2020 MCM NFP Summit Series

Nothing in this document should be construed as providing tax advice. Please consult with your own professional tax advisor. In addition, this document represents the information that we have up to the date the presentation was made and cannot be relied upon for additional updates beyond that date.

Managing Cash Flows for Non-Profits

June 18, 2020

Presenters

Rebekah Payne

CPA
Partner

Rebekah.Payne@mcmcpa.com

Debbie Smith

CPA
Partner

Debbie.Smith@mcmcpa.com

MCM CPAs & Advisors

- **What We Do:**
  - MCM is a large regional CPA and advisory firm employing more than 350, including more than 160 CPAs. We serve both privately and publicly held businesses, non-profit organizations, small businesses and individuals
- **Mission:** We exist to help both our clients and team succeed.

Core Values

People Matter – We genuinely care about our people, personally and professionally, and ensure relevance in their work.

Leaders Inspire – We inspire each other to sustain our vision and advance our mission as a firm.

Excellence Rules – We are committed to superb client service, high quality expertise and significant client relationships.

TECHNOLOGY SOLUTIONS

CAPITAL MARKETS GROUP

HR SOLUTIONS

PrimeGlobal

Introduction

- Virtually every business and non profit is looking for ways to ease the financial burden of COVID-19, or any other financial crisis
- There are some strategies to help counter the economic downturn in order to weather the storm and improve cash flow
- You know your organization best

SWOT Analysis

- Strengths (internal)
- Weaknesses (internal)
- Opportunities (external)
- Threats (external)

	Opportunities (external, positive)	**Threats** (external, negative)
Strengths (internal, positive)	**Strength-Opportunity strategies** Which of the company's strengths can be used to maximize the opportunities you identified?	**Strength-Threats strategies** How can you use the company's strengths to minimize the threats you identified?
Weaknesses (internal, negative)	**Weakness-Opportunity strategies** What action(s) can you take to minimize the company's weaknesses using the opportunities you identified?	**Weakness-Threats strategies** How can you minimize the company's weaknesses to avoid the threats you identified?

Key Ratios and Calculations During Economic Downturns

- Liquidity
- Current ratio
- Quick ratio
- Operating reserve

Other Suggestions

- Budgeting
- Cash forecasting
- Scenario planning
- Business continuity plan
- Open communication from the top down – reassure staff
- Keep the line of communication open with your Board
- Be prepared to react quickly if necessary
- Stay in touch with your contact at MCM, we are here to help

Budgeting

- Generally created by staff and approved by the board
- Should be used as a guide to help throughout the year
- It may be necessary to amend the budget during the year for unforeseen circumstances
- Focus on the organization’s primary goals and objectives

Budgeting tips

- Determine timeline for approval, generally before the beginning of the budget year
- Identify personnel to be involved in the budget process
- Understand the organization’s current financial situation
- Document assumptions and formulas
- Review, approve and implement budget
- Monitor and respond to changes in the budget as necessary

Cash flow forecasting

- Used to manage cash and to help prevent cash flow shortages
- Often done by week or month
- Helps to see where a shortage may take place and allows you to plan ahead for how to avoid a shortage
- Be realistic in the forecasting to try and provide a conservative picture
- Update regularly as new information is available
- Be proactive when a cash shortfall is evident

Scenario Planning

- Designed to help an organization think about the future with a more structured approach
- Consider factors outside of the organization's control and determine how it could respond
- This is not a one time process, but one to revisit over time
- Methodology
  - Identify key factors
  - Determine outcomes and probabilities for each factor
  - Analyze each response and determine the best path
  - Determine when and how to respond
  - Monitor and implement

Common Revenue Sources

- Contributions
- Grants
- Member fees
- Convention/event revenue
- Service/admission fees
- Merchandise sales
- Investment income

Possible Cash Flow Solutions

- Find new sources of cash
- Delay payments/Accelerate revenue
- Decrease personnel costs
- Decrease program expenses
- Other expense cuts
- Line of credit/term debt

New sources of cash

- Appeal to new donors within donor base
  - Many are more willing to donate/help during times of crisis
  - Beginning in 2020, taxpayers can claim $300 in charitable contributions without itemizing
- Reach out to most steadfast supporters
  - Ask for introductions to other potential donors
- Find creative ways to generate income through virtual events
- Seek contributions without donor restrictions
- Try to collect on pledges receivable
- Liquidate investments

Delay payments/Accelerate revenue

- Work with vendors for cash flow solutions that may work for both entities
- If there are funders with outstanding grant or pledge commitments, try to collect those gifts
- Ask core donors and board members to consider accelerating giving
- Consider asking funders providing restricted gifts to modify restrictions to allow for more flexibility

Decrease personnel costs

- Reduce work hours/days and reduce pay
- Layoffs/furloughs
- Seek assistance from Board members
- Seek outside volunteer help
- CARES Act Payroll Provisions
  - Option to defer employer portion of FICA
  - Employee retention credit

