UNIVERSITY OF
SOUTH CAROLINA

MULTI-FACTOR AUTHENTICATION PROJECT

James Perry, CISO
Jeremy Parrott, Deputy CISO

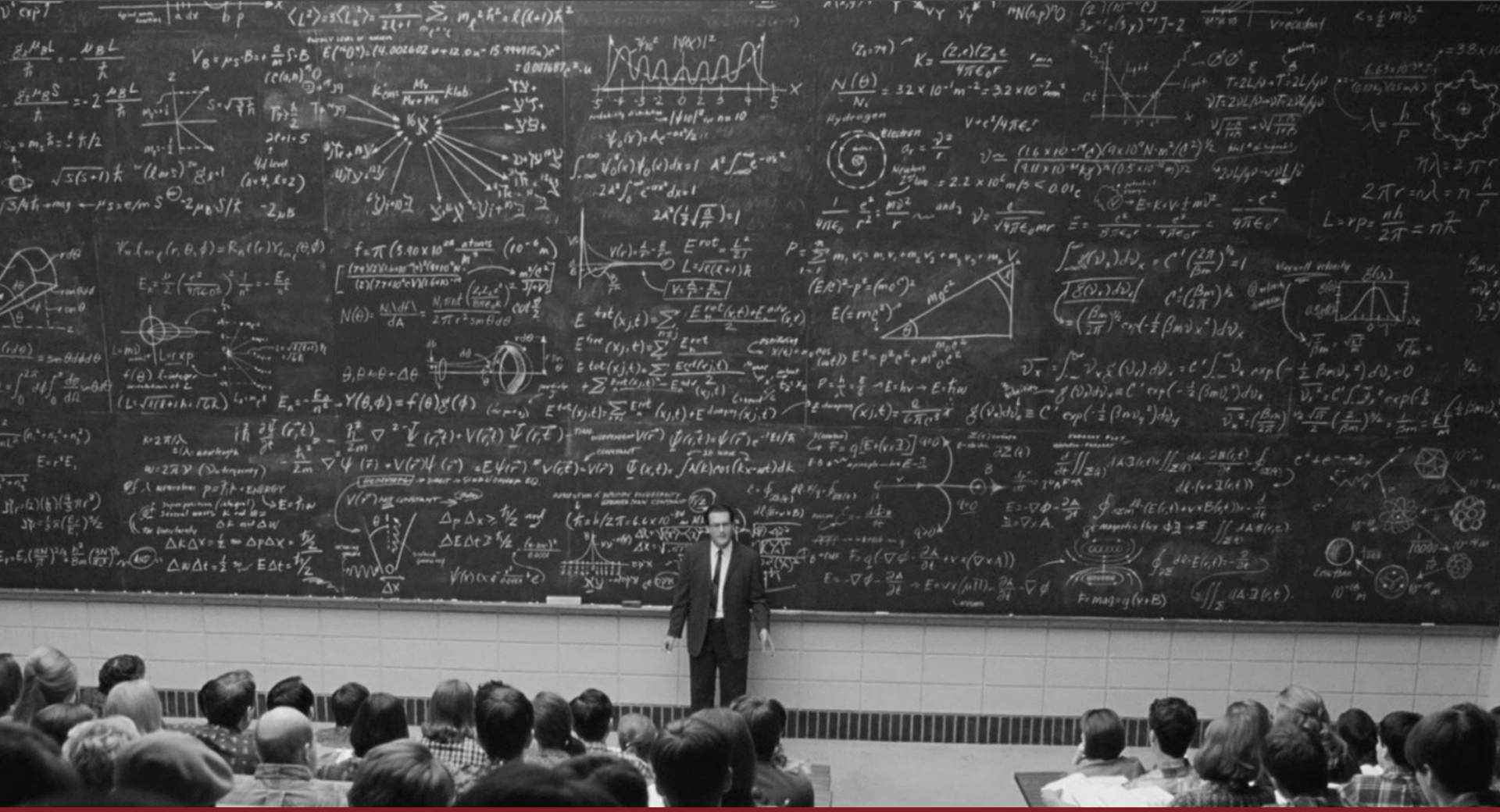

Why
What
How
Lessons Learned

Something you know...

Something you have...

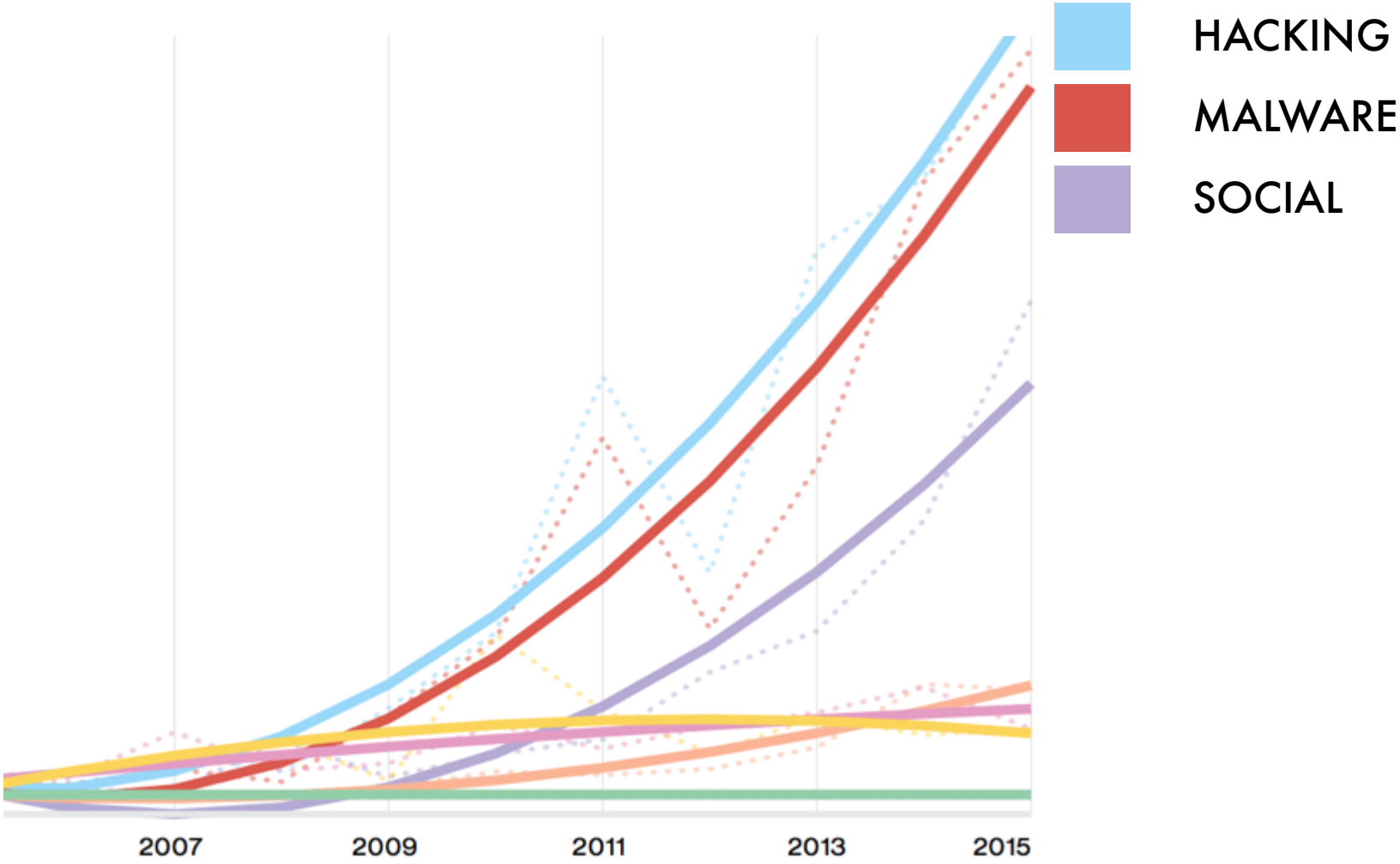
Something you are...


