Managing Your Program's Cybersecurity Risk

NCSHA HFA Institute

January 17, 2020

Some Numbers

- 3 employees entered email system credentials as a result of a hostile phishing attempt
- 4 senior staff members reviewed 75,000 – 100,000 emails over a 5 week period
- Ultimately, 235 letters were sent to individuals with emails containing the critical combination of non-public personal information
- We estimate $50,000 - $75,000 in lost productivity salary costs for WCDA Executive, Legal, and IT staff members
- Estimate another $25,000 will be spent in legal costs, additional IT solutions, mailing costs, increased staff training, and Experian Identity Works memberships

What We Have Done Internally

- All employees changed passwords immediately and the requirement for future passwords changes was lowered from 90 days to 45 days
- Implemented 2-factor authentication for employee email
- Changed email retention policies from 2 years to 6 months
- Added a “Phishing Alert” button to all email-boxes to aid employees in notifying IT of suspicious emails
- Added a phishing warning to all externally generated emails received in employee email-boxes

What We Have Done For Affected Individuals

- Offered a one-year membership in Experian's Identity Works product (identity detection and resolution to identity theft)
- Provided information on how to enroll in the product by 2/28/2020
- Provided the phone number for Experian's customer care team
- Provided the phone number for Experian's agents if individuals believe their information was used fraudulently
- Directed individuals to information about freezing their credit file
- Provided info about obtaining a free copy of their credit report
- A 1-800 number to WCDA if individual wants to discuss the matter with our Director of Legal or our Executive Director

Where We Are Now

- Have received less than one dozen phone calls to our office
- Waiting to see how many took advantage of Experian Identity Works
- Currently drafting personnel policies to address:
  - Failure of internal phishing campaign
  - Self-reporting vs. eventual discovery of entering system credentials
  - Access to company systems by unauthorized parties (an actual breech)
  - Notification by email filters of attempts to send unencrypted emails with NPI
  - Definition of what constitutes sensitive information and/or NPI for disciplinary actions
  - Time periods under which actions are tracked (annual, rolling two years, etc.)
  - Consequences of unwanted behavior by staff (grace periods, escalation, etc.)