What Every Nonprofit Should Know About Cyber-Security

June Webinar
Presented by BlumShapiro

Thanks for joining us. A few instructions before we begin:

- You may **join the audio** by selecting the radio button for either “Telephone” or “Mic & Speakers”. If you are using telephone, please dial in using the conference line and audio pin provided.
- If you are having any technical issues, please let us know in the chat box.
- We will have time for **Q&A** at the end of the webinar. Please feel free to enter your questions in the chat box at any time.
- This webinar is being recorded and we will distribute the **slides and recording** after the webinar has concluded.

Emily Tamanaha
Director of Membership & Programs

Massachusetts Nonprofit Network

www.massnonprofitnet.org

Let’s imagine doing.

BlumShapiro Consulting

a division of Blum, Shapiro & Co., PC

Webinar Agenda

I. Webinar Objectives
II. Cybersecurity Trend and Statistics
III. Cybersecurity Impact of a Data Breach
IV. Emerging Risks
V. Cybersecurity Threats
VI. Cybersecurity Findings
VII. Cybersecurity Best Practices – Top Ten List
VIII. Questions?

Things to Think About

Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months.~Clifford Stoll ***

I. Webinar Objectives

- Raise awareness of the threats and the potential cost that a breach could have on your organization
- Provide general information about the types of threats that exist
- Establish an understanding of what your organization can do to reduce the likelihood and impact of a breach

II. Cybersecurity Trend and Statistics

- ✓ 77% of organizations reported an increase in cybersecurity attacks in 2015
- ✓ 50% of organizations feel they lack the talent to combat today's cybersecurity threats
- ✓ Nearly every state has a data protection law, most include fines for data breaches
  - ✓ **CMR 17.00 – MA Data Protection Law**
- ✓ Global cybersecurity spending came in at $77 billion for 2015
- ✓ 59% of employees steal proprietary corporate data when they quit or are fired
- ✓ **Ransomware and targeted attacks are on the rise**
- ✓ Attackers have found ways to monetize many types of personal data, and aren't just targeting SSNs and credit cards
- ✓ **80% of board members say that cyber security is discussed at most or all board meetings**

