MULTIFACTOR AUTHENTICATION 2016'S ESSENTIAL SECURITY PROJECT

Chuck Kesler - CISO, Duke Health

Jon Sternstein – Principal Consultant, Stern Security

NC HIMSS

Stern Security

DukeHealth

INTRODUCTION

Jon Sternstein

- Founder & Principal Consultant at Stern Security
- WakeMed – Former Data Security Manager
- Co-chair of NCHICA Technology Workgroup
- SANS Institute – Mentor
  - SANS 560: Network Penetration Testing and Ethical Hacking

INTRODUCTION

Chuck Kesler, MBA, CISSP, CISM, CISA, PMP

- Chief Information Security Officer for Duke Health since 2011
- Previous managed Symantec's Security Advisory Services consulting practice
- 30 years of IT experience, with 10 years focused on information security
- B.S. in Physics and an MBA from NC State University

AGENDA

- What is Multifactor Authentication and why do we need it?
- Duke Health's case study
- Hacking Multifactor Authentication… what can go wrong?

STEAL MY PASSWORD

- Could you access my account if you stole my password?
- DEMO

WHAT IS MULTIFACTOR AUTHENTICATION?

- Also called two-factor authentication or two-step verification (sometimes)
- Added protection for accounts
- Two out of the three options:
  - Something you KNOW (e.g. password, PIN)
  - Something you HAVE (e.g. phone, badge, card, RSA token)
  - Something you ARE (e.g. fingerprint, retina scan, heartbeat)
- Common uses
  - Email accounts
  - VPN accounts
  - Debit cards

WHY USE MULTIFACTOR?

- It is required for e-prescribing controlled substances
  - DEA requirement: http://www.deadiversion.usdoj.gov/fed_regs/rules/2010/fr0331.htm
  - "*two-factor authentication including a hard token separate from the computer for accessing the signing functions*"
- Passwords are easy to steal
  - Passwords are written down
  - Phishing
  - Malware
  - Guessed
  - Publically available passwords: https://haveibeenpwned.com/
- Best practice

HEALTHCARE DATA BREACH

- Middlesex Hospital, CT
  - Breach occurred in October 2015
  - 946 records
  - Phishing email was sent to employees
  - Four employees typed in their credentials
- Partners Healthcare System
  - Breach discovered in November 2014
  - 3,300 records
  - Patient names, dates of birth, contact telephone numbers, addresses, medical record numbers and health insurance details
  - Several physicians responded to phishing email

NC HEALTHCARE SURVEY

- In 2014, NCHICA Surveyed 51 North Carolina Healthcare Organizations
  - 90% between 1 & 20 healthcare providers
- Can providers remotely access the EHR from the Internet?

- Is two-factor authentication enabled?

