Free Cyber Tips and Bad Jokes!

@patrickcleary01

SEC REQUIREMENTS FOR CYBERSECURITY: A DIY GUIDE

As Of Date:
11/8/2018

Patrick Cleary

T: +1.215.882.9983
F: +1.216.245.3686
ir@alphaarchitect.com
213 Foxcroft Road
Broomall, PA 19008

alpha architect

We Empower Investors Through Education | Affordable Alpha

2017 © Alpha Architect. All Rights Reserved.

Objectives

Provide a quick overview of what cybersecurity is

Demonstrate that basic cybersecurity is quite “doable” for RIAs

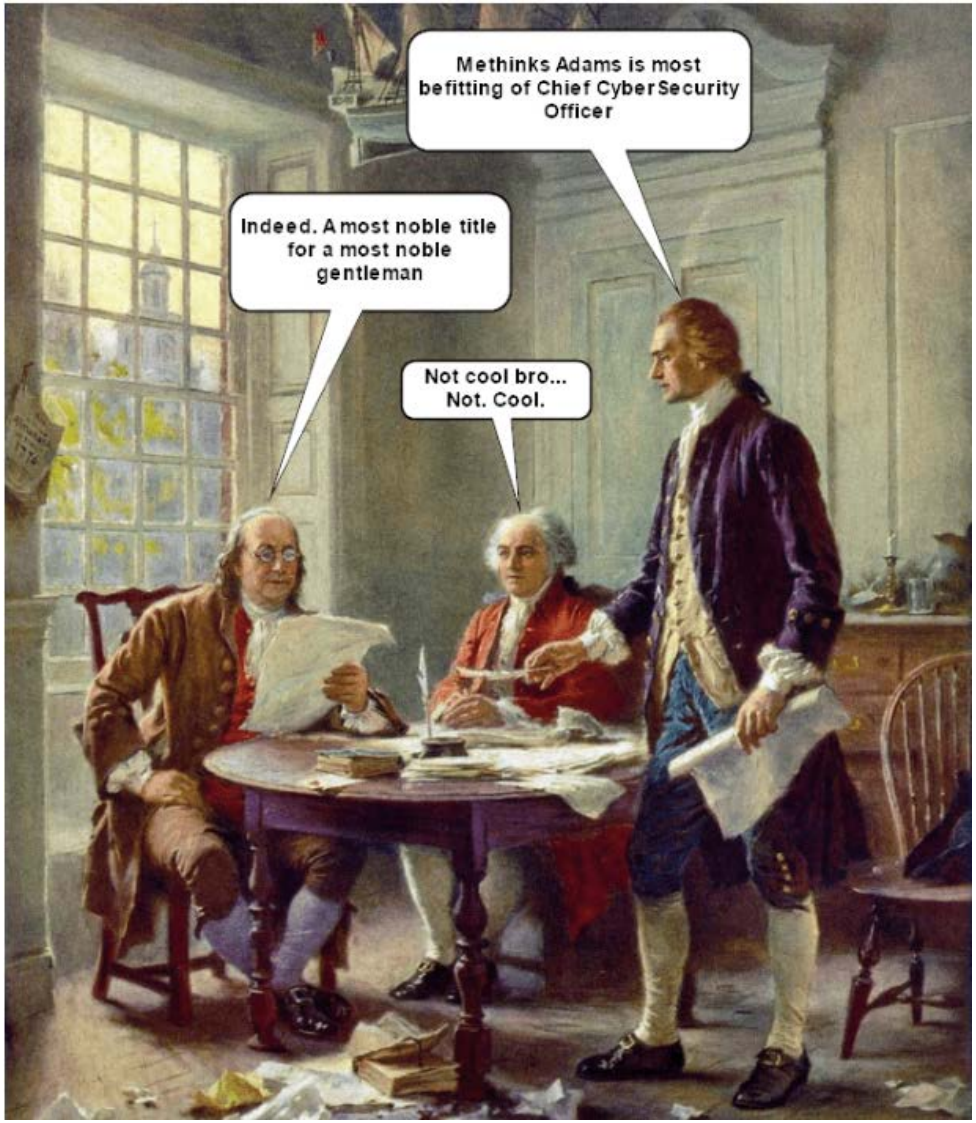
Provide next steps to build an efficient, effective cybersecurity program

Bottom Line: You can do this!

alpha architect

2017 © Alpha Architect. All Rights Reserved.

