Duo at BU

Our two-factor authentication plan…

BOSTON UNIVERSITY

Tom Grundig - Information Security, Boston University

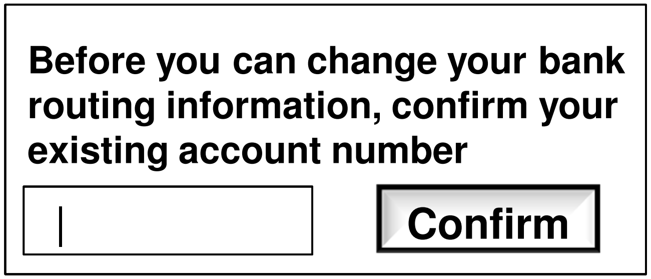
- Information Security Operations Manager
- SAP Security & GRC Lead
- Former Asst. Dir of Internal Audit
- Duo Project
    - A little of this, a little of that…

Where we left of last…

- We got phished. Bad.
- People were tricked by a believable e-mail message into giving their passwords to the bad guys
- Spear-phishers and their tactics
  - Message crafted for BU
  - Sent to a small number of selected people
  - Strike on weekends & holidays, when you are less protected
- Goals
  - To collect information that will let them steal money:
  - Passwords, social security numbers,
    bank account or credit card numbers

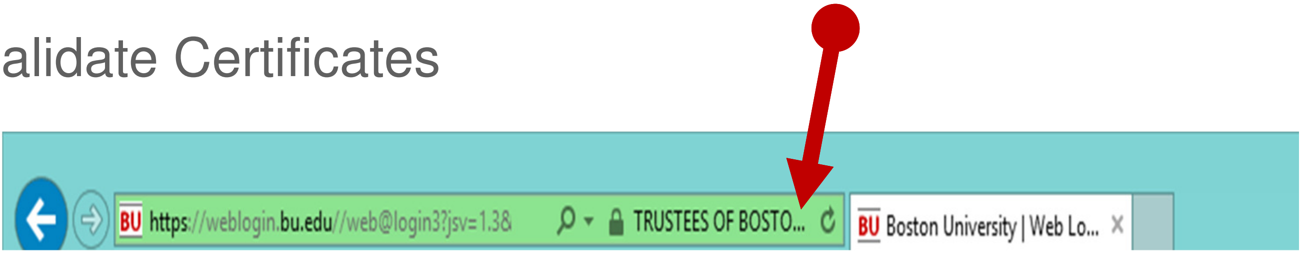
Response – Short-term

- Creation of a notification tool that to alert users when you're their direct deposit account or home address is changed
- Requiring you to enter the existing bank account be entered before it can be changed



Before you can change your bank routing information, confirm your existing account number

- Revamp Spam Assassin Code
- Extended Validate Certificates



BU https://weblogin.bu.edu//web@login3?jsv=1.38
TRUSTEES OF BOSTO...
BU Boston University | Web Lo...

