Cyber Security Webinar

Awareness, Advice, and Resources

December 2019

Presented By:

Ted Penfield, AVP of Information Technology, CJP

Nancy Viner, Vice President, Enterprise Cybersecurity Services, Fidelity Investments, Board of Directors, CJP

cjp

Webinar Contents

- Threat Landscape
- What is a Cyber Security Initiative?
- Key Aspects of a Cyber Security Initiative
- Path to Improving your Cyber Posture
- Call to Action
- Cyber Tips
- Q&A

Threat Landscape

81%
How often do hacking-related data breaches leverage stolen or weak passwords

91%
of cyberattacks begin with a phishing email

Outdated and unpatched software constitutes 22% of security issues

14.4 million consumers were **victims of identity fraud** in 2018, with out of pocket fraud costs of $1.7 billion

70% of employees don't understand cybersecurity

↑ $13M
Average cost of cybercrime in 2018

46% of websites have high cyber security vulnerabilities

Cybercrime damages to reach $6T annually

Passwords:
On average people have 23 accounts that require passwords

Does Your Organization Have A Formal Cyber Security Initiative?

What is a cyber security initiative?

- A **comprehensive set of on-going policies, procedures, and processes** directed at securing the information assets of the organization (i.e. your data)

- Staff within your organization assigned the various roles encompassed within cyber security

- **Continuously reviewed and enhanced** according to the changing threat landscape and related best practices

What are the Components of a Cyber Security Initiative?

Four primary areas, encompassing a total of 22 controls:

- Computer Systems (Servers, End-user Devices)
- Network (Internal & External)
- Business Applications
- Preparedness

Computer Systems

1. **Inventory of Authorized Devices – Computers, Servers, Network Equipment, etc.**
   - Hardware Standards & Policies ?
   - Listing of Prohibited Devices ?

2. **Inventory of Authorized Software – Office Suite, Business Applications, etc.**
   - Software Policies ?
   - Prohibited Software ?

3. **Standardized and Secure Configurations of Hardware & Software**
   - Documented?
   - Updated?

4. **Vulnerability Management and System Updates**
   - Are software updates being installed in a timely fashion?
   - What in your hardware/software infrastructure is vulnerable to attack?

5. **Limited Use of Administrative Privileges**
   - Who has administrative privileges on your computers and servers?
   - Should they have those privileges?

Computer Systems

6. **Monitoring of System Logs**
   - Process in place? Documented?
   - Who is reviewing these logs? How often?

7. **eMail and Web Browser Protections**
   - SPAM filtering, attachment and link filtering

8. **Anti-virus, Malware, and Ransomware Protections**
   - What AV/Malware software?
   - Is it continually being updated?
   - Do your systems have Ransomware protection?

9. **Limitation of Open Network Ports**
   - Firewall and network settings
   - What types of traffic to you allow in and allow out?

10. **Data Protection & Recovery**
    - Data Backups
      - Frequency? Where is this stored? How frequently is it tested?
    - Portable Device Protection?
      - Passwords
      - Encryption
      - Mobile Device Management

Network

11. **Secure Configurations of Network Devices**
    - Are the network switches/routers merely set at factory default?
12. **Boundary Protection**
    - Firewall
    - How Robust? Updated?
    - Remote Access
    - Backdoor types of access
    - Rogue Internet connections ?
13. **Data Protection**
    - How is it protected?
    - Access controls in place and ability to see exfiltration of data?
    - Is there a Non-disclosure policy and agreement in place with your employees?
14. **User Access Controls**
    - Who has access to what?
15. **Wireless (WiFi) Access Control?**
    - Security protocol in use?

Business Applications

16. **User Account Management**
    - Is there a policy as to who gets access to what of your organization's data?
    - Are there designated staff who approve/grant access?

17. **User Life-cycle Management**
    - Who performs terminating or modifying access when employees change roles or leave the organization?
    - Is this process documented? How are they notified?
    - Is User access being reviewed on a regular basis?

18. **Cyber Security Awareness Training**
    - Are your employees aware of . . . Social Engineering, Phishing, Vishing ?
    - What cadence are you testing?