Congrats! You are the Cybersecurity Officer for your firm!!!



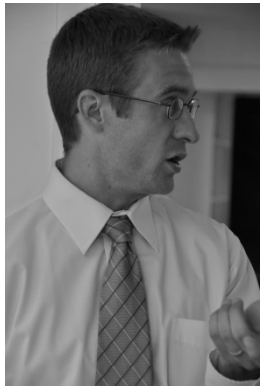
Source: Wikipedia

alpha architect

2017 © Alpha Architect. All Rights Reserved.

Our Firm Impact Mission and *Passion*:

We Empower Investors Through Education



In order to

Develop ***Sustainable*** Investors

alpha architect

Source: Alpha Architect

2017 © Alpha Architect. All Rights Reserved.

You can be a cyber geek! ZERO IT experience in my prior life

Source: Animal House

2000-2004

- Wharton undergrad
- Finance, Accounting, Chipotle
- (Note: I am not John Belushi)

Source: Alpha Architect

2004-2008

- Marine Corps (Combat Engineer)
- Blow stuff up and build stuff
- Tech experience limited to DVD player

Source: Alpha Architect

2008 - today

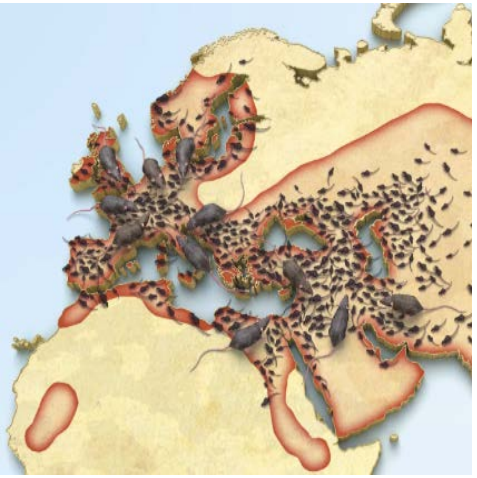
- Harvard Business School for MBA
- Consultant (Boston Consulting Group)
- COO / CCO, Alpha Architect
- Pending MS in Cybersecurity (2019)

alpha architect

2017 © Alpha Architect. All Rights Reserved.

Many scary things can be solved with a simple approach…

Plague



Source: Factinate.com

Source: Amazon.com

Polio

Source: Catalogue archives.gov

Source: vaccines.gov

Mother In-law

Source: Quora.com

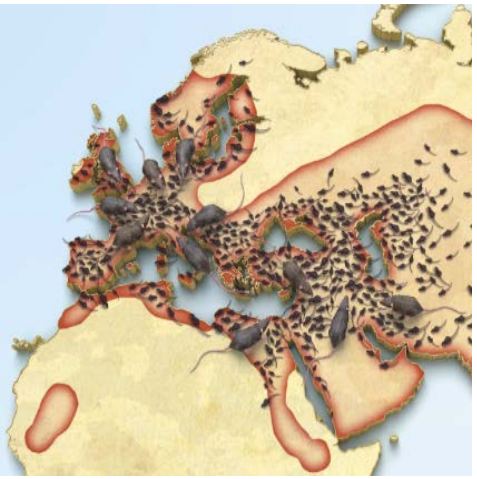
Source: Aeroflot

alpha architect

2017 © Alpha Architect. All Rights Reserved.

…but poor knowledge can create bad solutions

Plague



Source: Factinate.com

"Swallow-eth three turnips whole, lest the plague befall ye"

Polio

Source: Catalogue archives.gov

"Give Oxygen through the lower extremities, by positive electricity"

Mother In-law

Source: Quora.com

"Look honey! This home has an in-law suite!"

alpha architect

Source: Fair use (photos varied)

2017 © Alpha Architect. All Rights Reserved.

First – let's define cybersecurity

cybersecurity (sigh-brr-seh-cure-ih-tee)
(noun)

Money pit. A black hole for IT dollars to disappear

Catalyst for converting profits into losses ("lawyer" - synonym)

(sentence) "Tommy, we can't buy groceries this week, we spent all of our food budget on *cybersecurity*"

alpha architect

2017 © Alpha Architect. All Rights Reserved.

