CYBERSECURITY AND NOT-FOR-PROFIT ORGANIZATIONS

Presented By
Chris Ellingwood, CISA

BerryDunn

AGENDA

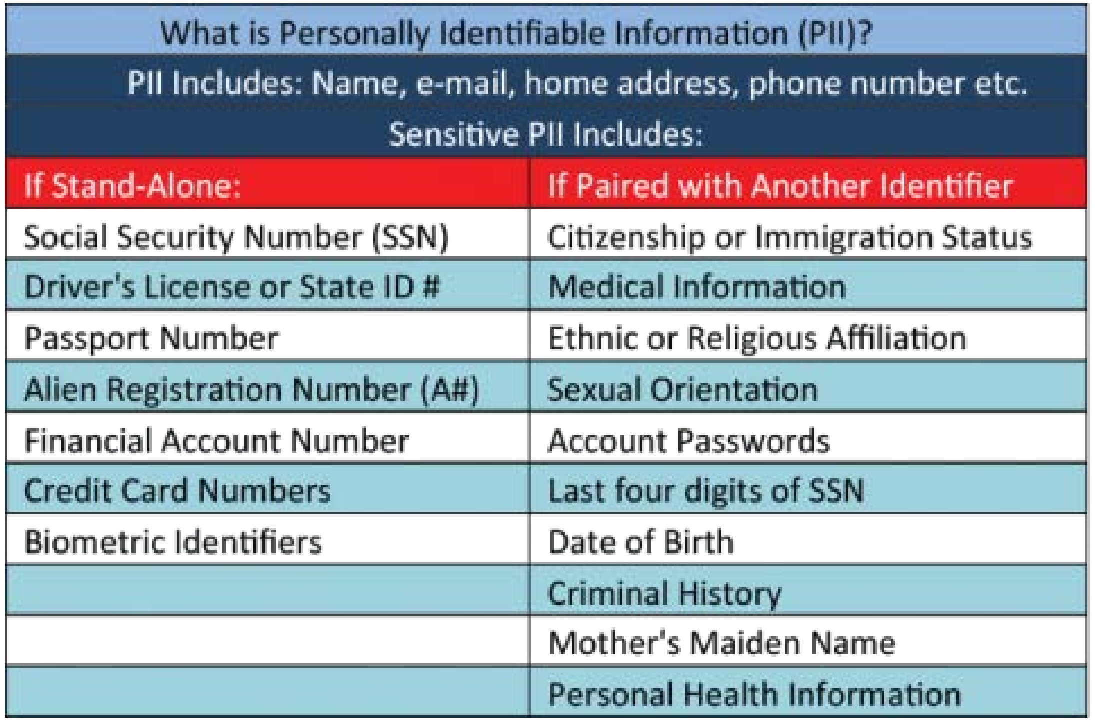
1 WHY NOT-FOR-PROFIT ORGANIZATIONS SHOULD BE AWARE

2 RISKS TO BE AWARE OF

3 5 BASICS STEPS TO TAKE NOW

NOT-FOR-PROFITS HAVE WHAT HACKERS WANT

- NFP healthcare organizations – Personal Health Information (PHI)
- NFP Community Organizations – Donor and Clientele Information
- NFP Educational Organizations – Personal Information, PHI, and Research Data