Defer employer portion of FICA

- Available for employers and self-employed individuals
- Defer employer share of FICA
- Requires deferred employment tax to be paid half by December 31, 2021 and the other half by December 31, 2022
- Contact MCM if you have specific questions

Employee retention credit

- Provides a refundable payroll tax credit for 50% of wages paid by eligible employers to certain employees during COVID-19 crisis
- Credit available if:
  - Operations were fully or partially suspended due to COVID-19 related shut down order, **OR**
  - Gross receipts decreased by more than 50% from same quarter in prior year
- Qualified wages for furloughed or reduced hour employees
- Available for the first $10,000 of compensation, including health benefits, paid to eligible employee
- Applies to wages paid or incurred between March 13, 2020 through December 31, 2020
- Not available if receiving assistance through Paycheck Protection Program
- Contact MCM if you have specific questions

Decrease program expenses

- Prioritize key activities and initiatives
- Maintain organization's identity

Other expense cuts

- Tighten travel expenses
- Eliminate non-essential spending
- Maintain support of key initiatives

Line of credit/term debt

- Draw on line of credit or increase line of credit
- Take on term debt
  - Government loan opportunities (see next slide)
  - Traditional lending from bank

COMPARISON: 7A Payroll Forgiveness Loan & EIDL

General Provisions	SBA 7A Payroll Forgiveness Loan	SBA Economic Injury Disaster Loan
Qualified Business	Up to 500 employees including full and part time	Based on SBA guidelines for NAISC codes related to number of employees and revenue limits
Amounts Available	2.5 times average monthly payroll up to $10MM	Up to $2MM; Amount based on SBA Calculation
Interest Rate	1%	3.75% For Profit; 2.75% Non Profit
Collateral	None required	None for loans <$25000; required for loans in excess with focus on real estate
Guaranty	None required	Not required for loans less than $200,000
Repayment	Extended from 2 years to 5 years for unforgiven portion	Payments deferred for 12 months; Amortized principal and interest over up to 30 years
Affiliate Rules	Common control rules apply; hospitality exception	Common control rules apply
Loan Process	One time ask through SBA Lender; funds are limited	May apply multiple times based on need through December 31, 2020

Closing

- Understand where your organization is financially
- Monitor your options
- Communicate with management and the Board
- Continually reassess
- Be proactive

Questions?

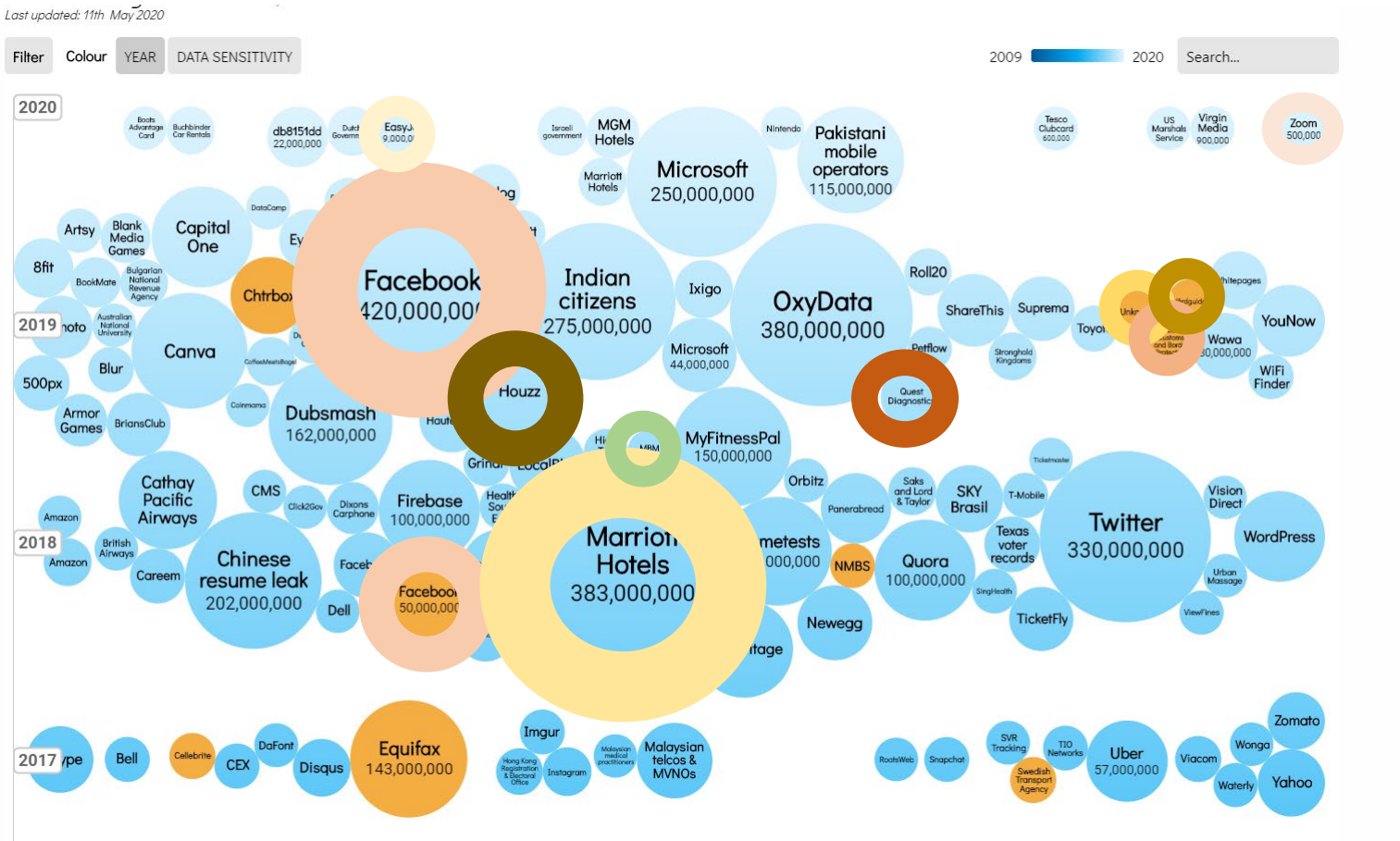
Cybersecurity – Managing the evolving risk

