Healthcare, Pandemics and the Continued Need for Cybersecurity

Presented by

Jason Cope and Erick Cutler

EisnerAmper LLP

Disclaimer

Disclaimer Statement

The information in this presentation is provided for general educational purposes only and may not reflect changes in federal or state laws subsequent to the presentation date. Before taking any action based on this information, we strongly encourage you to consult with a professional accounting advisor about your specific situation.

IRS Circular 230 Disclosure

Pursuant to requirements imposed by the Internal Revenue Service, any tax advice contained on this presentation is not intended or written to be used, and cannot be used, for purposes of avoiding penalties imposed under the United States Internal Revenue Code or promoting, marketing or recommending to another person any tax-related matter. Please contact us if you wish to have formal written advice on any matter presented on this presentation.

In Today's Session

- Why is cybersecurity important?
- Covid-19's impact on cybersecurity
- Cybersecurity risks in a remote environment
- Monitoring your cybersecurity environment

Why Is Cybersecurity Important?

- Notable breaches
- Healthcare and small business impacts
- Why these entities are targeted

Notable Breaches

- Target (2013)
  - 110 million customers credit/debit card information compromised
  - Hackers gained access through a third-party HVAC vendor to the point-of-sale card readers
  - Cost the company $18.5 million, plus additional compliance requirements

Notable Breaches

- Uber (2016)
  - 57 million Uber users and 600 thousand drivers personal information exposed
  - Uber failed to disclose the breach for more than one year
  - Paid the hackers a "bug bounty" fee of $100 thousand to destroy the data with no way to verify the destruction occurred
  - Valuation dropped from $68 billion to $48 billion

Notable Breaches

EQUIFAX

- Equifax (2017)
  - Personal information (including Social Security Numbers, birthdates, addresses, drivers' license numbers) of 143 million consumers compromised
  - Caused by a website application vulnerability; using old outdated systems
  - Setup a dedicated website to take care of consumers
  - Provided free credit monitoring for one year for all consumers affected
  - Cost the Company $700 million after reaching a settlement with the government

Notable Breaches

- Capital One (July 30, 2019)
  - Personal information of 100 million consumers compromised (names, addresses, phone numbers, email addresses, dates of birth, annual income disclosures)
  - Outside individual gained access to the network by exploiting a misconfigured web application firewall
  - Will provide free credit monitoring for one year for all consumers affected
  - Fined $80 million in civil penalties, and ordered to create an action plan to detail steps it's taking to improve security

Healthcare and Small Business Impact

- Per IBM Security Intelligence Report; organizations take, on average, 206 days to identify a breach and 73 to contain it
- Average loss per attack averages more than $188 thousand
- Healthcare sector is targeted twice as much as any other industry
- 2020 was the worst year ever for healthcare industry data breaches (Hipaajournal.com)
  - 616 data breaches of 500 or more records
  - Overall 28 million healthcare records were exposed or compromised
  - More financial penalties issued in 2020 for HIPAA violations than in any other year ($13.5 million)
- Texas Lawbook survey states four out of five law firms operating in Texas in 2017 and 2018 were victimized by a cyber attack
- 40% of small and mid-sized companies that experience data breaches are out of business within six months

Why are Healthcare and Small Businesses Targeted?

- Approximately 43% of cyber-attacks target small business, and this number is growing, but why?
- Small businesses are more exposed
  - Often lack the in-house knowledge or resources to invest in security protocol and regulations
  - Estimated 71% of actual breaches occur at small businesses
- Small businesses have sensitive data, all in high demand from a hackers point of view
  - Personal information
  - Credit card numbers
  - Health records
- Small businesses are vulnerable to phishing attacks

State Law Requirements

- State laws have subtle differences, but in Texas you must do the following if you do have a breach:
  - Notify affected individuals of the unauthorized acquisition of their personal information
  - Notice must be made as quickly as possible
  - Breached third parties must notify relevant data owners or licensees immediately after discovering a breach
  - If more than 10,000 individuals must be notified, breached entities must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwise basis

Civil penalties

- Civil penalties
  - At least $2,000 but not more than $50,000 for each violation
  - Failure to comply with notification requirements penalties are $100 per person to whom notification is due, per day, not to exceed $250,000 per breach

HIPPA Requirements and Penalties

- Covered entities must provide notification to affected individuals, the Secretary of Health & Human Services, and in some cases the media
- Notification is required “without reasonable delay” but in no case later than 60 calendar days from the discovery of the breach
- Penalties assessed on a tiered system containing 4 levels
  - Penalties can range from $100 to $50,000 or more

