ONEPATH

CYBERSECURITY FORUM

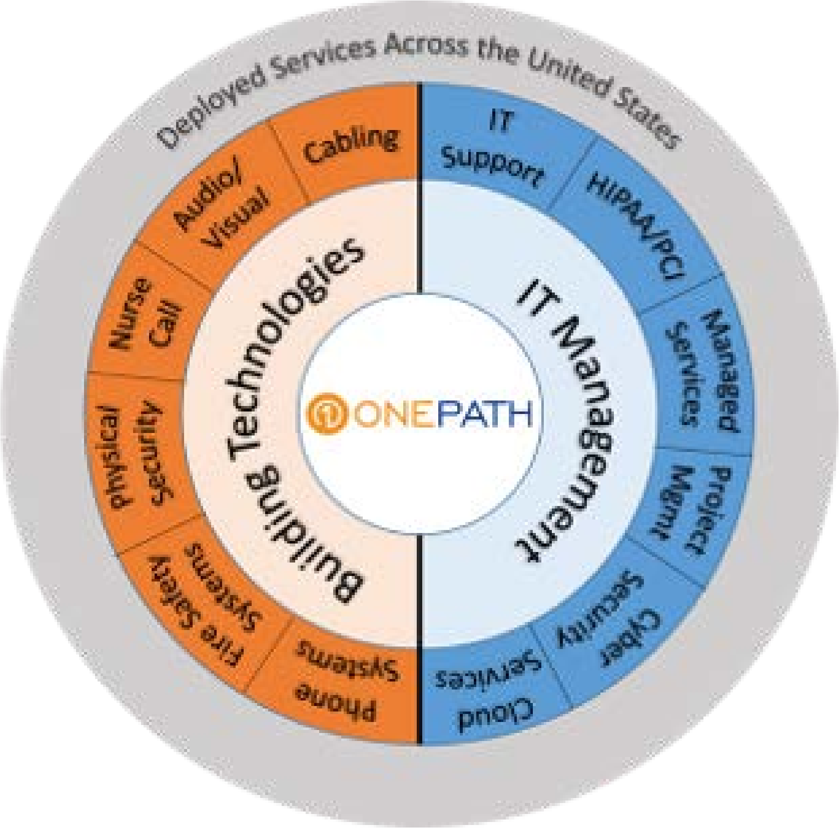
Suncoast ALA General Membership Luncheon

May 14, 2019

Onepath At-a-Glance

Onepath is the one source for all things to do with designing, deploying, and supporting technology – from cable to cloud.

- 800 Employees Strong.
- #14 largest MSP globally.
- 100+ Microsoft Certified Engineers:
  350 W2s in pure Managed IT Services.
- Ten (10) Regional NOCs and Support hubs.
- 3,500 Field Engineers throughout US.
- Net promoter score 2.5X industry average.
- 95% YoY client retention rate
  (Best in Class).
- SOC2 Certified & Attested.



About MJ Shoer www.mjshoer.com

- Onepath Director, Project and Technical Account Management Teams & vCIO.
- Onepath Director, Client Engagement & vCIO.
- Chief Technology Officer of Internet & Telephone, LLC.
- Founder & President of Jenaly Technology Group, Inc.
- Past-Chairman of the Board of Directors of the Computing Technology Industry Association, CompTIA.
- Officer & Member of three non-profit Boards of Director.
- Technology Writer & Speaker.

Seacoastonline.com

fosters.com

amazon.com BEST SELLING AUTHOR

- Testified before the United States House, United States Senate and Massachusetts Office of Consumer Affairs and Business Regulation on cybersecurity and net neutrality.

The Risk – Industry Research

ABA

- 25% of law firms in the United States have experienced AT LEAST one data breach.

CompTIA

- Cyber Crime represents an existential threat to small business.
- 14% of business with less that 100 employees feel they have a good cybersecurity strategy, compared to 20% of businesses with 100-499 employees and 27% of businesses with 500 or more employees.

verizon

- 58% of breach victim are small businesses.