Presented by: Jim Kramer

Learning Objectives

- Understand that Cyber Security is not a new or always high-tech concept.
- How is the cyber threat changing?
- Learn methods you can use to evaluate the threats to your organization
- Learn methods you can use to educate employees about threats
- Learn ways you can minimize the risk of threats to your organization

What were some recent data breaches?



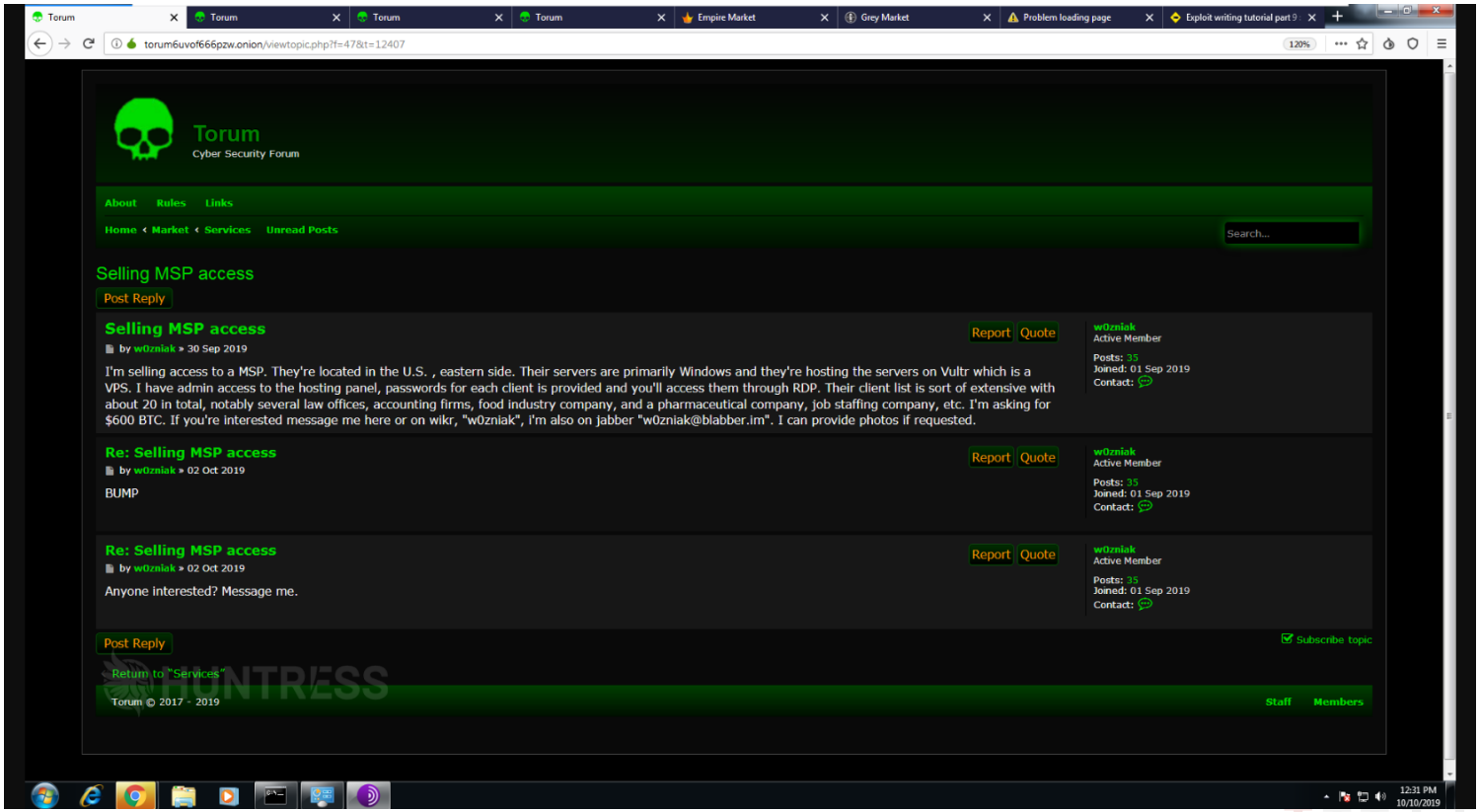
What does the hacker of today look like?

