Armstrong Teasdale

Cyber Security Basics
What Educators Need To Know

Scott Casanover, General Counsel – West Coast University
Bruce Denson, President – Cobbs Allen
Daniel Nelson, C|EH, CIPP/US, Partner _ Armstrong Teasdale LLP
Bill Ojile, Partner – Armstrong Teasdale LLP

Agenda

- Why is Information Security ("InfoSec") important?
- User Security: Your biggest concern
- Incident Response: What to do before, and after, it all hits the fan
- Cyber Insurance: What to look for, and why
- Vendor Due Diligence and Contracting

Why InfoSec?

Regulators Require Cybersecurity Measures

- ***E.g.*, Department of Education Dear Colleague Letter: 7/1/16**
  - School's Program Participation Agreements and the Graham-Leach-Blilely Act (GLBA) require schools to protect student financial aid information
  - This includes
    - Maintaining a written InfoSec program
    - Appropriate Vendor Selection
    - Implemented information safeguards program
    - Designated person(s) responsible for InfoSec

Other Laws

- **HIPAA**
  - Your institution is subject to HIPPA if:
    - You are self-insured for Employee health insurance; or
    - You maintain on-campus health facilities

- **FERPA: Cybersecurity is an essential part of ensuring educational records privacy**
- **State Law, for example:**
  - California Data Breach Notification Statute
  - California Invasion of Privacy Act

Data Breach is only one of many threats

- Ransomware
- Cyber extortion
- Denial of Service Attacks
- Data Integrity Attacks
- Pivoting
- Non-malicious data loss/corruption
- Control System attacks

Armstrong Teasdale

The Stark Reality

Education Institutions are targets

You don't have to be targeted to get hit

YOU WILL GET HIT

The Most Basic Cyber Security Truth

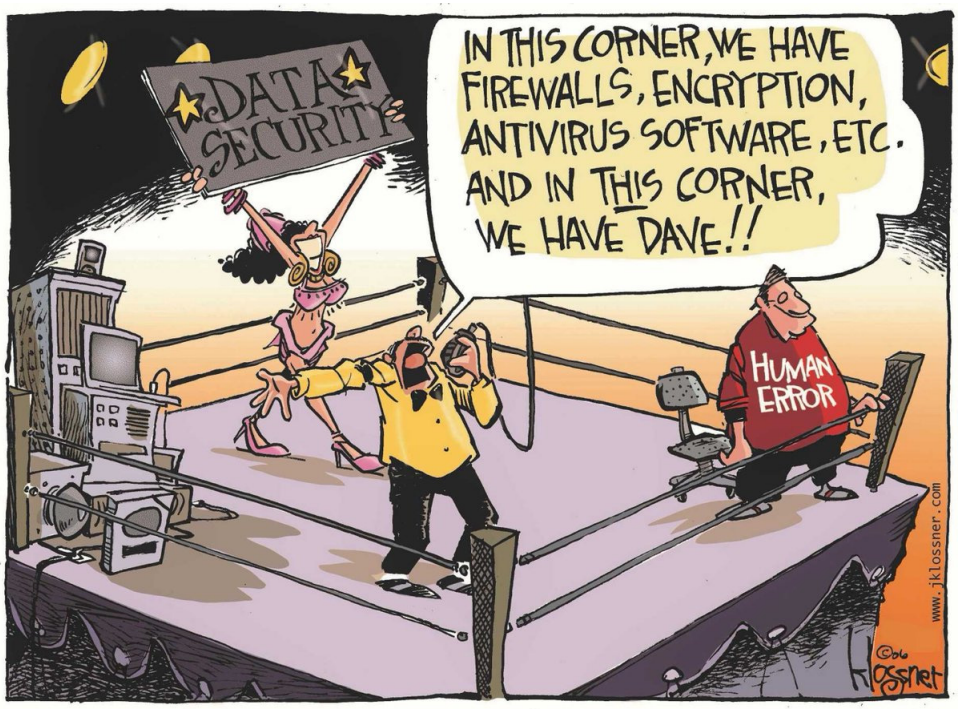
There is not now, and never will be, a "box" that provides "Cyber Security"