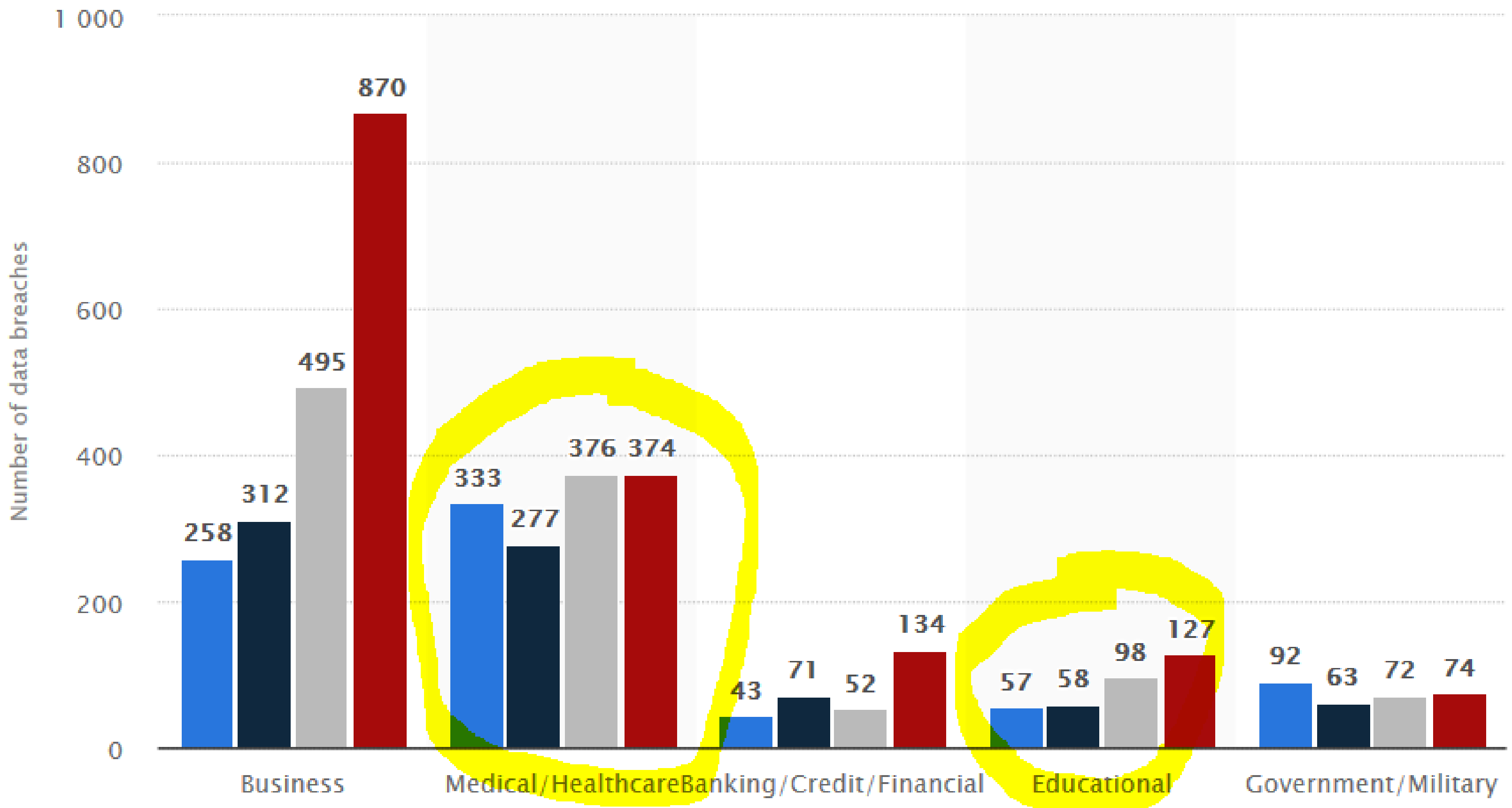
What is Personally Identifiable Information (PII)?

PII Includes: Name, e-mail, home address, phone number etc.

Sensitive PII Includes:

If Stand-Alone:	If Paired with Another Identifier
Social Security Number (SSN)	Citizenship or Immigration Status
Driver's License or State ID #	Medical Information
Passport Number	Ethnic or Religious Affiliation
Alien Registration Number (A#)	Sexual Orientation
Financial Account Number	Account Passwords
Credit Card Numbers	Last four digits of SSN
Biometric Identifiers	Date of Birth
	Criminal History
	Mother's Maiden Name
	Personal Health Information

MANY OF YOU ARE ALREADY TARGETS



https://www.statista.com/statistics/273572/number-of-data-breaches-in-the-united-states-by-business/

HEALTHCARE (AND HIGHER EDUCATION)
A NEW EMPHASIS ON HIPAA COMPLIANCE

- The Office Of Civil Rights Has Started Audits
- Must prove compliance to HIPAA
- Higher Education – healthcare clinics on campus, healthcare programs if working with patients

THE MOST COMMON FINDING?

HIGHER EDUCATION
A NEW EMPHASIS ON SECURITY

- 2016 Dear Colleagues Letter, DOE
- Requires all Institutions who receive Federal Student Grants (financial aid) to comply with Graham Leach Bliley Act (GLBA
  - Information Security Program
  - Data Privacy
  - Incident Response
- Annual audit requirements (coming!)

HIGHER EDUCATION
A NEW EMPHASIS ON SECURITY

- Compliance may be achieved through the National Institute for Standards and Technology Special Publication 800-171
- Recommended by DOE
- A note on the European Union’s General Data Protection Rule --- this may apply!