64% - State Sponsored or Organized Crime

30% - Insider Threats

6% - Individuals or Petty Thieves

Social Engineering – Who's the target



Why do hackers want data?

Here are several examples of the price for your stolen data:

Spotify Account $2.75	Hulu Account $2.75	Netflix Account $1.00 - $3.00	PayPal Credentials $1.50	Social Security Number $1.00
Driver's License $20.00	Credit Card $8.00 - $22.00	Email Address & Password $0.70 - $2.30	Medical Record from Large Scale Attack $1.50 - $10.00	Complete Medical Record Up to $1000.00

Who will pay the most for your data?

YOU!

- Primary Reasons a "Bad Actor" will steal you data
  - To Damage or Destroy the owner
  - Sell
  - Ransom
  - Blackmail

Threat Landscape

- Remote exploits
  - Made more difficult by the advent of advanced defenses.
  - Resurgence of exploits with remote users
- Insider threats
  - An often overlooked threat to the organization.
- Social engineering
  - Has become the number one attack vector.

Remote Exploits

What is a remote exploit?

- A remote exploit is a weakness in software that allows a remote attacker to take control of a system or expose non-public information from the system.
- As defenses have evolved, remote exploits have become less of a concern than social engineering.
- With remote users & BYOD this is becoming more of an issue recently

Remote Exploits (Continued)

How can I prevent remote exploits?

- Technical measures
  - Firewall
  - Intrusion prevention/intrusion detection systems
  - Anti-virus/anti-malware
- Policies
  - Patch management
  - Regular vulnerability assessments

Insider Threats

What is an insider threat?

- Threats inside the organization, such as employees, former employees, contractors/vendors, and business associates.
- Examples
  - Fraudulent transactions
  - Data theft
  - Intellectual property theft
  - Sabotage

Insider Threats (Continued)

Policies

- Job rotation
- Mandatory vacation
- Separation of duties
- Dual-control
- After-hours logoff

Insider Threats (Continued)

Technical measures

- Data loss prevention systems
- Anomaly-based intrusion prevention
- Secure, regularly tested backups
- Data encryption

Social Engineering

What is Social Engineering?

- Exploiting the weaknesses in human interaction!
- This attack is often one of the most devastating to people and organizations
- Often difficult to detect in such a fast paced world

Why is it so Effective?

- Three common psychological traits help social engineers succeed:
  - Our desire to be helpful
  - We are naturally curious
  - We have a fear of getting into trouble
- Social engineers have the upper hand:
  - Have unlimited time
  - Know what they are after and the probable weakness of those who guard it
  - Have a vast toolkit of attacks and techniques

Most Common Techniques

- Pretexting
- Baiting
- Physical access
- Familiar Attacker
- Ramsomware
- Phishing
- Spear Phishing
- Scareware
- Man-in-the-middle attacks

Note: attacks can take place in person, via phone and via the web/e-mail

Pretexting

- Involves the use of an invented scenario, or pretext, that will engage the mark and begin a series of events that leads them to hand over information or carry out the attackers wishes
- Common examples include business email compromise (BEC) and tech support programs

Baiting

- An attacker leaves a malware-laden device, like a USB drive in a place where it will be found
- The finder picks it up and plugs it into their computer, unintentionally loading malware onto their machine

Physical Access

- Unsecured access
  - An attacker will often just walk in the door and walk through open areas to secured environments
- Piggyback
  - An attacker may walk in with a group of users
- Repair technician
  - Just because someone has a badge (with or without a picture) does not equal access.

Familiar Attacker

- An attacker gains access to an email account and then spams everyone in the account's contact list
- Tactic relies on people trusting e-mails that appear to come from someone they know

Ransomware

What is it?