PEOPLE

Armstrong Teasdale

Why "People"

- Because Artificial Intelligence hasn't gotten around to eliminating us yet
- We design, control, configure, and interact with the information and technology
- We are the weak link
- And every hacker knows it



Armstrong Teasdale

Human Threats

- Social Engineering
- Malicious Insiders
- Design Error
- Human Mistakes

Armstrong Teasdale

Social Engineering

- **"Hacking the Wetware"**
- **The most direct, efficient and effective form of attack**
- **Takes Many Forms:**
  - Phishing/Spearphising
  - Physical Intrusion
  - Information Gathering
- **Odds are strongly in Hacker's favor**

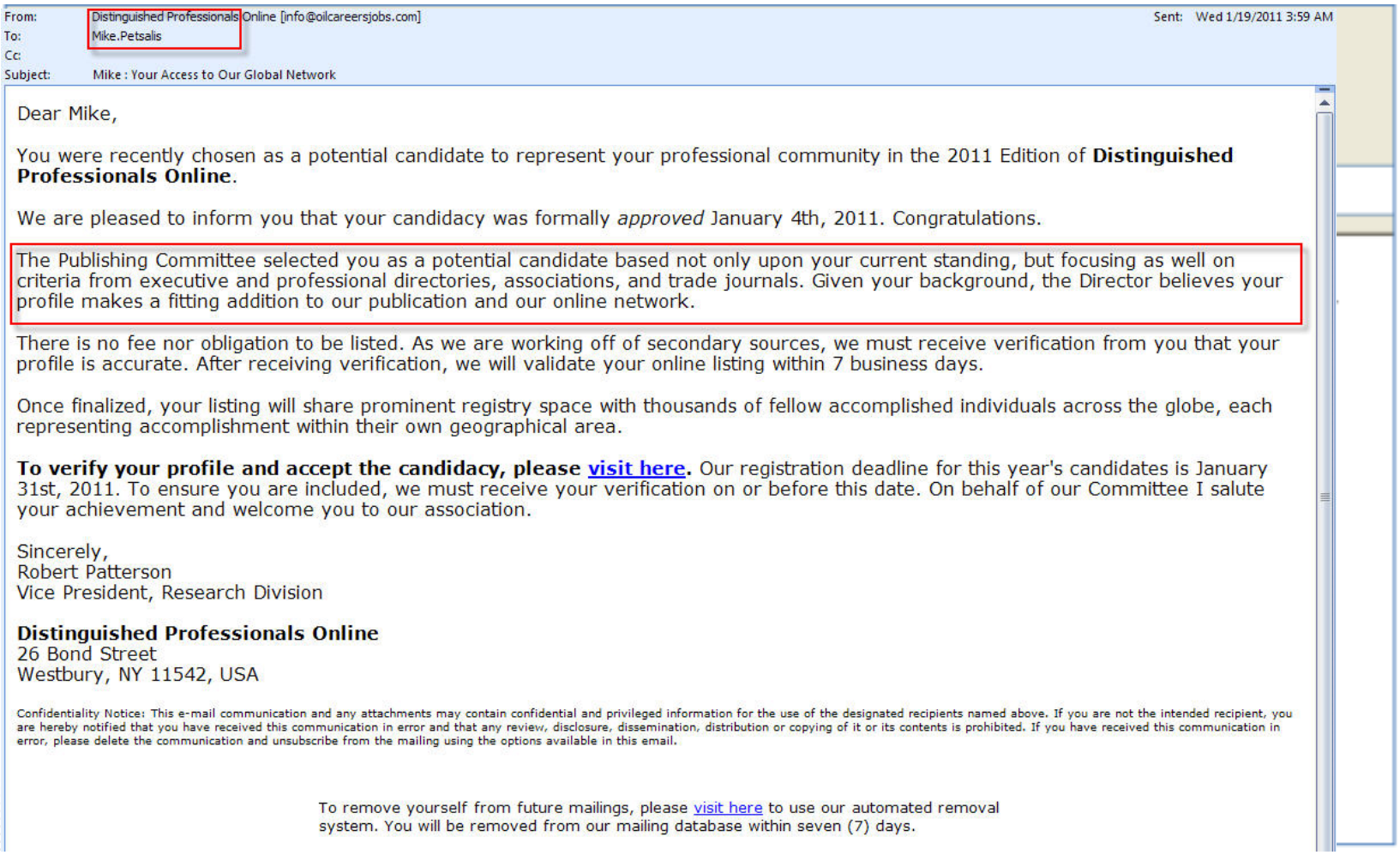
Armstrong Teasdale

Phishing/Spearphishing

- **Phishing: Impersonal "blast" email**
- **Spearphishing: Uses personal information about "sender" or recipient to encourage recipient to trust the email**
  - Vacation plans
  - Recent promotions
  - Company events
  - Hobbies
- **This information is all too easy to find:**

Armstrong Teasdale

Spearphishing Takes Many Forms



From: Distinguished Professionals Online [info@oilcareersjobs.com]
Sent: Wed 1/19/2011 3:59 AM
To: Mike.Petsalis
Cc:
Subject: Mike : Your Access to Our Global Network

Dear Mike,

You were recently chosen as a potential candidate to represent your professional community in the 2011 Edition of **Distinguished Professionals Online**.

We are pleased to inform you that your candidacy was formally *approved* January 4th, 2011. Congratulations.

The Publishing Committee selected you as a potential candidate based not only upon your current standing, but focusing as well on criteria from executive and professional directories, associations, and trade journals. Given your background, the Director believes your profile makes a fitting addition to our publication and our online network.

There is no fee nor obligation to be listed. As we are working off of secondary sources, we must receive verification from you that your profile is accurate. After receiving verification, we will validate your online listing within 7 business days.

Once finalized, your listing will share prominent registry space with thousands of fellow accomplished individuals across the globe, each representing accomplishment within their own geographical area.