19. **Application Software Security**
    - Is your business software secure?
    - Is it in the Cloud or On-premise?
    - Paid Licenses/Subscriptions, or 'Free-ware'

Preparedness

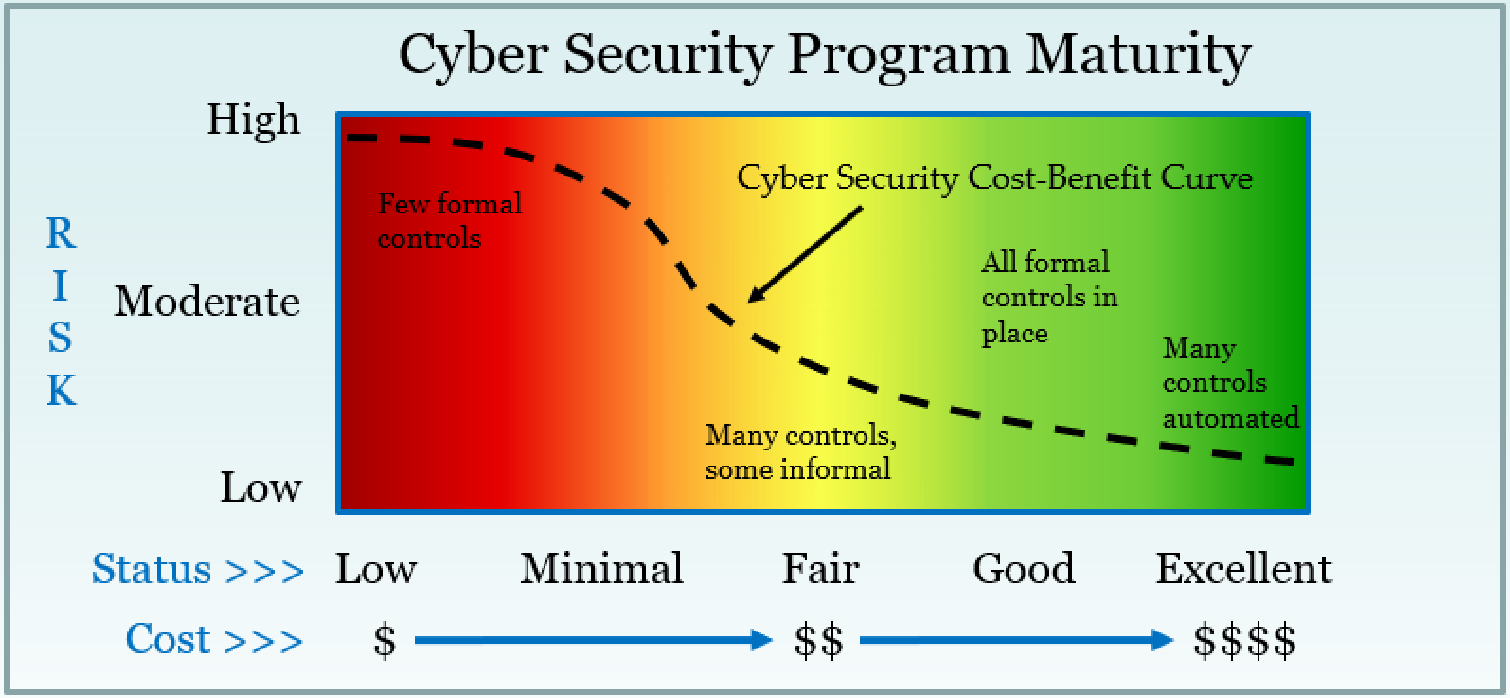
20. **Incident Response Plan**
    - Documented plan in place?
    - Roles assigned?
    - Has it been practiced? How often?

21. **Penetration Tests and 'Red Team' Exercises**
    - Are you hacking your Website/applications?
    - Is there a plan when that happens?

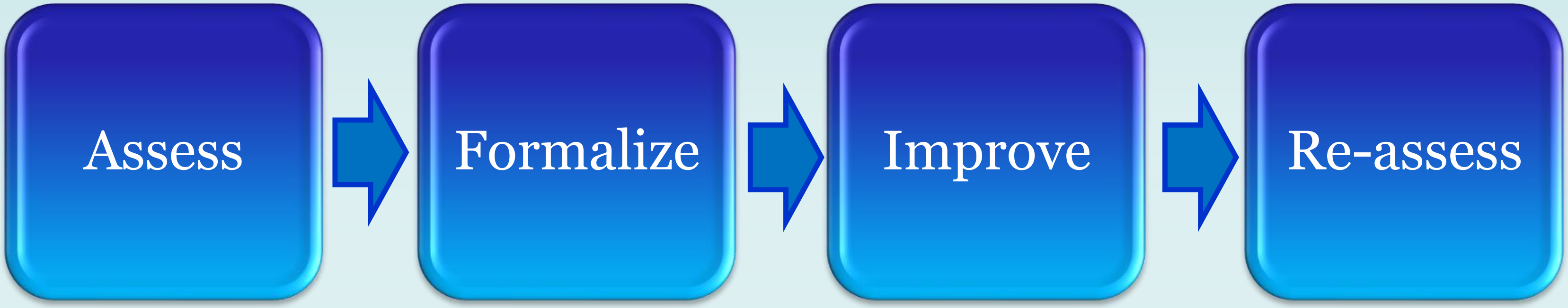
22. **Got Cyber Incident Insurance Coverage?**
    - Will you be financially covered for the expenses of an incident?

