About us

Cara Bonnett

• 15+ years in communications
• At Duke since 2008
• Transitioned to infosec in 2013
• Focus in policy, risk, outreach

Phillip Batton

• In IT since 2000
• At Duke since 2004
• Joined ITSO in 2012
• SecOps Team Lead
• Policy, Risk, & Awareness
• GCED, GCIE, GPEN, GCFE, & GCFA
What is your goal?

Who is your audience?

What is your message?

How do you measure success?
IT @ Duke

Central IT (300) ~600 in schools

225 on listserv ~30-40 at monthly meetings

CISO + 9 FTE
Awareness (the old way)

• National Cybersecurity Awareness Month
• “Spot the phish” quiz / contest
• Learn IT @ Lunch sessions
Then the bottom fell out
TWO-STEP VERIFICATION REQUIRED TO ACCESS DUKE@WORK

Starting July 1, staff and faculty must use multi-factor authentication to access personnel information
What’s our goal?
we built it ourselves!
The design
Who:

• 1 cohort (~20) of university IT staff
• 18 from schools/units, 2 from central IT
• Mostly desktop/server admins

What:

• 4 core classes, based on security frameworks
• 8 electives (Duke-specific tools and applications in the Duke environment)
• Once-a-month sessions (Feb-Nov)
Objectives

- Become familiar with the principles and methods of information security, and when/how best to apply them
- Understand the terminology used in information security
- Relate security principles to real-life situations and identify lessons learned
- Integrate information security into your IT role and function
Protect: Objectives

Familiarize with the current reality of protection

Approach protection in a layered format

Provide SME contact information
Protect: A Layered Approach

Central Server Configuration & Patch Management, Endpoint Management

Multifactor Authentication, Whole Disk Encryption, Host-based Firewalls

Anti-virus, Host-based Intrusion Protection, File Integrity Monitoring, Application Whitelisting

Core

Middle

Outer
Protect: Tasks and Case Studies

Task: Deploy web kiosks for guest access in four different student lounges

Task: Deploy 30 new laptops that will contain patient medical data

What could go wrong?
Detect: Objectives

Differentiate between an event and a security incident

Value the importance of security in each role at Duke

Become familiar with detection methods and technologies at the institution

Collaboration is key (internal and external)
Detect: Types of incidents

- Phishing
- Data leakage
- Compromised credentials
- Vulnerable applications / systems
- Infected / compromised hosts
- Threat intelligence
React: Objectives

Identify and/or develop processes

Empower the individual

Walk through scenarios
React: Incident examples

• Compromised accounts
• Suspicious emails
• Data Leakage
• Departmental system is spamming
• Ransomware
• Website defacement
Duke’s electives

- Bigfix
- SCCM
- Casper
- Vulnerability Assessment
- Data Loss Prevention (DLP)
- Endpoint Protection
- Log Analysis / Correlation
- Packet Analysis
Halfway there
What we learned

• Group had limited knowledge of centralized IT services
• Participants wanted more interaction with each other in a safe space
• Give us cheat sheets and homework (!!!!)
• Include managers
Unexpected takeaways

• IT staff need training/onboarding in security, networking, identity management
• Group wanted ongoing involvement – even after the program concluded
• We need to change: Education is everyone’s job
Academy 2.0

- 2nd cohort launched February 2017
- Still a yearlong program, structured differently (mix of core and electives)
- NEW: IT security fundamentals course for all IT + consulting service
What they said

• “Develop new reports in Splunk; Manage live SEP upgrade more efficiently; Use portable wireshark to help with performance analysis on servers.”

• “Securing all endpoints including mobile devices and maintaining an inventory of software/apps require MFA for access to department resources.”

• “Making sure all of our database servers are protected by Duo.”

• “I plan to work more with Security Center in creating and running custom scans, and developing useful reports for presenting the scan results.”

• “We had run DLP scans before, but that was before I had started and they hadn't been done in a while. Over the past few months, we've already scanned a number of department servers and addressed a lot of issues.”
Security Awareness Maturity Model

Before

After

Non-Existent

Compliance Focused

Promoting Awareness & Behavior Change

Long Term Sustainment & Culture Change

Metrics Framework
One brick at a time
Relationships lead to awareness
It’s easier than you think!
If you build it...
Questions?
Thank you!

Cara Bonnett
Cara.Bonnett@duke.edu

Phillip Batton
Phillip.Batton@duke.edu