To be clear, cybersecurity MUST be taken seriously…

Source: Yahoo

2013-2014 3 Bn user accounts

Source: ebay

May, 2014 145 Mn user accounts

Source: SEC

2013 4 Mn security clearance applications

Source: S.W.I.F.T.

Feb, 2016 $101Mn stolen, almost $1Bn

alpha architect

2017 © Alpha Architect. All Rights Reserved.

…and regulators are upping their game

Source: SEC

- 2014 Cybersecurity Examination Sweep
- 2015 – Launched Cybersecurity Exam Initiative
- 2016 – EDGAR filing portal hacked. Major political pressure
- 2018 – Fines Voya (BD/IA) $1M for poor cybersecurity controls
- 2018 – warning companies to enhance cyber controls or risk violating federal law

"I'm just getting warmed up!"

Source: Scent of a Woman Fair Use. Al Pacino does not, nor has he, work at the SEC's cybersecurity unit

2017 © Alpha Architect. All Rights Reserved.

No shortage of third party solutions for Advisors…

You need cyber insurance custom tailored for Advisors

These computers are obsolete, you need new ones!

You need a special server room with onsite monitoring!

You definitely need legal opinions here

Have you considered our cyber consulting practice?

Try our turnkey compliance portal

We have special encryption tools just for you

We handle all aspects of vendor management

You need our WHAM-O cloud service

Try our cutting edge SEC cyber exam simulator

alpha architect

Source: Wikipedia – Danny Devito is not a cyber consultant

2017 © Alpha Architect. All Rights Reserved.

How about a different approach?

Common sense

Low cost

Robust

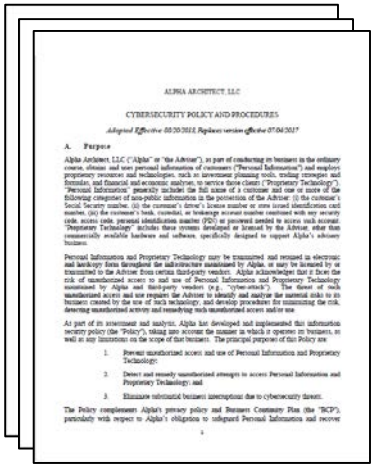
Use vendors as needed, but not by default

alpha architect

2017 © Alpha Architect. All Rights Reserved.

A robust cybersecurity program rests on three elements

Cybersecurity Manual



Source: Alpha Architect, FINRA

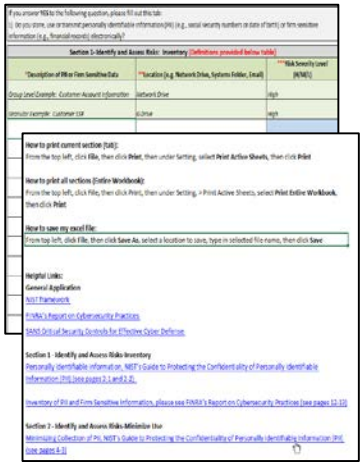
What we do

Enabling Processes

Source: Alpha Architect, FINRA

How we do it

Risk Assessment



Source: Alpha Architect, FINRA

How we get better

alpha architect

2017 © Alpha Architect. All Rights Reserved.

Step 1: Go to SEC and learn what the standards are

https://www.sec.gov/spotlight/cybersecurity

(ICOs)
Implementation of Dodd-Frank Act
Interactive Data and XBRL Initiative
Investor Advisory Committee
Jumpstart Our Business Startups (JOBS) Act
Market Structure and Data Analysis
Microcap Fraud
Money Market Funds
Regulation SCI
SEC and Fintech
Whistleblower Awards

related misconduct by utilizing the division's substantial cyber-related expertise.

investigations, including cyber investigations.

