ANNUAL CONFERENCE & SHOWCASE
OCTOBER 27 – 29
VIRTUAL 2020

Managing Cybersecurity Risks

NCSHA

LESLI WRIGHT, DEPUTY EXECUTIVE DIRECTOR | WYOMING COMMUANITY DEVELOPMENT AUTHORITY

JOSHUA N. MACDIARMID, SPECIAL AGENT, MONEY LAUNDERING, FORFEITURE, AND BANK FRAUD UNIT | FEDERAL BUREAU OF INVESTIGATION

TODD KINNEY, PARTNER | KUTAK ROCK LLP

NICOLE MORIARTY, PARTNER | KUTAK ROCK LLP

PRESENTERS

NCSHA

Some Numbers

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

Some Numbers, cont.

- Average time to identify & contain a breach: 280 days (IBM report)
  - The costs—direct and indirect—are directly tied to how long it takes you to identify and contain a breach
- Lesli's team: 82 days
- Everything Lesli is going to mention today—what they did, how they handled it, etc.—resulted in a much shorter time period

Poll Question

Has your organization ever experienced a cyber incident?

Data Breach

- Chances of suffering a data breach: 28%
- May not sound like a lot, BUT….
  - Odds have been increasing at significant rate the past 5 years
  - Data breach = fire (.5% chance) or tornado hitting your business
- Excuses for lack of data breach preparedness
  - We'll get to it later
  - Too expensive
  - I don't understand it
  - It won't happen to us
  - Imagine applying those excuses if you knew there was a 28% chance of your building catching on fire

Data Breach Risk in a Nutshell

“Cybercrime is the greatest threat to every profession, every industry, every company in the world.”

— Ginni Rometty, IBM’s Chairperson and former CEO

Good news is: You can take steps to significantly manage your risk. This is absolutely doable.

What WCDA Has 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
- Engaged email filters to notify IT staff of attempts to send unencrypted emails containing NPI
- Engaged system to auto-encrypt such emails and then send out safely
- Subscribed to an online file sharing system to reduce the amount of emails containing nonpublic personal information (NPI)

What WCDA Has Done Internally

- 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 WCDA Did 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 Identity Works
- 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

Dealing With Affected Individuals

- Everything I learned about dealing with affected individuals, I learned in kindergarten
  - Acknowledge what happened
  - Apologize
  - Listen to them
  - Provide information
  - Sounds simple, but it doesn't always happen

WCDA

Where WCDA is One Year Later

- Received less than one dozen phone calls to our office about the breach
- 23 (or 10%) of the affected individuals took advantage of Experian Identity Works
- Revised the IT Sensitive Information and Encryption policy:
  - Provided detailed list of what constitutes NPI
  - Added a list of actions that constitute a violation of the policy;
    - Opening an email, followed by clicking on its attachment and/or clicking on a link in said email that is subsequently found to be a phishing scam or illegitimate site.
    - Emailing NPI or transmitting NPI without it being properly encrypted.
    - Disclosing NPI, or any other category of sensitive information to any unauthorized person.
    - Breaching of any WCDA system containing NPI, or any other category of sensitive information, that allows access to non-WCDA persons or any unauthorized person.

Where WCDA is One Year Later

  - Established time periods under which actions are tracked (rolling two year period)
  - Detailed consequences of unwanted behavior by staff (coaching, security training, verbal/written warnings, termination)
- Have had one additional breach by a program staff person since the initial breach
  - Bad news – Was due to an oversight of not adding 2-factor authentication to a new staff person's email system
  - Good news – Because of some of the steps taken over the last year, no NPI was found in the staff person's emails, thus notification was unnecessary
- Still sorting out best ways to document and enforce violations of the revised IT Sensitive Information and Encryption policy.

The Big Picture and R.O.I.

- On a macro level, the steps Lesli described put her organization in a much better place to handle the next breach.
- On a more specific level, it has been proven over and over again that these types of steps save real money.
  - IRP = $14 per record
  - Employee training = $9 per record
  - Encryption = $13 per record
  - Insurance = $5 per record

Poll Question

Has your organization developed written policies and procedures for if/when an information security incident occurs?