CONSUMERS EXPECT PRIVACY TO BE CONSIDERED

17%

Are confident in US Organizations' ability to protect their data

85%

Believe much more can be done

62%

Believe their data will be hacked within the next 5 years

Harris Poll Data on behalf of IBM

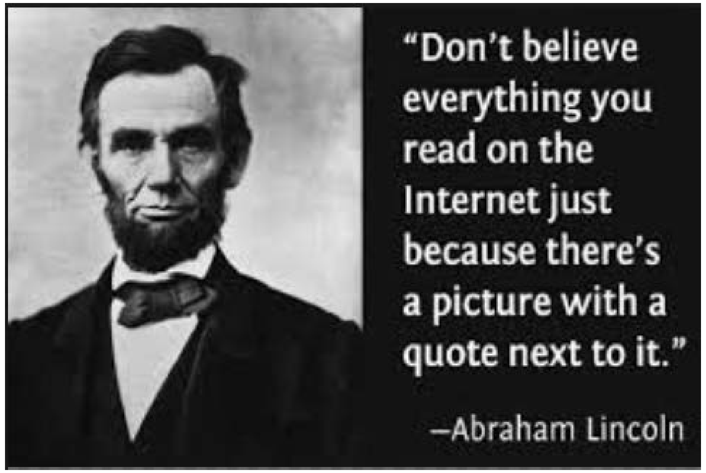
RISKS TO BE AWARE OF

TOP SECURITY RISKS

1. The Internet of Things (IoT)
2. Network Secured Only At Perimeter
3. **The World of Fakes**
4. Smartphone Hacking
5. Mergers and Acquisitions
6. **Lack of Data Classifications**
7. Cyber Insurance
8. **Phishing**
9. **Lacking Risk Assessments**
10. **Ransomware**

INTERTWINED WITH SOCIAL MEDIA

- 89% of NFPs and Charitable Organizations use Social Media for marketing and fundraising
- Social Media followers and donor lists are valuable hacker resources
- Phishing emails to your donors, followers, alumni, etc. asking for money on your behalf
- Impersonate your organization on Social Media (fake pages)


"Don't believe everything you read on the Internet just because there's a picture with a quote next to it."
–Abraham Lincoln

YOU CAN’T PROTECT WHAT YOU DON’T KNOW YOU HAVE…

HARDWARE AND SOFTWARE INVENTORY

- What does our network look like?
- What software do we use and how do we use it?
- What data is stored on our network?