Covid-19's Impact on Cybersecurity

- Monumental shift to remote work that's unlike anything that's ever been seen in the U.S. and around the world
- More virtual meetings because of shelter-in-place restrictions and social distancing guidelines

Security Issues Emerging from the Rapid Move to Remote Working

- IT infrastructure is not prepared for widespread remote working
- New risks arise from the band-aid approach to remote working
- Allowing employees to use personal devices to accomplish remote working
- Difficult to detect anomalies in unprecedented times – for humans and machines alike
- Software is often designed for convenience rather than security
- Security often falters at the password layer

Cybersecurity Risks in Remote Environment

1. Employees
2. Systems and infrastructure
3. Social engineering

Employee Risks

- Hackers know that over **90% of data breaches** are the result of human error
- 77% of remote employees are using unmanaged, unsecure "BYOD" devices to access corporate systems
- 93% of employees have reused passwords across applications and devices
- 29% admitted that they allow members of their household to use corporate devices for activities like schoolwork, gaming, and shopping

Systems and Infrastructure Risks

- New forms of cyber attacks designed to exploit system vulnerabilities
  - Credential stuffing; when hackers use stolen login credentials from previous breaches to automate logins at a massive scale in order to backdoor their way into your accounts
  - Automated Microsoft Teams notifications in attacks that attempt to harvest Office 365 credentials
- Attacks against consumer-based cloud services
  - Allowing employees to use personal email accounts and cloud storage
- Forced digitalization, getting it wrong, creates gaps in the remote access system
  - Allowing employees personal devices to connect to the remote environment means employees can bypass the policies and procedures required to protect corporate assets, making it significantly easier for hackers to access this information
- Using video conference platforms to host meetings

Create Security Plan

- Remote access to company information systems whether using company provided devices or personal devices
- Set standards, expectations and processes for employees
- When allowing personal devices to connect to the network, policies should include:
  - Requirement to provide up-to-date antivirus software
  - Require the use of strong passwords on personal devices
    - Do not allow reuse of passwords across accounts
    - Use a password manager
    - Require use of multi-factor authentication (MFA) where possible

Avoiding Gaps in the Remote Access System

Home wi-fi does not have the same defenses as a businesses firewalls or network-based intrusion detection systems.

- Ensure home routers are running the latest firmware version
- Disable remote management from the internet facing interface
- Ensure router is set up securely with a strong password
- Change the default name of your wi-fi network
- Use WPA2-AES security for your router; WPA3-AES if your router supports it
- Disable wi-fi protected setup (WPS)
- Prevent cross contamination of devices, if possible
- Monitor for unknown device connections

Avoiding Gaps in the Remote Access System (cont.)

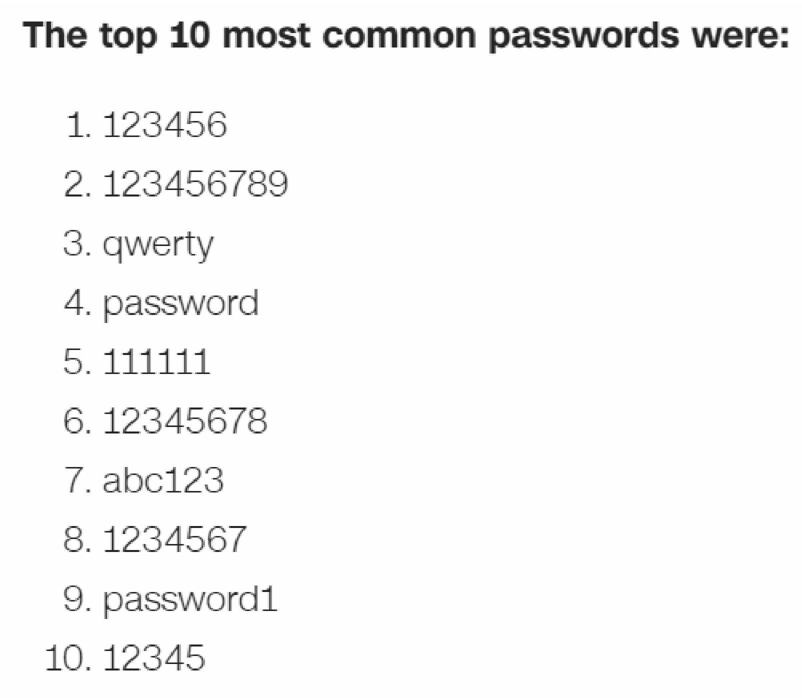
- Use a virtual private network to access the network remotely
  - Implement multi-factor authentication on all VPN connections or otherwise use strong passwords
  - Limit split tunneling when access if from personally owned devices
- Encrypt data wherever possible
  - Issue guidance on how IT will be communicating about policies and procedures
  - Include reminders on phishing vigilance
- Electronic work files from company resources should remain on company approved devices and not placed on personal devices

Compromised Credentials Could Lead to Break into Systems

- Reinforce security weaknesses with patches, ensuring software and systems are up-to-date
  - Enable automatic updates to keep software up-to-date
- Use of strong passwords, security often falters at the password layer
  - 8-20 characters
  - Require combinations of capital and lowercase letters, numbers and special characters
- Require periodic password changes
  - Every 30-90 days
  - Trade password length for maximum password age

What can you do?