CYBERSECURITY VENTURES

- Cybercrime damages will hit $6 Trillion by 2021.

The Reality

"It's not a matter of *if*, but a matter of *when*"

The Threats

- Compromised Web Sites.
- Email Links and Attachments.
- Email Phishing.
- Key Loggers.
- Malware.
- Office 365 Exploits.
- Ransomware.
- Remote Access.
- Removable Media; USB Hard Drives and Memory Sticks.
- Technical Support phone scams.
- Unmanaged Mobile Devices.
- Unencrypted Email.
- Unencrypted Data.
- Vendors, especially those that require remote access.

It's messy and confusing, just the way hackers want it!

Why Your Firm is a Target

Think about the data a law firm may hold:

- PII – Personally Identifiable Information.
- IP – Intellectual Property.
- Client List.
- Patent Filings.
- Civil and Criminal case files.
- Financial data belonging to clients and the firm itself.
- Trademark filings.
- Real Estate filings.

One of You Has Been Breached

In November 2018, security researcher Bob Diachenko identified an unprotected database hosted by data aggregator "Adapt".

Compromised data: Email addresses, Employers, Job titles, Names, Phone numbers, Physical addresses, Social media profiles.

In July 2018, the sales engagement startup Apollo left a database containing billions of data points publicly exposed without a password.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Salutations, Social media profiles.

In June 2018, the marketing firm Exactis inadvertently publicly leaked 340 million records of personal data.

Compromised data: Credit status information, Dates of birth, Education levels, Email addresses, Ethnicities, Family structure, Financial investments, Genders, Home ownership statuses, Income levels, IP addresses, Marital statuses, Names, Net worths, Occupations, Personal interests, Phone numbers, Physical addresses, Religions, Spoken languages.

In February 2019, the email address validation service verifications.io suffered a data breach.

Compromised data: Dates of birth, Email addresses, Employers, Genders, Geographic locations, IP addresses, Job titles, Names, Phone numbers, Physical addresses.

In May 2016, LinkedIn had 164 million email addresses and passwords exposed.

Compromised data: Email addresses, Passwords.

In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text.