Malware that locks up your data and won't unlock it unless you pay a ransom

+Very popular

+Single reason that Bitcoin maintains high value

+Proper security awareness and techniques can help protect you

+Many companies pay the ransom to get their data back

Phishing

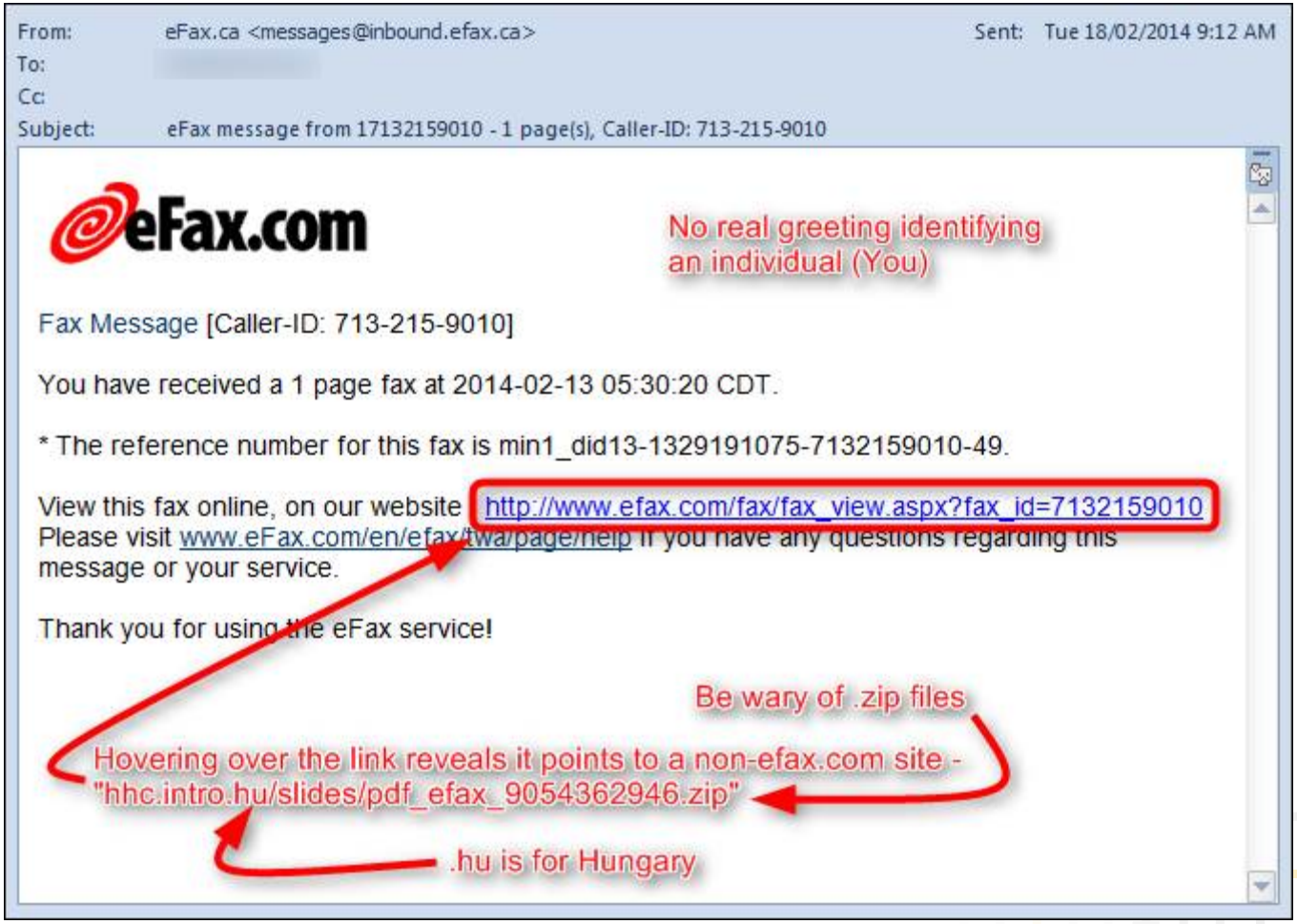
Simply, gathering information via fraud

- Most common data they're after? User credentials (work, bank, home), banking information, etc.
- They do this by posing (masquerading) as someone or something else.
- Phishing and Social Engineering are often the first lines of attack when trying to breach an organization
- Rebuffing their attack here, can show a solid security presence and hopefully thwart an attack or at least alert IT to its presence.
- A malicious party sends a fraudulent e-mail disguised as a legitimate e-mail, often purporting to be from a trusted source
- The message is intended to trick the recipient into sharing personal or financial information or clicking on a link that installs malware