Cyber Security Summary

- A formal cyber security initiative is an extensive and continuous process.
- Cyber security becomes part of your business processes, extending well beyond your I.T. team.
- Where does YOUR organization stand in terms of its cyber security maturity?


Cyber Security Program Maturity

Improving Your Level of Cyber Security Maturity



Assess

Formalize

Improve

Re-assess

Self-Assessment

- Go through the 22 aspects of a security program.
- Which ones are you doing and how well?

Cyber Security Consultants

- External Perspective
- Formal Methodologies
- Understanding what you didn’t know

- Make cyber security a priority, and top of mind for management and staff.
- Policies & Procedures
- Documentation

- Refer to your assessment
- Fill in the gaps.
- Infrastructure upgrades and services.
- How much will it cost?
- Continuous improvement – It is not going to happen all at once.
- Cultural shift –> Everyone plays a part.

See your progress on regular intervals

- Understand your end-game.
- The ‘bar’ is constantly being raised as malicious intenders continually become more sophisticated.

Look for Easy 'Wins'

As an example:

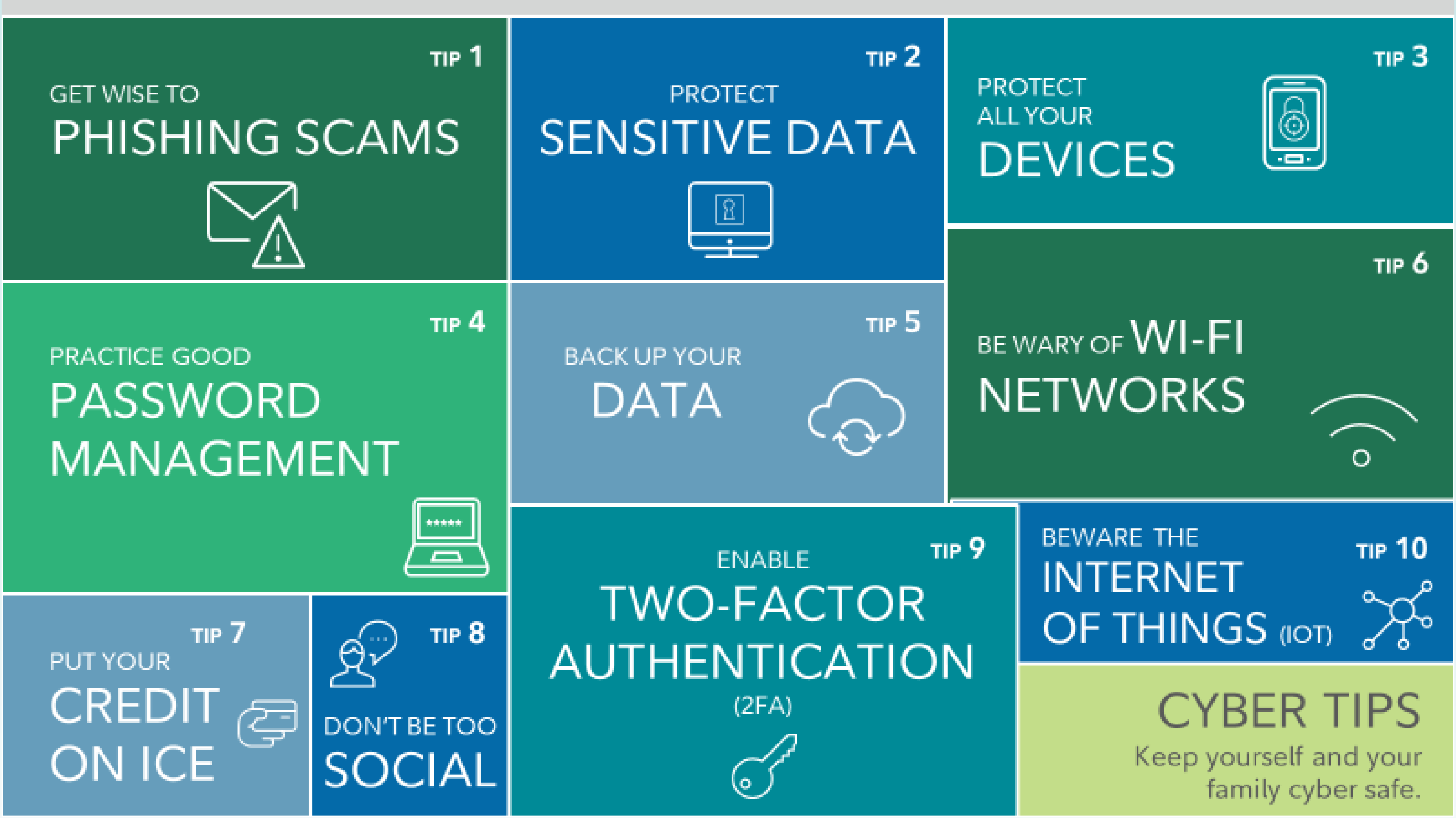
Training employees to think and act with security in mind is the most underfunded activity in cybersecurity budgets. . .