DUKE HEALTH'S CASE STUDY

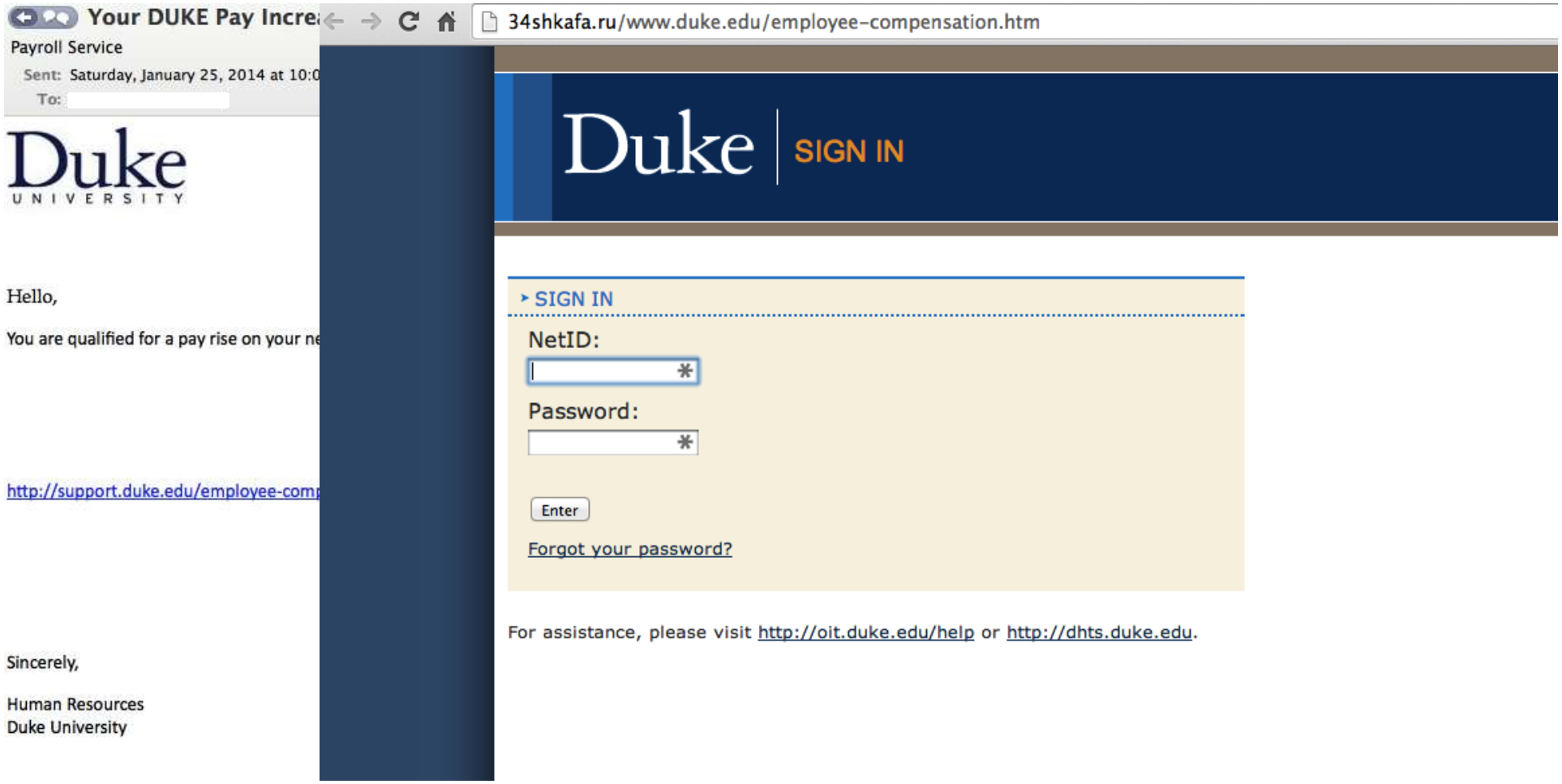
DIRECT DEPOSIT PHISHING SCAM

The Attack

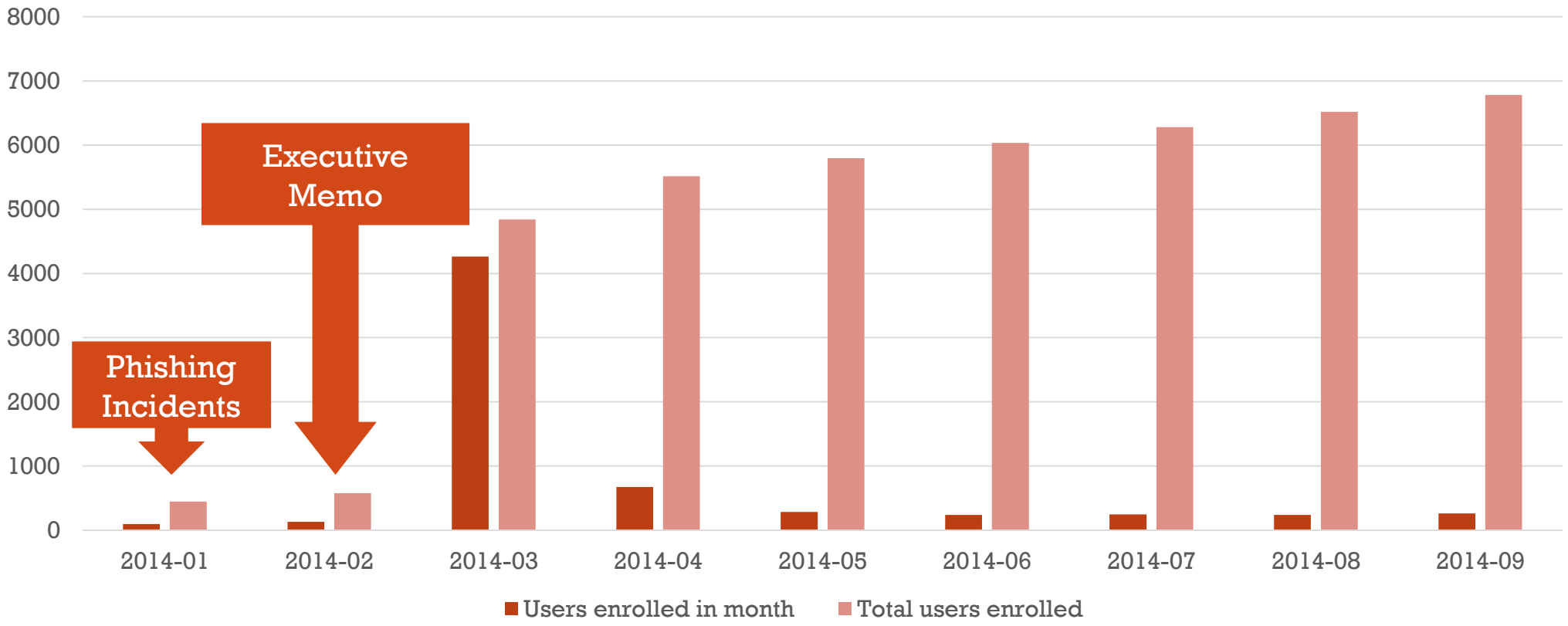
4 waves of phishing targeting
600-700
faculty & physicians

10 people lose paychecks

REALLY . . . THAT WORKED?!



STICK & CARROT: SHORT TERM GAINS



But even the nearly 1400% increase since February is only about 17% of the Duke faculty & staff population; extrapolating the 250/month rate since May would mean it would be **October 2025** before we reach entire population

NC HIMSS

GETTING THE BOARD'S ATTENTION

"By targeting Anthem employees with phishing emails and luring them to the fake sites, it may have been possible for the attackers to collect the logins and passwords and eventually access the insurer's real systems.

ThreatConnect, an Arlington, Virginia-based security company, found that Premera appears to have been targeted by the same style of attack."

-ComputerWorld

Anthem BlueCross

PREMERA | BLUE CROSS

Anthem data breach cost likely to smash $100 million barrier

Summary: *The company's cyber insurance policy is likely to be exhausted following the theft of up to 80 million records.*

COMPUTERWORLD

Popular Now:

Home >

NEWS

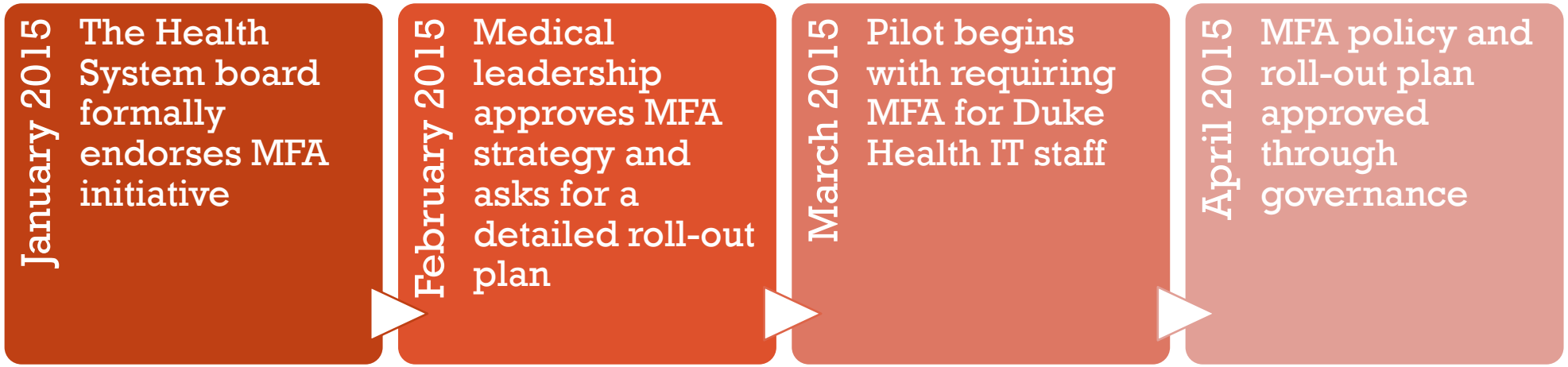
Premera, Anthem data breaches linked by similar hacking tactics

NC HIMSS

THE TIPPING POINT

Today, Multifactor Authentication should be considered "table stakes" for information security – you just have to do it.

(paraphrasing one influential Health System board member's comments)



9/1/2015 established as target date for requiring MFA for remote access to clinical systems

NC HIMSS

KEY POINTS FOR OUR MFA POLICY

System Scope	• Remote access to applications that house sensitive information
User Scope	• All Duke Health workforce members required to enroll in MFA
Awareness	• Ensure broad, multi-modal communications and training
Enforcement	• Managers track and enforce enrollment for their teams
Exceptions	• Managed through the Information Security Office

MANAGING THE CHALLENGES

Cost

- Piggybacked on the University's contract with Duo
- Encouraged BYOD for MFA tokens
- Addressed hardship cases and other one-offs by centrally funding fallback solutions (e.g. Yubikeys)