Response – Long-term - Goals

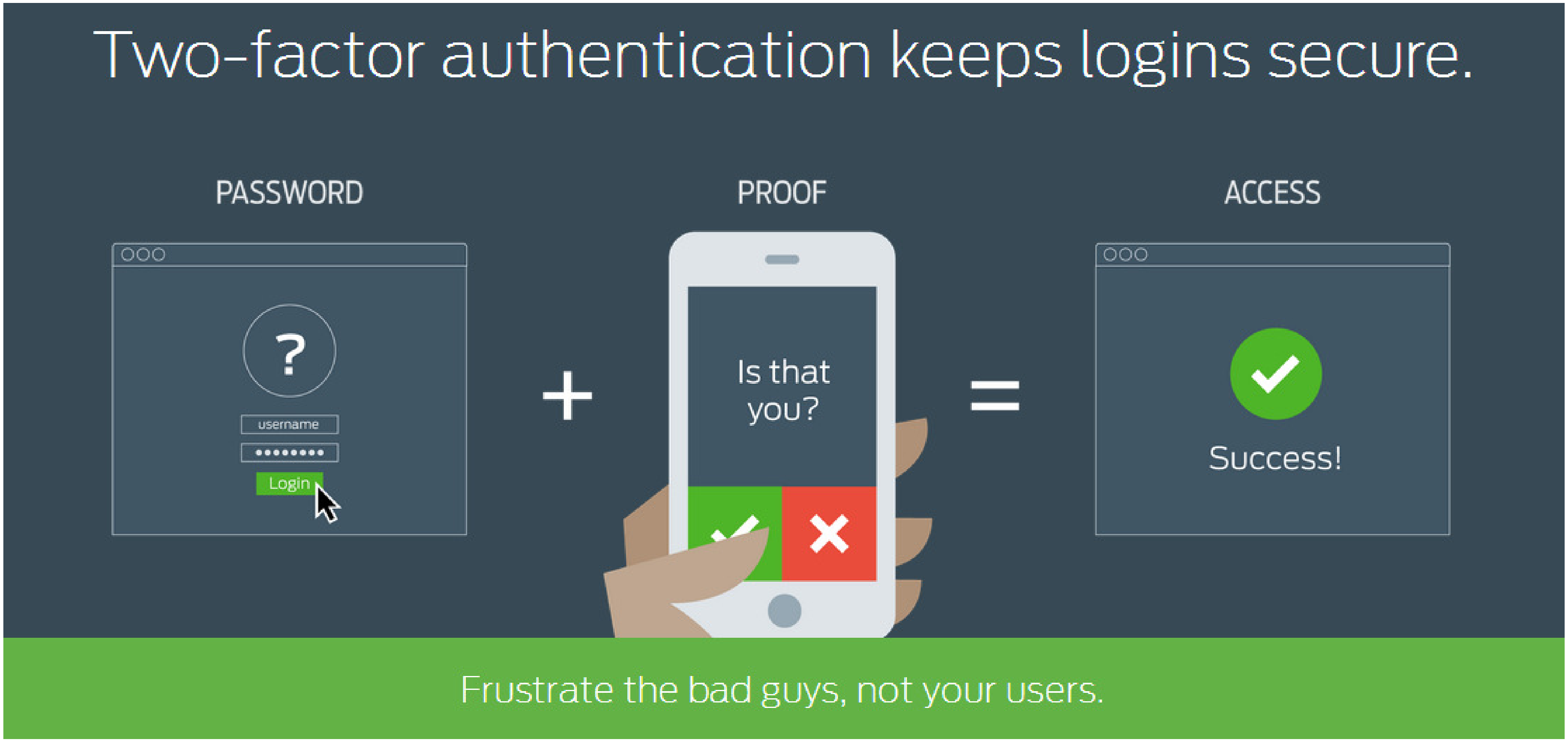
- Address problem, not the symptom
  - Problem – Compromised credentials
  - The only real defense is to use something more than just knowledge
- Integrate with current authentication plans
- Modern and flexible option
- Rapid deployment
- Easy to administer and support
- Affordable
- Need a ‘Big Win’

Response – Long-term - Challenges

- Social/Political
  - Unions, Faculty, Past History
- Technical
- Short Timeframe
  - Needed to act while issue was fresh
- Potential Costs
- Can’t be seen as a ‘Road block’

Two-Factor Authentication

…for everyone

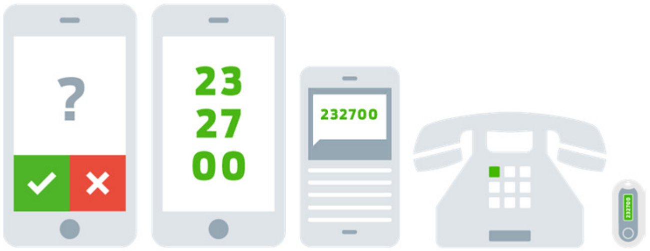


Two-factor authentication keeps logins secure.

Frustrate the bad guys, not your users.