THE TYPE OF DATA YOU HAVE

- Restricted
- Private
- Public

YOU CAN'T PROTECT WHAT YOU DON'T KNOW YOU HAVE…

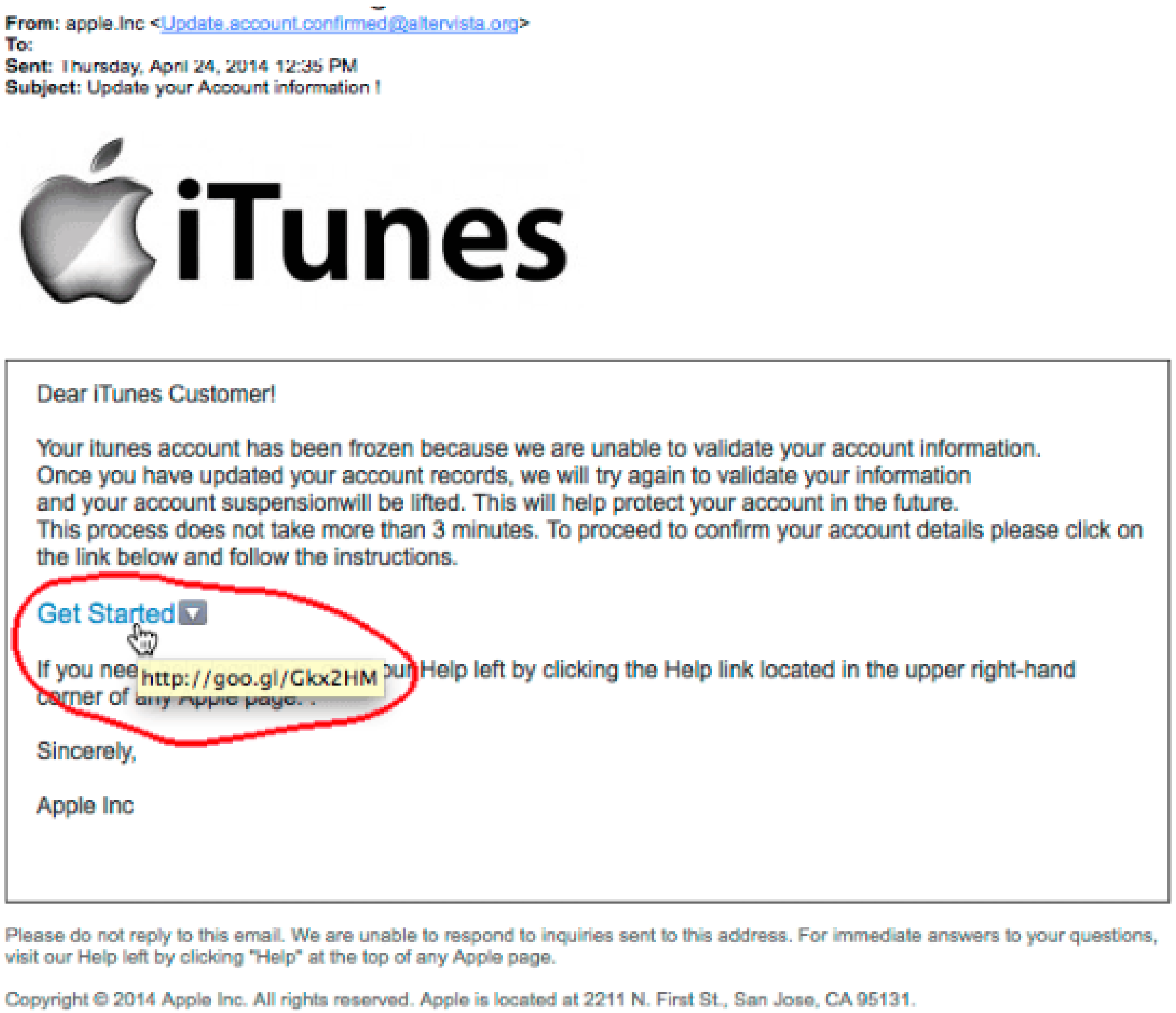
- Security measures for each level
- Policies for data transmission and retention

WITH GDPR, ABILITY TO "FORGET" A PERSON.

THE FOCUSED ATTEMPT TO GET YOU TO CLICK.

- Emails that appear legitimate, but are fake
- Typically require action
- Seeking Information
    - Name, birthdate, address
    - Username and passwords
    - Account numbers
    - Credit Cards

PHISHING EMAILS TO YOUR ORGANIZATION



From: apple.Inc <Update.account.confirmed@altervista.org>
To:
Sent: Thursday, April 24, 2014 12:35 PM
Subject: Update your Account information !

Dear iTunes Customer!

Your itunes account has been frozen because we are unable to validate your account information.
Once you have updated your account records, we will try again to validate your information
and your account suspensionwill be lifted. This will help protect your account in the future.
This process does not take more than 3 minutes. To proceed to confirm your account details please click on the link below and follow the instructions.

Get Started

http://goo.gl/Gkx2HM

If you nee our Help left by clicking the Help link located in the upper right-hand corner of any Apple page. .

Sincerely,

Apple Inc

Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help left by clicking "Help" at the top of any Apple page.

Copyright © 2014 Apple Inc. All rights reserved. Apple is located at 2211 N. First St., San Jose, CA 95131.

SPEAR PHISHING

- Phishing emails with thought. Research you and seek specifically you out
- Social Media and website
- Normally done at the executive level

FAKE INVOICE MESSAGES ARE THE #1 TYPE OF PHISHING LURE.