PASSWORD
PROOF
ACCESS
?
username
Login
Is that you?
Success!



THE PROBLEM

"81% of hacking-related breaches leveraged either stolen and/or weak passwords."



–2016 VERIZON DBIR

UISO Threat Mitigation Strategy

WEB APPLICATION ATTACKS

#1 Incident Pattern for the Education Industry (2016 Verizon DBIR)

Attack Area	Challenges
 URLS, ATTACHMENTS, & SOCIAL ENGINEERING	• > 5,500 Phishing Emails Reported • 67 Confirmed Security Incidents • Targeted Executive Phishing • Blocking of *.ZIP files
 KNOWN MALICIOUS DOMAINS & URLS	• 19.4M Blocked Requests • 901K Malwares Prevented *—Data from 1/1/17 to 2/28/17*
 DOWNLOADS & OTHER NETWORK TRAFFIC	• ~60% of network traffic now encrypted – limits effectiveness of security monitoring • Existing tools largely alert only
 STOLEN USERNAMES & PASSWORDS	• **> 1,000 accounts compromised last year** • **Unauthorized payroll direct deposit changes and IRS tax fraud at peer institutions**
 FILE SHARES, PORTABLE MEDIA, & PERSONAL EMAIL	• Traditional signature based Anti-Malware ineffective due to polymorphism • Only ~30% of University systems have needed security tools deployed

UNIVERSITY OF SOUTH CAROLINA

A SOLUTION


TRAINING
RETIRE
MFA
COMPLEX PASSWORDS

A PERFECT SOLUTION?

IMPLEMENTATION

2014

- Procurement
- Ad-hoc adoption

2017

- June 5th deadline
- 72,000 users

- April project launch
- July Implementation

2016

Phase I Work Plan

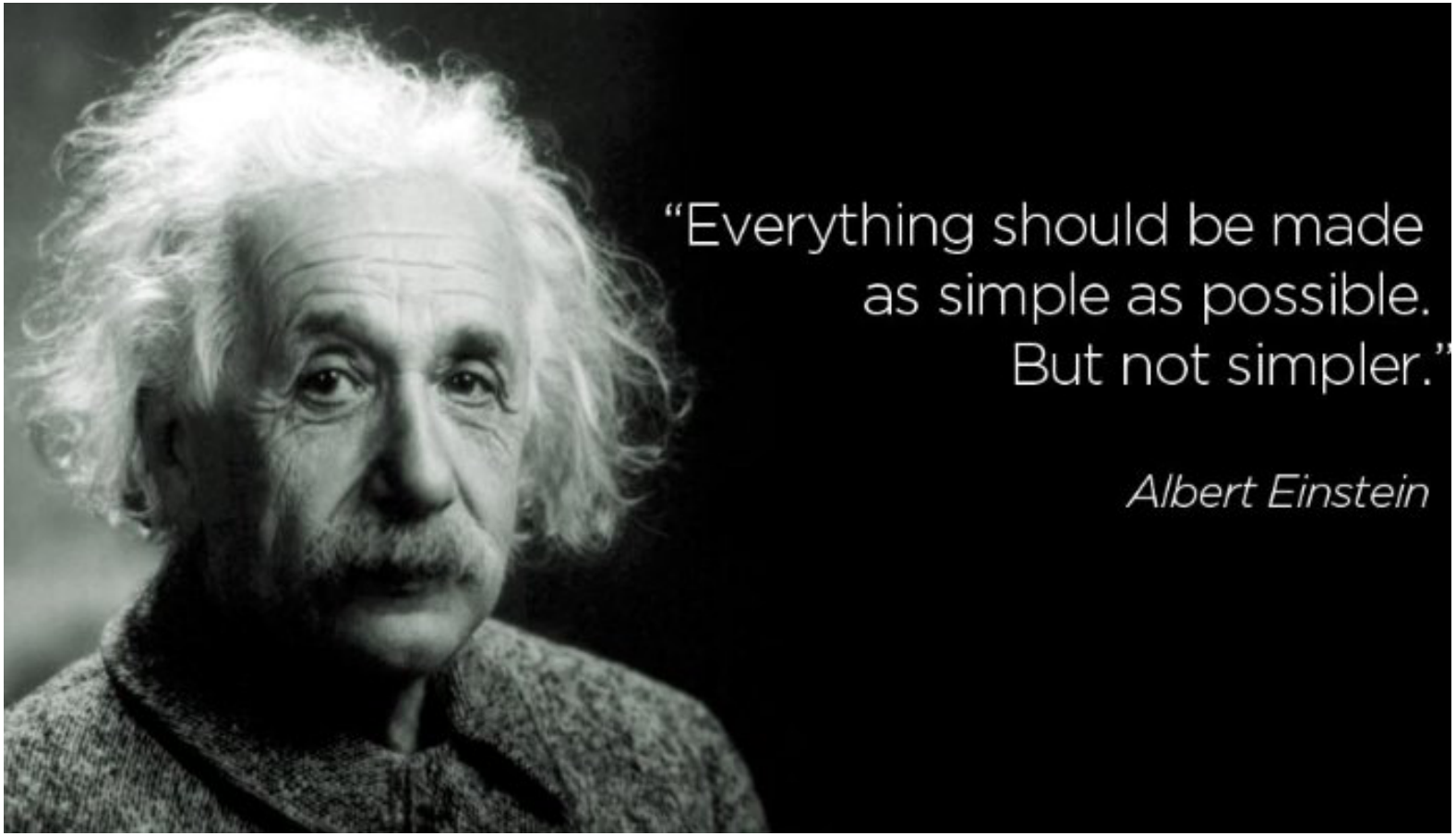
- Integrate servers
  - Scan network for SSH / RDP direct connections
  - Identify UTS owned
  - Onboard to UTS VPN or add MFA and test
- Execute Public Relations plan
  - Build awareness within the university system users
  - Call to action to enroll in the service in preparation
  - Notify vendors with local accounts to migrate to AD accounts
- Move all users from an old UTS VPN to the existing UTS VPN
- Identify applications in scope for MFA by June 30, 2017

