want attendance, questions, and involvement.
- In Attendance: Joe Jacquot, Bill Stewart, Alexis Lambert, Florence Snyder, Sarrah Troncoso, Sam Morely, Sharyn Smith, Deborah Stevens, Nelson Hill, Nelson Munn, Ramin Kouzekhani, Mike Russo, Dave Taylor.
- From Research in Motion: Jack Plating, Mark Zentz, David Coley.
- Mark Zentz: The blackberry is a platform, not just a device in your hand.
- David Coley: RIM established a paradigm of enterprise managed wireless.
- Fast voice and data networks, fast processors, memory and audio/video applications.
- Wireless push= standard for mobile smart phones
- Users demand both business and personal capabilities. Smart phones are a "lifestyle tool."
- Huge increase in capabilities means security of mobile solutions is more important than ever.
- Multiple communication options: emails, phone, PIN, SMS, social networking, instant messaging.
- Biz value of options: a connected employee = a more effective/productive employee
- Increased flexibility offers better quality of life and increased job satisfaction.
- Crisis Communications: On 9/11/01, voice networks were saturated, SMS was unreliable, email potentially unavailable
- PIN to PIN was often the only option
- Increasingly social networking and IMing are likely to play a role.

The Government Challenge

- Maintain flexibility alongside transparency

- Some agencies created policy templates for blackberry. (Example: the DoD STIG)
- The Blackberry Enterprise Solution: securely connects mobile users to corporate apps and data
- Optimized data for wireless performance and handheld efficiency.
- Provides CIO approved management
- BIS solution (less secure)
- Get email from cloud-based service
- No controls like password or encryption or auditing requirements

Blackberry Message Flows

Device ----encryptionkey--→ wireless carrier------→ BB infrastructure--→ internet --→ firewall-→ BB enterprise server--→ email server B--→inbox

Blackberry Internet Service: Message Flow

PC-→ email server-→ BBI/BIS-→ wireless carrier--→handheld B

PIN to PIN: message flow

Blackberry A (encryption key is the same on both devices)-→wireless carrier-→ BB infrastructure--→wireless carrier--→Blackberry B

PIN = unique identifier

Blackberry doesn't capture PIN traffic w/o law enforcement. Wireless carriers can.

Management/Logging/Auditing:

IT policy- there are over 450 options (passwords, automatic timeouts)

Organization policies can be applied to devices.

Application Control: is done with the server, not the consumer side. Allows admins to regulate which apps you can/can't use. (Brick Breaker vs. a travel log)

SMS, phone, PIN to PIN

- Can you log SMS traffic? YES.
- You can disable SMS messages, disable phone call log, and disable PINS
- All logging is done to a comma separated text file on the BB enterprise server

BB Messenger (IM type environment)

- Messenger audit email address
- Configure with destination email address to enable blackberry messenger auditing
- Messenger audit max report interval default is to report every 168 hours if no messenger traffic
- Messenger audit report interval
- Packet files: there are apps available to make them searchable
- GWAVA provides interface for logging/organization of PIN to Pin messages
- Also redaction of PINs is an issue

Deborah Stevens: concern is that in order for agencies to log all PINS consistently. A third party product may be the way to go.

Coley: Government and Sarbanes-Oxley both motivated structural changes for PIN logging

Dave Taylor: Are XML files possible for logging? Yes.

Where are the risk points of losing content?

Network is like email. It's queued temporarily when device sends.

BB Messenger is stored in a digest.

GWAVA cost is typically 60% of the cost of licensing your agency BBs.

Social networking and public IMing

- You can allow public IM services
- Disable public social networking apps
- Disable public photo sharing apps
- Disable RIM value-added apps

App Control Policy

- Use to control/specifically block individual 3d party applications
- SMS/PIN, phone, IM have value. They all provide flexibility and valuable communication options for government.
- Internal application policies can control external apps.
- If one party is a BB, conversation is logged on BB enterprise server.
- You can restrict browser paths and force users to use the proxy so same policies on desktop browser can apply to a handheld.

- SMS rides on the same circuits voices do.
- PIN messaging uses data packets and can be a good fallback in times of emergency or crisis.
- Communication Assistance for Law Enforcement= CLEA
- Question re: GPS and BBs. Problems with packets w/o connectivity (especially in the Panhandle.) Some devices triangulate, others use GPS. Legacy devices don't have GPS, but carriers are opening up more.
- Need to address non-BB users as well.
- Suggestion: agency collaboration for an enterprise solution instead of each one doing something different.
- DOT has 2000+ regular text enabled cell phones that aren't BBs.
- Need to consider how employees will archive/delete files in accordance with administrative rules.
- Also redaction issues.
- Technology won't plug every hole. We need our employees to have integrity.
- GSA- General Services Admin- has a popup to opt in or out of records management.

Adjourned 3:10 PM.