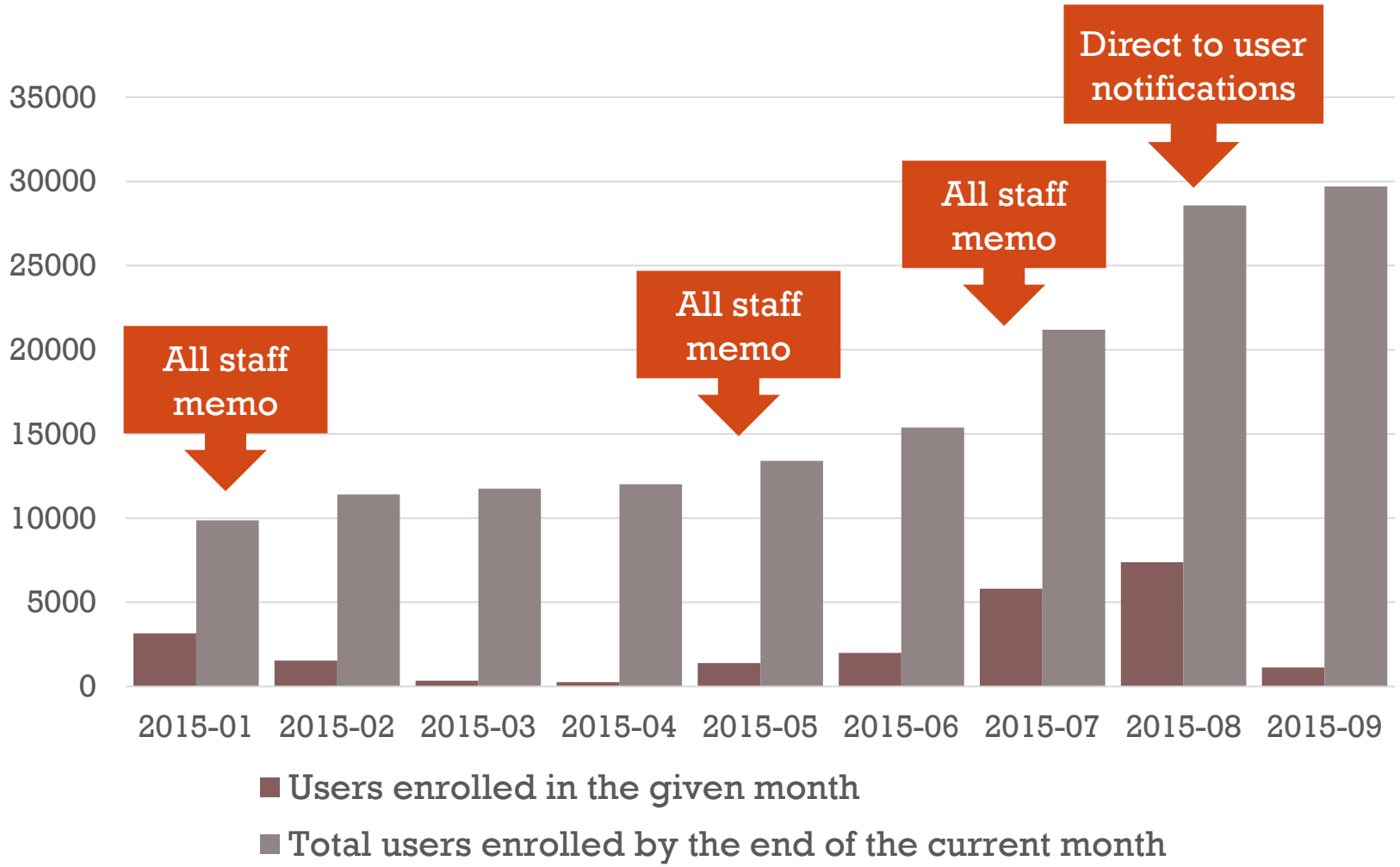
Complexity

- Minimize disruptions to clinical workflows
- Leverage work already done by the University with Duo and Shibboleth
- Provided flexible options for MFA tokens
- Limited initial scope to highest risk areas, and build from there