Phase II Work Plan

- Develop a communication plan to include
  - Notification process of applications that require multifactor authentication
  - Continued call to action to enroll in the service in preparation of multifactor authentication being added to applications
- Integration of multifactor authentication
  - Based on the authentication method. Some of those identified include
    - CAS
    - Shibboleth
    - LDAP
    - Direct connect via SQL.NET 1521 Oracle

LESSONS LEARNED

Communication



Communication Plan

UNIVERSITY OF SOUTH CAROLINA
Division of Information Technology

Multifactor Authentication
Communication Strategies and Timeline

Ongoing from April to June 2017	Representatives of the UISO and CIO's office will make presentations and speak about Duo implementation at every opportunity available. Questions will be encouraged and used to update FAQs as necessary. *Responsible: Chief Information Security Officer, CIO, and Communications Director*
Ongoing from April to June 2017	Use social media channels to publicize multifactor and the importance *Responsible: Communications Director*
Ongoing from April to June 2017	Update FAQs on website and simply instructions *Responsible: UISO*
Wednesday, April 5	Email to Network Managers regarding May 20-21 outage required to upgrade Shibboleth and CAS to ensure compatibility with Duo *Responsible: Communications Director*
Friday, April 7	Email to all faculty/staff/students at all campuses regarding May 20-21 outage *Responsible: Communications Director*
Monday, April 17	Meet with Faculty Welfare Committee *Responsible: CIO*
Monday, April 24	*Last day of classes*
Monday, April 24	Meeting with College of Engineering faculty to gain input *Responsible: Chief Information Security Officer and CIO*
Tuesday, April 25	Email to all faculty/staff/students at all campuses – Multifactor is coming. Here is how to set-up your account now, link to FAQs and instructions. *Responsible: Communications Director*
By April 28	EA group to begin contacting individual system owners regarding Duo implementation, what they should expect, etc. *Responsible: Project Manager and IBM/EA implementation team*
By Monday, May 1	Splash page on my.sc.edu, Blackboard, and VIP will be updated to include a brief message regarding the May 20-21 outage *Responsible: Communications Director and IBM/EA implementation team*
Wednesday, May 3	Email to Council of Academic Deans regarding Duo implementation, give reasons why it's happening, links to instructions, and FAQs. Encourage questions. *Responsible: Communications Director and CIO*
Wednesday, May 3	Email Security Liaisons and ask them to encourage their departments to use the self-service sign-up for Duo now, rather than waiting
	Responsible: CISO and UISO
Thursday, May 4	Second reminder to faculty/staff/students at all campuses of May 20-21 authentication outage; Encourage to set-up Duo *Responsible: Communications Director*
Thu./Fri., May 5-6	*Commencement (most students and faculty will leave campus for the summer)*
Tuesday, May 9	Train Service Desk and Carolina Tech Zone employees on use of Duo/set-up *Responsible: Project Manager and UISO*
May 8-19 window	Work with USC Communications for article in @UofSCToday; work with Student Affairs to have information listed in *What's New @UofSC* (student e-newsletter) *Responsible: Communications Director* *First article in @UofSCToday ran on April 26, 2017; Second article on May 23, 2017*
May 8-19 window	Place information regarding Duo on digital signs across campus – first image *Responsible: Communications Director*
Tuesday, May 16	Final reminder to all faculty/staff/students of authentication outage, May 20-21; Stress how to set-up Duo *Responsible: Communications Director*
Monday, May 22	Email to all faculty/staff/students following upgrade; VIP login screen is different *Responsible: Communications Director* *Message title: FollowingUpgrade*
Week of May 22-26	Email to UAN and UAC (student advisors) with steps on how to assist new students in setting up *Responsible: Communications Director, Orientation Office*
Wednesday, May 24	Email Campus CIOs and indicate that another reminder regarding Duo will be sent to all students/faculty/staff at all campuses next week. *Responsible: Communications Director*
May 25-July 31	Representatives from DoIT will be available at New Student Orientation to assist students in Duo registration *Responsible: Communications Director, Orientation Office*
Thursday, May 25	Posters displayed in Undergraduate Admissions and Orientation offices regarding multifactor requirements *Responsible: Communications Director, Orientation Office, Undergraduate Admissions*
Friday, May 26	Undergraduate Admissions send targeted email to incoming students re: how to sign up for MFA *Responsible: Undergraduate Admissions*
Wednesday, May 30	Final reminder to all faculty/staff/students that Duo will be implemented on Monday, June 5. Reminder of how to set-up and how to claim VIP ID *Responsible: Communications Director*
Thursday, June 1	Duo demonstration at Network Managers meeting *Responsible: CISO*
Approx. June 1	Post card sent to all current and incoming students at all campuses encouraging them to sign up for Duo *Responsible: Communications Director*
Friday, June 2	Financial Aid Office begin to include information on MFA requirement in notifications to students *Responsible: Director of Student Financial Aid and Scholarships*
Monday, June 5	Go live
Monday, June 5	Place information regarding Duo on digital signs across campus – 2nd image *Responsible: Communications Director*
Monday, June 5	Presentation at luncheon for faculty who serve as academic advisors *Responsible: Chief Information Security Officer*
Tuesday, June 6	System-wide email to all faculty/staff/students that Duo is here; here's what has changed; if you can't authenticate, set-up Duo *Responsible: Communications Director* *File title: AfterGoLiveFinal*
Tuesday, June 6	Update splash pages - If you can't authenticate, set-up Duo *Responsible: Communications Director and IBM/EA implementation team*

