DKIM Deployment At Cisco

John N. Stewart

Chief Information Security Officer

Agenda

- Phishing: A Dangerous Security Problem
- Phishing for Cisco Accounts
- Our Response
- Messaging Infrastructure Overview
- Our DKIM Deployment
- Results So Far / Next Steps

Phishing

- Phishing has quickly surpassed Spam as a more dangerous email threat.
- Previously high value domains like Banks, Paypal, and Ebay were targeted.
- But that is changing…

From: Accounts@metrobanc.com
To: "Metrobanc Account Holder"
Subject: Your profile needs updating

Dear Sir/Ms:
In a recent audit, we discovered that your account profile needs updating. Please visit the following link to enter your most recent Information.

http://update.metrobonc.com

Update Department

Cisco.com Phishing

- **Non-financial targets are being phished now.**
- **There have been attempts to phish Cisco.com accounts.**
- **Increase in targeted attacks (“spear phishing”).**
- **Attacks have gotten smarter. The latest variants have attached Trojan executables to the email.**

Subject: Important Notification
From: administrator@cisco.com
Date: Mon, 27 Jun 2005 02:37:32 +0800

Dear Valued Member,

According to our site policy you will have to confirm your account by the following link or else your account will be suspended within 24 hours for security reasons.

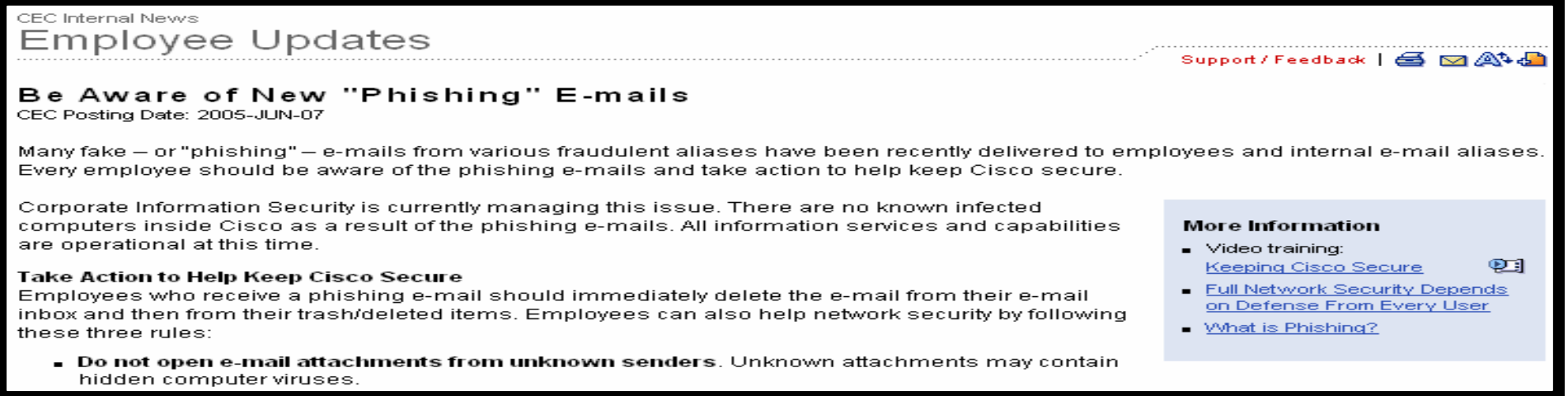
http://www.cisco.com/confirm.php?email=xxxxxx

Thank you for your attention to this question. We apologize for any inconvenience.

Sincerely,
Cisco Security Department.

User Education is Not Enough

- To combat the phishing, we have attempted to raise awareness about the issue.
- But that has led to a new problem…



CEC Internal News

Employee Updates

Support / Feedback |

Be Aware of New "Phishing" E-mails

CEC Posting Date: 2005-JUN-07

Many fake – or "phishing" – e-mails from various fraudulent aliases have been recently delivered to employees and internal e-mail aliases. Every employee should be aware of the phishing e-mails and take action to help keep Cisco secure.