. . . despite the fact that it can provide a significant improvement in an organization's cyber maturity level at a relatively low cost.

Call to Action

- ✓ Set the tone that cybersecurity is a critical business issue; the time and effort the board spends on cybersecurity signifies if it is a priority for the company
- ✓ With the risk landscape changing constantly, create a formal plan to address some key areas: patching, phishing, access controls
- ✓ Education is key
- ✓ Hack yourself by auditing your systems in search of weaknesses
- ✓ Have a thorough understanding of the cybersecurity incident and breach escalation process and protocols within the organization, including when the board should be notified
- ✓ **Create culture of security - everyone plays a role**

10 Cyber Tips



TIP 1
GET WISE TO
PHISHING SCAMS

TIP 2
PROTECT
SENSITIVE DATA

TIP 3
PROTECT
ALL YOUR
DEVICES

TIP 4
PRACTICE GOOD
PASSWORD
MANAGEMENT

TIP 5
BACK UP YOUR
DATA

TIP 6
BE WARY OF WI-FI
NETWORKS

TIP 7
PUT YOUR
CREDIT
ON ICE

TIP 8
DON'T BE TOO
SOCIAL

TIP 9
ENABLE
TWO-FACTOR
AUTHENTICATION
(2FA)

TIP 10
BEWARE THE
INTERNET
OF THINGS (IOT)

CYBER TIPS
Keep yourself and your
family cyber safe.

cjp

Cyber Security Webinar

Additional Resources

- ✓ Leverage NIST's Small Business Cybersecurity Framework Fundamentals https://www.nist.gov/cyberframework/small-and-medium-business-resources

- ✓ National Council of Nonprofits https://www.councilofnonprofits.org/tools-resources/cybersecurity-nonprofits