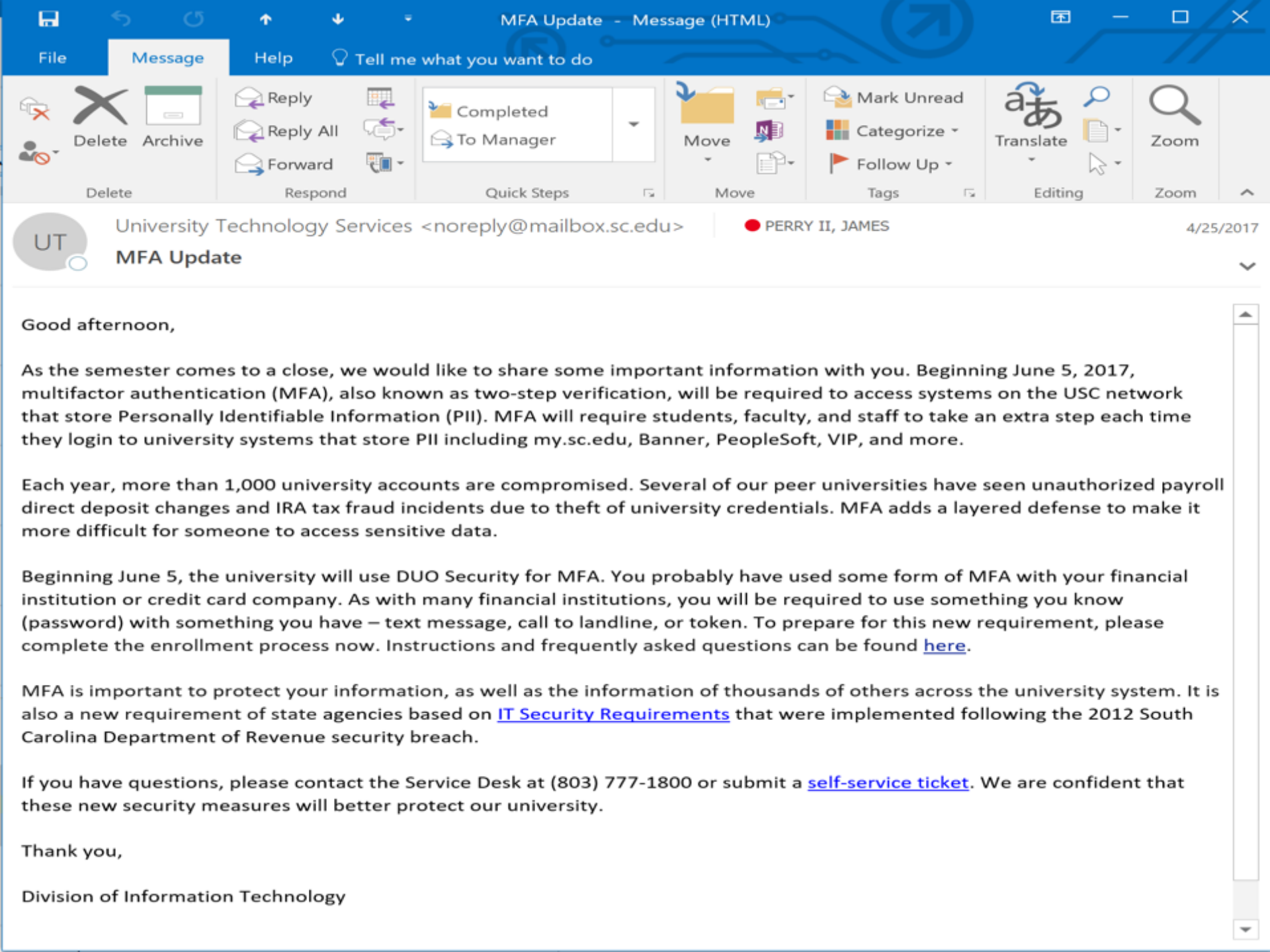
UNIVERSITY OF SOUTH CAROLINA

Communication Plan

UNIVERSITY OF SOUTH CAROLINA
Division of Information Technology

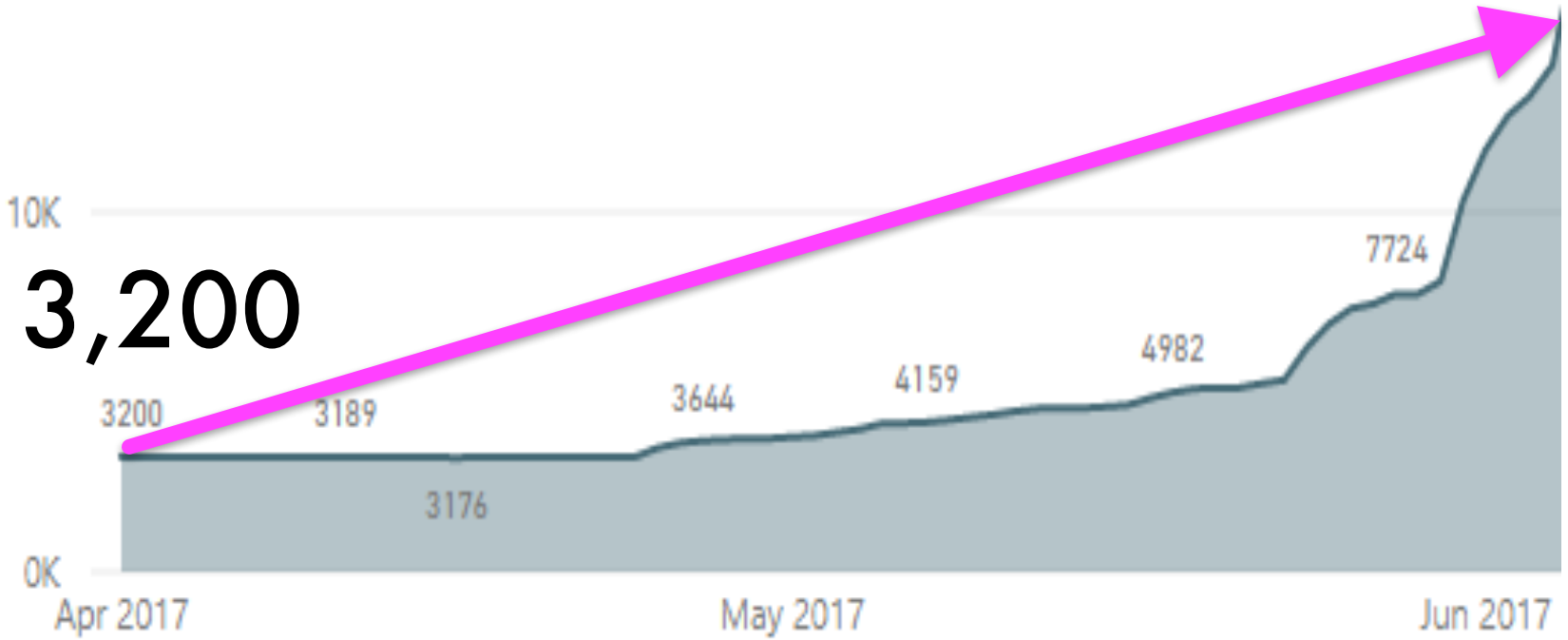
Multifactor Authentication
Communication Strategies and Timeline