Phishing Examples

Phishing Examples

Phishing Examples



Phishing vs. Spear Phishing

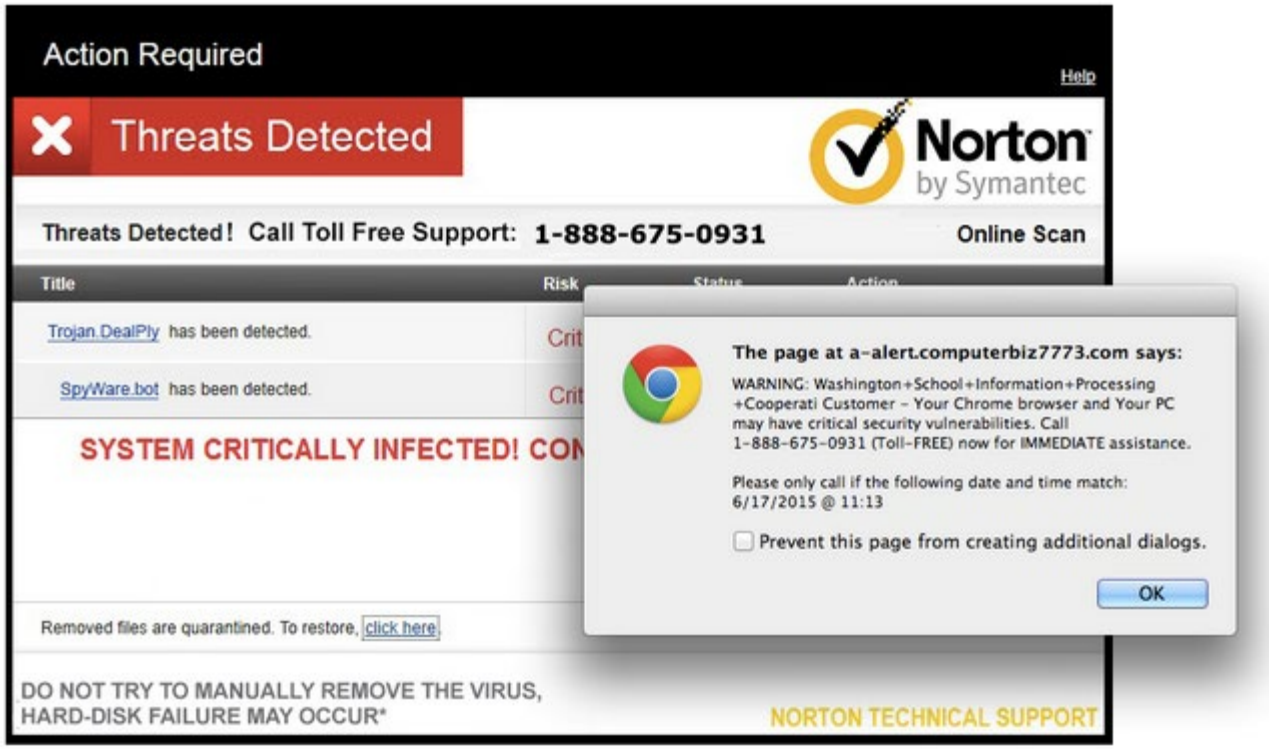
+ Similar techniques…

Phishing	Spear Phishing
Generally an exploratory attack targeting a broader audience	A more targeted version
Typically more straightforward in nature – once information is stolen, attackers have what they intended to get	Theft of credentials or personal information is usually the beginning of the attack, used to gain access to the target network

Scareware

- Involves tricking a victim into think his or her computer is infected with malware or has inadvertently downloaded illegal content
- Attacker then offers the victim a solution that will fix the bogus problem
- What really happens is the victim is tricked into downloading the "fix", which is the attacker's malware

Scareware Example



- Appears to be from a valid source
- Sense of urgency created by pop-up box
- False sense of security with confirmation of date and time

Man-In-The-Middle Attacks

- Involves an attack where the attacker will setup a wireless AP using the same SSID as a Free / Open Wireless network
- When users connect to the AP, the attacker will pass your data to the real network and collect the data stream

Evaluate the Threats

Establish Your Baseline

+ Evaluate existing policies and procedures governing security
+ Conduct system vulnerability and penetration testing
+ Perform a security controls assessment

Put Your Team to the Test

- Expose your team to scenarios that could reasonably happen in the course of business
- Share the results of the scenarios with the team
- Focus on education and remediation rather than blame and shame to engage employees in the process

Cybersecurity

Ransomware Increased 45% in 2019

- Crypto-ransomware (encrypting files) pushes pass locker-style (locking the computer screen)
- Crypto-style ransomware grew 60%
- Ensnares PC users and expands to any network –connected device
- New target in smart phones, Mac and Linux systems
  - Most recent attack was an iPhone

Phishing Increased 400% in 2020

- More workers outside the protection of the network
  - Workers must be aware of their surrounding and communications

Social Engineering Prevention

How can I prevent successful social engineering attacks?

- Security awareness training
- Policies
  - Requests for confidential employee information must be made in-person.
  - Wire transfer information must not be sent or accepted via email.
  - Visitors must wear a visitor badge and be escorted when in the building.

Social Engineering (Continued)

Technical measures

+ Visual cues
+ Least-privilege
+ Email spam/malware filtering
+ Web content filtering
+ DNS Filters
+ Anti-malware/anti-virus

Email Security

Keeping it SIMPLE!

