Emerging Fraud Risks:
Harmful Tactics, Techniques and Procedures
- *and how to stop them with* Cyber Security

2019

SS&C

AIMA
THE ALTERNATIVE INVESTMENT MANAGEMENT ASSOCIATION

Important Notice

Notice: This document is provided for informational purposes only, and the contents hereof are subject to change without notice or update. This presentation is not an offer or a contract. No contractual obligations, representations or warranties are formed either directly or indirectly by SS&C in providing this information, nor is it intended for this information to take the place of your and your organization's own independent due diligence and investigation. SS&C has a variety of available services; in the event that SS&C is or has been chosen to provide certain services, those services shall be specifically described in and subject exclusively to a services agreement between SS&C and your organization. The pricing, service and technical information contained herein is proprietary to SS&C and is SS&C's confidential information. Any use or distribution of this information other than internally within your organization on a need-to-know basis is strictly prohibited.

This webinar and information provided does not constitute for legal advice but rather an effort to share knowledge, views and strategies. Information taken from common standards practices from industry practitioners. These will be depicted within the resource slide at the end of the webinar.

These security best practices considerations have been compiled from various sources but should not be considered to be a comprehensive list of practices or specific advice. Organizations should evaluate the specific risks to their own environment and implement appropriate practices to mitigate anticipated risks.

Today's Presenter

Lisa McLaughlin

VP, Risk Advisory

SS&C Technologies

Preparing for rough seas ahead as fraudsters are thriving in the digital ecosystem

Examples of publicly-known data breaches

- https://www.institutionalinvestor.com/article/b1hqqxdl6pf03f/Cyber-Attack-Hits-Prominent-Hedge-Fund-Endowment-and-Foundation
- https://compliancex.com/cybersecurity-firm-says-large-hedge-fund-attacked/
- https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627
- https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-sony-implemented-36022
- https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

What *are* the greatest cyber-risks to the Funds Business?

- **91% of cyberattacks start with a phishing email** (Dark Reading)
- **68% of targeted attacks have resulted in data loss or exposure** (Verizon)
- **Jun 27, 2019 - Phishing is still the #1 cause of data breaches** (Info phish lab)
- **One of three Americans fell victim to cybercrimes last year** (Morgan Stanley)
- **80% of hacking-related breaches leveraged either stolen and/or weak guessable passwords** (KnowBe4, Verizon)

What are the impacts *if* technology infrastructure is compromised at a fund manager or investor?

It is challenging to maintain your firm's digital presence while tackling internet-borne attacks…how can your firm be better prepared to handle this?

…with proven tactics, techniques, and procedures!

Tactics, Techniques & Procedures

Ways to Lower your Risk Profile -

1

*Proofpoint

2

** WARNING EXTERNAL EMAIL – this email is from an external source. Do not open attachments or click links from an unknown source ***

3

- Malicious Code
- Spoofing
- Phishing
- Business Email Compromise (BEC)
- Fake Domains
- Malware

- Encryption: Files/Email
- Web\Email filtering
- Access Controls (+ MFA)
- Complex Passwords
- Lock down USB/DVD
- Anti-Malware Solutions
- Monitoring (system & domain)
- Secure Configuration: Patching
- User Training, Testing