Ongoing from April to June 2017	Representatives of the UISO and CIO's office will make presentations and speak about Duo implementation at every opportunity available. Questions will be encouraged and used to update FAQs as necessary. *Responsible: Chief Information Security Officer, CIO, and Communications Director*
Ongoing from April to June 2017	Use social media channels to publicize multifactor and the importance *Responsible: Communications Director*
Ongoing from April to June 2017	Update FAQs on website and simply instructions *Responsible: UISO*
Wednesday, April 5	Email to Network Managers regarding May 20-21 outage required to upgrade Shibboleth and CAS to ensure compatibility with Duo *Responsible: Communications Director*
Friday, April 7	Email to all faculty/staff/students at all campuses regarding May 20-21 outage *Responsible: Communications Director*
Monday, April 17	Meet with Faculty Welfare Committee *Responsible: CIO*
Monday, April 24	*Last day of classes*
Monday, April 24	Meeting with College of Engineering faculty to gain input *Responsible: Chief Information Security Officer and CIO*
Tuesday, April 25	Email to all faculty/staff/students at all campuses – Multifactor is coming. Here is how to set-up your account now, link to FAQs and instructions. *Responsible: Communications Director*
By April 28	EA group to begin contacting individual system owners regarding Duo implementation, what they should expect, etc. *Responsible: Project Manager and IBM/EA implementation team*
By Monday, May 1	Splash page on my.sc.edu, Blackboard, and VIP will be updated to include a brief message regarding the May 20-21 outage *Responsible: Communications Director and IBM/EA implementation team*
Wednesday, May 3	Email to Council of Academic Deans regarding Duo implementation, give reasons why it's happening, links to instructions, and FAQs. Encourage questions. *Responsible: Communications Director and CIO*
Wednesday, May 3	Email Security Liaisons and ask them to encourage their departments to use the self-service sign-up for Duo now, rather than waiting *Responsible: CISO and UISO*
Thursday, May 4	Second reminder to faculty/staff/students at all campuses of May 20-21 authentication outage; Encourage to set-up Duo *Responsible: Communications Director*
Thu./Fri., May 5-6	*Commencement (most students and faculty will leave campus for the summer)*
Tuesday, May 9	Train Service Desk and Carolina Tech Zone employees on use of Duo/set-up *Responsible: Project Manager and UISO*
May 8-19 window	Work with USC Communications for article in @UofSCToday; work with Student Affairs to have information listed in *What's New @UofSC* (student e-newsletter) *Responsible: Communications Director* *First article in @UofSCToday ran on April 26, 2017; Second article on May 23, 2017*
May 8-19 window	Place information regarding Duo on digital signs across campus – first image *Responsible: Communications Director*
Tuesday, May 16	Final reminder to all faculty/staff/students of authentication outage, May 20-21; Stress how to set-up Duo *Responsible: Communications Director*
Monday, May 22	Email to all faculty/staff/students following upgrade; VIP login screen is different *Responsible: Communications Director* *Message title: FollowingUpgrade*
Week of May 22-26	Email to UAN and UAC (student advisors) with steps on how to assist new students in setting up *Responsible: Communications Director, Orientation Office*
Wednesday, May 24	Email Campus CIOs and indicate that another reminder regarding Duo will be sent to all students/faculty/staff at all campuses next week. *Responsible: Communications Director*
May 25-July 31	Representatives from DoIT will be available at New Student Orientation to assist students in Duo registration *Responsible: Communications Director, Orientation Office*
Thursday, May 25	Posters displayed in Undergraduate Admissions and Orientation offices regarding multifactor requirements *Responsible: Communications Director, Orientation Office, Undergraduate Admissions*
Friday, May 26	Undergraduate Admissions send targeted email to incoming students re: how to sign up for MFA *Responsible: Undergraduate Admissions*
Wednesday, May 30	Final reminder to all faculty/staff/students that Duo will be implemented on Monday, June 5. Reminder of how to set-up and how to claim VIP ID *Responsible: Communications Director*
Thursday, June 1	Duo demonstration at Network Managers meeting *Responsible: CISO*
Approx. June 1	Post card sent to all current and incoming students at all campuses encouraging them to sign up for Duo *Responsible: Communications Director*
Friday, June 2	Financial Aid Office begin to include information on MFA requirement in notifications to students *Responsible: Director of Student Financial Aid and Scholarships*
Monday, June 5	Go live
[illegible]	Place information regarding Duo on digital signs across campus – 2nd image *Responsible: Communications Director*
Monday, June 5	Presentation at luncheon for faculty who serve as academic advisors *Responsible: Chief Information Security Officer*
Tuesday, June 6	System-wide email to all faculty/staff/students that Duo is here; here's what has changed; if you can't authenticate, set-up Duo *Responsible: Communications Director* *File title: AfterGoLiveFinal*
Tuesday, June 6	Update splash pages - If you can't authenticate, set-up Duo *Responsible: Communications Director and IBM/EA implementation team*


MFA Update - Message (HTML)
File
Message
Help
Tell me what you want to do
Delete
Archive
Reply
Reply All
Forward
Completed
To Manager
Move
Mark Unread
Categorize
Follow Up
Translate
Zoom
Delete
Respond
Quick Steps
Move
Tags
Editing
Zoom
UT
University Technology Services <noreply@mailbox.sc.edu>
PERRY II, JAMES
4/25/2017
MFA Update
Good afternoon,
As the semester comes to a close, we would like to share some important information with you. Beginning June 5, 2017, multifactor authentication (MFA), also known as two-step verification, will be required to access systems on the USC network that store Personally Identifiable Information (PII). MFA will require students, faculty, and staff to take an extra step each time they login to university systems that store PII including my.sc.edu, Banner, PeopleSoft, VIP, and more.
Each year, more than 1,000 university accounts are compromised. Several of our peer universities have seen unauthorized payroll direct deposit changes and IRA tax fraud incidents due to theft of university credentials. MFA adds a layered defense to make it more difficult for someone to access sensitive data.
Beginning June 5, the university will use DUO Security for MFA. You probably have used some form of MFA with your financial institution or credit card company. As with many financial institutions, you will be required to use something you know (password) with something you have – text message, call to landline, or token. To prepare for this new requirement, please complete the enrollment process now. Instructions and frequently asked questions can be found here.
MFA is important to protect your information, as well as the information of thousands of others across the university system. It is also a new requirement of state agencies based on IT Security Requirements that were implemented following the 2012 South Carolina Department of Revenue security breach.
If you have questions, please contact the Service Desk at (803) 777-1800 or submit a self-service ticket. We are confident that these new security measures will better protect our university.
Thank you,
Division of Information Technology

42 MESSAGES

June 5th
17,259



Visit *my.sc.edu/multifactor to get started*

Don't get locked out.

