Information Security for Nonprofits

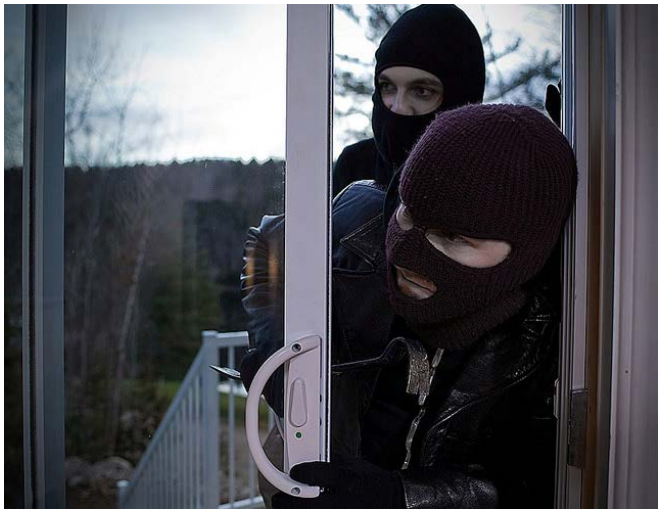
March 30, 2017

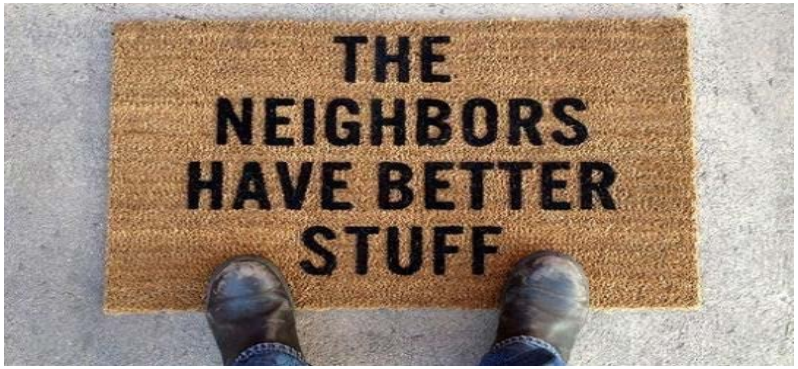
Kevin P. Martin & Associates, P.C.

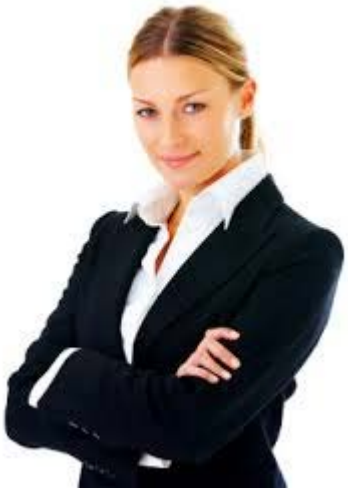
ASSURANCE | TAX | RISK MANAGEMENT | IT ADVISORY

What is the goal of information security?

What is the goal of information security?







&

Recent Breaches

www.mass.gov/ocabr/docs/idtheft/data-breach-web-report-2017.pdf

Apps | Google | Viper Consulting Inc | Gmail | Google Maps | Dictionary.com | Wikipedia | Google Calendar | Weather.com | Office 365

CHARLES D. BAKER
GOVERNOR

KARYN E. POLITO
LIEUTENANT GOVERNOR

COMMONWEALTH OF MASSACHUSETTS
Office of Consumer Affairs and Business Regulation
10 Park Plaza, Suite 5170, Boston, MA 02116
(617) 973-8700 FAX (617) 973-8799
www.mass.gov/consumer

Data Breach Notification Report

Assigned Breach Number	Date Reported To OCA	Organization Name	Breach Type Description	Breach Occur at the Reporting Entity?	MA Residents Affected	SSNBreached
10287	1/5/2017	American Express Travel Related Services Company, Inc.	Electronic		12	
10288	1/5/2017	American Express Travel Related Services, Inc.	Electronic		49	
10289	1/5/2017	PCC Technology	Electronic	Yes	2	Yes
10290	1/5/2017	Bank of America	Paper	Yes	2	
10291	1/5/2017	Massachusetts General Hospital	Paper	Yes	1	Yes
10292	1/5/2017	Massachusetts General Hospital	Paper	Yes	1	
10293	1/6/2017	American Express Travel Related Services, Inc.	Electronic		18	
10294	1/6/2017	R&A Design d/b/a/ Unison Home	Electronic	Yes	46	
10295	1/6/2017	Legal Aid Society of Orange County	Electronic	Yes	2	Yes
10296	1/9/2017	People's United Bank	Paper	Yes	2	Yes
10297	1/9/2017	Family Service Association	Paper	Yes	278	Yes