SEC Resources

Investors | Issuers / Public Companies | Investment Advisers / Investment Companies | Brokers and Dealers | Self Regulatory Organizations

Investment Advisers/Investment Companies

Regulation S-P

Regulation S-ID

Subpart C - Regulation S-ID: Identity Theft Red Flags

Adopting release

Compliance Rules

Investment Company Act Rule 38-1

Investment Advisers Act Rule 206(4)-7

Adopting release for ICA Rule 38-1 and IAA Rule 206(4)-7 (see Section II(A)(1) of the Adopting Release, which provides additional information about issues that the policies and procedures of funds or advisers should consider, certain of which are related to cybersecurity)

Engaging Government Agencies and Industry

Cybersecurity Guidance for Investment Advisers and Registered Investment Companies

Guidance on Business Continuity Planning for Registered Investment Companies

Assessing Market Participant Readiness

OCIE August 2017 – Observations from Cybersecurity Examinations

OCIE May 2017 – Cybersecurity: Ransomware Alert

OCIE September 2015 Cybersecurity Examination Initiative

OCIE Summary of 2014 Cybersecurity Examination Sweep

SEC Cybersecurity Roundtable

Email Updates

Signup for news about this topic.

Email address

Subscribe

Read all of these

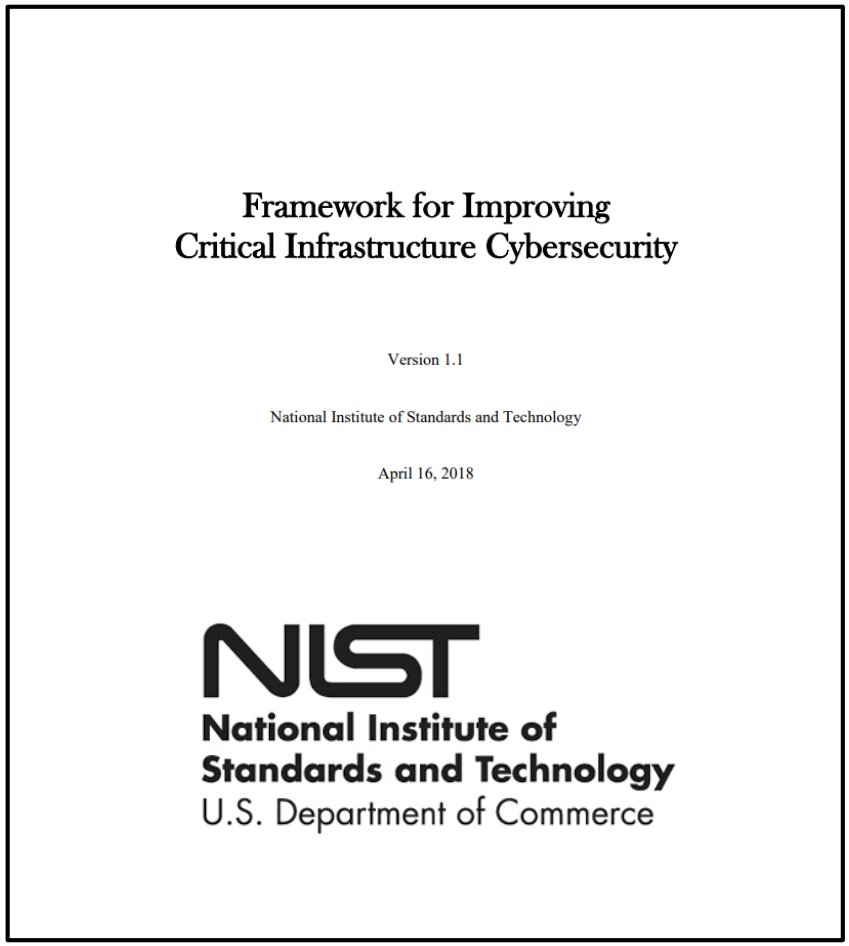
Source: SEC

alpha architect

https://www.sec.gov/spotlight/cybersecurity

2017 © Alpha Architect. All Rights Reserved.

Step 2: Go to NIST cybersecurity section, read framework



Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

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

Source: NIST

alpha architect

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

2017 © Alpha Architect. All Rights Reserved.

Step 3: Export NIST framework and write your manual

Download Excel Version from NIST website…

Function	Category	Subcategory
	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried
		ID.AM-2: Software platforms and applications within the organization are inventoried
		ID.AM-3: Organizational communication and data flows are mapped
		ID.AM-4: External information systems are catalogued
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

…and write a step that meets each subcategory

Source: NIST

alpha architect

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

2017 © Alpha Architect. All Rights Reserved.