II. Cybersecurity - Trend and Statistics

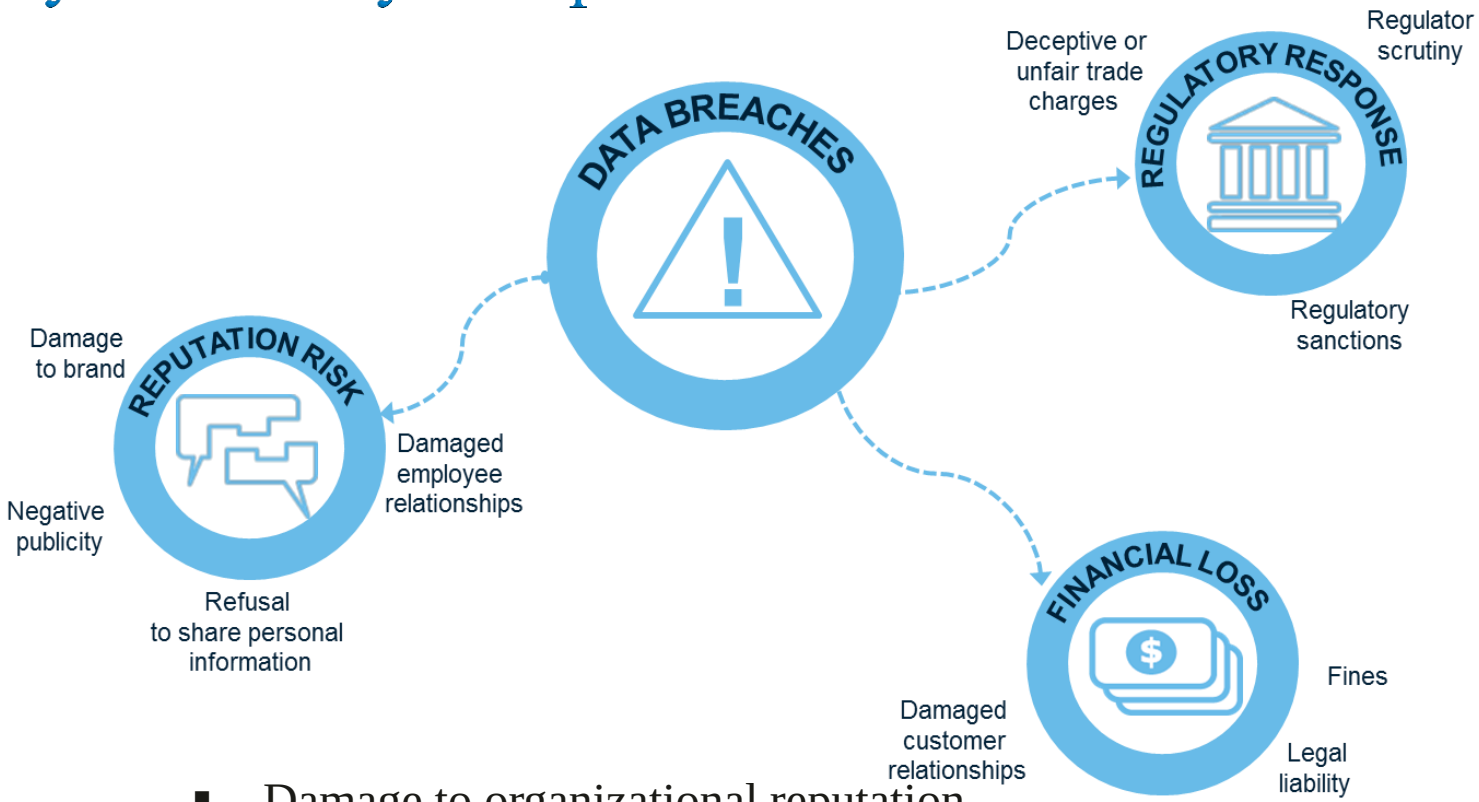
- Insiders responsible for 60% of all cyber attacks*!
  1) One-Third of these attacks are “inadvertent actors”: Well-meaning employees who either mistakenly allow an attacker to access your data, or fail to pay attention to your cyber security policies, or both.
- Employees Open Malicious Emails…
  1) 30% of targets open phishing emails
     1) 1 minute, 40 seconds = median time to open
  2) 12% proceed to click on malicious attachments
     1) 3 minutes, 45 seconds = median time to click
- 63% of breaches involved weak/default passwords!
  1) Not new, or glamorous, but IT WORKS!

Sources: * IBM Data Breach Report 2015, and **2015 Verizon report.

II. Cybersecurity - Trend and Statistics-Why Attacks Occur

1. Access to and selling of confidential information
   a. Credit Card numbers
   b. Bank Account information
   c. Personal information (SS#'s, etc.)
2. Access/Control over key information
   a) Deleting/erasing information – Holding information for *Ransom*
   b) Direct Spam – intend is to confirm your email address and sell it
   c) Link Injection – web pages are hijacked and include links to other sides… ads, etc.
1. Stealing intellectual property
   a. Selling IP
   b. Reproducing counterfeit products