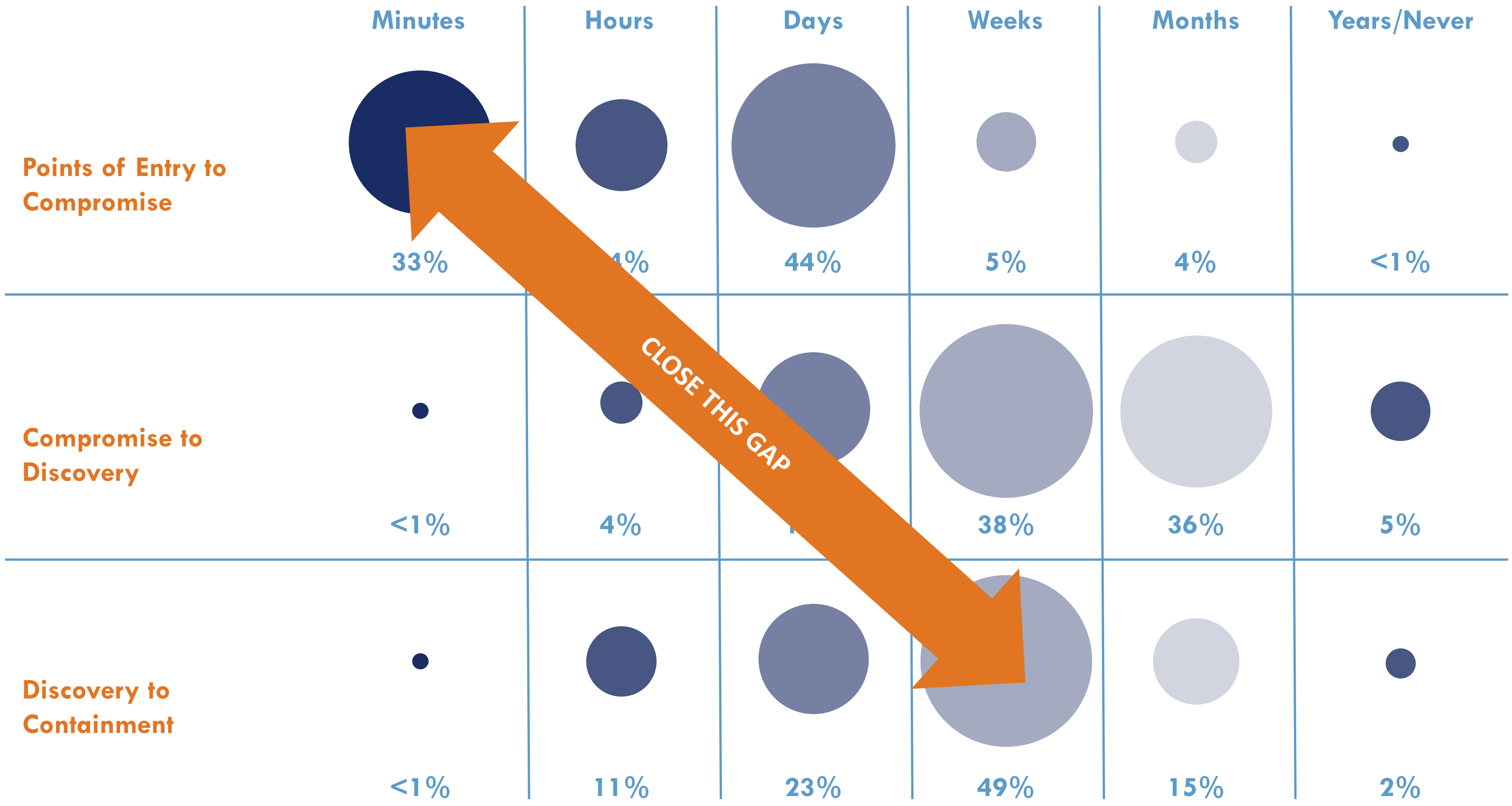
Compromised data: Email addresses, Password hints, Passwords, Usernames.

In November 2018, security researcher Bob Diachenko identified an unprotected database believed to be hosted by a data aggregator.
Compromised data: Email addresses, Employers, IP addresses, Job titles, Names, Phone numbers, Physical addresses.

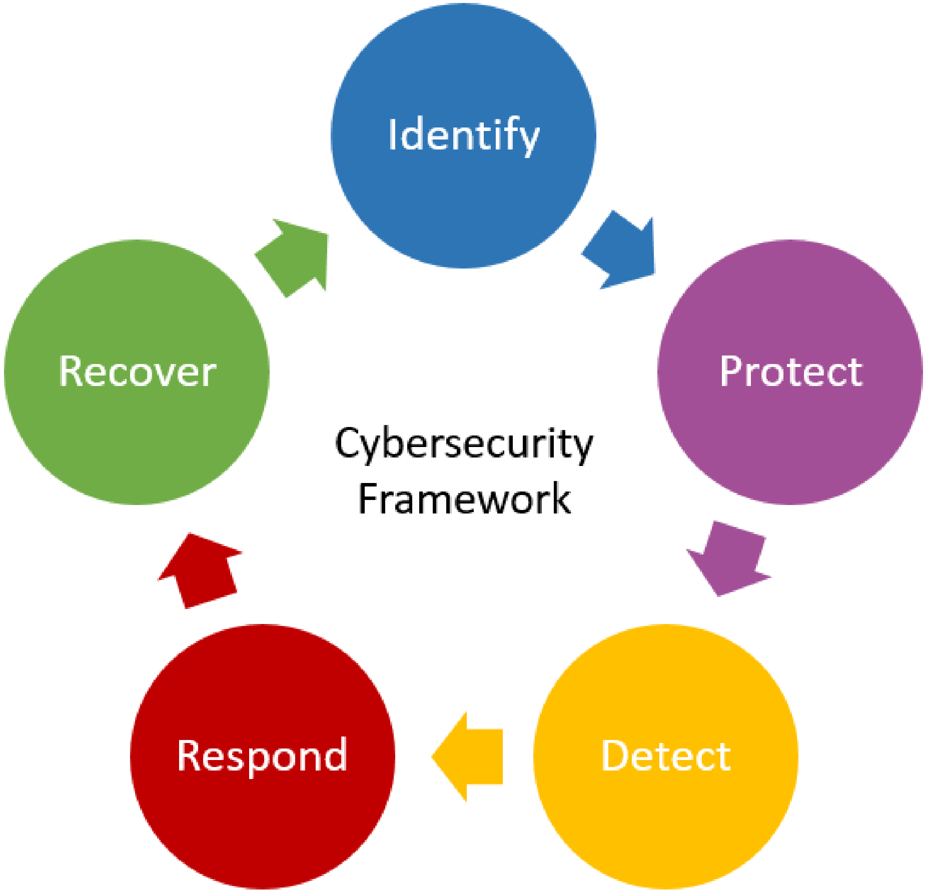
3 Critical Points in Time for Data Breach