Duo Security – why it works for us

- Strategic & Affordable
  - From InCommon/Internet2
  - Integrates with our strategic weblogin replacement



- Simple and flexible
  - No tokens required
  - Rapid initial setup
  - Single-button confirmation when using the app
  - Also supports text message, phone calls, tokens and other approaches
  - Can remember a device for 30 days (single-user systems only)
    - Only need to do your two-factor confirmation once a month
  - Work anywhere in the world
  - Can work with no connection

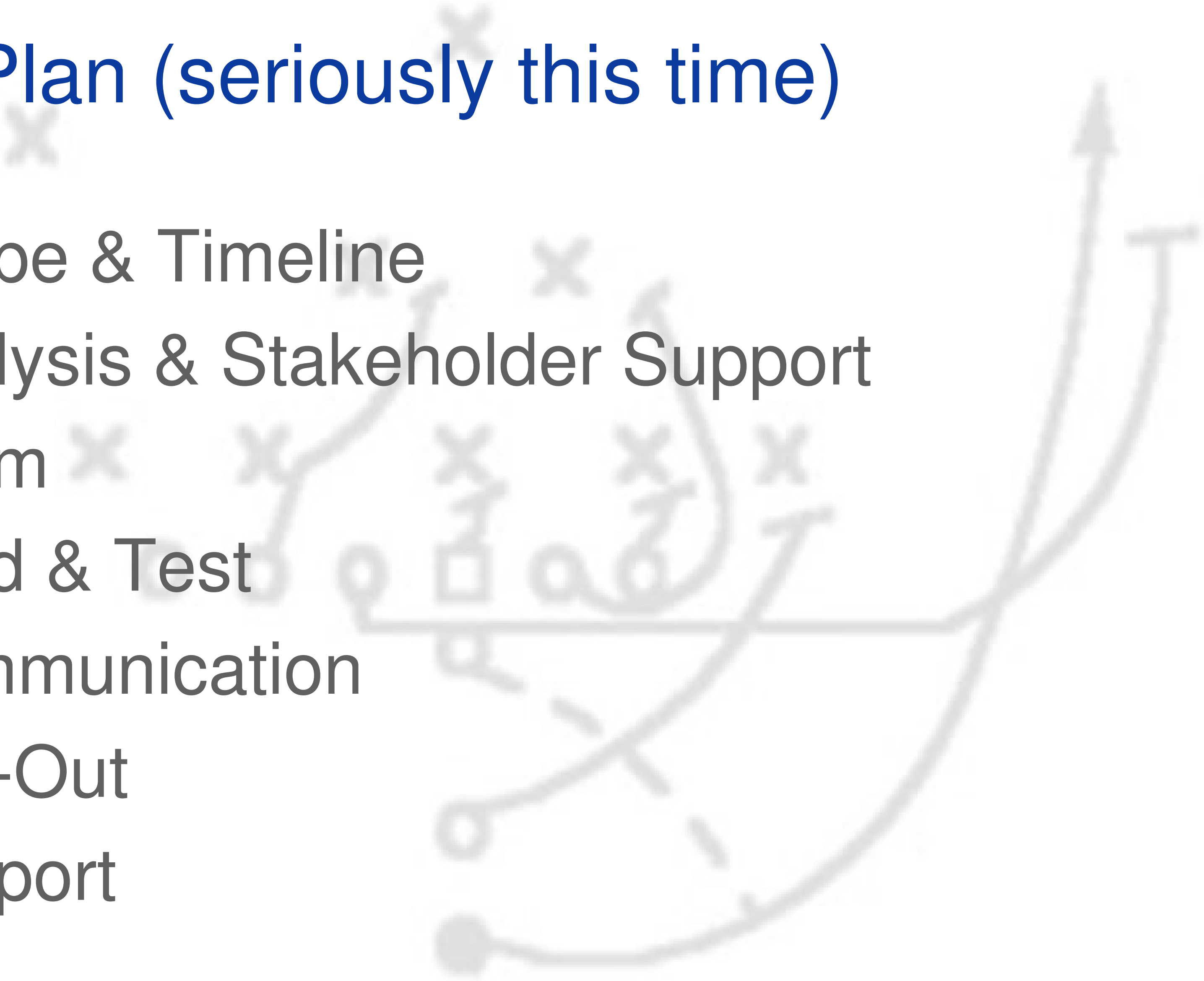
The Plan…

OVERKILL (in a good way)

