• Thank you very much for having us
• Quinn: I am Quinn Shamblin, Executive Director & Information Security Officer at Boston university and am very pleased to be here with
• Jane:
• We are here to talk about a problem faced by every organization in the world, most definitely those in higher-ed

Disclaimer:
Presenters cannot be held liable under any circumstances for any information presented here. Presenters expressly disclaim and exclude all express and implied warranties, representations or claims of fitness for any purpose. By viewing this presentation, each and every person, group and organization agrees to hold Presenters harmless from any legal action. This document or file is provided "as is" without warranty of any kind. In no event shall presenters be liable for any special, indirect or consequential damages or any damages whatsoever resulting from or arising out of or in connection with the use or performance of material and/or information contained herein. Presenters in no way can be held liable for typographical or technical errors or for omissions.

COPYRIGHT NOTICE (NOTICE SPECIFIC TO THIS DOCUMENT)
Permission to use and duplicate this is granted, provided that (1) the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear, (2) use of documents is for informational use only, and (3) should the documents or portions of those documents be used by others in future presentations, that a link back to Presenters (and where appropriate back to the source document) be established. To the best of its knowledge, all graphics, text and other presentations not created by Presenters in this presentation are in the public domain and freely available from various sources on the Internet and links to sources have been provided where known.
Quinn Shamblin
Executive Director & Information Security Officer
Boston University
CISM CISSP ITIL | GCFA PMP
qrs@bu.edu
www.bu.edu/infosec | @BU_infoSec
www.linkedin.com/in/quinnshamblin/

Jane Drews
Senior Director & Chief Information Security Officer
The University of Iowa
CISSP
jane-drews@uiowa.edu
itsecurity.uiowa.edu
• On January 2nd of 2014, a number of senior faculty members at Boston University checked their bank account and found that their paycheck had not been deposited.

• They reported the issue and investigation revealed that this was a …
• … heist

• Their direct deposit information had been changed; their money had been re-routed into other peoples’ bank accounts.

• Throughout 2014, all of higher-ed was constantly under this one particular attack … amongst many others…

• But what is the *real* problem here?
• Take a moment to look this over.  {Pause 5}

• A message very similar to this was received by approximately 160 individuals on November 27 and 28;
• This was the start of the event leading to the compromise of 33 accounts held by faculty members of this university,
• 13 of which had their paycheck stolen on January 1 of this year.
• This was a real event and BU lost real money due to this.

• Look how good this is
  • Used the BU logo, good English
  • Excellent text (if a bit stilted) and very believable formatting
  • Confusing but specific and real technical information to add credibility
  • Message pretended to be from IT and security -- this is a common trick

• Only two tells:
  • One blunder with the name of our organization (most people wouldn’t notice)
  • One with the structure of the URL, it doesn’t really go to BU, but again, most people wouldn’t see that
• Exact same message, only the names, dates, time, and phish site changed

• I’d have to guess many of your schools also received the same phishing messages.....
• And the bad guys were very much watching us.
• On January 7, we went public in BU Today to try to help our people understand what happened and how to protect themselves
• The weekend after that, the attackers published…

• …this message, trying to leverage our attempts to alert BU to the danger to deliver a second attack.
• This attack went to a greater number of targets and a great number responded, but we were monitoring for unusual activity and were able to detect anomalous account access activity and attempts to misdirect funds
• This message was even better.
• Only one of the commonly used phishing detection tricks that would work with this message. The trick is to hover – don’t click – over the link. When you do that, a small box will pop up or if you’re in a browser the lower left corner of the window will show you the real link that you will be taken to if you click

• If we do that for this message, we’ll see that the link does not really go to .BU.EDU

• BTW, If you are using a smartphone were other portable electronic device, you have to use a different trick to see the real link
• In an iPhone for example you click and hold the link for a couple of seconds to show the real URL and be asked if you want to go there
Its interesting to note that the attackers had very quietly done recon on our system with a single account in september, then did one diversion of funds Oct 1, and then two more for Nov 1, and then were going for the big payout. When we caught it in November, about 130 self-service accounts had been compromised and accessed, and about 30 had their DD information changed. They singled out high paying execs, faculty, and clinical staff. We were able to identify at least 3 phishes that were associated, but we were not able to determine everyone who responded. Had we not caught this before the dec1 payroll, those 30 people would have lost all or part of their paycheck.