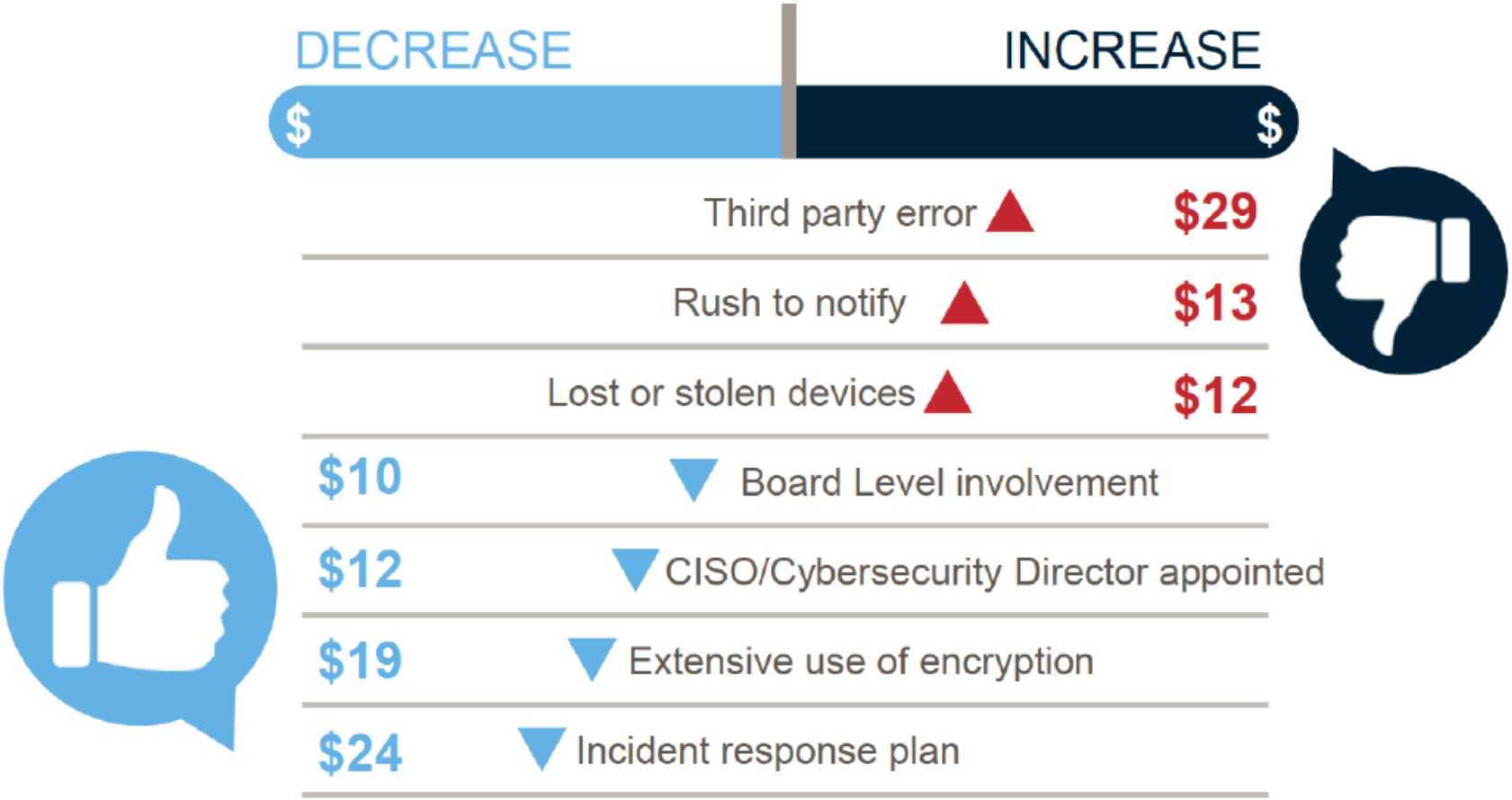
III. Cybersecurity – Impact of a Data Breach



- Damage to organizational reputation
- Loss of trust in data repositories
- Cost to Nonprofit organization
- Potential disruption to business
- Loss of donor confidence