Corporate Information Security is currently managing this issue. There are no known infected computers inside Cisco as a result of the phishing e-mails. All information services and capabilities are operational at this time.

Take Action to Help Keep Cisco Secure

Employees who receive a phishing e-mail should immediately delete the e-mail from their e-mail inbox and then from their trash/deleted items. Employees can also help network security by following these three rules:

- **Do not open e-mail attachments from unknown senders**. Unknown attachments may contain hidden computer viruses.

More Information

- Video training: Keeping Cisco Secure
- Full Network Security Depends on Defense From Every User
- What is Phishing?

How Can You Tell?

From: donotreply@cisco.com
[mailto:donotreply@cisco.com] Sent: Saturday, June 18, 2005 9:03 AM
To: xxxxxx (xxxxx@cisco.com)
Subject: Please Revalidate User Access Request

Hi,

Resource User accounts require your approval for their continued access.

The Resource User's manager/supervisor has already approved their access to the resource(s). Now as the Resource Approver,you must also approve/revalidate their access.

Please use the URL listed below to approve the user's access in the OnRamp system:

http://url.cisco.com/reset

Legitimate Request?

Subject: Important Notification
From: administrator@cisco.com
Date: Mon, 27 Jun 2005 02:37:32 +0800

Dear Valued Member,

According to our site policy you will have to confirm your account by the following link or else your account will be suspended within 24 hours for security reasons.

http://www.cisco.com/confirm.php?email=xxxxxx

Thank you for your attention to this question. We apologize for any inconvenience.

Sincerely,
Cisco Security Department.

Legitimate Request?

To the end-user both emails “look” the SAME!