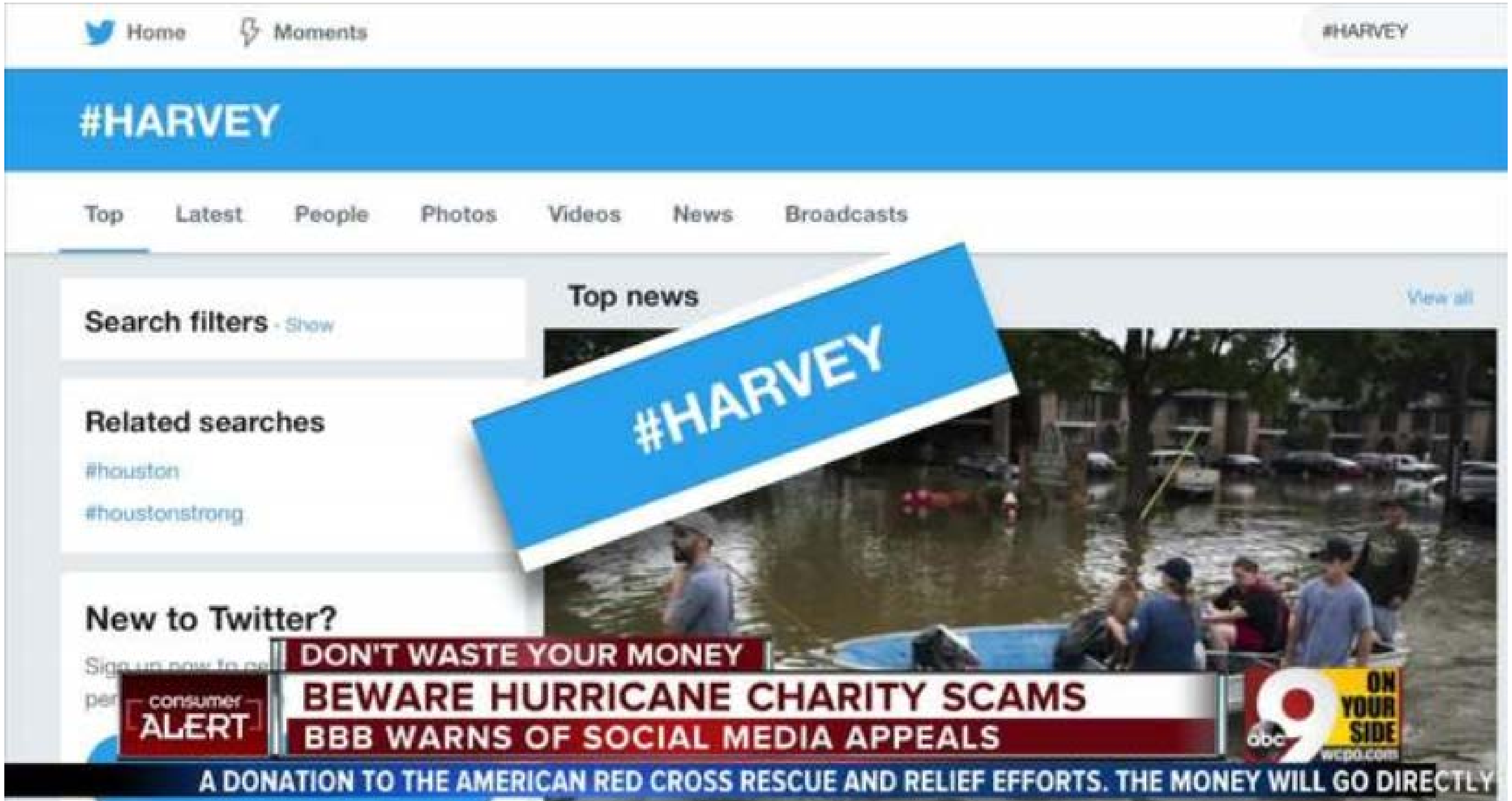
THE AVERAGE CLICK RATE OF A PHISHING EMAIL CAMPAIGN?

20%

It only takes one person.

Symantec

- Someone posing as your organization
- Seeking donations through an online campaign
- Common after a tragedy or disaster



THE FUNDAMENTAL FIRST STEP TO ANY SECURITY PROGRAM

- What can go wrong?
- What are the impacts?
- What controls do I have in place to mitigate the risk?
- What do I need to do?

COMPLIANCE

- What is required?
- Do I have controls in place to address?
- Where are the gaps?

VENDOR MANAGEMENT

- How important is the vendor to our organization?
- What data do they have, or have access to?
- How do they protect it?
- How do I monitor them?