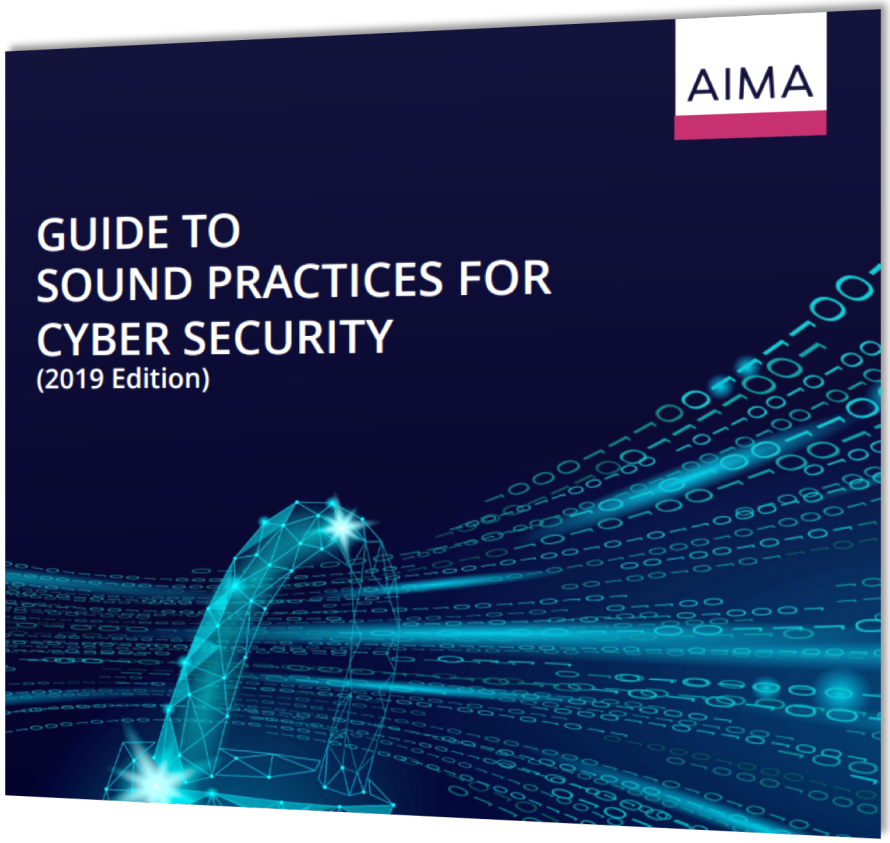
Given our rapidly evolving environment, what should our audience take away today?

What should they do upon returning to their organizations?

AIMA – Guide to Sound Practices
- For Cyber Security (2019)

Table of Contents - *Snapshot:*

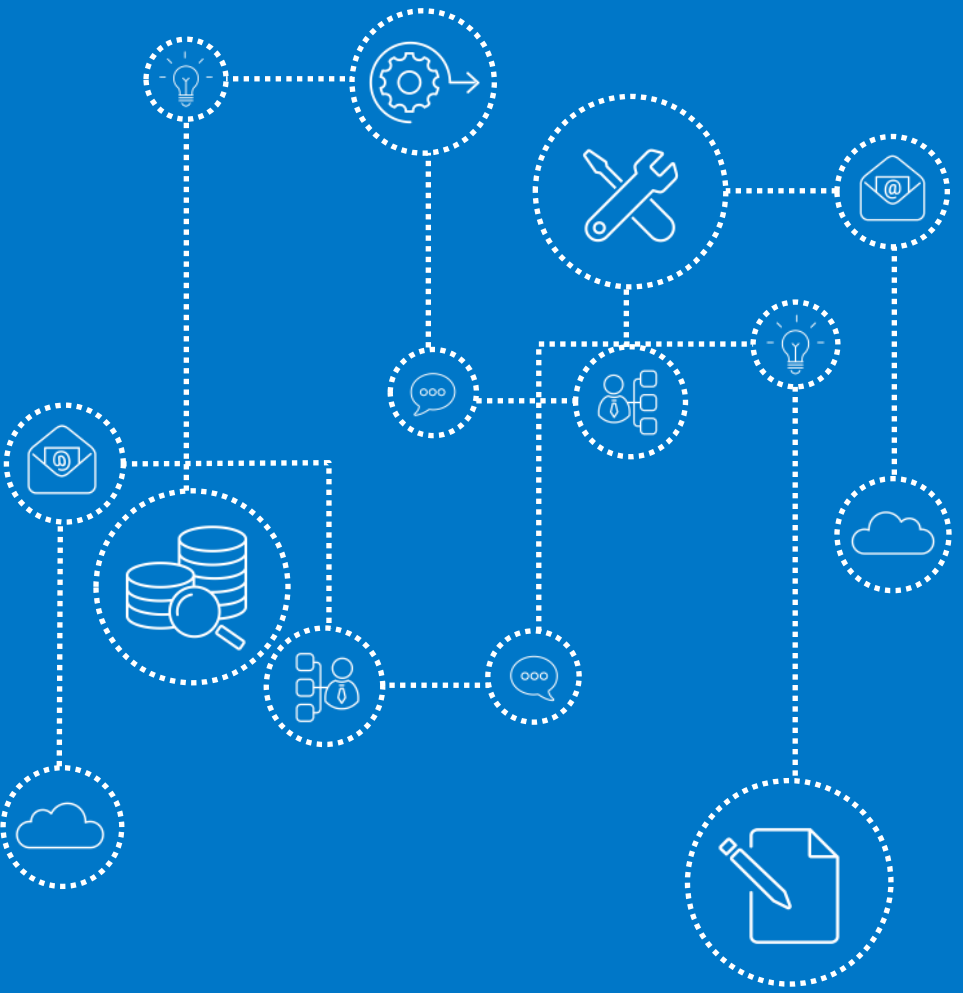
- Nature and scope of cyber threat
- Regulatory & technical context
- Initial considerations for cyber security
- Elements of effective cyber security
  - Governance
  - Employees
  - Technology, data protection measures, control and cloud service considerations