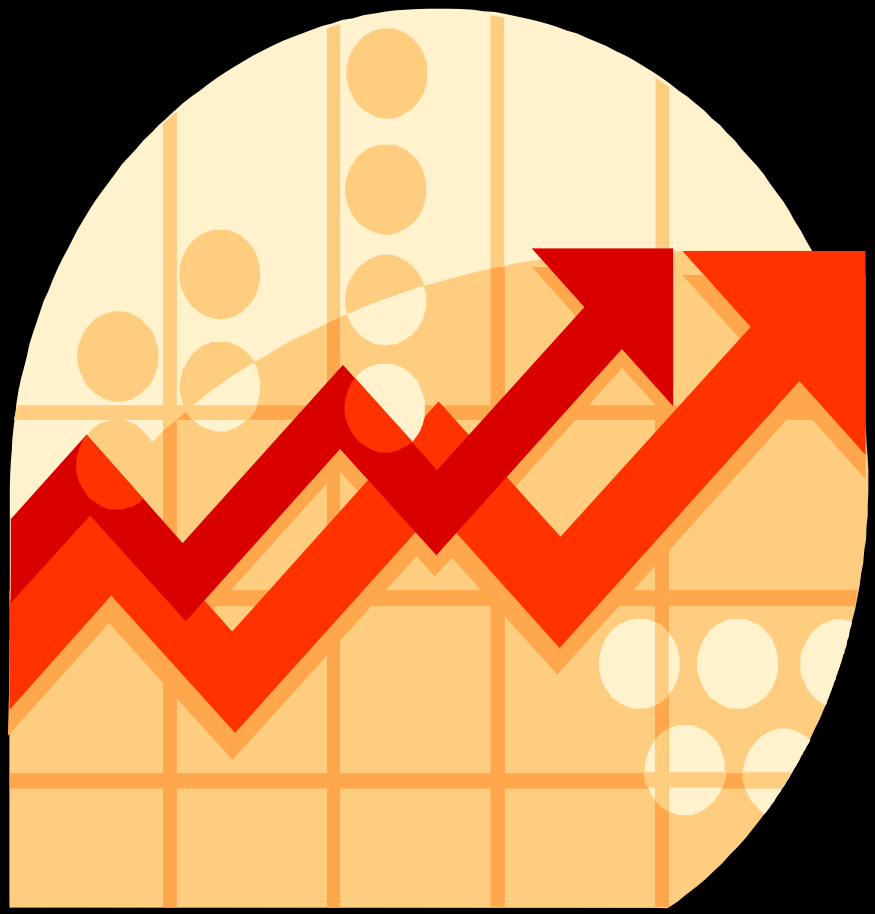
DKIM Can Help

- The DKIM project was initiated as a way to authenticate email coming from the cisco.com domain.
- By authenticating, we are hoping to see the following benefits:
  - Sign IT application email with DKIM.
  - Outside domains can verify valid cisco.com email.
  - Forged cisco.com email can be identified.
  - Warn employees about forged email (Cisco or other DKIM protected domains).

DKIM Project at Cisco

Cisco Messaging Stats

- Approximately 5.2M messages inbound on a daily basis. (72% identified as SPAM)
- Approximately 4.6M messages intercompany and outbound on a daily basis.
- Process approximately 6M messages on a daily basis (5.2M * 28% Inbound Not Spam + 4.6M internal and outbound).



DKIM Project Checklist

- Establish Project Goals
- Communicate Intent and Obtain Support
- Establish Policy
- Inventory Mail Flows
- Determine Architecture
- Maintain and Control
- Results to Date
- Lessons to Date
- Timeline
- Next Steps

DKIM Project Goals

- Don't break email!
- Verify all inbound messages.
- Sign all outbound messages.
- Sign all IT application generated emails.
- Warn end-users about messages that fail verification.

From: administrator@cisco.com
Date: Mon, 27 Jun 2005 02:37:32 +0800
Subject: [CISCO UNVERIFIED] Important Notification

Dear Valued Member,

According to our site policy you will have to confirm your account by the following link or else your account will be suspended within 24 hours for security reasons.

http://www.cisco.com/confirm.php?email=xxxxxx

Thank you for your attention to this question. We apologize for any inconvenience.

Sincerely,
Cisco Security Department.

Communicate Intent & Establish Policy

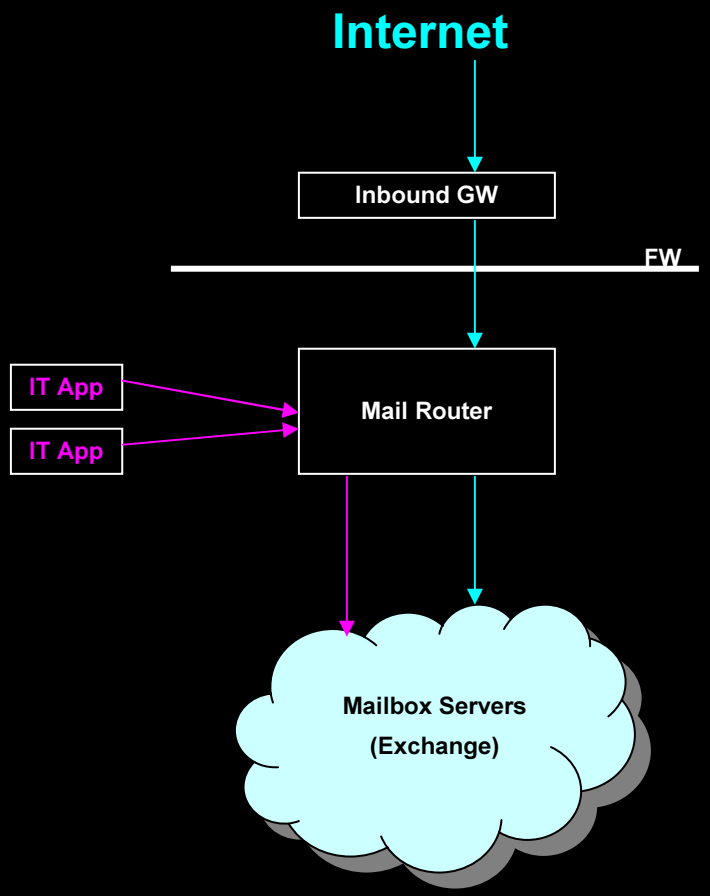
- **Discuss intent with key stakeholders:**
  - Client support groups
  - Infosec
  - IT Infrastructure (messaging support organization)
  - Marketing
  - Partner support groups
- **Establish Policy:**
  - All outbound emails will be signed.
  - Outsourced marketing campaigns must comply.