Breaches from the Headlines

Utah Food Bank security breach exposes donor's personal info

- 10,385 donors had to be notified of security breach
- Breach appears to have happened between October 2013 and July 2015

Breaches from the Headlines

MetroHealth reports data breach for 981 heart patients due to malware

- *Malware was discovered March 17, 2015*

A business associate disabled the antivirus software on computers to facilitate a software update.

Patient info on the computers consisted of: patient name, date of service, date of birth, medications administered during procedure, medical record number, case number.

Breaches from the Headlines

Data Breach at Anthem May Forecast a Trend

- *Breach was detected on Jan 29, 2015.*

Medical identification numbers, social security numbers, addresses and email addresses were taken, which can be used for medical fraud.

Exposed information on about **80 million** people.

Investigators Suspect Anthem Breach Began with ‘Phishing’ of Employees

By Brandon Bailey | February 10, 2015

The hackers who stole millions of health insurance records from Anthem Inc. **commandeered the credentials of five different employees while seeking to penetrate the company’s computer network** — and they may have been inside the system since December.

Investigators now believe the hackers somehow compromised the credentials of five different tech workers, possibly through some kind of “phishing” scheme that could have **tricked a worker into unknowingly** revealing a password or downloading malicious software.

Risk of Exposure from a Data Breach

- **Donor/Customer/Employee Data:**
  - Names
  - Addresses
  - Date of Birth
  - Phone Numbers
  - Social Security Numbers

- **Your Company's Reputation**

How do businesses protect themselves?

Protect the Company / Data

- **Access Controls**
  - **Physical**
  - **Logical**
- **Backups**
- **Awareness & Education Training**

Network Security – Perimeter Solutions

- **Perimeter solutions should be intelligent enough to distinguish good web traffic from bad.**

- **Next-generation firewalls (NGFW):**
  - Integrated network solution, with improved network filtering
  - Provides “deep-packet” inspection of traffic at the application level.
  - Security policies are enforced at the application level
  - Many can also provide gateway antivirus and intrusion prevention/detection

Logical Access - Authentication

- **Develop authentication controls**
  - Objective: ensure persons logging into the system are who they say they are
  - Best methods combine two or more types of authentication:
    - username, password, code number, secret questions, biometrics, etc.

Logical Access - SOD

- **Restrict access based on job requirements**
  - Role-based access system (RBAC)
    - I.E. an AP employee does not have the same rights as an AR employee. Access is restricted based on job role

- **Segregation (or Separation) of Duties (SOD)**
  - Sharing responsibilities so that critical controls and functions are not in the hands of just one person
    - Prevent Fraud & Error

Logical Access – Least Privilege

- **Principle of Least Privilege (PoLP)**
  - If you don’t need access to it, you don’t get access to it
  - If you do need access to it, you only get access for the time you need it

Logical Access - Reviews

- **Conduct Access Reviews:**
  - Periodic reviews of Active Directory and Applications
    - Check to ensure all active users are appropriate
      - Promotions / Job Change – remove old rights
    - Check that terminated users have been disabled or removed
    - Conducted at least annually

Passwords: Lock your doors

Company X requirements:

- Minimum characters = 6
- No complexity requirements
- Maximum Age = 180 days

Passwords: Lock the deadbolt

Complex = Strong

What makes a password complex?

- Alphabetic characters
- Upper and Lower
- Numbers
- Special Characters
- Lots and lots of characters – the longer the better

Passwords: Why the deadbolt?

Passphrase

…..gave three experts an encrypted password file with over 16,000 entries, and asked them to break them. The winner got 90% of them, the loser 62% -- all in just a few hours.