- Don't trust email for critical decisions
- If what you're doing is critical, a phone call isn't too much!
- Spoofing: Pretending to be someone you're not
- It's easy, unfortunately. Live demo if possible
- If something doesn't seem right, pick up the phone, or walk to their office

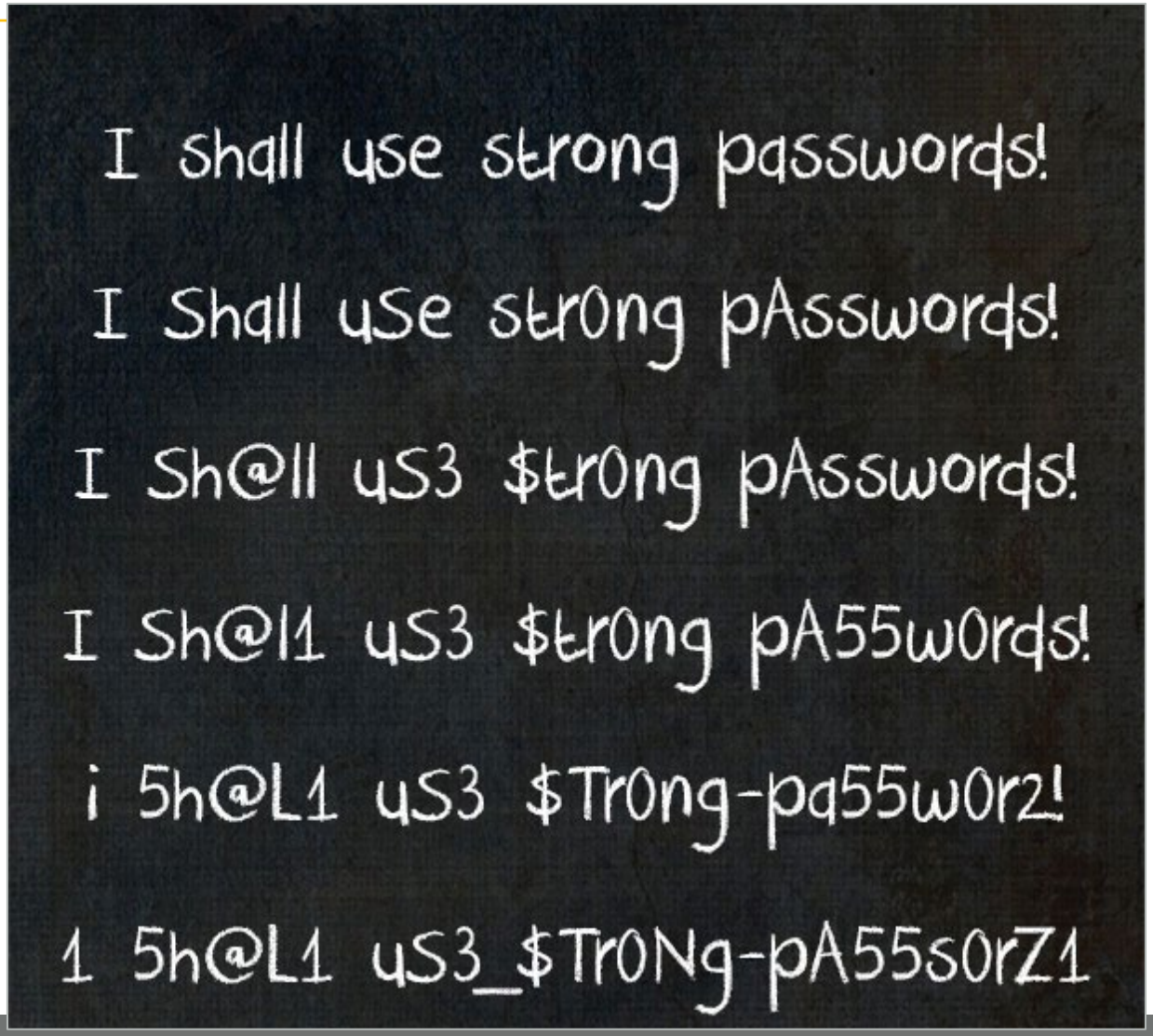
Educate Your Team

Password Security

If your password looks anything like the ones below, change it!

1. 123456
2. Password
3. 12345678
4. Qwert
5. Abc123
6. 123456789
7. 111111
8. 1234567
9. Iloveyou
10. Adobe123
11. Admin
12. Letmein
13. Photoshop
14. Monkey
15. shadow

Password Security



Password Security

Tips For Home

- WiFi Router Password
- WiFi Security
  - WEP
  - WPA
- Change your PWs for home often!
- Different accounts for family members/guests

Tips for Work

- Simple rule: If you ever find yourself speaking your PW…STOP!
- Complex helps but length is better
- Use Pass Phrase – not Password
- Come up with your own unique algorithm
- Don't reuse key passwords
- Under no circumstances do you give it away!

