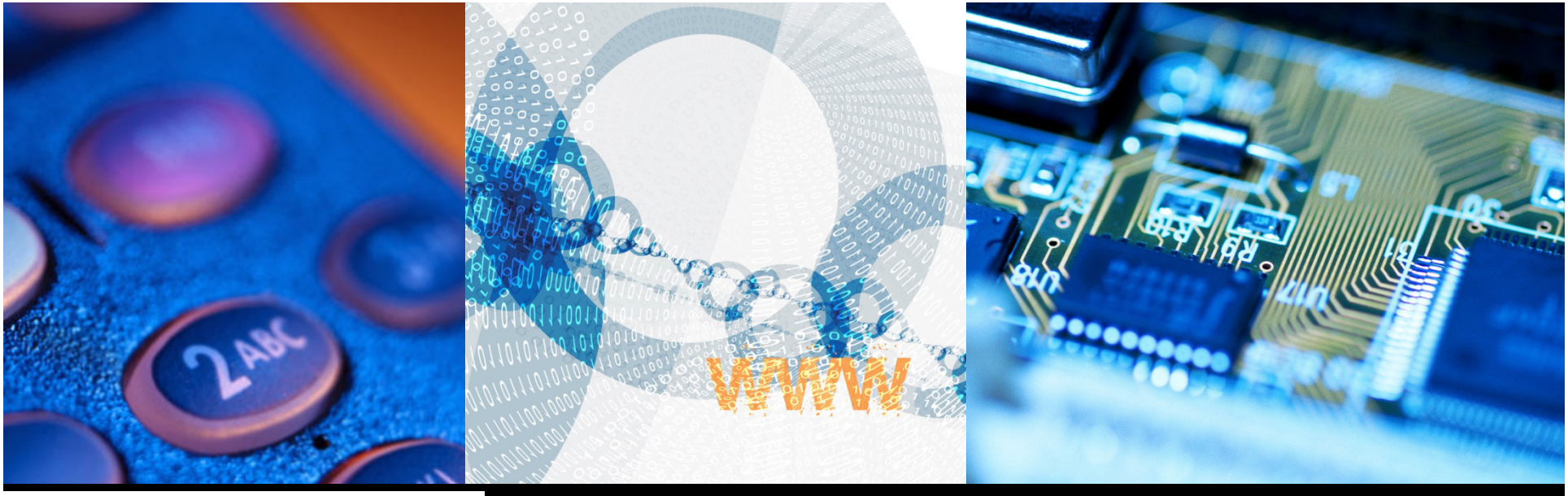

Secure Web Delivery

Ron Miller – PIM Manager

BCCS
Keeping You Connected

BCCS
Keeping You Connected

McAfee Email Gateway (MEG)

- Implemented new MEG solution in January 2014
- Enterprise mail routing, virus protection, SPAM filtering, DOS protection with Quarantine Services
- Allows for more security for outbound messages by providing tools to ensure email is traveling securely. Secure Web Delivery being one of them.

BCCS
Keeping You Connected

TLS - Transport Layer Security

TLS

- Encrypts the email while in transit
- More recipient domains are using TLS by default
- TLS is accepted as a form of transferring Sensitive Data Securely.
- Transparent to end user. Clients have no idea TLS is happening in the background since email is received and viewed normally.
- Only secures email data during transportation not data at rest within recipient's email system.

BCCS
Keeping You Connected

Major Providers using TLS

- Gmail.com
- Yahoo.com
- Aol.com
- Comcast.net
- Hotmail.com
- Msn.com
- Live.com
- Outlook.com

BCCS
Keeping You Connected

Email Delivery

Server Delivery Options

- Internal Enterprise Exchange email travels TLS
- Opportunistic TLS
  - Asks to do TLS first, if TLS not available will send clear text with no encryption between sender and recipient servers
- Required TLS
  - TLS connection has to be coordinated with both parties for secure email to be delivered
  - If TLS is disabled on the receiving end, messages are rejected
- Secure Web Delivery (SWD)
  - Allows us to place further controls against email traveling to external domains.
  - It ensures email either travels TLS or is retained on our SWD servers.

Client Encryption Options

- Entrust PKI
  - Message is Encrypted at Desktop and sent. Can only be decrypted by intended recipient(s). With this, the delivery method isn't as important
- Password Protect
  - Password protecting attachments is not ideal since there are password crackers. Body of message is still clear text if it cannot deliver TLS

BCCS
Keeping You Connected

McAfee Secure Web Delivery (SWD)

- McAfee SWD is used if the email being transmitted meets the requirement to be secured via trigger word in the subject line.
- The secure word chosen is #secure#
  - Not case sensitive
  - Any part of the subject: ex: *Here is the patient information #secure#*
  - Have also included the most common misspellings (#sucure#, #sercure#, #sacure#, #scure#, #secrue#)

BCCS
Keeping You Connected

McAfee SWD Pull Method

- McAfee SWD receives the outgoing email and attempts TLS first. If it can't send TLS then it uses the McAfee Secure Web Delivery Pull Method.

- Web Pull Method
  - With pull delivery, the secure email message is stored on the McAfee Email Gateway, and, after receiving a notification, the external recipient must log into their Secure Web Mail account and "pull" the message from the McAfee Email Gateway.

BCCS
Keeping You Connected

How it Works (Web Pull)

1. Email is sent out from end user with #secure# anywhere in subject.
2. McAfee Email gateway sees the #secure# and passes it to the SWD server.
3. McAfee SWD checks to see if message can be delivered TLS. If it can, it delivers the original email to recipient's mailbox.
4. If McAfee SWD cannot deliver via TLS, it keeps the message locally and sends an email to the user with a link to retrieve the message.

BCCS
Keeping You Connected

How it Works (continued)

5. Recipient is sent a welcome message to self register if they haven't already been registered.
6. Once successfully registered, they can view the secure email from SWD server.
7. Once viewed, users can:
   - Reply
   - Print
   - Delete
   - Leave message on server
   - Read messages will expire in 60 days
   - Unread messages will expire in 30 days
   - Messages cannot be forwarded
   - Attachments can be opened and saved locally.

BCCS
Keeping You Connected

Who Can use SWD service

- Any of the 54 Entities we provide email services

- Any Entity we provide Perimeter email delivery.
  - However, if their email system is not setup with TLS; they could receive email via SWD pull method.

BCCS
Keeping You Connected

Future SWD Features

Pattern based SWD

- Searches for trigger patterns in the subject/content/attachments of the email
- SSN, Drivers License #s, Credit Cards #s
- False Positives

BCCS
Keeping You Connected

Other PIM services

- Enterprise Exchange Email services
- Enterprise-class Email Perimeter defenses
- Enterprise Archiving vault services
- Mobile Messaging Services
- Email Journaling
- File Transfer Utility with email functionality
- Email List services
- Enterprise Electronic Fax Services
- Electronic Stored Information (ESI) Request Tracking System

BCCS
Keeping You Connected

SWD on BCCS service Catalog

- http://www.illinois.gov/bccs/services/catalog/hosting/swd/Pages/Default.aspx
- http://www.illinois.gov/bccs/services/catalog/hosting/swd/Pages/SWD-FAQ.aspx

Thank You

BCCS
Keeping You Connected