Inventory Mail Flows

- What are the sources of email?
  - Official mail servers
  - "Lab" or "test" servers
  - Application email
  - Sales & Marketing
  - Case Management
  - Corporate/Investor Relations
- What/Where are the end destinations?
  - Corporate Intranet
  - DMZ
  - Forwarded to partners

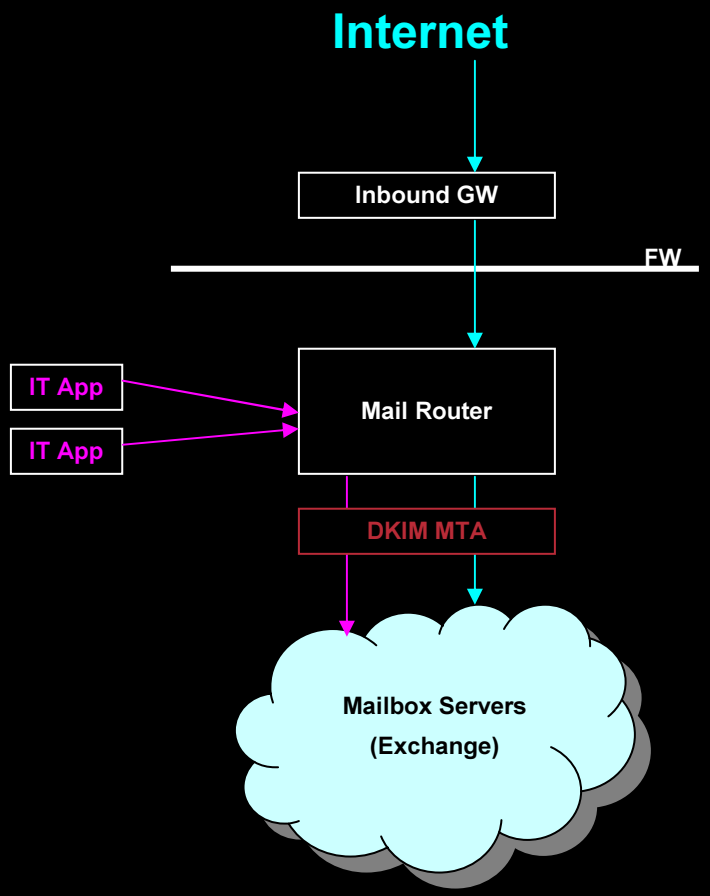
Determine Architecture: Cisco's Messaging Infrastructure

- Cisco uses a traditional 3 layer mail infrastructure:
  1. Inbound Gateway
  2. Routing Layer
  3. Mailbox Cloud (Exchange)
- Internal applications send through routing layer.