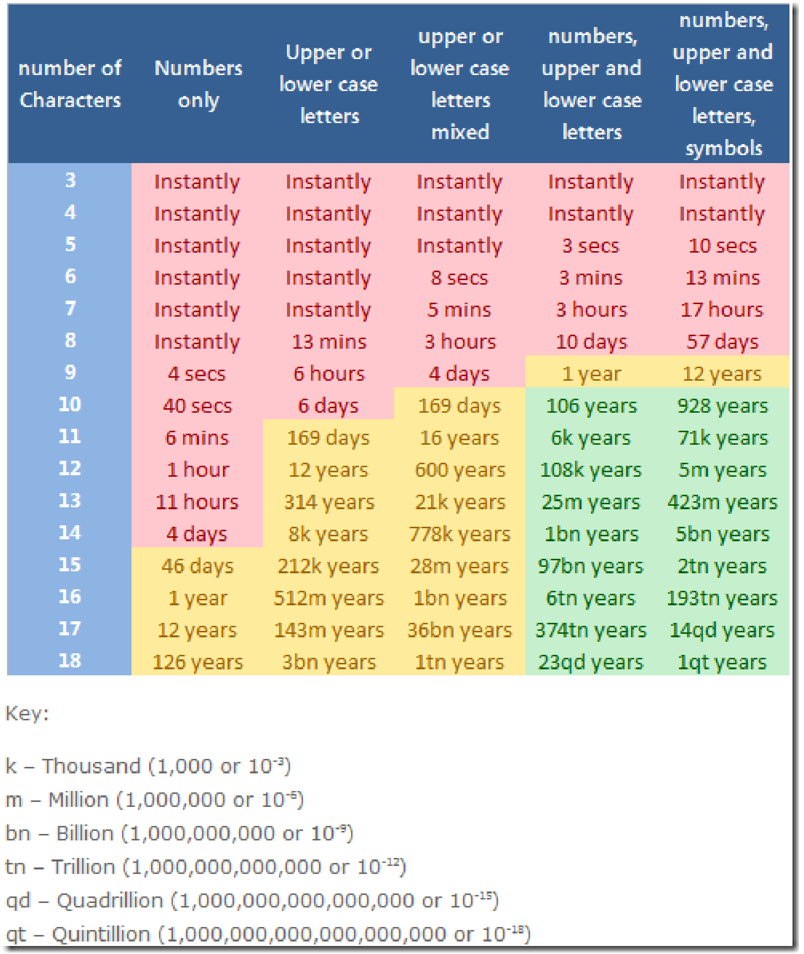
- Use a strong password (not one of these…)



The top 10 most common passwords were:

1. 123456
2. 123456789
3. qwerty
4. password
5. 111111
6. 12345678
7. abc123
8. 1234567
9. password1
10. 12345

Strong passwords



number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

Key:

k – Thousand (1,000 or 10^{-3})
m – Million (1,000,000 or 10^{-6})
bn – Billion (1,000,000,000 or 10^{-9})
tn – Trillion (1,000,000,000,000 or 10^{-12})
qd – Quadrillion (1,000,000,000,000,000 or 10^{-15})
qt – Quintillion (1,000,000,000,000,000,000 or 10^{-18})

Social Engineering Risks

- Art of manipulating people so they give up confidential information
- Criminals use social engineering tactics because it is usually easier to exploit humanity's inclination to trust than it is to discover ways to hack your software
- Common forms:
  - Phishing
  - Ransomware
  - Smishing

Phishing

- The fraudulent attempt to obtain sensitive information such as usernames, passwords and other personal details by disguising oneself as a trustworthy entity in an electronic communication
- In May 2020, the Department of Homeland Security, Department of the Treasury, the IRS, and the Secret Service issued an alert regarding scammers attempting to steal personal and financial information from individuals related to the CARES Act
- Phishing attacks have skyrocketed with a ***350% increase*** since the beginning of 2020
- Google's Threat Analysis Group reported in mid-April that they blocked approximately 18 million Covid-19 themed malware and phishing emails per day

Spear Phishing

- Same as phishing, except targeted
- Emails specifically crafted to look like they are coming from someone you know
  - Usually researched and planned ahead of time
    - Investigate names, roles within a company
  - "From" part of an email often spoofed to make it look like it's coming from a known entity or individual
- Often contains malware or links to credential stealing sites

Phishing Responses

- Educate employees on various scams and what to do if they believe they’ve received malicious email content.
- Remind employees to be suspicious of emails from unknown sources.
- Do not open file attachments or click on links in emails from unknown senders.
- Remind employees that the IRS does not conduct business by email.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.