Thankfully, our HR system and the self-service employee web portal do extensive logging. We were able to identify the source of the first known victim, then looked for other access from those IPs, backtracked to previous logs, and pivoted to other accounts, found more activity and sources, and then again pivoted to other accounts to find them all. I don’t think we would have found all of the victims or changes without the full logging.

We made emergency changes in just one day to stop the bleeding. We blocked all remote access to certain functions, and added a temporary 2nd factor for those sensitive functions from on campus. We sent a campus email about the emergency changes, and immediately began putting together an awareness campaign. About detecting phishing scams. The attackers launched new phish the next day to collect our temp second factor, and persisted to try and gain access.

We were of course concerned about what other applications may have been accessed, since we a single credential at our campus. So, we also reviewed a lot of other logs to determine if anything else had been compromised.
…Phishing
…or watering hole attacks
…or shoulder surfing
…or people recording your login with their google glass or phone
…or that the sound of your keystrokes can be recorded with a phone and your password determined algorithmically
…or brute force attacked over ssh

…or any of the thousands of other ways that a password can be stolen.

The real problem is:
• Credentials were compromised.
• This can happen a thousand different ways. This time it happened to be via the ever-popular phishing attack.
• It’s popular because it works
• Remember, over a dozen highly educated, very smart, senior faculty members fell prey to this and had their paychecks diverted to someone else’s bank account.
• Your password is a piece of knowledge, of information.
• As long as the only thing required in order to get access to money or to sensitive information is a piece of knowledge – a password or even a password and a bank account number – we are at risk.
• As has been proved over and over across the globe that knowledge is easy to steal. Even when you know that that piece of knowledge is the key to your financial kingdom.

The real solution
The only way to realistically protect against compromised credentials is to try to make sure they are not *entirely* compromised.

One of the most effective ways we have to do that at the moment is to require *more than knowledge* in order to access sensitive information. When it comes to your bank account, social security number, medical information, etc., a password is just no longer enough.

- Two-factor is becoming much easier, common and accepted
- Google, facebook, twitter, major online games like WoW,

- It is a sad state of affairs when the gold in my WoW vault is protected better than the money in my real bank.

- Many modern two-factor solutions leverage smart phones or other mobile devices, so we also need to improve the security of those devices
  - If the bad guys can compromise your computer and your phone at the same time, they can get around MF
• The solution in its primary form is amazingly simple
• Login, click yes, done
• If someone is messing with the system, click no to report
We reviewed Gartner, looked at a few options but quickly homed in on an option offered by a strategic partner, an higher-ed consortium: InCommon

- Strategic connection to Shib
- Very compelling enterprise cost
- Incredible flexibility

**Duo Security - Simple and flexible**

- No tokens required
- Rapid initial setup
- Single-button confirmation when using the app
- Supports text messages, phone calls that can be responded to with a single button or a code, tokens and more
- Can remember a device (single-user systems only)
- Work anywhere in the world
- Can work with no connection
Duo was an easy choice to select for a small pilot. We already had a small number of licenses, it looked to meet our needs initially and into the future, was simple to integrate, flexible, and cost effective.

Why Duo Security at Iowa?

- Had licenses, experience (VPN pilot)
- Simple integration with CAS based web login tools
- Internet2 Net+ application security vetting and pricing
- Phone based second verification is an emerging “industry standard”
- Provides a framework for future integrations
Approximately 50 people involved in a 6 week pilot, including HR, ITS, and UIHC-HR staffs, as well as senior leaders and distributed power users.

Overwhelmingly, issues were related to getting enrolled, rather than using Duo for login verification.