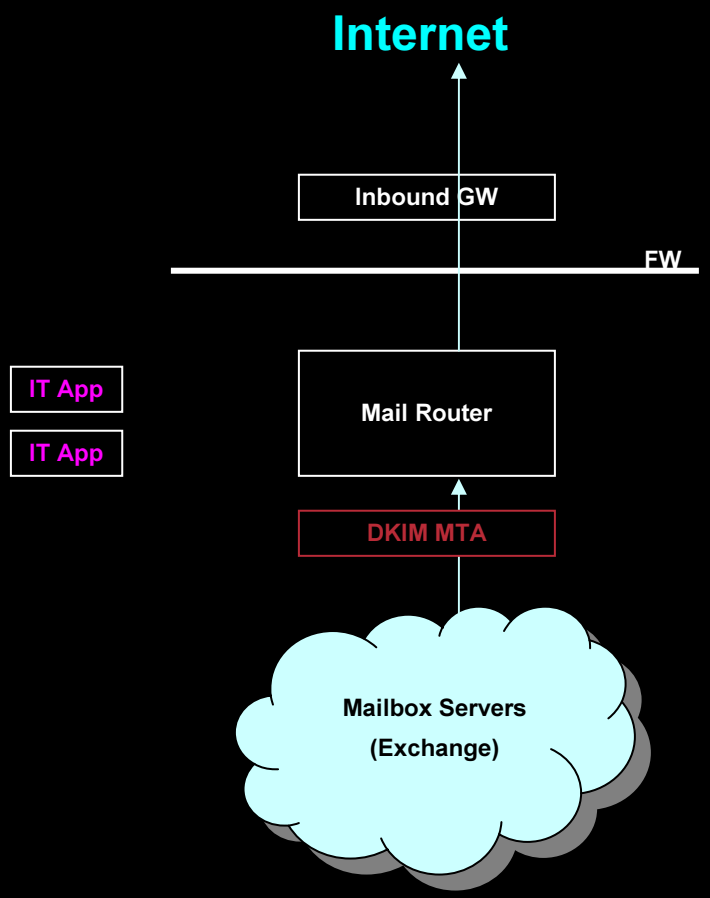
Determine Architecture: Inbound and Intercompany Flows

- Project architecture calls for addition of DKIM enabled MTA after the routing layer.
- Messages originating outside will be DKIM verified.
- Messages originating inside will be DKIM signed.
- DKIM MTA will not only perform signing & verification, but also munge the Subject: line if needed.



Determine Architecture: Outbound Flows

- Messages leaving cisco.com will flow through DKIM MTA.
- As a result, message will be DKIM signed.



Maintain and Control

- Block outbound SMTP access for unknown hosts.
- Outbound SMTP request includes notification to email group.
- Alert Infosec and Messaging Group when a Cisco message fails verification.
- Regularly communicate policy with all sending sources.