To verify your profile and accept the candidacy, please visit here. Our registration deadline for this year's candidates is January 31st, 2011. To ensure you are included, we must receive your verification on or before this date. On behalf of our Committee I salute your achievement and welcome you to our association.

Sincerely,
Robert Patterson
Vice President, Research Division

Distinguished Professionals Online
26 Bond Street
Westbury, NY 11542, USA

Confidentiality Notice: This e-mail communication and any attachments may contain confidential and privileged information for the use of the designated recipients named above. If you are not the intended recipient, you are hereby notified that you have received this communication in error and that any review, disclosure, dissemination, distribution or copying of it or its contents is prohibited. If you have received this communication in error, please delete the communication and unsubscribe from the mailing using the options available in this email.

To remove yourself from future mailings, please visit here to use our automated removal system. You will be removed from our mailing database within seven (7) days.

Armstrong Teasdale

POLICY

Armstrong Teasdale

Most Companies Lack

- **BYOD**
  - Employee Privacy + Company Data = Technical & Legal Mess
- **<u>Good</u> Acceptable Use Policy**
  - The claims you will call me about most often relate to "exceeding authorization," but that's not often well defined
- **Termination Procedures**
  - Your companies newest ex-BFF has a lot more access to company information than you think
- **Incident Response**
  - Does your local Fire Department have a plan? Then so should you

Armstrong Teasdale

Your Hardest Task, and Your Biggest Win

Combat Social Engineering

Raise Awareness

Repeat

Armstrong Teasdale

"Awareness" is not "Training"

- **Attempting behavior change:**
  - Pause before clicking that link
  - Lock your computer
  - Promptly disclose suspected incidents
  - Question strangers
- **Attackers are trying to trigger a particular "no-thought" response**
- **Fight them on their terms: trigger better behaviors**
  - More Advertising than Education

Making Your Awareness Program an EPIC FAIL

- Do it annually
- Use only a single medium
- Explain at length
- Do not use humor
- Make it look like every other company communication
- Punish, Don't Reward
- Nothing Flashy, Nothing Catchy

How Effective is This?