Ransomware Risks

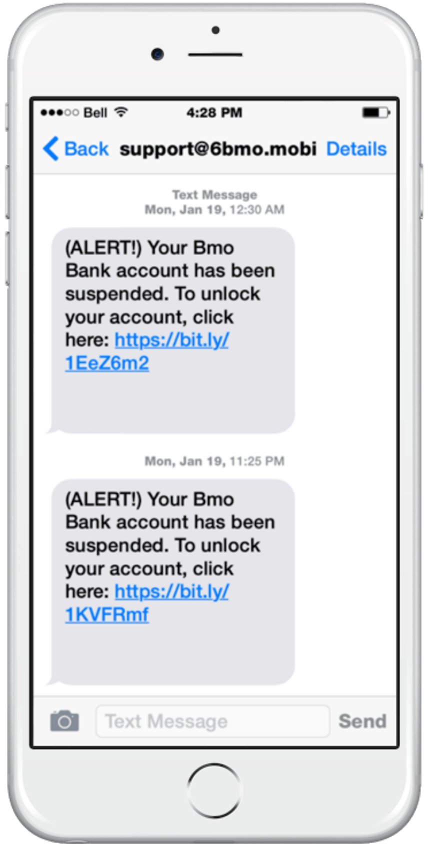
- A type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid.
- Typically spread through phishing emails or by unknowingly visiting an infected website.
- This type of attack and payments continue to rise.
  - 62% of organizations were victimized in 2019, up from 56% in 2018

Ransomware Defense

- Regularly back up your system and store on a separate system
- Encrypt your data
- Educate employees to recognize phishing attempts
- Maintain and update software

Smishing

- A type of Phishing attack using SMS messaging on cell phones.
- Just like email phishing scams, smishing messages typically include a threat or enticement to click a link or call a number and hand over sensitive information.
- People tend to be more inclined to trust a text message than an email.



support@6bmo.mobi

Text Message
Mon, Jan 19, 12:30 AM

(ALERT!) Your Bmo Bank account has been suspended. To unlock your account, click here: https://bit.ly/1EeZ6m2

Mon, Jan 19, 11:25 PM

(ALERT!) Your Bmo Bank account has been suspended. To unlock your account, click here: https://bit.ly/1KVFRmf

Monitoring Your Cybersecurity Environment

- Monitor employee remote-work practices
  - Most data breaches are caused by insiders, not outside hackers
- Install patches and updates often
- Monitor network traffic continually
- Monitor system logs for unusual connections (VPN) or account activity

Vulnerability Assessment

- Intended to identify and assign a criticality rating to potential security weaknesses in an organization's technical environment, but not to exploit the weaknesses
- External
- Internal

Vulnerability Assessment

- External
  - Checks for vulnerabilities between the external network and the internet.
- Internal
  - In-depth analysis of the organization’s internal network.
  - Estimated that approximately 80% of security breaches occur from inside the internal network.

Vulnerability Assessment

- Deliverables
    - Technical vulnerability assessment report
    - Recommendations for remediation

Penetration Testing

- Identifies the ease and likelihood with which a malicious attacker could compromise the target environment
- Finds weaknesses in the target environment and attempts to exploit them.

Social Engineering Assessment

- Consist of various methods to determine susceptibility to common people-based attacks to obtain credentials, convince users to circumvent security controls, install unauthorized software, disclose sensitive information, or enable assess to unauthorized areas.
- Focus is on humans rather than weaknesses in the IT infrastructure.

Key Takeaways

- Prioritize taking a comprehensive look at your cybersecurity environment to avoid potential embarrassment, penalties and legal ramifications from a breach
- Keep systems updated and monitor regularly
- Create a remote cybersecurity plan, and educate employees on best practices to protect their home work environment
- Educate employees on the myriad scams and techniques often employed by hackers to obtain access to sensitive data
- Consider hiring an outside IT specialist that can assist in evaluating and assessing risks, and provide education and stress testing services to your organization