- One in three people experienced an issue getting enrolled and set up
- Some issues with the “remember me” feature
- Most feedback was very positive for using Duo – It’s super easy to use, once you have it set up
- Some concern expressed over the frequency of logins

Developed an implementation proposal based on findings.

Enrollment strategy

- Separate the enrollment function from the use function
  - Improved perception of ESS .. it “just works” once you are enrolled
  - Help Desk can focus assistance on getting users enrolled
  - Marketing to focus on protecting ones personal info

- Build a stand-alone user enrollment and update web application – flexible to support MANY integrations of which ESS is the first
  - Access enrollment from on-campus location
  - User login with HawkID
  - Enroll device(s) and methods
  - Return later to update profile (remove lost or add new device, etc)

Administrative view for Help Desks to assist users (DNA Tools)
Two-step authentication was enabled for your account on Friday, April 4, 2014 (at setup history). Any future configuration changes will require two-step authentication and will send email to your java-diree@uiowa.edu account notifying you of the change. We suggest that you add additional devices or generate a list of backup codes that you will keep in a safe place in case any of your devices are not available.

Getting Help with Duo: See Setup Smartphone, Setup Phone call, Setup Text Message, or Duo Support Center. Or, contact the ITS Help Desk at 384 HELP or its-helpdesk@uiowa.edu.

**Two-Step Devices**

You have setup the following devices. Select the device phone number or label to update or delete the device.

<table>
<thead>
<tr>
<th>Device</th>
<th>Method(s)</th>
<th>Added</th>
</tr>
</thead>
<tbody>
<tr>
<td>(319) 555-1234</td>
<td>Text message</td>
<td>Mar 3, 2014</td>
</tr>
<tr>
<td>(319) 555-2345</td>
<td>Duo Push app - iOS</td>
<td>Apr 1, 2014</td>
</tr>
<tr>
<td>(319) 555-3456</td>
<td>Voice call</td>
<td>Apr 4, 2014</td>
</tr>
</tbody>
</table>

**ADD DEVICE**

- **Phone number**: (319) 555-5555
- **How should we send security codes?**
  - Text message (SMS)
  - Voice call
  - Via the Duo Push application on available smart phones and tablets

- **Device Platform**: iOS ( iPhones, iPads, and iPod Touches )

- **Label**: A short descriptive label for this device (e.g., My iPhone, My office phone, etc.)

You will need to confirm a security code before adding this device.
Manage Duo Accounts

Query and/or clear a user's HawkID DUO service. Also, whitelist access can be enabled or disabled. Or enter a Phone Number to select the list of HawkIDs that reference the phone number. The Phone Number is ten-digits of the form 9999999999.

HawkID: | Phone Number: | Lookup | Clear

The following Duo information pertains to HawkID jtwrews.

<table>
<thead>
<tr>
<th>Status</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device:</td>
<td>Label: (319) 530 ; Phone: 219-530 ; Method: SMS; Confirmed: True</td>
</tr>
<tr>
<td>Device:</td>
<td>Label: Backup - desk; Phone: 319-333 ; Method: VOICE; Confirmed: True</td>
</tr>
<tr>
<td>Whitelisted</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Clear Duo Devices | Enable Whitelist | Extend Whitelist
• MFA is not the magic bullet – but it’s a very strong step

• BU has had MFA for years, but – like most university that have it at all – only used in limited cases for staff (never faculty) with access to our most sensitive data

• But this event proved that it was not just other people’s data we need to care for, but our own as well

• So we began a journey. A journey that we could not allow to fail…
… so we made sure to staff the project with that in mind

- Top talent to manage, architect, build and deploy the solution
- Didn’t have time for much of a learning curve

- Had to have visible and vocal support from everyone
- Particularly from senior leadership

- Outro: once we had the right people on the bus...