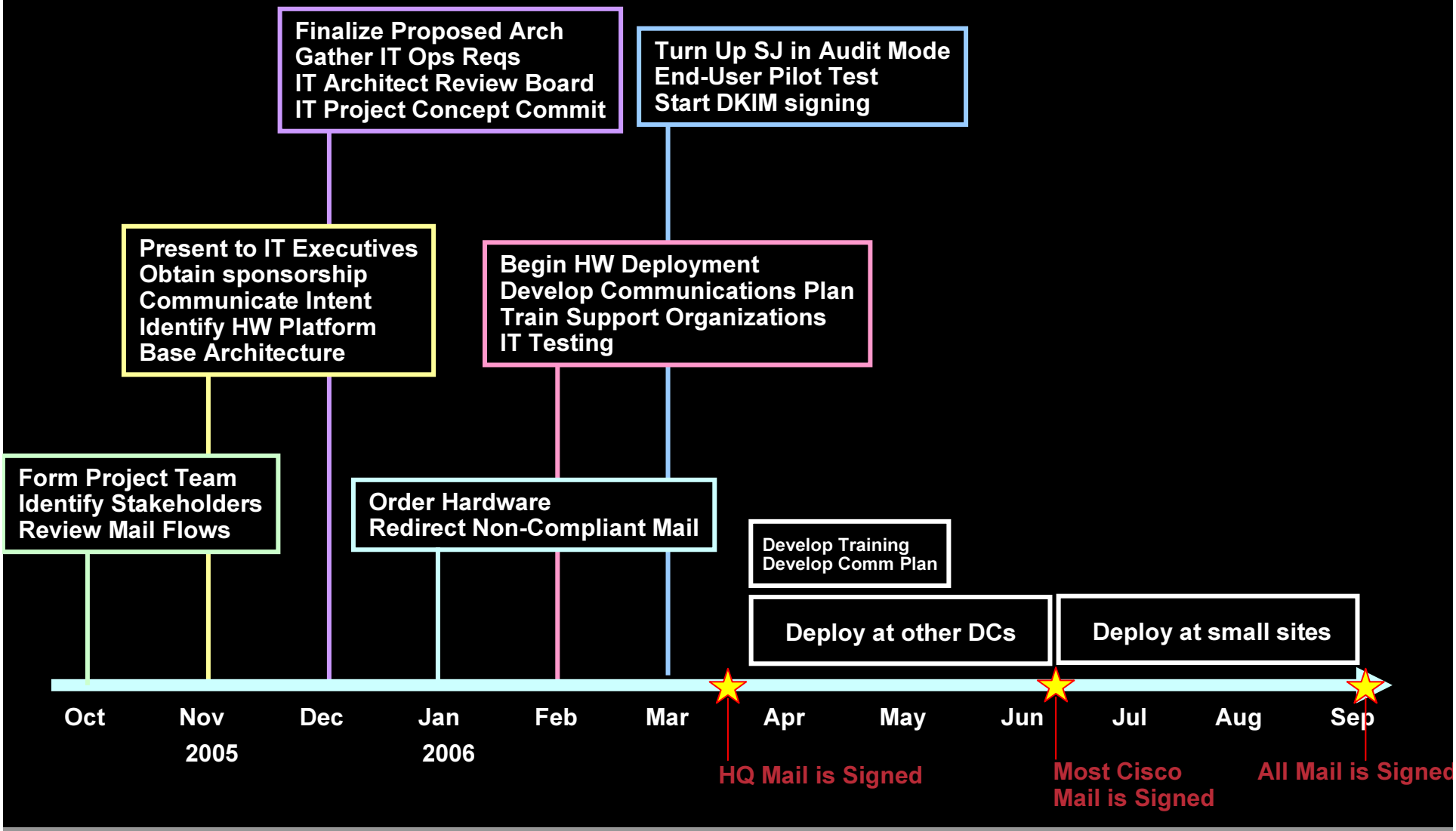
Results to Date

- DKIM MTA hardware and software has been identified.
- HW spec is dual 3.4GHz Xeon Linux system.
- This platform to provide 3X the capacity of our current mail flow.
- 24 systems to be deployed worldwide. This is actually overkill from a capacity standpoint, but makes sense from a networking perspective.
- Project to deploy DKIM has executive sponsorship and has been through internal IT review boards.
- Project has been through project commit. Machines are being staged as we speak.

Lessons To Date

- DKIM deployment requires the participation of many different groups:
  - –Messaging Group
  - –Infosec
  - –DNS
  - –Client Support Group
  - –Marketing/Sales Organization
  - –eCommerce Support Group
  - –Partners Support Group
- There are “rogue” or undocumented mail servers in the infrastructure.
- Would be nice if email clients supported DKIM natively.

Timeline



Next Steps

- San Jose (Cisco's HQ) will be the first site to start DKIM signing. Estimated go-live date is March 2006.
- Followed by major datacenter sites (RTP, Amsterdam, and Sydney): Q2CY06.
- Project wrap up at small regional sites: Q3CY06.
- Run Pilot Program
- End-User Communication

Next Steps

- **Soon Cisco mail will look like this!**

```
From: John N. Stewart <john@cisco.com>
To: Mary Smith <msmith@example.net>
Content-Type: text/plain
Message-Id: <1098727240.13184.0.camel@dkim-it.cisco.com>
Mime-Version: 1.0
Date: Wed, 25 March 2006 11:00:40 -0700
Content-Transfer-Encoding: 7bit
DKIM-Signature: a=rsa-sha1; d=cisco.com; s=march2006;
  i=john@cisco.com; c=nowsp; q=dns; t:1098727241; x:10988893641;
  h=Subject:From:Date;
   b=QQgUTUMvDA1BPxxIpSrAiAUXB5rtOt4tJT1BcN3zB01pUARhybDLGF7KLU7ens
  Wie1Zcm7+h5lfOhYvuy3DUTQ==;

Cisco is now signing messages with DKIM!

-John
```

Q and A