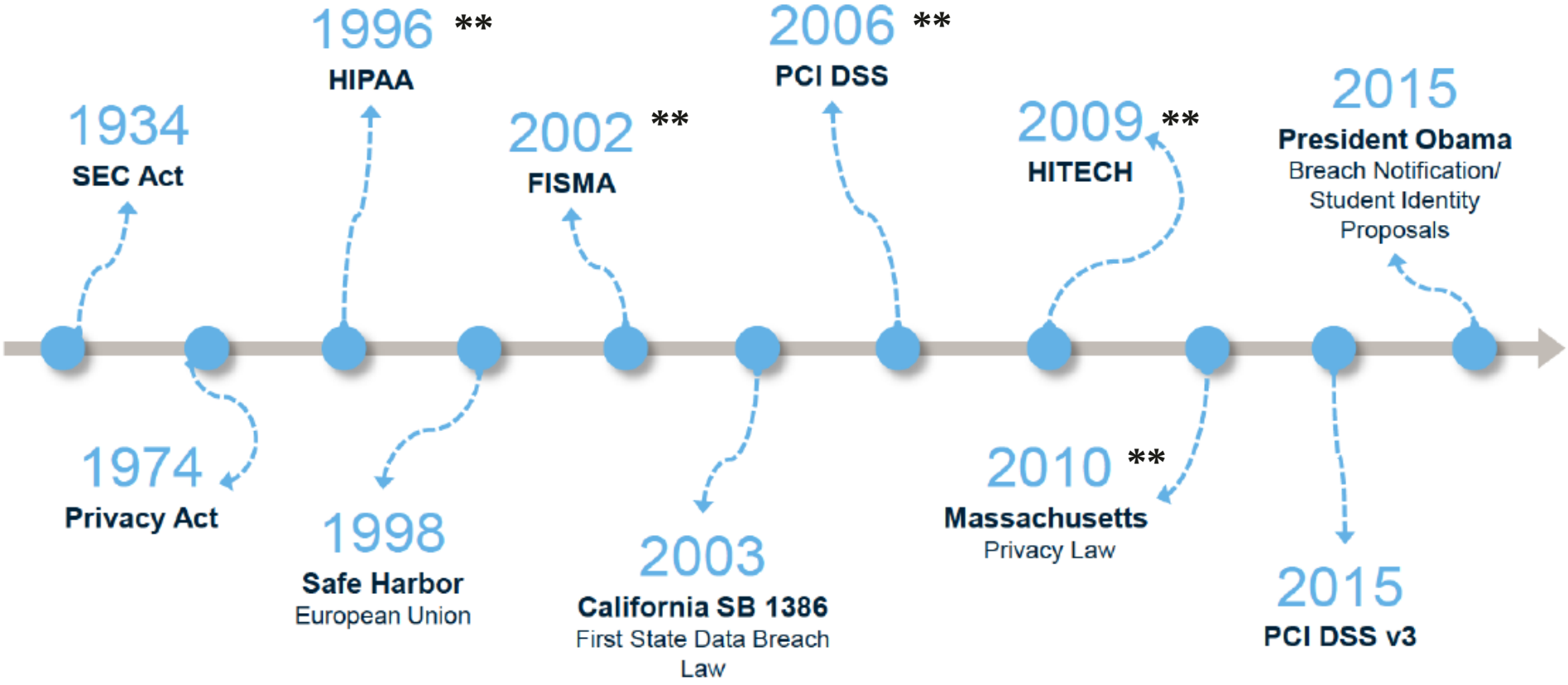
III. Cybersecurity – Impact of a Data Breach - Costs

- **Average cost of a data breach is reaching $4 million dollars**
- **The more records lost, the higher the cost of the data breach**