Image courtesy of the security awareness company @ www.thesecuritywarenesscompany.com

Armstrong Teasdale

Incident Response

Armstrong Teasdale

7 Stages of a Data Breach Response

- Preparation
- Identification
- Containment
- Eradication
- Notification
- Recovery
- Lessons Learned

Armstrong Teasdale

Why Have a Plan

- **Often required**
  - PCI
  - HIPAA
  - GLBA
- **Regulators/Accreditors care**
  - FTC Guidance: Reasonable plan, reasonably followed, may be the difference with respect to regulatory action decision
- **Insurers care**
  - You will be asked in the underwriting process
- **Third parties increasingly intolerant of botched response**

Prepare Your Plan

- **Statement of Purpose: Why we have this plan**
- **Identify Your Breach Response Team**
  - Incident commander (and backup)
  - Breach coach (lawyer)
  - Internal resources (primary & backup)
    - HR, IT, Customer Relations, Communications, Major Business Units
  - External Resources
    - Breach Coach, Forensics Vendor, Identity Theft Services Vendor, Crisis Communications

Define "Incident"

- **Not all incidents are a five-alarm fire**
- **May be different communications structures for different incident levels**
  - No incident is "minor"
  - Level 1, Level 2…

Map Team Communication

- **Who is called first?**
  - What if they are not available?
- **Have pre-established communications**
- **Plan alternate communication modes**
- **Standards for Senior Management/Board Communication:**
  - When? Who? How?
- **Names, numbers, email,**

Map External Communication

- Who is notified of a breach and when and how?
  - Does every breach require notice?
  - Mail vs. Email notification.
- Draft document templates.

Recovery

- **Pre-Analysis of "What Next" for Likely Scenarios**
- **Technical**
  - E.g. Restoration from Backup
- **Business**
  - E.g. Post-event communications

Key Data Breach Steps

- **Identify Live vs. Historical**
- **Isolate**
  - Do not turn-off, power down, log in
- **Gather & Preserve other evidence (e.g. logs)**
- **Contact counsel**
- **Counsel hires external forensics**
- **Appoint a leader**
- **Gather a team**

Key Information

- **What data**
  - How is this verified
- **How did breach occur**
- **Date of incident/intrusion (if known)**
- **Date of discovery**
- **Method of discovery**
- **Number of affected individuals**
- **Residence of affected individuals**
- **Who has knowledge of incident**

Biggest Mistakes

- Failure to Plan
- IT Takes Control
- Lack of Centralized Control
- Self-Investigation
- Delay

Cyber Insurance

Armstrong Teasdale

Cyberinsurace

- **Most E&O, CGL, P&C policies specifically include cyber losses**
- **Called the "Wild West" of insurance for good reason**
  - Pay very close attention to definitions, coverages, exclusions and sublimits
- **Heavily underwritten, so be prepared**
- **Finding a policy tailored to your specific needs is difficult**
  - Need to work with a truly qualified broker
  - Integrate with risk assessment
- **Often too much focus on data loss, not enough on business interruption**

Contracting

Armstrong Teasdale

Can Vendors Hurt You?

Fazio Mechanical

The damage is often not done at the point of entry

Armstrong Teasdale

Contracting

- **Vendor Due Diligence on InfoSec**
- **Least Access to sensitive data and systems**
- **Contract clauses in all vendor contracts:**
  - Security clause
  - Required cyber cover
  - Defense and indemnity for costs and claims

Questions?

Presenter 1

Presenter 2

Dan Nelson, C|EH, CIPP/US, Partner
720.722.7191 dnelson@armstrongteasdale.com
www.linkedin.com/in/danielcnelson

Armstrong Teasdale