Register for multifactor authentication in order to:

- login to my.sc.edu
- access vip.sc.edu
- make changes to your personal information

WOULD YOU LIKE TO:

- see your grades?
- register for future classes?
- request football tickets?

Then register for
multifactor authentication
sc.edu/multifactor

Want to see your grades?

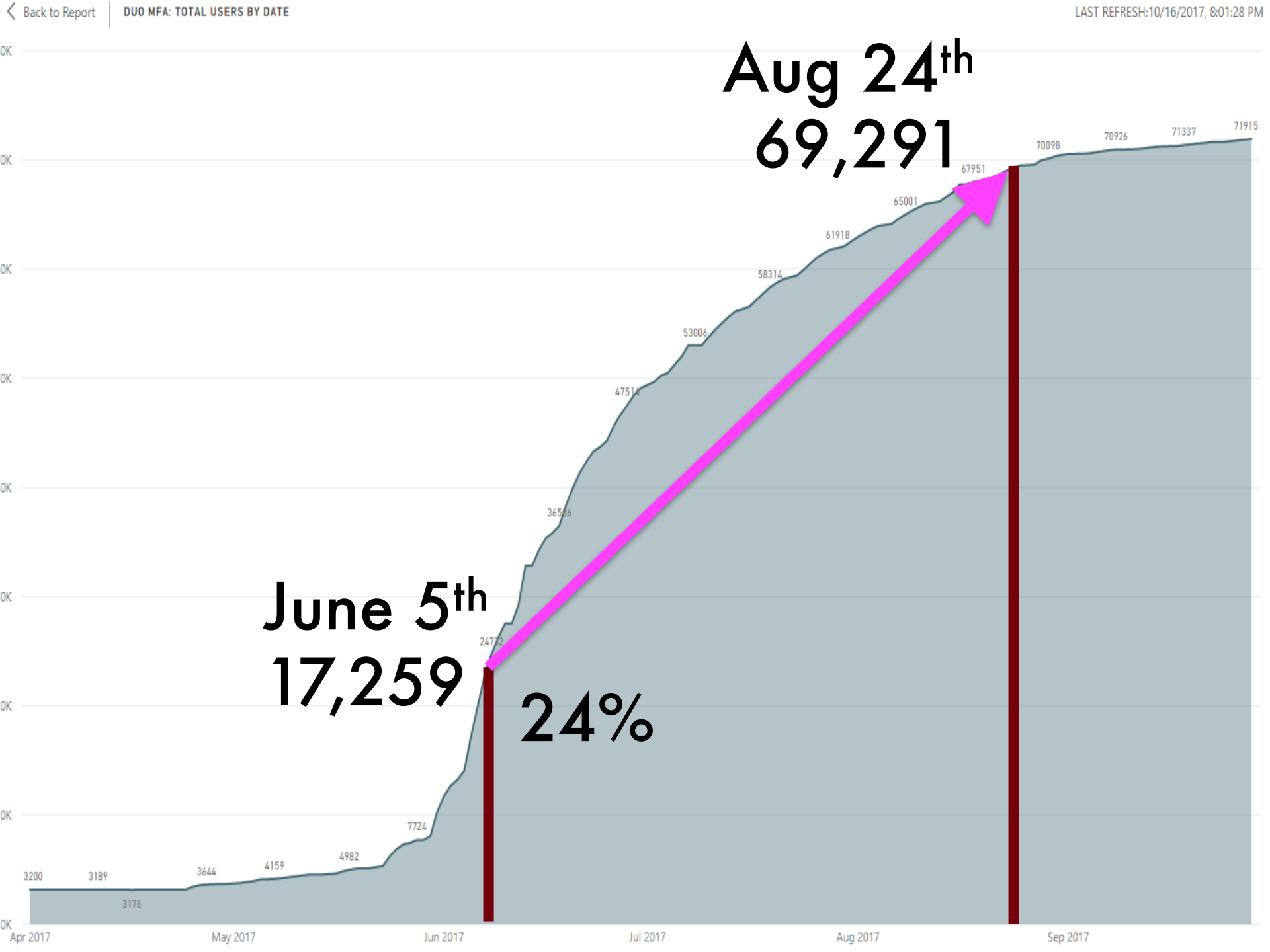
You need to sign-up for multifactor

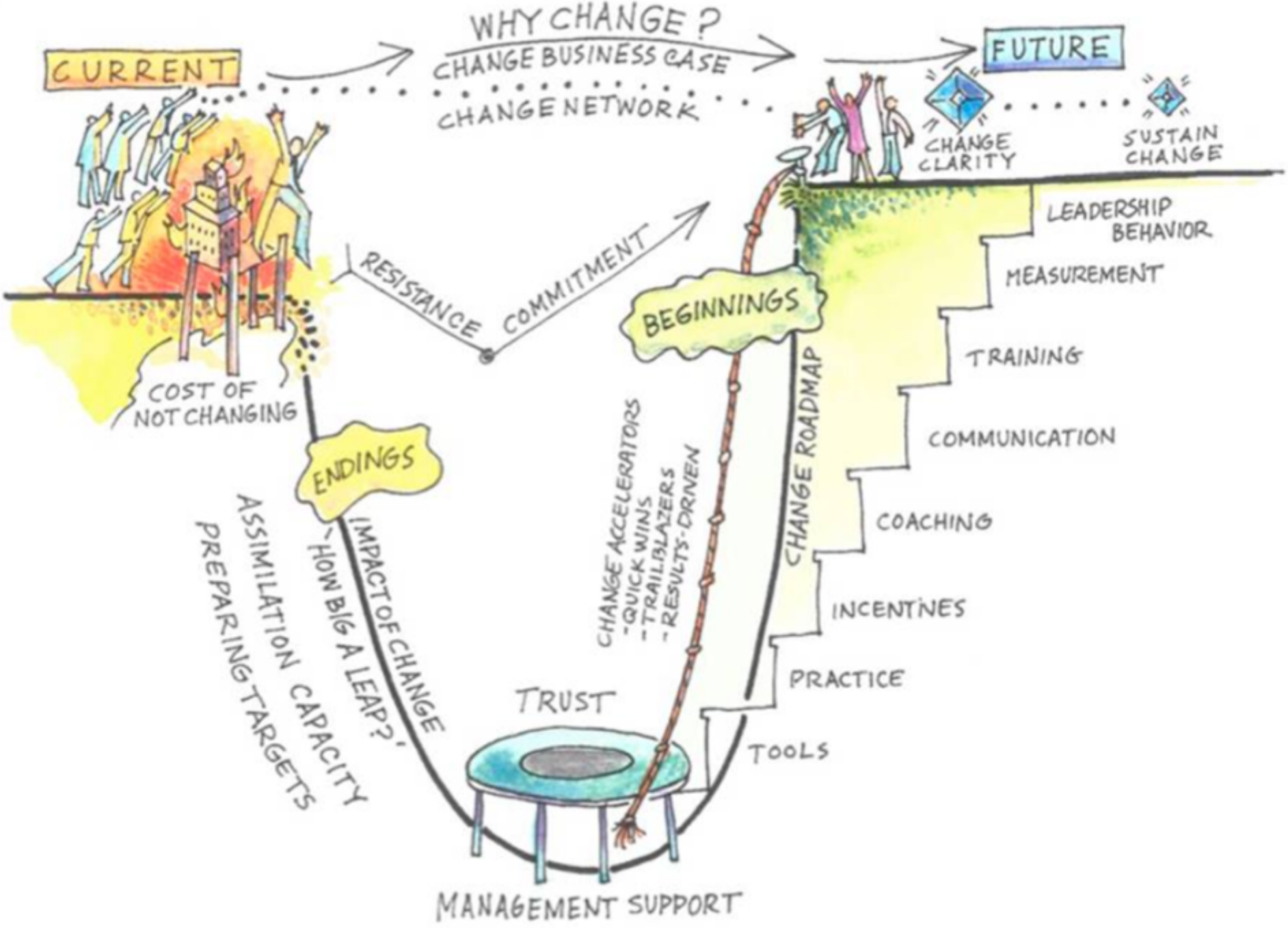
All students, faculty, and staff must sign-up for multifactor authentication in order to access university systems, effective June 5, 2017.