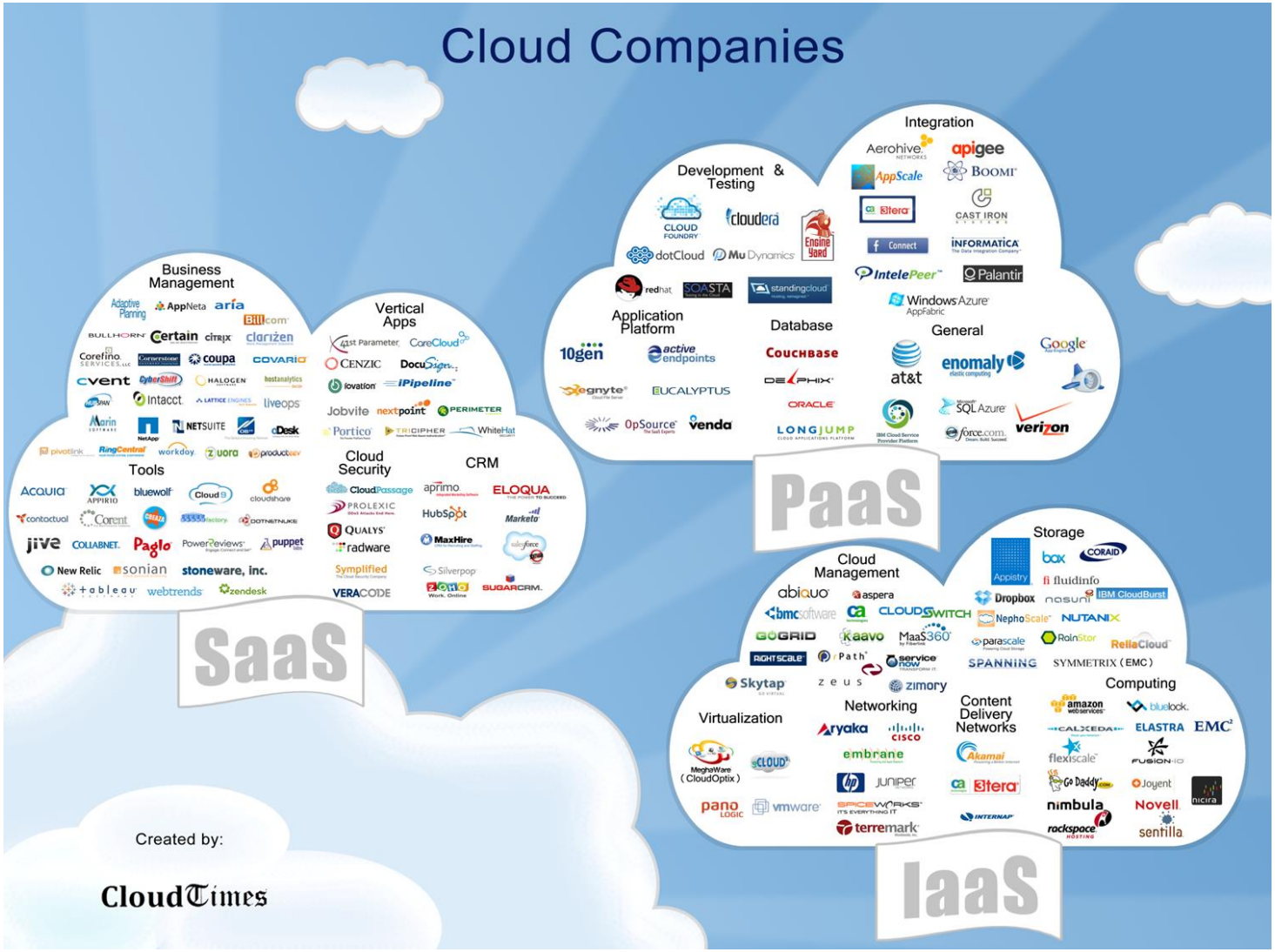


"2015 Cost of Data Breach Study," Ponemon Institute LLC

III. Cybersecurity – Impact of a Data Breach-Legal Landscape



IV. Emerging Risks



IV. Emerging Risks

Cloud Risks

- Reliability
- Performance
- Security
- Compliance
- Vendor Management
- Legal
- Reputational
- Data Management

Interesting Thoughts

- Take it or leave it contracts
- What Data goes in the Cloud?
- Where is the Data once it is there?
- What if the provider fails?
- Vendor Lock In
- How do I audit it?
- High profile attacks

IV. Emerging Risks

Mobile Device Risks

IV. Emerging Risks

Mobile Device Risks

- Physical Security Controls
  - *What happens when one goes missing?*
- Trusted Sources
- Trusted Networks
- Apps Created by Unknown Parties
  - *Jailbroken devices*
- Interaction w/Other Systems
- Synchronization w/Other PCs
- Location Services

IV. Emerging Risks – Poll Question -1

Poll Question

- Does your organization allow unknown external devices (eg. mobile phones, iPads, etc.) on your network?

V. Cybersecurity Incidents

Breaking into: Networks, Laptop, Wireless Devices

- **Hacking** – Someone who seeks and exploits weaknesses in a computer system and/or network. *(Typically steal large volumes of data: credit cards, bank accounts, etc.)*
- **Keylogger**- Software installed on a PC that captures all key strokes
- **Like-jacking** – occurs when a hacker posts a fake Facebook "like" button on webpages. Users who click the button end up downloading malware
- **Ransomware** – Software designed to encrypt files. Decryption key requires paying a ransom.
- **Phishing** - malware sent by email. Provides a link or downloads files to PC.
- **Viruses** - A small computer program that infects other application software by attaching to and disrupting the application's function.
- **Denial of Service** - Act by the criminal, who floods the bandwidth of the victims network.
- **Trojan Horses** - Malware disguised as a legitimate program that may be downloaded and installed by users without realizing it is a virus.

V. Cybersecurity Threats

Why Are They Happening?

Hacking
- Lack of updating (patching) software
- Lack of password rotation or complexity
- Limited monitoring/auditing tools

Keylogger
- Lack of Anti-virus/Spyware updates or not working
- Lack of security updates on PC
- Too much user permission on desktop

Ransomeware
- Lack of Anti-virus/Spyware updates or not working
- Lack of security updates on PC

Phishing
- Limited/Lack of Firewall configuration
- Lack of user education/training

V. Cybersecurity Threats

April 8, 2014

July 14, 2015

V. Cybersecurity Threats

V. Cybersecurity Threats –Phishing Example

From: IT Dept [mailto:it@nameoforganization.org]

Sent: Wednesday, July 22, 2015 2:55 PM

To: Matthew Rankin;

Subject: Confirm Your Credentials

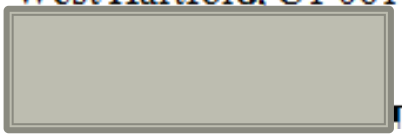
To All:

I am working on a project with your Information Systems Department to update user account information within (Name of Organization)'s network. Please click on the link below to confirm and/or update your email address and password. Your prompt reply is appreciated.