	Minutes	Hours	Days	Weeks	Months	Years/Never
Points of Entry to Compromise	33%	14%	44%	5%	4%	<1%
Compromise to Discovery	<1%	4%	17%	38%	36%	5%
Discovery to Containment	<1%	11%	23%	49%	15%	2%

3 Critical Points in Time for Data Breach



NIST Cybersecurity Framework



The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data.

The Framework is voluntary.

It gives your business an outline of best practices to help you decide where to focus your time and money for cybersecurity protection.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

www.nist.gov/cyberframework

1. Identify

Do you have a Cybersecurity Policy? You should and it should cover the following:

- Employee responsibilities.
- Vendor responsibilities.
- Remote access policy.
- Password policy.
- Two-Factor Authentication.
- Least Privileged Access.
- Archiving policy.
- Data Loss Prevention.
- Notification policy, both internal and external.

Know What You Have!

- Real-time Inventory
    - Server’s
    - PC’s
    - Mobile Devices
    - Cloud Services
    - BYOD

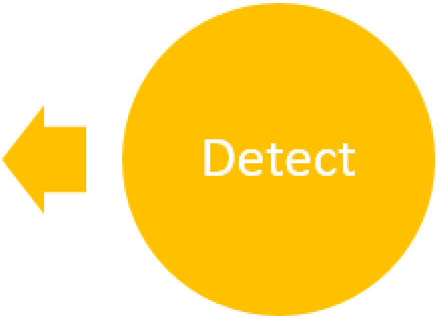
2. Protect

- How do you protect your data? Are you encrypting your data?
- Do you regulary monitor and audit who logs on to your network?
- Do you backup your data daily or in real-time?
- Do you test your backups?
- Do you have a cybersecurity training program in place?
- Do you test your users, to see if they would act on a phishing email sent to them?
- Do you regularly patch your systems?
- Do you have managed anti-virus/anti-malware software installed on all systems?
- Do you have a spam filtering system in place?
- Do you have IDS/IPS in place?

Protect

3. Detect

- Monitor your network for unauthorized logins.
- Restrict access to portable media like USB hard drives and memory sticks.
- Have an approved list of installable software.
- Monitor for unauthorized software installations on your network.
- Monitor for rogue wireless access points and connections to your wireless.
- Monitor firewall logs for unauthorized intrusion attempts.
- Monitor outbound access through your firewall.



Detect

4. Respond

What’s your response plan?

