

The Encryption Enigma

October 9, 2012

Underwritten by:

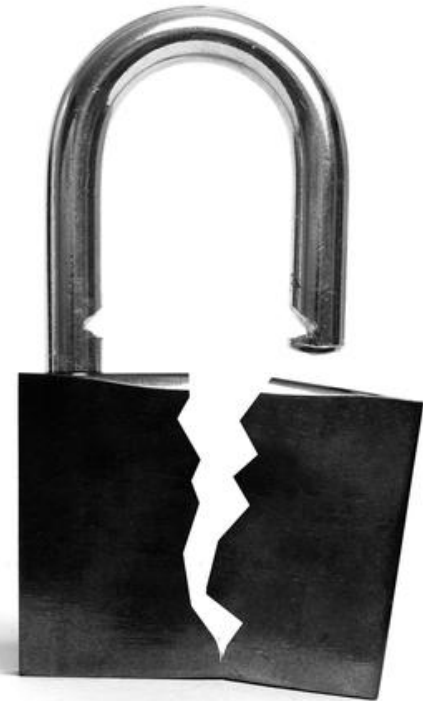


Two years ago, WikiLeaks posted 400,000 pages on the Iraq War that the Pentagon called “the **largest leak** of classified documents in its history.”* The problem? Nearly 4.9 million people have access to classified U.S. government information.** Nearly all of those also have access to email.

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

- Federal agencies send and receive massive amounts of email each day

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**



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”



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.

Take Away: On The Inside Looking Out...

- Despite security measures, Feds say standard work email is the #1 way unauthorized data leaves their agency

Current security measures:*



provide users with the ability to encrypt outbound email



provide the capability to validate digital certificates



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%

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

*Except just **69 percent** of agencies have issued PIV cards*

X

Agencies have proper email policies in place

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

X

Users follow correct email policies

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

X

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

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

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?

- Information security experts point to a concern today; a crisis tomorrow



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

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?



More
significant



Stay
the same



Less
significant

Take Away: A Stitch in Time Saves Nine Congressional Hearings

Other Concerns: Digital Signatures

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

*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?**

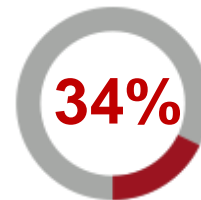
Are users in your organization required to digitally sign emails?



ALL USERS



SOME USERS



NONE



UNSURE

DoD:

57% All users

16% None

26% Some users

1% Unsure

Civilian:

13% All users

52% None

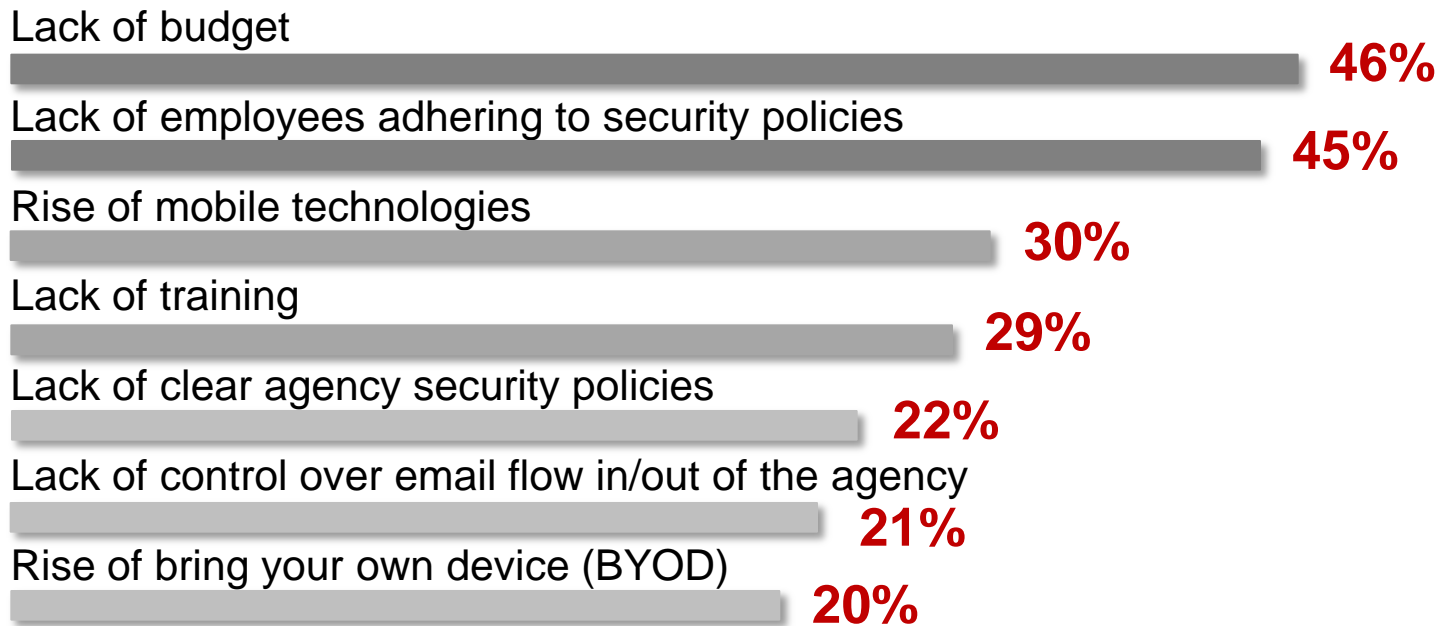
31% Some users

4% Unsure

Take Away: Close the Gap

- Feds point to lack of budget and employee discipline as the top barriers to securing Federal email


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



Take Away: Solutions Exist; Agencies Must Capitalize

- It's not all about Federal mandates and regulations – to improve, agencies must upgrade training, tech, and policies

What do agencies need in order to **overcome** email security challenges?*

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

Take Away: Many Enhancements within Feds' Control

- ✓ Recognize the encryption threat
- ✓ Information security and email professionals: talk to each other
- ✓ 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

Title:

3%	Chief/Deputy Chief Information Officer
1%	Chief/Deputy Chief Technology Officer
1%	Chief or Deputy Chief Information Security Officer
14%	IT Director/Manager
2%	Email/File Transfer Director/Manager
6%	Email/File Transfer Administrator
51%	IT Supervisor, Specialist, or Engineer
20%	Program/Project Manager
2%	Email Support Services Manager

Organization:

50%	Federal Civilian
50%	Federal DoD

100% are involved with information assurance, cyber security, email management, or handling of large file transfers.

Thank You

Erin Leahy – MeriTalk

eleahy@meritalk.com

(703) 883-9000 ext. 139



www.meritalk.com