Password Security

Tips for Work

- If you think you've made a mistake, change your password!
- In general, it's best not write passwords down anywhere.
- Passphrases are better than passwords
- Don't use the same passwords across multiple platforms
  - ***MOST ESPECIALLY – Don't use password on personal sites/services that you use for work***
- Breathe easy, Passwords won't be around forever!
  - Biometrics on the rise

Train Teams to be Greatest Security Asset

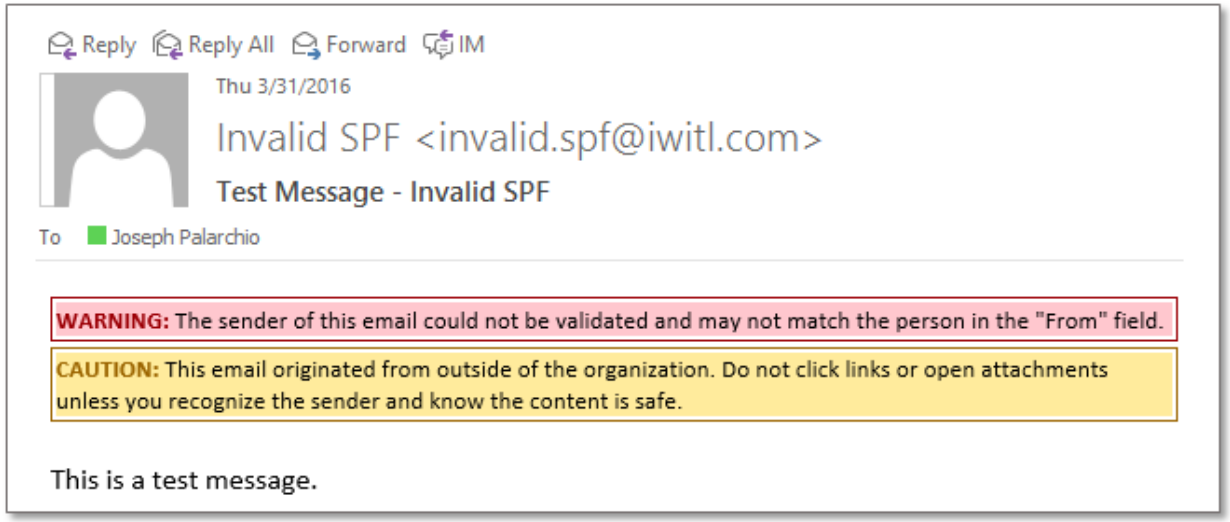
- Taking the time to train employees on their responsibility to keep the company's facilities and computer systems secure is an investment that will pay dividends
- Heighten awareness of threats and risky behavior
- Personal Responsibility for security is paramount!

Train Teams to be Greatest Security Asset

- Never give out credentials over email
- Verify and validate everything – double, even triple check
- If it cannot be verified, do not respond
- Don't click on/open suspicious or unsolicited links/attachments
- Report anything even remotely suspicious to your supervisor or to the IT department

Social Engineering (Continued)

How can I prevent successful social engineering attacks?



Physical Security

- No piggy backing
- Make sure doors close and lock
- See someone you don't know? Greet Them.
- Don't assume a badge equals access! With or Without Photo!
- Check the referrer. No referrer, no admittance!
- Be aware, very aware

Physical Security

- If you must use a secondary entrance/exit, double check it.
- If you feel uncomfortable confronting an unknown visitor, find/tell someone else. Confrontation isn't for everyone!
- Be wary of leaving ANY information on your desk. Prying eyes could be anywhere
- Lose your badge? Report it immediately!

Physical Security

- Make sure there's locks on your phones
- Don't leave your phone / laptop in the car, ever if possible
- Loss/Theft of any device containing any work information should be report immediately. No matter what time of day/night.

Cybersecurity

Ways to Reduce Risk

+ Patching vulnerabilities
+ Maintaining good software
+ Deploying effective email filters
+ Using intrusion prevention and detection software
+ Restricting third-party access to company data
+ Employing encryption where appropriate to security confidential data
+ Implementing data loss prevention technology
+ Employee and customer awareness programs

5 Questions CEOs Should Ask About Cyber Risks

- 1) How Is Our Executive Leadership Informed About the Current Level and Business Impact of Cyber Risks to Our Company?
- 2) What Is the Current Level and Business Impact of Cyber Risks to Our Company? What Is Our Plan to Address Identified Risks?
- 3) How Does Our Cybersecurity Program Apply Industry Standards and Best Practices?
- 4) How Many and What Types of Cyber Incidents Do We Detect In a Normal Week? What is the Threshold for Notifying Our Executive Leadership?
- 5) How Comprehensive Is Our Cyber Incident Response Plan? How Often Is It Tested?

Other Ways to Minimize the Risk of Threats

Risk Minimization

- Security Posture
  - Layered Protection
  - Documented Security Policy and Manual
  - SOC Compliance or other verification
- Management Support
  - Solutions come from the top down
  - Leadership awareness and promotion
- Equipment Documentation
  - Compliant HW and SW
  - Training
  - Outside Verification

Methods to Minimize the Risk

- Develop a security policy and manual
  - Make this available to all employees
  - Update on a routine basis as threats are continually evolving
- Prioritize and address any gaps or observations resulting from vulnerability and penetration testing
- Where possible, use technology to take decision making away from the employee
- Consider implementing 2-Factor Authentication


Ask
Answer
Who
Where
How
Question
Apply
Why
Understand
What
When
Answers
Query
Questions

Contact Information

+ Jim Kramer

+ Jim.Kramer@mcmcpa.com
+ 502.882.4348
+ www.mcmcpa.com