At Iowa, we had senior architects (Dev, IDM, Sec, HR) involved, as well as Strategic Communications, Help Desk

- our big issue was developing the enrollment app. Could have done without but we were thinking strategically about other integrations and used our best developers to get it done quickly.
- created a multi-mode communication plan. Gave a lot of talks about what and why. Created a phased deployment
- reported status and outcomes to ITS, HR, F&O, Budget officers, HR Reps, ITAdmins
- Involved administrators, senior leaders in pilot to generate buy in
We could then best figure out where to drive it and how.

We needed to make sure we had a fighting chance in the face of overwhelming constraints. MFA, particularly in higher ed, has historically been fraught. Everyone thinks of the old pain-in-the-butt token approach.

At Iowa, we were under a lot of pressure to “fix” ESS, so we could remove the emergency changes that were made. We ran the pilot and gathered a lot of feedback, and worked out a proposal that was accepted first by VP for HR, then also CIO, CFO, Provost, and rest of our cabinet.

We didn’t engage faculty much because we decided to make it optional for “regular” users.
Plan the route

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

(Index slide of the areas we will cover)

- So we new from a high level what we wanted to do and had the right people to help us do it. Now we could start planning. We’ll dig in to each of these areas in turn.

- First…
Similarly, we licensed all employees, and implemented our PeopleSoft using CAS based web login tool.

Our timeline was also short, and we were able to develop the two support tools, communication plan, training, etc. in 2 months.

We also chose a phased roll-out, which began in April.
Gaining stakeholder support at Iowa was accomplished by doing a pilot very quickly, inviting key stakeholders to participate, and see it for themselves.

Once our Pilot was complete, we developed a full production implementation plan that addressed all the feedback we had gathered.
Communication was absolutely the key.

- involve key stakeholders, mention at key meetings, well-timed broadcasts, remind of the phishing attack
- We started with a commission from the very top
  - A memo from president to entire org + mgmt meeting
- Focus Groups – Helped build awareness, get more input (more use cases like union rules), develop buy-in. Champions/SME’s.
- Broad email, 23 responses: 3 supportive, 3 detractive, the rest “how would I?” or “did you think of?”
- Training videos and Documentation
- Websites, FAQs, videos, banners
- All this activity allowed us to develop a comprehensive solution
- Analysis – technical analysis – what can and can’t the product do.
  - User cases. phones, txt, token, bypass network
- Telephone vs smart phone – talked to other schools (Stanford, Duke)
- Social/Political analysis
  - Get a feel for staff and faculty acceptance

- This process gathered support and approval from key stakeholders
- They knew we were taking their concerns seriously, not just bulldozing this through

### Have answers to stakeholder questions

<table>
<thead>
<tr>
<th>Question</th>
<th>Concern</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do I have to carry a token?</td>
<td>No. You can use your smart phone.</td>
<td></td>
</tr>
<tr>
<td>OK, How?</td>
<td>You can install an app or get a text or call</td>
<td></td>
</tr>
<tr>
<td>Will I be charged?</td>
<td>If you use the app, it is free</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you choose texts or calls, the University is charged &amp; your normal carrier charges apply</td>
<td></td>
</tr>
<tr>
<td>Do I have to enter the two-factor every time?</td>
<td>No. If on a computer that you alone use, you can have the system remember you *</td>
<td></td>
</tr>
<tr>
<td>I don’t have a smart phone</td>
<td>You can use the text or call option</td>
<td></td>
</tr>
<tr>
<td>I travel and sometimes have no data or voice connection</td>
<td>That’s OK, none is required</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The app can generate a code for you</td>
<td></td>
</tr>
<tr>
<td>I don’t have a mobile phone at all</td>
<td>The call can go to your desk phone</td>
<td></td>
</tr>
<tr>
<td>I don’t have any phone at all (or BU is contractually prohibited to use it for BU business)</td>
<td>We can set up a special hardened computer for you that will be your second factor</td>
<td></td>
</tr>
<tr>
<td>I hate all these options.</td>
<td>..........we can give you a token</td>
<td></td>
</tr>
</tbody>
</table>
Service Strategy at Iowa

- Help Desk needs visibility into enrollments
  - Enrollment and registered devices can be viewed
  - Ability to delete someone’s enrollment
  - Support Tool utilizes the Duo API
- Service description pages, FAQ’s, instructions
- Troubleshooting the enrollment tool
- Second level support is Security Office
InfoSec, service desk, IT partners in schools

Admins are admins, no granularity
  • we had a risk reward scenario
  • everything it logged
  • will role back when solution supports it

Pros and cons - rather have a risk of 70 admins vs 20k users.