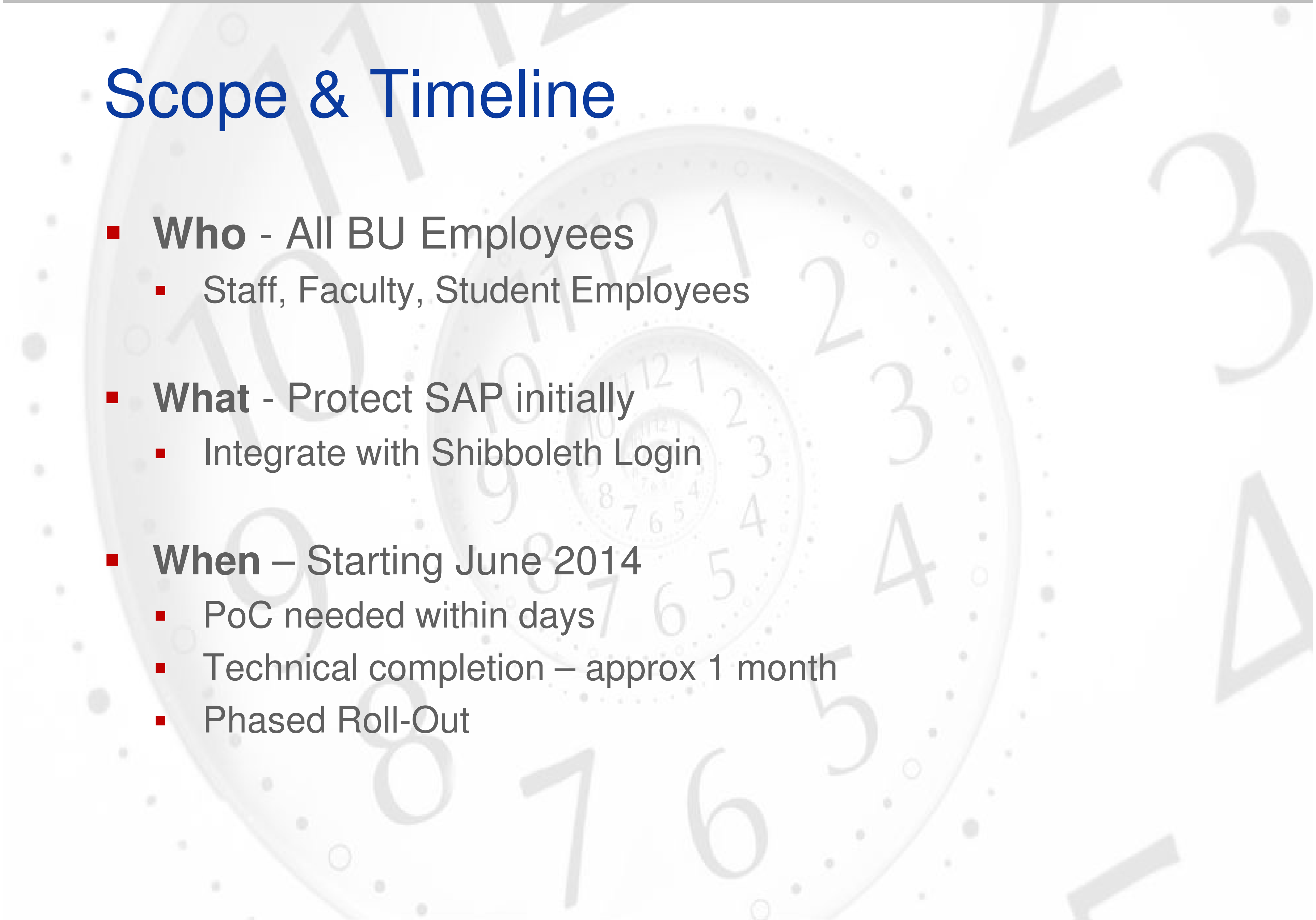
Nothing succeeds like excess.

