The Encryption Enigma

October 9, 2012

Underwritten by:

axway

www.meritalk.com
Two years ago, WikiLeaks posted 400,000 pages on the Iraq War that the Pentagon called “the largest leak of classified documents in its history.”* The problem? Nearly 4.9 million people have access to classified U.S. government information.** Nearly all of those also have access to email.

Feds think encryption, among other security measures, should keep sensitive data safe. But what if encryption isn’t the answer? What if encryption – especially encryption deployed at the desktop – is part of the problem?

MeriTalk surveyed 203 government information security managers and email managers to better understand the potential threats associated with email encryption and digital signatures.

“The Encryption Enigma Report” captures insights from those who know the topics best and gauges their awareness of, and attitudes toward, email security and encryption issues.

• Federal agencies run on email:
  • A Federal agency sends and receives 47.3M emails daily*
  • The Federal government sends and receives a whopping 1.89B emails daily**

• We built walls… …and then we dug a new tunnel:
  • Nearly 90% of Federal agencies say the email security policy changes they made following the release of sensitive information on WikiLeaks improved their overall email security***
  • 83% provide users with the ability to encrypt outbound email at the desktop

• The Encryption Enigma:
  • Email encryption at the desktop is supposed to improve security…
  • …but it might make security worse. 80% of Federal information security managers fear data loss through encrypted email; and 58% state that encryption makes it harder to detect data leaving

• Way forward:
  • Feds point to improved end-user training (55%); advanced email security technology (54%); and improved end-user security policies (47%) as ways to overcome email security challenges

*According to email managers **Assuming 40 primary Federal agencies ***Of those who made changes to their email security policies, n=92
Daily, a *Federal agency* sends and receives, on average:

**47.3M** emails*

For the *Federal government*, that’s an average of:

**1.89B** emails per day**

*According to email managers **Assuming 40 primary Federal agencies

**Take Away:** Federal Agencies Run on Email
While cyber security is a top priority in nearly all agencies, just one in four rate the security of their current email solution an “A”.

79% say cyber security is a top IT priority for the next 12 months*

39% say it is the top IT priority**

However, just one in four agencies rate the security of their current email solution an “A”.

Take Away: On The Inside Looking Out…

*Respondents who ranked cyber security an 8-10 on a scale of 1-10, where 1=not at all a priority and 10=top priority **Those who ranked it a 10

What is the assessment of the internal threat vs. the external threat?

Just 45% of Feds made changes to their email security policies because of sensitive data published on sites like WikiLeaks.
• Despite security measures, Feds say standard work email is the #1 way unauthorized data leaves their agency

**Current security measures:**

- 83% provide users with the ability to encrypt outbound email
  - DoD: 92%
  - Civilian: 74%

- 86% provide the capability to validate digital certificates
  - DoD: 93%
  - Civilian: 78%

**Still:**

In which of the following ways does unauthorized data leave your agency?

- Standard work email: 48%
- Agency-issued mobile device: 47%
- USB flash drives: 40%
- Personal email: 38%
- Personal mobile devices: 33%
- Web-based work email: 23%

*According to those who know their agency’s status **Respondents asked to select all that apply

**Take Away:** …While the Inside is Leaking Out
Most agencies (84 percent) believe that they are safe, and that their email gateways support the inspection of desktop-encrypted email. True if:

- Agencies can validate all email users
- Agencies have proper email policies in place
- Users follow correct email policies

Except just 69 percent of agencies have issued PIV cards

Except 47 percent of agencies cite the need for better email policies

Except 45 percent of agencies report that employees don’t follow the policies

In fact, even if these three conditions are met, agencies may be unable to enforce email policies unless their email gateways explicitly decrypt and scan desktop-encrypted email.

Take Away: Three Strikes and the Information is Out
Information security managers say that email encryption is a threat. Email and file transfer managers are not convinced.

<table>
<thead>
<tr>
<th></th>
<th>Info security managers:</th>
<th>Email managers:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are you concerned with the possibility of data loss prevention (DLP) violations embedded in encrypted emails?</td>
<td>80%* yes</td>
<td>36%** yes</td>
</tr>
<tr>
<td>Does encryption make it harder for your agency to detect when valuable or sensitive information is leaving?***</td>
<td>58% yes</td>
<td>47% yes</td>
</tr>
<tr>
<td>Does encryption make it harder to track down information after it leaves?***</td>
<td>61% yes</td>
<td>47% yes</td>
</tr>
</tbody>
</table>

Mixed reviews:

“Encryption is the best way to safeguard sensitive info. We will continue to use it and perhaps use it to a greater extent.”

“Encrypted email is a security and operational problem. The more layers you add, the slower the [review].”

**Take Away:** Is It or Isn’t It?
Info security managers: In the next five years, do you expect email encryption to become a more or less significant security problem for Federal agencies?

- **51%** More significant
- **37%** Stay the same
- **12%** Less significant

Approximately one in four Feds see email encryption as a problem today.

Take Away: A Stitch in Time Saves Nine Congressional Hearings
The National Institute of Standards and Technology (NIST) recommends that agencies digitally sign emails and provides standards for successful implementation, so why aren't more agencies doing it?*

Are users in your organization required to digitally sign emails?

**Take Away:** Close the Gap

- Feds, especially civilian agencies, also clear digital signature policies.

In your opinion, what are the biggest barriers to a secure Federal email system?*

- Lack of budget: 46%
- Lack of employees adhering to security policies: 45%
- Rise of mobile technologies: 30%
- Lack of training: 29%
- Lack of clear agency security policies: 22%
- Lack of control over email flow in/out of the agency: 21%
- Rise of bring your own device (BYOD): 20%

*Respondents asked to select all that apply

Take Away: Solutions Exist; Agencies Must Capitalize
What do agencies need in order to *overcome* email security challenges?*

- Improved end-user training (55%)
- Advanced email security technology (54%)
- Improved end-user security policies (47%)
- Greater collaboration between information security/email professionals (33%)
- Improved understanding of information entering/leaving agency (30%)
- More budget dedicated to email management (26%)

*Respondents asked to select all that apply*
Recognize the encryption threat

Protect data from both sides

Get started today: don’t wait for a mandate to make changes
MeriTalk, on behalf of Axway, conducted an online survey of 203 Federal government information security and email managers in June and July 2012. The report has a margin of error of +/- 6.84% at a 95% confidence level.

<table>
<thead>
<tr>
<th>Title:</th>
<th>Organization:</th>
</tr>
</thead>
<tbody>
<tr>
<td>3% Chief/Deputy CIO</td>
<td>50% Federal Civilian</td>
</tr>
<tr>
<td>1% CIO</td>
<td>50% Federal DoD</td>
</tr>
<tr>
<td>1% CSO</td>
<td></td>
</tr>
<tr>
<td>14% ITD</td>
<td>100% are involved with information assurance, cyber security, email management, or handling of large file transfers.</td>
</tr>
<tr>
<td>2% E/FD</td>
<td></td>
</tr>
<tr>
<td>6% E/FA</td>
<td></td>
</tr>
<tr>
<td>51% ITS</td>
<td></td>
</tr>
<tr>
<td>20% P/PM</td>
<td></td>
</tr>
<tr>
<td>2% ESSM</td>
<td></td>
</tr>
</tbody>
</table>
Thank You

Erin Leahy – MeriTalk
eleahy@meritalk.com
(703) 883-9000 ext. 139

MeriTalk
The Government IT Network

www.meritalk.com