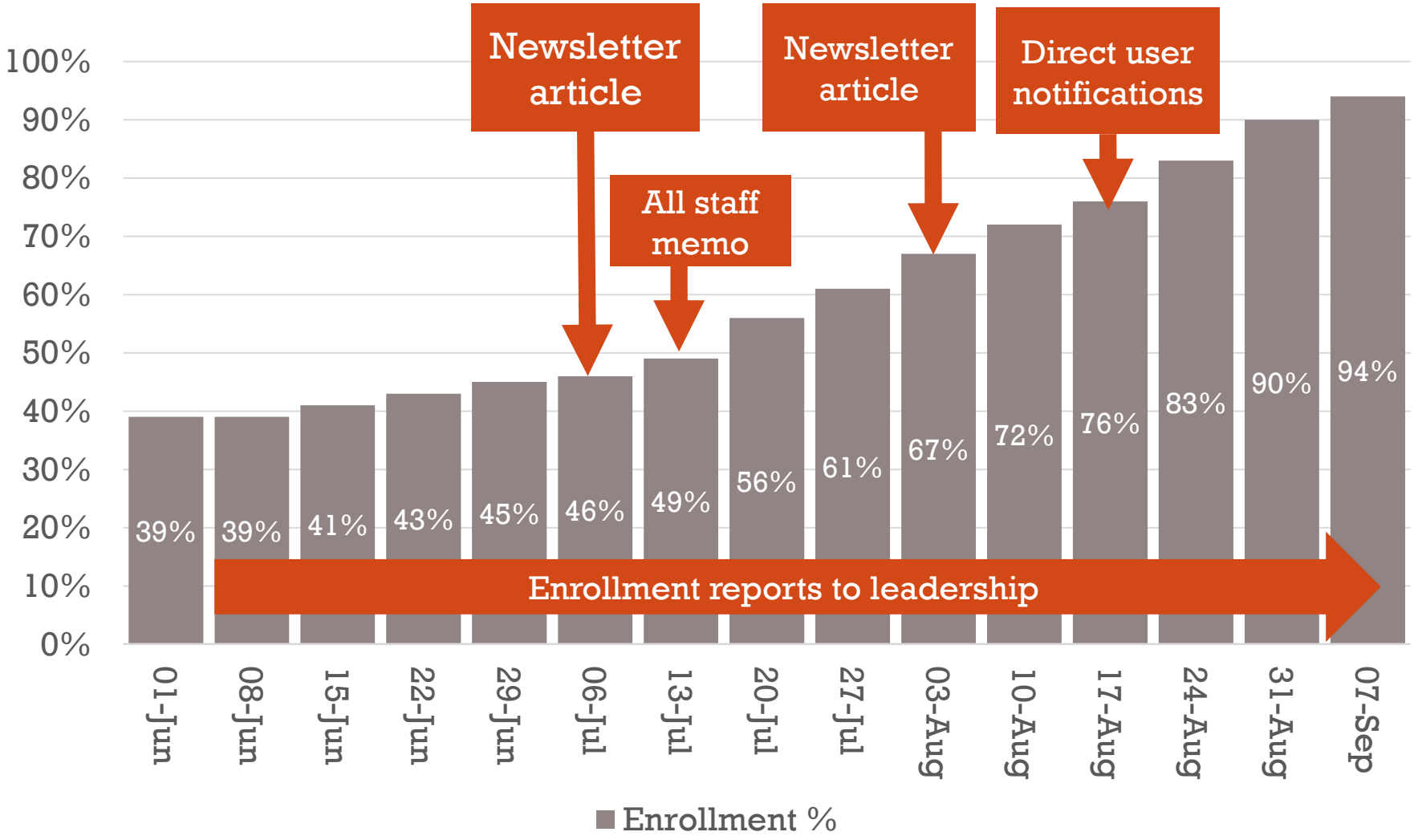
Timeline

- Put our bosses to work! Executive support was crucial
- Communications: newsletters, memos, in-person outreach, direct emails
- Created natural consequences for failing to enroll: no remote access