The Plan (seriously this time)

- Scope & Timeline
- Analysis & Stakeholder Support
- Team
- Build & Test
- Communication
- Roll-Out
- Support



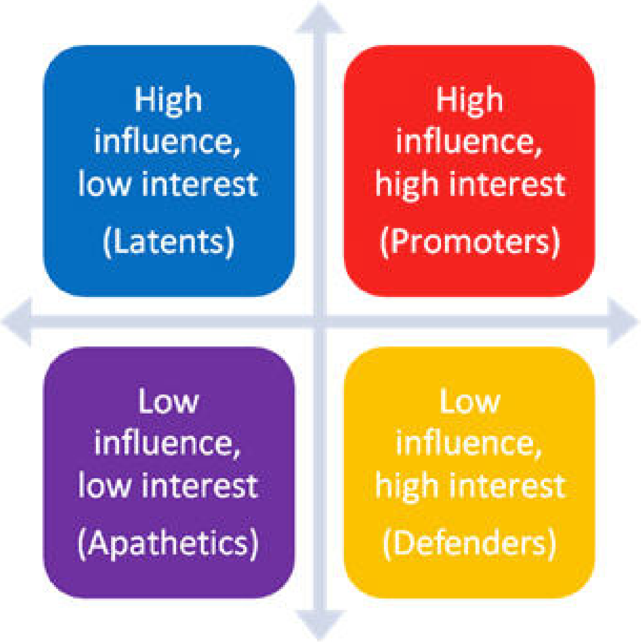
Scope & Timeline



- **Who** - All BU Employees
  - Staff, Faculty, Student Employees
- **What** - Protect SAP initially
  - Integrate with Shibboleth Login
- **When** – Starting June 2014
  - PoC needed within days
  - Technical completion – approx 1 month
  - Phased Roll-Out

Analysis and Stakeholder Support

- Analysis – Technical as well as Social/Political
- Support from the highest levels
  - President
  - Sr. VP for Financial Affairs
  - VP of Information Services & Technology
  - Exec Dir. of Information Security
- Reviewed with Council of Deans as well as Key Business Units



High influence, low interest

(Latents)

High influence, high interest

(Promoters)

Low influence, low interest

(Apathetics)

Low influence, high interest

(Defenders)