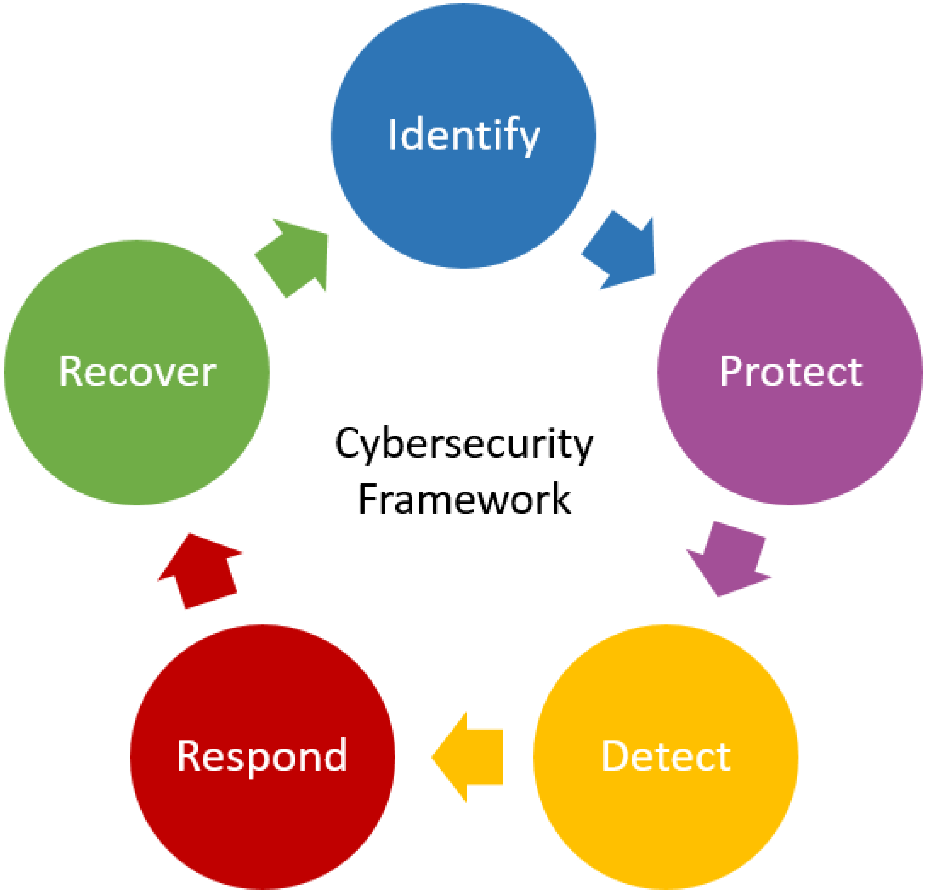
- How will you keep your business operating in the event of a cybersecurity incident?
- Do you have a notification plan and have you tested it?
  - How will you notify your clients, business partners and the public?
- Who is authorized to respond to external information requests related to the event?
- How will you contain a cyberattack?
- How will you investigate a cyberattack?
    - Will you notify law enforcement?
      - Don’t forget to consider weather events as well.
        - Know how you will mitigate any issues as a result of an event.
        - Remember to document your finding along the way.
        - Perform a post event analysis to capture any and all lessons learned.

5. Recover

Recover

- Be prepared to repair and restore impacted systems and data in the aftermath of an attack.
- If you activate your business continuity plan, have tested plan in place to deactivate the plan and restore normal operations.
- Continue your communications plan, keeping employees, clients, business partners and the public informed about your recovery efforts.
- Be sure to thoroughly debrief and review every step from initial notification to complete recovery and update your plan based on findings and lessons learned.

Onepath Cybersecurity Approach



Onepath fully endorses the NIST Cybersecurity Framework.

The Cybersecurity Framework forms the foundation of how Onepath approaches information security services for our clients.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce
www.nist.gov/cyberframework

What Should You Do?

- Talk about this presentation in your firm.

- Engage with your internal or outsourced IT partners.
  - Perform a Cybersecurity Risk Assessment.
    - Include an Internal and External Vulnerability Test.
    - Consider a Penetration Test.

- https://haveibeenpwned.com/

- Refer to the handouts I have provided.

- Train your staff!
  - Hold an Educational Information Session at the firm.
  - Deploy end-user Cybersecurity Training.
  - Send regular phishing tests to your staff.

Create a Culture of Cybersecurity Awareness

ONEPATH

Thank you.

Bret Roberts
Client Engagement Manager
(813) 283-0194
broberts@1path.com