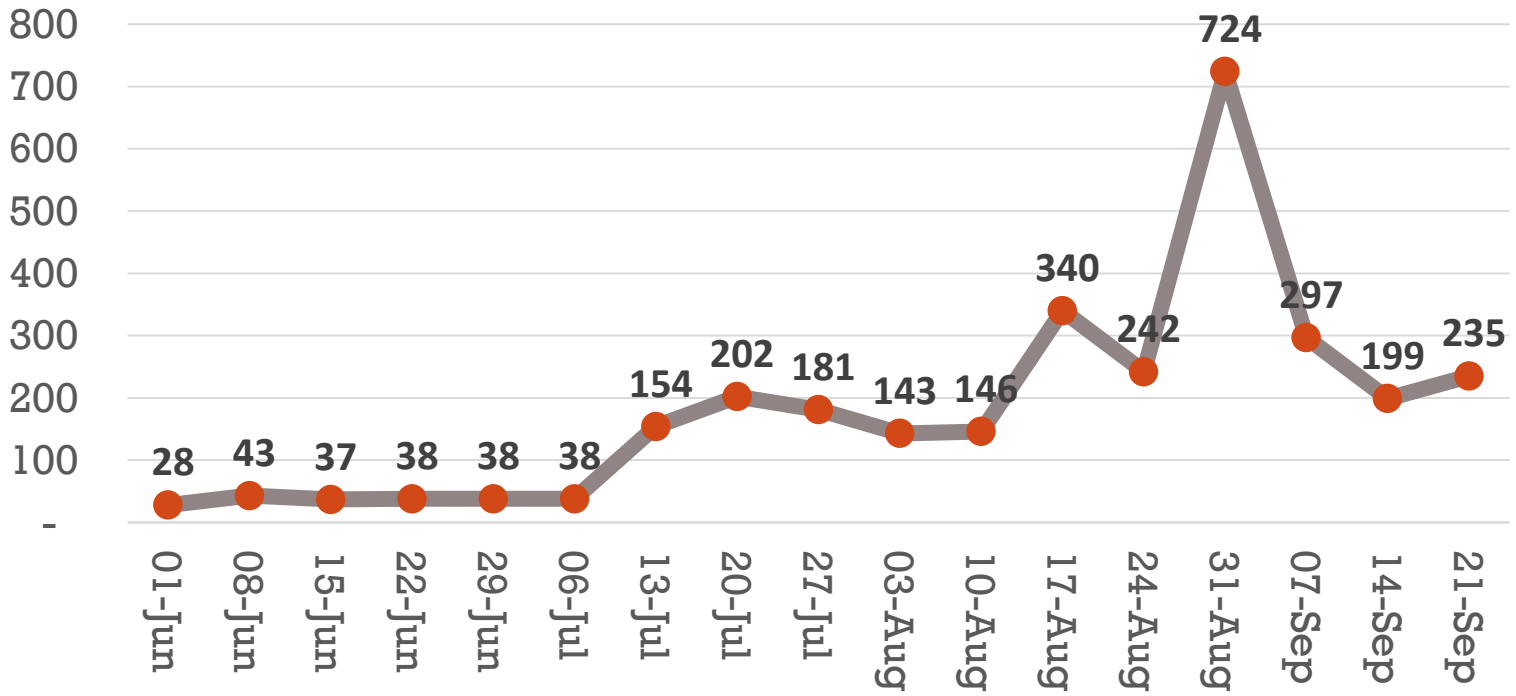
TURNING UP THE HEAT ON MFA



ENROLLMENT CRUNCH TIME

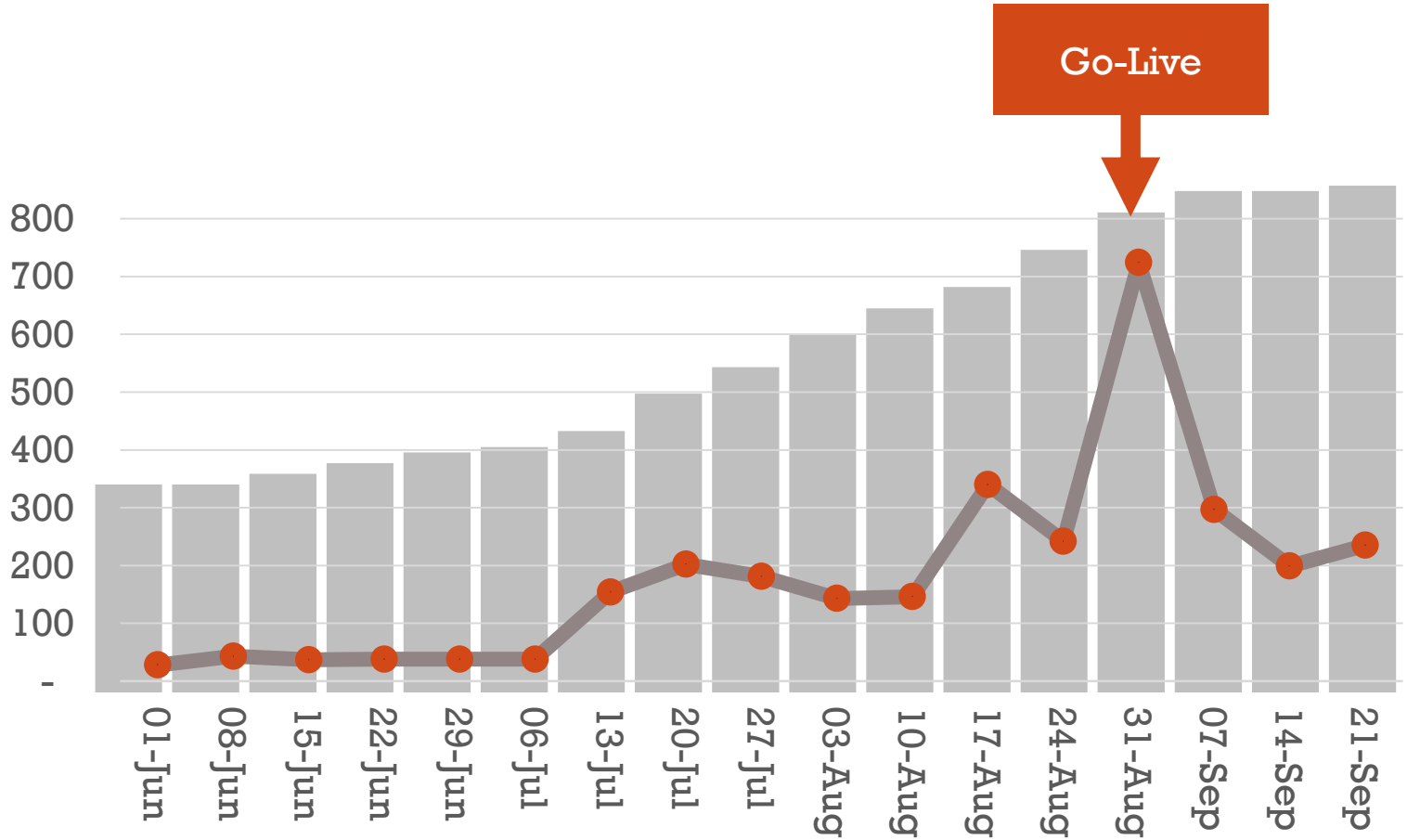


SUPPORT IMPACT ON SERVICE DESK CALLS



Based off 30,000 Duke Medicine employees (faculty, staff, doctors and nurses)

SUPPORT IMPACT ON SERVICE DESK CALLS



WHAT DID WE LEARN?

- Have a good communication plan and ACTIVE executive support
- Consider and document your policy
- Decide on an enrollment strategy (hands on sessions, and don't force-enroll)
- Set a date to complete enrollment and enforce on a service used by most people
- Focus on critical groups/assets first
- Think about other areas to add MFA – it's not just a "gateway" service
- Think about "edge cases" that don't regularly log in
- Be flexible!
- We should have started sooner!

HACKING MULTIFACTOR AUTHENTICATION

- Department of Homeland Security (DHS) hacked in 2016
  - Stole contact info for 9,000 DHS personnel and 20,000 FBI employees
  - Multifactor Authentication was enabled
  - Used password & a separate token code

- How did the attacker bypass two-factor authentication?
  - ANSWER: Attacker called the helpdesk to get access
  - *"So I called up, told them I was new and I didn't understand how to get past [the portal]." "They asked if I had a token code, I said no, they said that's fine—just use our one."*
- How can we prevent these attacks?

USERS SOMETIMES HELP THE HACKERS...

NC HIMSS

EDUCATION

- Train the Helpdesk
  - Confirm identity of caller
  - Confirm the phone number on file
  - Call the phone number on file

WORLD PASSWORD DAY
MAY 5TH 2016

- Thursday, May 5 is World Password Day
- Let's enable on two-factor authentication on all of our accounts by this day!

REFERENCES

- **DEA Interim Final Rule Electronic Prescriptions for Controlled Substances**: http://www.deadiversion.usdoj.gov/fed_regs/rules/2010/fr0331.htm
- **DEA two-factor questions**: http://www.deadiversion.usdoj.gov/ecomm/e_rx/faq/practitioners.htm
- **List of public breaches**: https://haveibeenpwned.com/
- **Phishing caused healthcare data breaches**: http://www.hipaajournal.com/healthcare-email-phishing-scam-claims-946-victims-8209/