Step 3 (example): “ID.AM-1” – inventory of physical assets

Subcategory
ID.AM-1: Physical devices and systems within the organization are inventoried

Source: NIST

“Acme Advisors will inventory all desktops, laptops, and mobile phones annually and check inventory monthly.”

alpha architect

2017 © Alpha Architect. All Rights Reserved.

Step 4: Download the FINRA small firm cybersecurity checklist

www.finra.org/industry/cybersecurity#checklist

- Vendors and Consultants
- Non-FINRA Resources

SMALL FIRM CYBERSECURITY CHECKLIST

FINRA has created a Checklist for a Small Firm's Cybersecurity Program (Excel *114 KB*) to assist small firms in establishing a cybersecurity program to:

- identify and assess cybersecurity threats, protect assets from cyber intrusions
- detect when their systems and assets have been compromised
- plan for the response when a compromise occurs
- implement a plan to recover lost, stolen or unavailable assets

Download the Cybersecurity Checklist

This checklist is primarily derived from the National Institute of Standards and Technology (NIST) Cybersecurity Framework and FINRA's Report on Cybersecurity Practices.

Use of this checklist does not create a "safe harbor" with respect to FINRA rules, federal or state securities laws, or other applicable federal or state regulatory requirements.

Source: FINRA

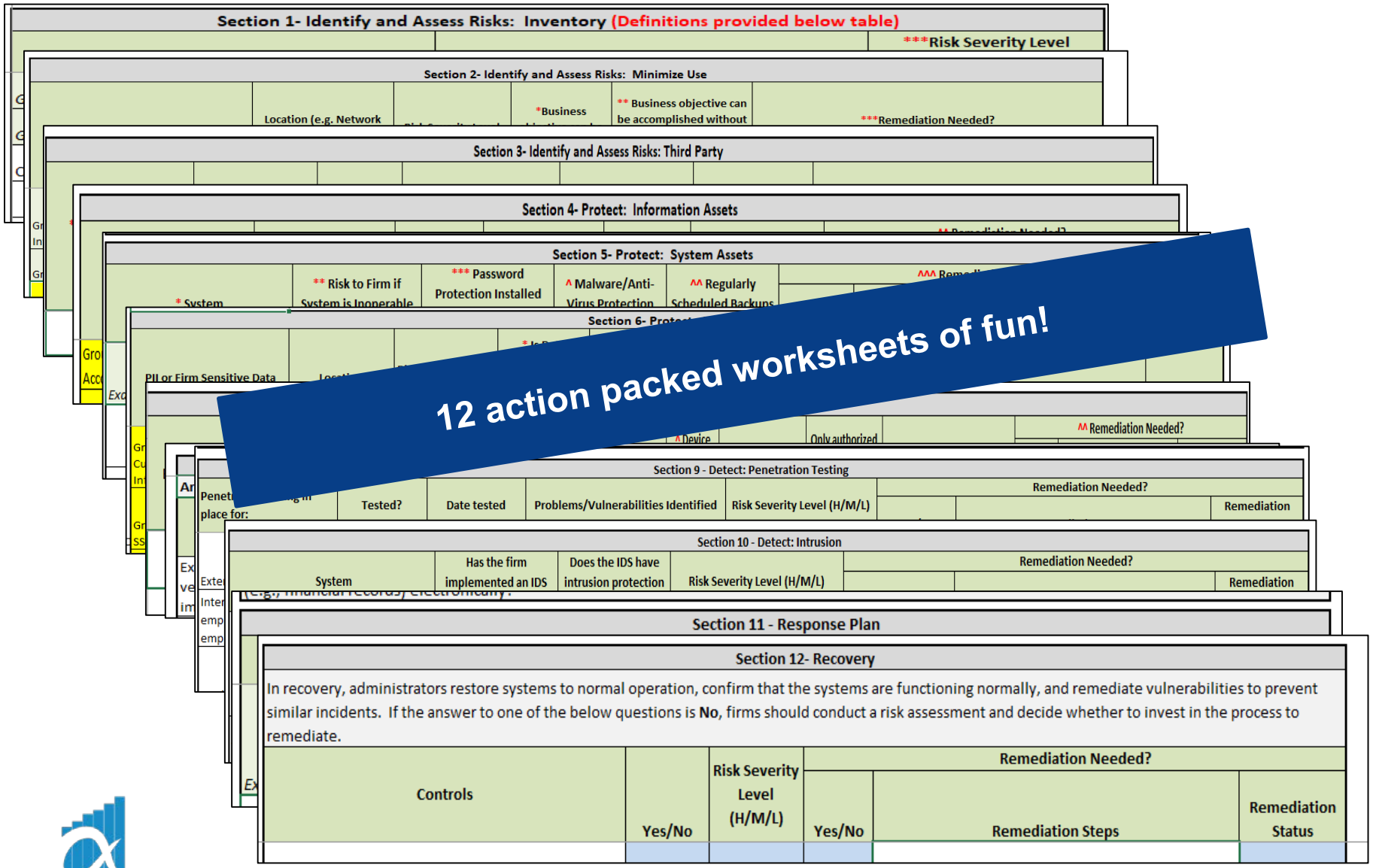
This is your risk assessment

http://www.finra.org/industry/cybersecurity#checklist

alpha architect

2017 © Alpha Architect. All Rights Reserved.