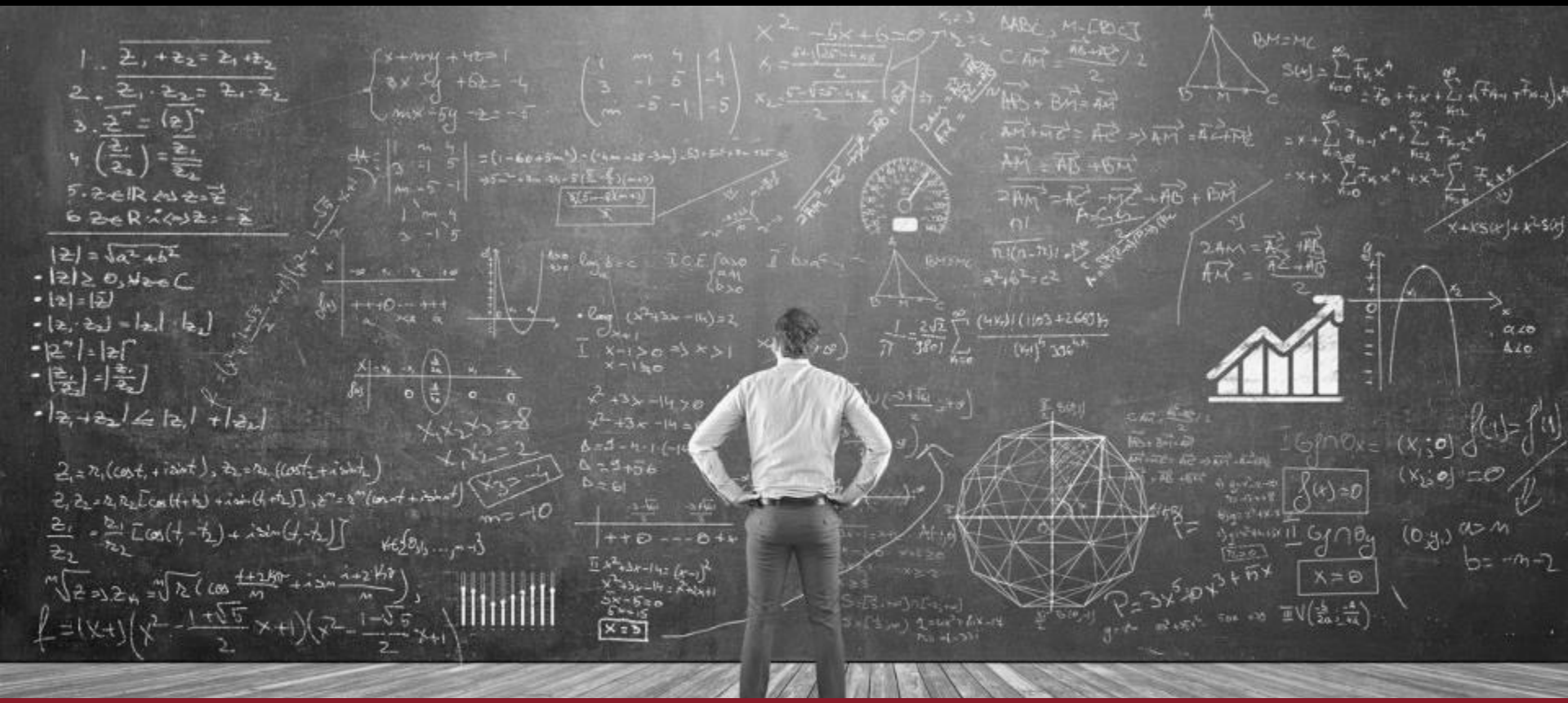
visit sc.edu/multifactor

UNIVERSITY OF SOUTH CAROLINA
Division of Information Technology

UNIVERSITY OF SOUTH CAROLINA


Back to Report
DUO MFA: TOTAL USERS BY DATE
LAST REFRESH:10/16/2017, 8:01:28 PM
Aug 24th
69,291
June 5th
17,259
24%
3200
3189
3176
3644
4159
4982
7724
24772
36506
47514
53006
58314
61918
65001
67951
70098
70926
71337
71915
Apr 2017
May 2017
Jun 2017
Jul 2017
Aug 2017
Sep 2017


WHY CHANGE ?
CHANGE BUSINESS CASE
CHANGE NETWORK
CURRENT
FUTURE
CHANGE CLARITY
SUSTAIN CHANGE
RESISTANCE
COMMITMENT
BEGINNINGS
ENDINGS
COST OF NOT CHANGING
HOW BIG A LEAP?
IMPACT OF CHANGE
ASSIMILATION CAPACITY
PREPARING TARGETS
CHANGE ACCELERATORS
-QUICK WINS
-TRAILBLAZERS
-RESULTS-DRIVEN
CHANGE ROADMAP
LEADERSHIP BEHAVIOR
MEASUREMENT
TRAINING
COMMUNICATION
COACHING
INCENTIVES
PRACTICE
TOOLS
TRUST
MANAGEMENT SUPPORT