(e.g., an Incident Response Plan)

ANNUAL CONFERENCE & SHOWCASE
OCTOBER 27 – 29
VIRTUAL 2020

Managing Cybersecurity Risks

NCSHA

KUTAKROCK

Vulnerabilities for Public Entities

- Housing Finance Agencies have to be concerned about:
  - Protecting HFA funds
  - Protecting borrower and other sensitive data
  - General HFA operations and environment
- Open records and open meeting laws make public entities particularly susceptible to attack
- Cybersecurity issues may impact public and investor trust and issuer credit ratings
  - Cost of responding (often a function of preparedness)
  - Short-term stability and long-term health

Poll Question

Has your organization ever included general cybersecurity disclosure language in your offering documents?

Tools for Mitigating Cybersecurity Risk

- Technical tools
- Vendor management
- Training
- Verification
- Act fast
- Insurance
- Sharing cyber experiences … and resources

Managing Risk & Ransomware

- To pick up on managing risk…a particularly problematic security threat that has been front and center over the last 6 months is RANSOMWARE.
  - Been exploding over past 6-8 months
  - ALL entity types are targets—think of how damaging it would be for any entity to have its entire system locked.
  - BACKUPS, BACKUPS, BACKUPS!
  - Relatively simple solution to what could be a major problem

Poll Question

Does your organization have cybersecurity insurance?

Cyber insurance

- Not expensive
- Coverage is pretty good
- Low rate of claim denials
- Not one size fits all; need to know what data you have, what you're protecting and what your risks are before you choose a policy
- Make sure you have enough coverage
- Cyber insurance is a no brainer. I have seen it provide a life line so many times. It is an absolute life saver. Considering the cost and the risk it mitigates, it's one of the best things your organization can spend money on
- If you want to have a discussion off line, please reach out. I am happy to talk to anyone, provide resources, etc.

Disclosures and Credit Ratings

- Growing position that cybersecurity disclosures are material to investors
- Balance between transparency and security
- Key questions to deal with both disclosure and rating issues:
  - Have you assessed and identified your risk and gaps? How and how often?
  - Are you prepared? How can you demonstrate preparedness (e.g., written plans and training programs)?
  - Do you have personnel dedicated to information management or cybersecurity?

Keys to an Effective Cyber Program

- An effective organizational privacy and data security risk management program requires
  - Fostering an organizational culture in which privacy and information security are valued and promoted
  - Providing adequate financial and human resources to build out and maintain a robust information security management program
  - Enforcement of information security policies and procedures
- Without the full support of management, in these three key areas, effective risk management simply cannot occur

Management Buy-in

- Strategies to foster management engagement:
  - Create a management-level information Security Risk Management Committee
  - Require management participation in security awareness training
  - Track and report security incidents to management on a regular basis
  - Bring in the insurance brokers and underwriters to talk about information security risk mitigation
  - Quantify the risk in monetary and regulatory (penalty) terms

Management Buy-in

- Can tell within 5 minutes of first call if management is engaged & taking the breach seriously
- Can't overstate enough how much it helps if management is engaged
- If not, it's a rough process
- Chances of exposure to entity go way up if management is not engaged
  - Regulators not so much concerned with breach itself
  - More concerned with response and changes moving forward
  - If management is not engaged, it will be clear to regulators

Contacts

Lesli Wright, Deputy Executive Director | Wyoming Community Development Authority
wright@wyomingcda.com

Todd Kinney, Partner | Kutak Rock LLP
Todd.Kinney@KutakRock.com

Joshua N. MacDiarmid, Special Agent, Money Laundering, Forfeiture, and Bank Fraud Unit | Federal Bureau of Investigation
jnmacdiarmid@fbi.gov

Nicole Moriarty, Partner | Kutak Rock LLP
Nicole.Moriarty@KutakRock.Com

ANNUAL
CONFERENCE
& SHOWCASE
OCTOBER 27 – 29

VIRTUAL
2020

Thank you!

NCSHA