Build into onboarding
  • The first sign-up window of weakness,
    • one time press + HR for new employees
Get in gear, feather the gas, and drive

- Set switch to “only those on this list” and begin
- 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 & Student Employees
- November – Flip the switch from opt-in to mandatory
  - All users who access SAP
- Help Desk prepared for an onslaught. Didn’t happen.

We were ready to go in March, but didn’t get final approval right away. Needed to build comfort.

- Phased roll out approach - key business users up front, faculty at end. mindful of busy/key time
- Technical options for forced enrollment vs bypass/manual

- Decisions made based on eventual mandatory usage. Willing to endure some manual processes for temp amount of time

We did a soft rollout in April, allowing staff to enroll. Those persons who had elevated access in ESS were given different communications, and told they would be required to use Duo.

Required employees were phased in gradually, starting with level 4 access, then level 3, level 2, and level 1, after a 2 month grace period.
### Ticking off the miles – Pilot & Opt-In

- **Pilot** – 487 users
  - Only 46 tickets in first month
- **Opt In Period** – 1168
  - (360 on first day)
  - Staff 55%
  - Faculty 28%
  - Student 17%
  - 135 tickets
- **1756 devices**
  - 912 iOS
  - 351 Android
  - 238 Landline
  - 161 Other (non smart phone)
  - 24 Windows Phone
  - 10 BlackBerry

- Pilot tickets – mostly add new device or people who wanted in to the pilot
- Opt in – less than 2 tickets a day
  - Tickets are very quick to resolve
- 26% non smart phone – 2 cent/call, 1 cent/txt
- Pilot tickets – mostly add new device or people who wanted in to the pilot
- Opt in – less than 2 tickets a day
  - Tickets are very quick to resolve
- 26% non smart phone – 2 cent/call, 1 cent/txt

At Iowa we have a similar use pattern. And we implemented a phased production implementation. About 12,000 users, and xx devices
We’ve had xxx duo tickets since yyy

Method profile is interesting…..
44% voice
28% text
24% push (smart phone)
4% passcode
User quotes

- On the user end this is actually pretty cool and super easy.
- …once a month to log onto my personal staff portal I just have to re-authorize my computer by hitting a button that pops up on my cell. … It’s remarkably instantaneous.
- I was hesitant to opt-in because anything two-factor sounds like a pain …. so I too find widespread willingness to adopt the technology a little surprising, but after initial adoption it’s been nearly invisible on my end, except that I know if someone tries to log onto my account from a new device I’d get an app alert to my cell or call to my office line.
• MFA on SAP may pave the way for coverage

• Remember, we had a number of people contact us asking if we could provide this level of protection for things beyond just SAP

• Potential for new services
  • High quality identity assurance enabling more helpdesk services
  • Win RDP, VMWare, Cisco, RADIUS…
After Effects

- People were worried, but this deployment turned out to not be a big deal
- Things we have done or are doing since
  - UI – VPN, HPC, additional CAS apps, data center remote access, IdM tools access, ...
  - BU – Working to standardize on Duo for all MFA, protect med campus server admin accounts, doing the same in two colleges, investigating the multi-context broker for context-sensitive SSO
Take action now. Limit the impact.

- As long as a piece of knowledge is the only thing between the bad guys and gain, the thing they want is at risk. – Compromise is “When”, not “if”.
- It’s time to be realistic about password security.
  - On it’s own, the protection it offers is minimal
- Consider modern MFA
  - The timing has never been better
  - The solution is very inexpensive and simple to deploy
- Don’t forget mobile device security.
  It will be the next target.