- System lockout through encryption
- Entire network encryption and lockout (worm)
- Webpage Denial of Service Attacks

1 IN 131 EMAILS CONTAINED MALWARE IN 2016, THE HIGHEST RATE IN 5 YEARS.

IN HEALTHCARE

ONLY INDUSTRY WHERE AN INCREASE IN RANSOMWARE IS SEEN IN 2018

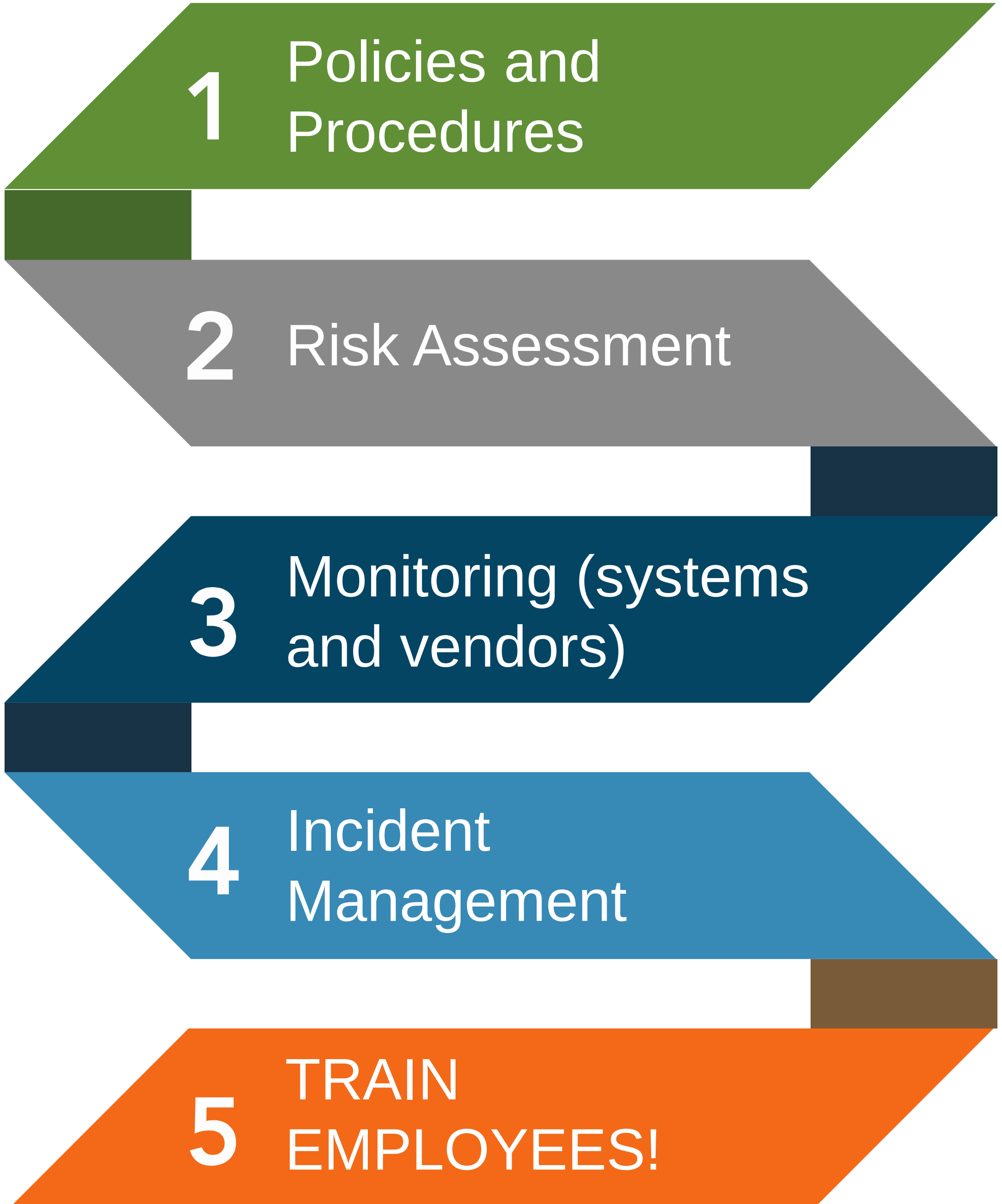
But a decrease in data breaches

USED AS A “FOIL ATTACK”

INCREASE IN BANKING TROJANS

- Steal your bank account info through key loggers and other methods
- Come though, hidden in a .pdf or .doc file

WHAT YOU CAN DO NOW!



1 Policies and Procedures

2 Risk Assessment

3 Monitoring (systems and vendors)

4 Incident Management

5 TRAIN EMPLOYEES!

CHRIS ELLINGWOOD, CISA
Senior Manager
cellingwood@berrydunn.com
207.541.2290