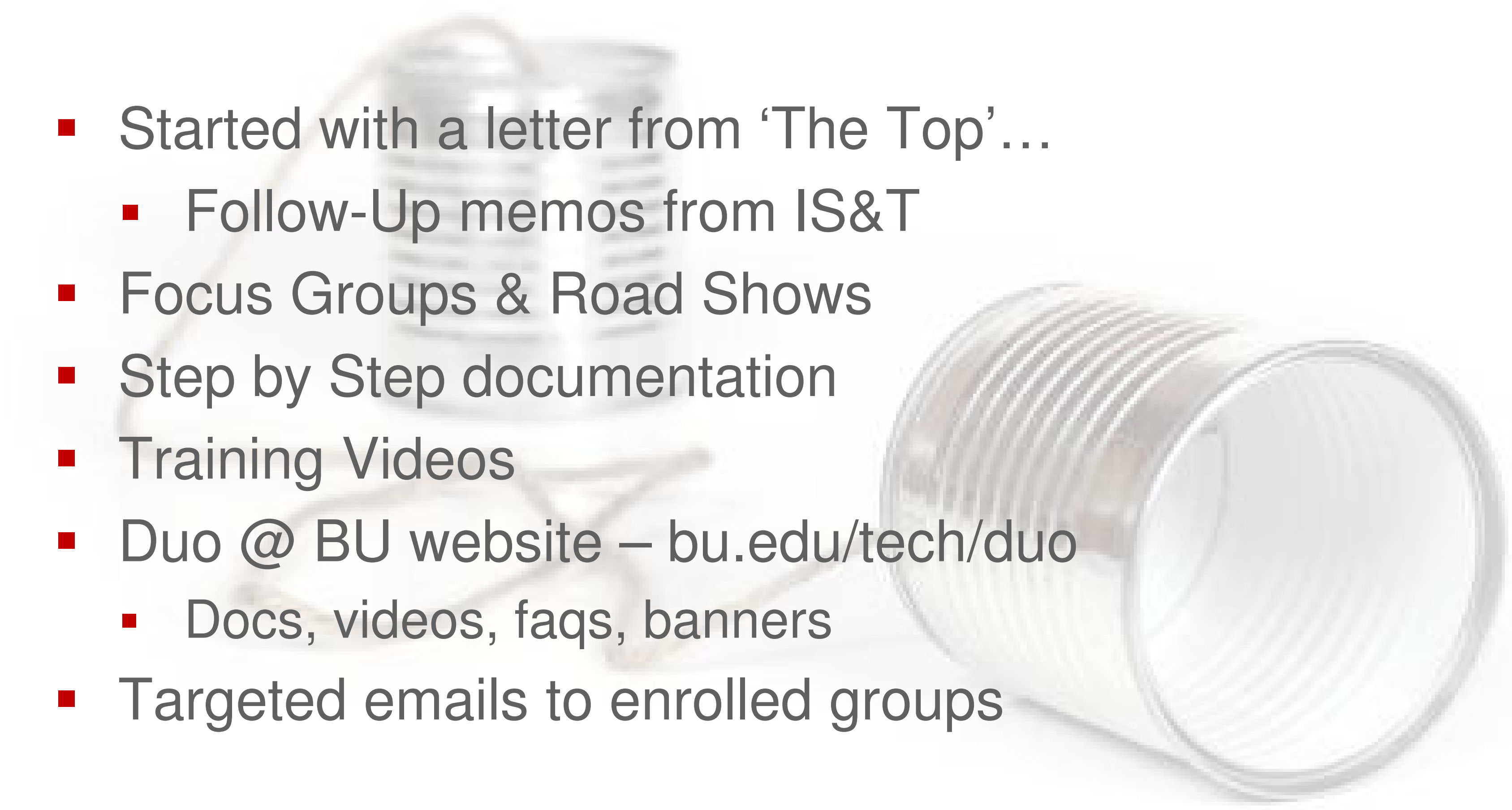
The Team

- Internal Experts in various areas
  - Project Management
  - Architecture and Engineering
  - Identity & Access Management
  - Process and Operations
  - Business Area Input & Audit
  - Quality Assurance
  - Documentation and Training
  - Communication
  - Service Desk

Build & Test

- Infrastructure Layout
  - F5 load balancer in front of 3 Centos 5 VM instances with short-term source IP affinity to ensure that entire IdP transaction occurs on same instance.
  - Each instance has 2 vCPUs and 4G of memory and standard disk allocation (64G).
  - Kerberos passwords are validated using our campus MIT Kerberos 5 servers while attribute resolution uses OpenLDAP servers with a copy of our campus database.
- Software Stack
  - Oracle Java 1.6
  - Tomcat 7.0.21
  - Shibboleth IdP 2.3.3
  - Duo integration is out of the box using the instructions at: https://www.duosecurity.com/docs/shibboleth
  - Only Boston University change was our branded login page.
- Cloud Service Considerations
  - Fail closed
  - Back up users
  - Features Changes

Communication



- Started with a letter from ‘The Top’…
  - Follow-Up memos from IS&T
- Focus Groups & Road Shows
- Step by Step documentation
- Training Videos
- Duo @ BU website – bu.edu/tech/duo
  - Docs, videos, faqs, banners
- Targeted emails to enrolled groups

Roll-Out

- June – Pilot - All of IS&T, SAP Support Team and Users with access to regulated data
- July – Open Opt In Period
- September- Staff
- October- Faculty
- November– Student Employees
- …mandatory for any/all users who access SAP

Support

- 70 Duo Administrators (!!!)
  - Information Security
  - Service Desk
  - Desktop Support
  - IT Partners

So…How's it going?

Statistics so far…

- Pilot - 487users
  - 46 tickets in first month (pilot)
- Opt In (7/7-today) - **941 have opted in** (*360 on first day*)
  - Staff 58%
  - Faculty 28%
  - Student 14%
  - 77 tickets
- 1428 devices
  - 729 iOS
  - 291 Android
  - 20 Windows Phone
  - 9 BlackBerry
  - **244 Landline**
  - **135 Other**

What’s Next

- Duo to replace all current 2nd Factor tools
  - NC-Pass (Mainframe)
  - Defender (Quest Terminal Services)
- Duo’s potential for new services
  - Win RDP, VMWare, Cisco, RADIUS…

Questions?

buinfosec@bu.edu

www.bu.edu/infosec