As big as the word lists that all three crackers in this article wielded -- close to 1 billion strong in the case of Gosney and Steube -- none of them contained "Coneyisland9/" or "momof3g8kids"

https://www.schneier.com/blog/archives/2013/06/a_really_good_a.html

Passwords: Use the deadbolt

Company X will be improving requirements to include:

- Minimum characters = 8
- Requiring Complexity
- Maximum Age = 90 days

Passwords:
Lock your doors and add a motion sensing light

Password Vault / Password Managers

Google: Top 10 Password Managers for XXXX (android, apple, etc…)

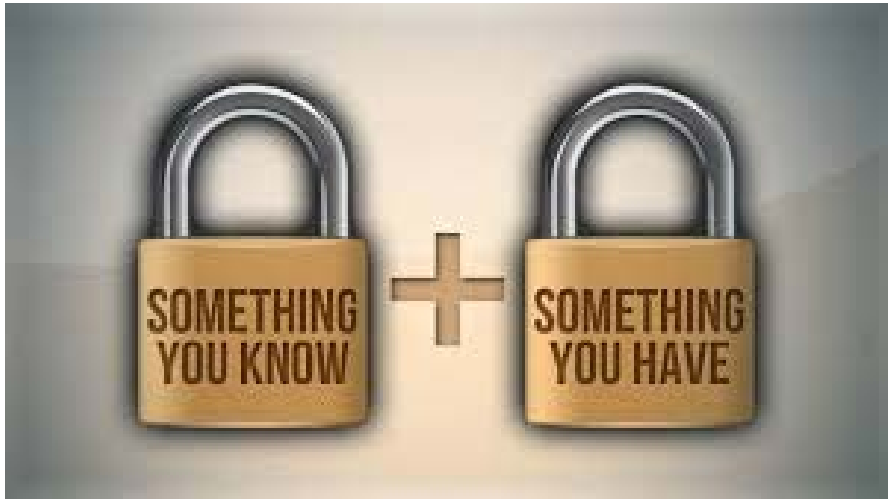
or Best Free Password Managers

- LastPass
- KeePass
- LogMeOnce
- Password Genie
- Secret Server

Passwords:
Lock your doors and add a motion sensing light

Two factor authentication

- Something you have
- Something you know



Passwords:
Lock your doors and add a motion sensing light

Patches and Updates

Keep your software up to date

Backups: Protect & Store Your Data

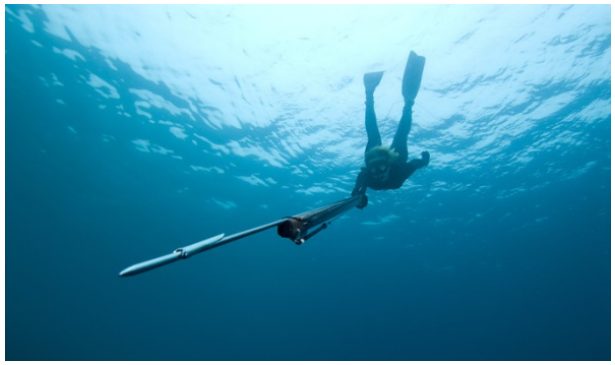
- **Backups**
  - On-site / Remote
  - Tape / Disk / Cloud
  - Encryption
  - Restore Test and Validate
  - End of life Disposal

Awareness

Phishing

VS.

SpearPhishing



Phishing

REQUEST FOR URGENT BUSINESS RELATIONSHIP

FIRST, I MUST SOLICIT YOUR STRICTEST CONFIDENCE IN THIS TRANSACTION. THIS IS BY VIRTUE OF ITS NATURE AS BEING UTTERLY CONFIDENTIAL AND 'TOP SECRET'. I AM SURE AND HAVE CONFIDENCE OF YOUR ABILITY AND RELIABILITY TO PROSECUTE A TRANSACTION OF THIS GREAT MAGNITUDE INVOLVING A PENDING TRANSACTION REQUIRING MAXIIMUM CONFIDENCE.

WE ARE TOP OFFICIAL OF THE FEDERAL GOVERNMENT CONTRACT REVIEW PANEL WHO ARE INTERESTED IN IMPORATION OF GOODS INTO OUR COUNTRY WITH FUNDS WHICH ARE PRESENTLY TRAPPED IN NIGERIA. IN ORDER TO COMMENCE THIS BUSINESS WE SOLICIT YOUR ASSISTANCE TO ENABLE US TRANSFER INTO YOUR ACCOUNT THE SAID TRAPPED FUNDS. ……

SpearPhishing

From: “James Murphy" <jmurphy@she1lcorp.com>
Date: July 8, 2015 at 10:01:57 AM EDT
To: “elisabethsmith" <esmith@shellcorp.com>
Subject: Capital Remittance

Elisabeth,

Process a wire of $38,750 to the attached account information right away. Code it to G&A and notify me once completed.