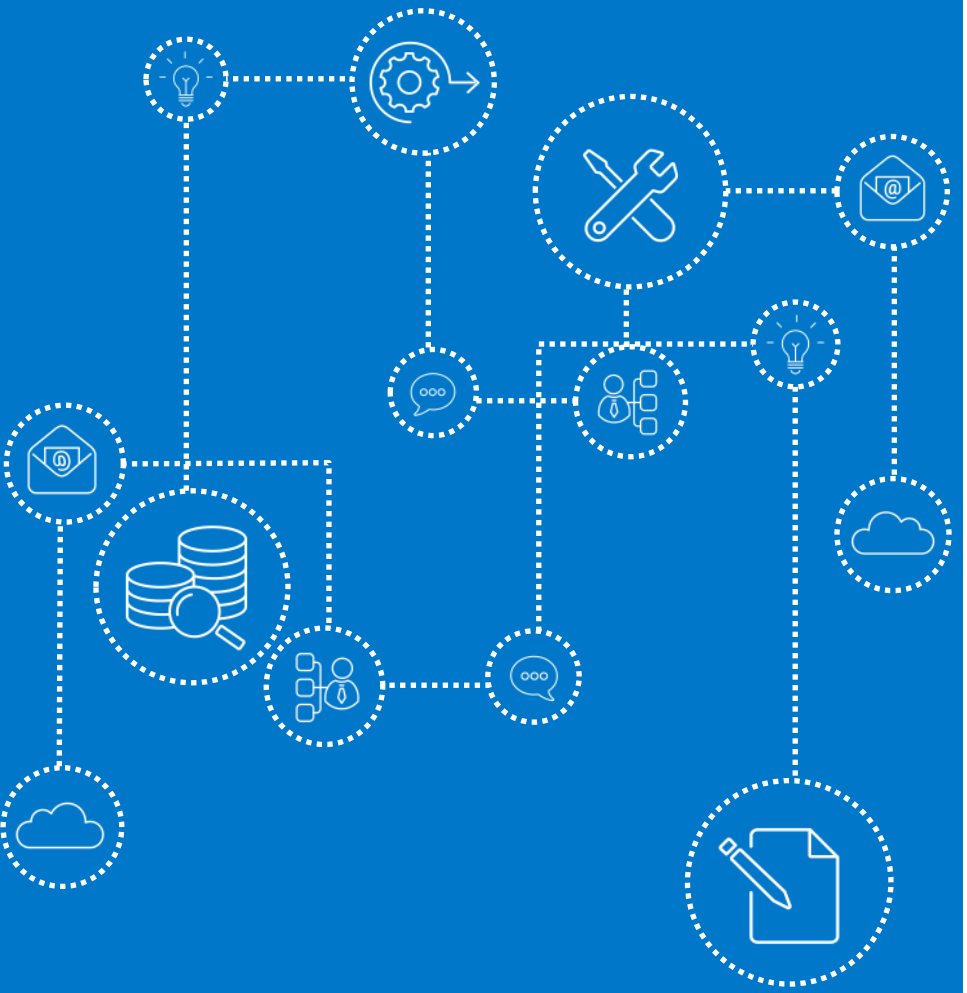
Disclaimer: As a general resource, the Guide should not be regarded as a substitute for professional advice, which should still be obtained where appropriate. Further, the Guide does not replace any applicable legal or regulatory requirements, which are likely to be more detailed than the sound practices described.

Resources, References & Acknowledgements

- ✓ AIMA: (Sound Practice Guides)
- ✓ SANS Institute
- ✓ US-Cert
- ✓ NIST
- ✓ Center for Internet Security (CIS)
- ✓ Dark Reading
- ✓ Verizon Data Breach Report
- ✓ Gartner Report
- ✓ CSO Online Publication
- ✓ NCSC (UK)
- ✓ US Department of Justice Cyber Security Unit
- ✓ SEC Cyber Guidance



Conclusion



Questions?

Thank you For Attending!

Questions – Contact Us:

AIMA Sound Practices Team | soundpractices@aima.org

Lisa McLaughlin | lmclaughlin@sscinc.com |860-298-4747