LESSONS LEARNED

SUCCESS FACTORS

1. STRONG PROJECT DRIVERS
2. COMPREHENSIVE COMM. PLAN (+consequences)
3. PHASED THE DEPLOYMENT

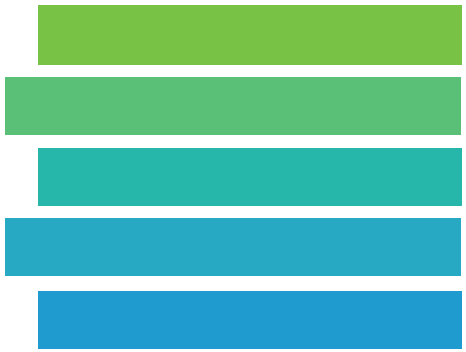
Fill in these questions with a name.

- Who's reputation is actually at risk? ____
- Who is asking about the status of tasks most often? ____
- Who is driving the project—and has the influence to make changes happen? ____
- Who is making the technical decisions even if they are unpopular? ____

**If the PM is the answer to the majority of these questions, then there is a problem.*

LEADERSHIP

MFA

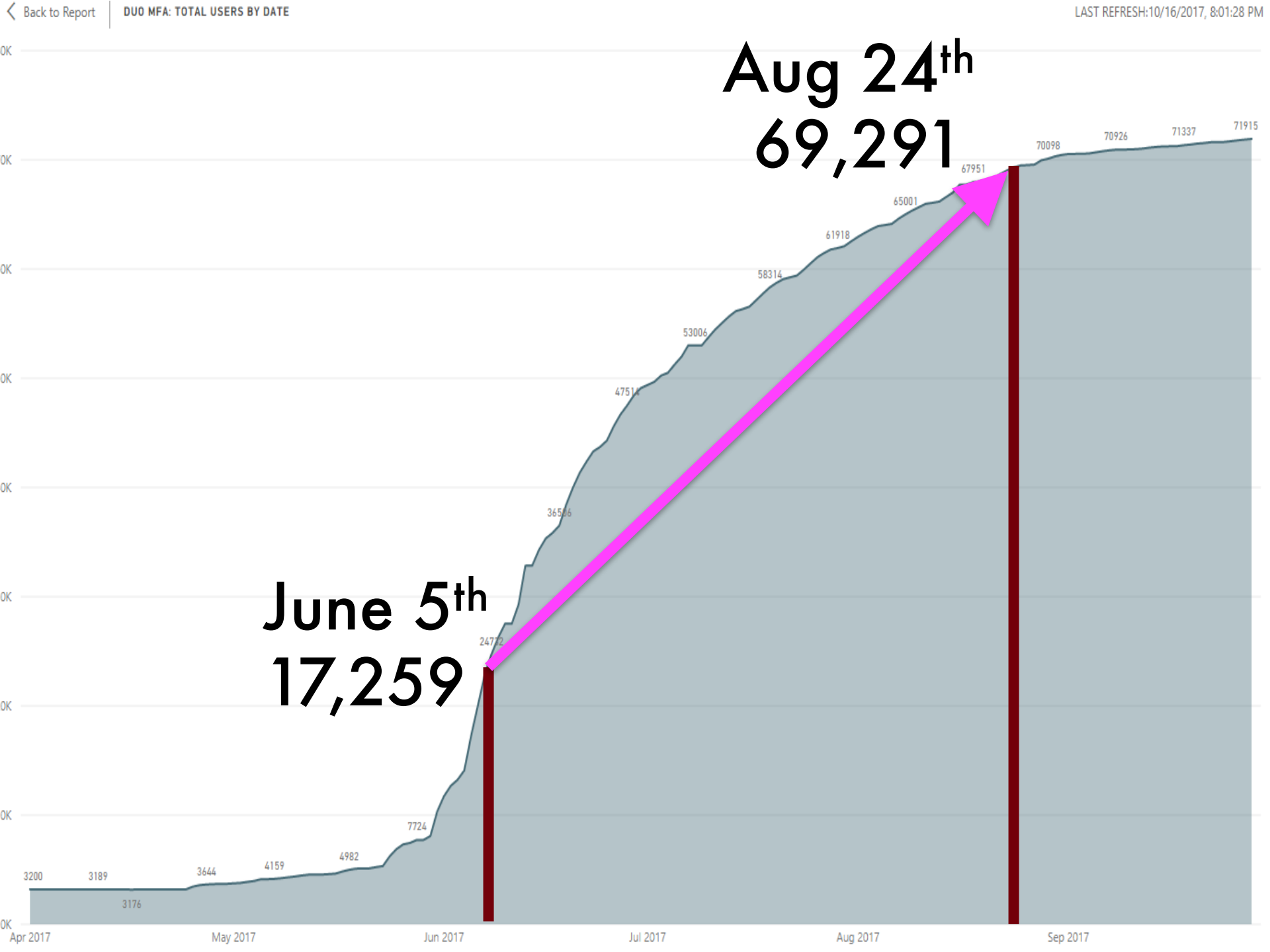


DECISIVE
ACTIVE
SENSE OF URGENCY
REPUTATIONAL RISK
OWNERSHIP

PROJECT

ADOPTION RATE

1. HAVE GATES
2. USE REAL, CONCRETE CONSEQUENCES
3. DEPT IT STAFF

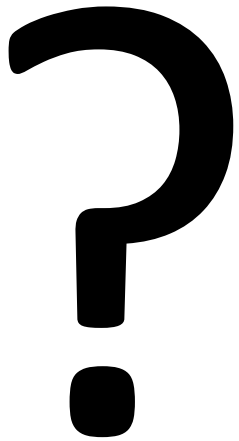

Aug 24th
69,291
June 5th
17,259
3200
3189
3176
3644
4159
4982
7724
24772
36506
47514
53006
58314
61918
65001
67951
70098
70926
71337
71915
Apr 2017
May 2017
Jun 2017
Jul 2017
Aug 2017
Sep 2017

AREAS FOR IMPROVEMENT

1. USER TESTING (Comm & Site design)
2. REAL-WORLD TRAINING
3. SCALE THE SERVICE DESK

INTERESTING TAKEAWAYS

1. PROJECT NAME
2. SR LEADERSHIP DEMO
3. COMM WITH PARENTS



UNIVERSITY OF

SOUTH CAROLINA