I'll send full support later.

James

SpearPhishing – Awareness

From: “James Murphy" <jmurphy@she1lcorp.com>
Date: July 8, 2015 at 10:01:57 AM EDT
To: “elisabethsmith" <esmith@shellcorp.com>
Subject: Capital Remittance

Elisabeth,

Process a wire of $38,750 to the attached account information right away. Code it to G&A and notify me once completed.

I'll send full support later.

James

SpearPhishing – Awareness

From: “James Murphy" <jmurphy@she1lcorp.com>
Date: July 8, 2015 at 10:01:57 AM EDT
To: “elisabethsmith" <esmith@shellcorp.com>
Subject: Capital Remittance

Elisabeth,

Process a wire of $38,750 to the attached account information right away. Code it to G&A and notify me once completed.

I'll send full support later.

James

Advanced SpearPhishing and Malware Attacks

How did they get in?

FIN4 used a spearphishing strategy, targeting executives

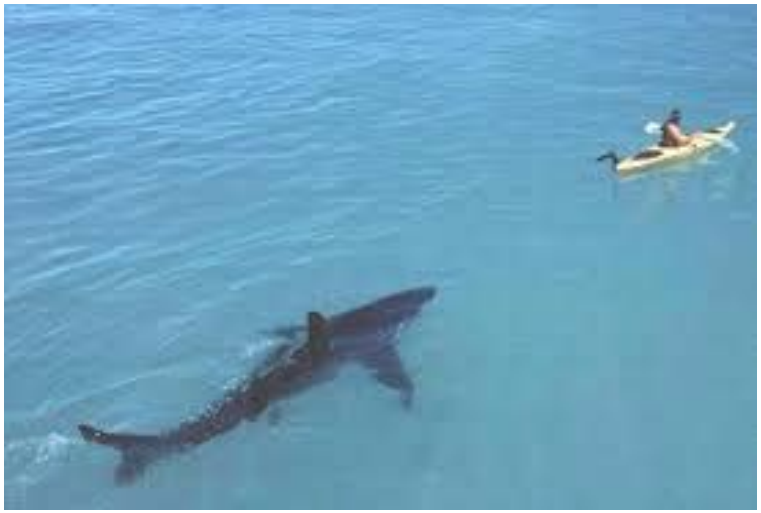
- Looking for email account login credentials
- Email a link, like an attached pdf document
- Click the link
- That generates an “Outlook session timed out” screen where to get back in you enter your User ID and Password just like you’ve done every day….pretty much routine without even thinking about it….

http://www.healthcarelawinsights.com/2014/12/03/data-security-lessons-learned-from-fin4-cyber-attacks/

Security Awareness

Phishing attacks

37%



Percentage of security incidents in 2014 caused by employee negligence, such as configuration errors or responses to phishing scams.

-BakerHostetler reported in CIO Magazine August 2015

Security Awareness: SpearPhishing

If someone you don't know emails and…

…asks you for personal information

…asks you to do something out of the ordinary

…it looks like a business email but it's from a free email service (yahoo, gmail, Hotmail)

…wants you to click on a link, or attachment

….It might be a Phishing Attack

Security Awareness: Don’t get hooked!

Recognize when emails are from people you don’t know.

- SLOW DOWN
- Ask yourself, “could this be a scam”
- Don’t click on things you are not 100% sure about

Recognize tone and context in emails from people you do know.

- If it doesn’t look right, or sound like them
- Don’t be afraid to ask for confirmation:
  - Phone call or
  - send a **separate** email back to your contact checking for confirmation

If you do…all is not lost

If you do make a mistake and accidentally click on something you realize you probably shouldn't have….

REPORT IT TO THE HELP DESK

Recap

Network Security: Defend the perimeter

Logical Access: Controls around authorization

Passwords: Strong and complex

Software: Keep it up to date

Backups and Recovery: Secure your data

Users: Training & Awareness

SpearPhishing: Stay aware

Incidents: Report them to the Help Desk

Topics for another day…

Some additional things to be aware of:

- Creating an Incident Response Plan
- Review of your MA Data Privacy Written Information Security Plan
- Running Vulnerability Scans on your Network


Q
&
A

Contact Us

Dan Keleher, CGEIT, CISA, CRISC
Executive Director
KPM Consulting, LLC
617.997.7320
dkeleher@kpmconsulting-us.com