Update account information

Thank you for your help in advance.

John Floutis, Consultant
One Abrahms Boulevard
West Hartford, CT 06117



V. Cybersecurity Threats –Phishing Example

Hello!
As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Spelling

Our system detected unusual Copyrights activity linked to your Facebook account , please follow the link bellow to fill the Copyright Law form:

http://www.facebook.com/application_form Links in email

Note: If you dont fill the application your account will be permanently blocked. Threats

Regards,

Facebook Copyrights Department. Popular company

V. Cybersecurity Threats – Poll Question -2

Poll Question

- Has your organization experienced some type of Cybersecurity Attack? (Ransomware, Phishing, Other)

VI. Cybersecurity – Findings - General

- General Findings
  - Lack of Password Security
    - Network and/or application passwords not periodically changed
    - User IDs not disabled after repeated unsuccessful login attempts
    - Shared passwords; Visible passwords around the computer screen
    - Same password for network and applications
  - Lack of Infrastructure Security
    - Lack of a patch management strategy/process***
    - Remote access to network**
    - Limited firewall capabilities; upgrades to firewall
    - No virus or spyware protection on remote computer
    - Unsecured wireless network

VI. Cybersecurity – Findings - General

- General Findings
  - Lack of Operational Security
    - No signed network security policies\procedures
    - Lack of controls over credit card information
    - Lack of segregation of duties
    - Lack of using Positive Pay
  - Lack of DR/BC Plan
    - Backups are not regularly tested
  - Lack of Training and Education
  - Lack of Understanding of Cloud Computing

VI. Cybersecurity – Findings - Passwords

- List of worst (and most frequent) Passwords

• 123456	• password
• 12345678	• qwerty
• abc123	• 123456789
• 111111	• 1234567
• iloveyou	• adobe123
• 123123	• admin
• 1234567890	• letmein
• qwertyuiop	

- Creating a complex Password
  - **I l**ove **w**atching **N**ew **E**ngland **P**atriots **o**n **7**unday**!**
  - IlwNEPo7!11
- Two factor authentication

VI. Cybersecurity – Findings – Cloud Vendors

- General Findings
  - Third Party Vendor (Cloud) Is Responsible For All Security
    - What does the contract/agreement say?
      - Who owns the information/data?
    - How do you know what security protocols they practice?
    - Do they have a SOC-1 or SOC-2 Type II

VII. Cybersecurity Best Practices

Top Ten List

1. Recognize that Cybersecurity is not just an IT issue
   a. Directors and Board Members should understand and approach cybersecurity as an enterprise-wide risk management issue
   b. Cybersecurity initiatives may need more visibility and action from the Top
2. Consider performing a Cybersecurity Risk Assessment
   a. Utilize the NIST standard (risk management framework)
   b. What protected information do you store?
3. Enforce regular password changes (every 60 to 90 days)
   a. Lockout users after 3 unsuccessful attempts
   b. Implement two factor authentication (2FA) capabilities
3. Review network and application permissions
   c. Evaluate segregation of duties/responsibilities
4. **Ensure backup/recover processes are in place and work effectively**

VII. Cybersecurity Best Practices

Top Ten List

6. **Maintain/Confirm anti-virus and spyware software is constantly working\updated**
7. Secure your wireless network
   a. Change standard defaults.
   b. Use WPA2 wireless protocol (make sure it is not WEP)
8. Make sure Cloud vendor(s) has a SOC-1 or SOC-2 (or something similar)
9. **Adopt security policies, procedures and protocols**
   a. Make sure to include a BYOD policy
   b. Ensure vendors with network access sign a network security & privacy agreement
10. **Encrypt all laptops and removable drives**
11. **Provide Cybersecurity training to employees**
    a. When in doubt delete email; Don't click that button

VI. Questions

Jeffrey Ziplow
Partner
Blum Shapiro Consulting
jziplow@blumshapiro.com
860.561.6815