10 Tips for a Successful Cyberaudit

Peter Brickman

Chief Technology Officer

WNET New York

WNET- Overview

- 3 Stations
- 375 Staff
- 180 Edit Stations
- Outsourced & Insourced Software
- Collect data on Staff, Members, Viewers, Boards
    - Credit Cards
    - SS#
    - Medical
    - Banking

The HACK

- Phishing email
- Acquired user Passwords
- Accessed users computer
- User 1:
  - Accessed users HCM account
    - Changed Direct Deposit info
    - Created Outlook rule to delete notifications
- User 2:
  - Had access to a spreadsheet with employee confidential information
    - No confirmation that the file was actually accessed.

#1 Proactive or Reactive?

If your company was subject to an attack, remedy the attack first

- Hire a Cyber firm capable of providing a full spectrum of assistance
  - Don’t exclusively rely on internal teams
  - Once remedied, include lessons learned in the RFP for the Cyber Audit

If you THINK you’re safe, get an understanding of your use of private data

- Credit Cards, Personnel files, Vendor information

# 2 Develop an RFP

- Get CEO buy in
- Form a working group to define the RFP
  - Assists in company acceptance of the results
    - Finance, Legal, HR, IT, Production, etc
- Identify your needs
  - Written Documentation
  - BCP
  - Workflow using private data
  - Staff Training
  - Internal and external Penetration Testing.

#3 Identify qualified vendors

- Recommendations from your industry
- Recommendations from your Cyber Insurance vendor
    - You have a Cyber Security Insurance Policy don’t you?
- Certifications
    - CISSP, GCED, GPEN etc.

#4 Don’t underestimate the time needed to

- Interview key departments
- Train the staff (everyone)
- Remedy the recommendations post audit

#5 Engage a Cyber Security partner

- Execute an NDA and insure that all findings are attorney/client privileged information

#6 It’s all about the follow through

- Assign a staff PM
  - Attends all departmental interviews
  - Schedules staff training
  - Works with departments to modify vulnerable workflow
  - Works with IT staff to analyze and remedy penetrations results
  - Minimize scope cream and scheduling delays

#7 Training should be fun

- Primarily instructs the staff how to behave in a Cyber Predatory world.
  - Valuable information in their personal and office life
  - Social Engineering
    - Our CEO is the source of most of the Phishing
  - Include how big companies made the news when their data was compromised or ransomed
  - Encourage staff to get personal credit reporting tools
  - Included training for your staff on boarding
    - Video the session

#8 Implement MFA ASAP

- Multifactor Authentication- The lowest hanging fruit
    - Is it really you?

#9 Phase 2: Pull the bandage off

- Identify secure alternative for cloud based tools
  - File and video transport
  - Document sharing
  - Collaboration Software
- Create a DMZ to import files
- Insure all formal documentation is in place and updated for:
  - Personally Identifiable Information (PII)
  - Protected Health Information (PHI)
  - Payment Card Information (PCI)
  - Trade Secrets / Intellectual Property

#10 How’s your patching?

- Always up to date
- Test first when you can

You still can’t sleep but it’s ok to nap

- Keep up the discipline
- Keep your Cyber Audit company engaged for a yearly refresh
- Make sure that your staff understands that Cyber Security is a part of your companies new culture

THANK YOU!