- ✓ For further information feel free to reach out: TedP@cjp.org

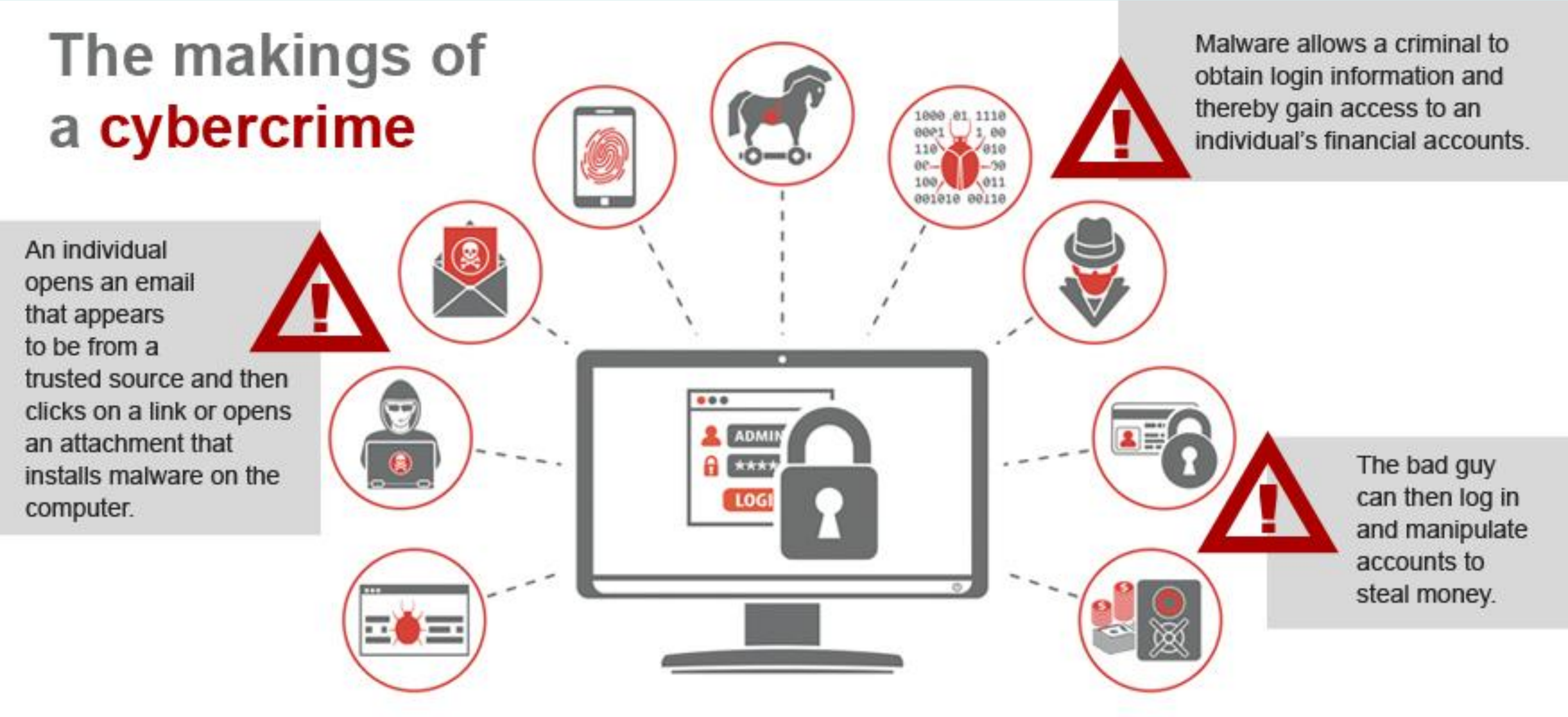
Cyber Security Webinar

Thank You !

Slide Deck to be emailed to all participants

cjp

The Makings of a cybercrime



The makings of a cybercrime

An individual opens an email that appears to be from a trusted source and then clicks on a link or opens an attachment that installs malware on the computer.

Malware allows a criminal to obtain login information and thereby gain access to an individual's financial accounts.

The bad guy can then log in and manipulate accounts to steal money.

Cyber Scam Dictionary

- **KEYLOGGER**: A technology that records consecutive keystrokes on a keyboard to capture username and password information
- **PHISHING**: An attempt to obtain financial or other confidential information from a user, typically by sending an email that mimics a legitimate organization, but links to a malicious site or contains malware
- **SPEAR PHISHING**: A highly personalized form of phishing where an email appears to be from a friend or financial institution, with an attachment or link to a site that downloads malware – usually spyware or a keylogger that operates in the background to collect sensitive information
- **MALWARE**: A software program designed to damage or cause unwanted actions on a computer system, including viruses, worms, and Trojan horses
- **RANSOMWARE**: A type of malware that restricts access to computer systems until the target pays a ransom to the malware operators to remove the restriction
- **WHALING**: a spear-phishing technique that targets high-net-worth-individuals, family offices, and corporate executives

Understand Your Home Computing Environment

Assess your computing environment, a cyber risk assessment at home maybe appropriate to protect your information

A good risk assessment will be specific to each person and should consider questions like:

- How many computers, mobile devices, tablets, TVs, home security systems, and appliances are connected to your home Wi-Fi network?
- Are they shared across personal and home office use?
- Do non-family members regularly in your home have access to your Wi-Fi network or computing devices?
- What backup procedures are in place for each device?
- Have you changed the original passwords on your IoT devices?
- Are you or other household members active on social media like Facebook, Twitter, or Pinterest?

Educate your family members about smart social media practices, passwords, safe web surfing and e-commerce protocols