Step 5: Complete the checklist and identify gaps / needs



alpha architect

Source: FINRA

2017 © Alpha Architect. All Rights Reserved.

Step 5: Checklist generates a list of “to-dos” → do them!

Cybersecurity Summary Report

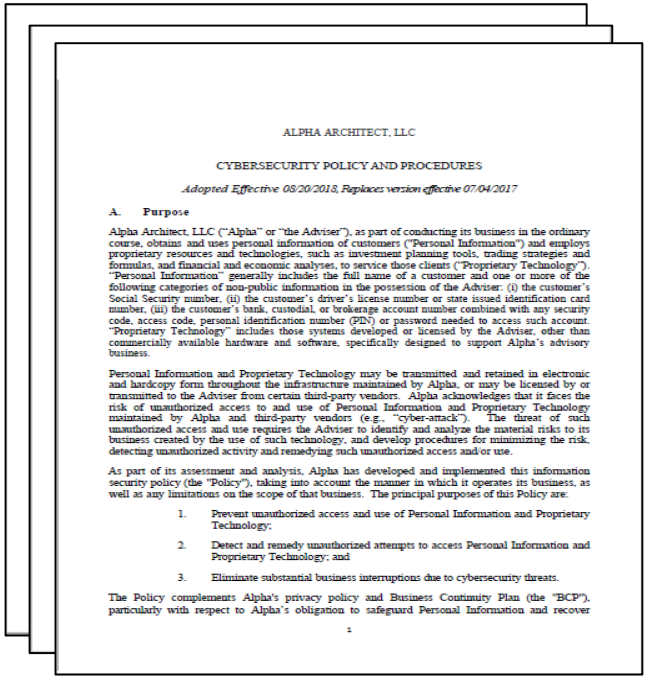
Firm Name:	0
Person(s) Responsible for Cybersecurity Program:	0
Last Updated:	January 0, 1900
Last Updated: (FINRA's last update)	Version 1.1 December 2016

Cybersecurity Summary Report: This report consolidates your responses from sections 1-12 and can be used understand where your cybersecurity risks are, where you may need to dedicate budget and resources to remediate, and where you can choose to accept the risk. This report may also be useful for executive and board level updates. The report includes 10 responses per section. If you would like to add more rows please contact us at **memberrelations@FINRA.org**. Note you can filter your report by clicking on the down arrow on the column you would like to sort, check the boxes for the data you want to display, then click okay.

	Cybersecurity Function	Firm Asset	Risk	Need to Remediate?	Remediation Status
1	Section 2 - Identify and Assess Risks: Minimize Use	Group Level Example: Customer Account Information	High	0	0
1	Section 2 - Identify and Assess Risks: Minimize Use	Granular Example: Customer SS#	High	0	0
1	Section 2 - Identify and Assess Risks: Minimize Use	0	0	0	0
1	Section 2 - Identify and Assess Risks: Minimize Use	0	0	0	0
1	Section 2 - Identify and Assess Risks: Minimize Use	0	0	0	0
1	Section 2 - Identify and Assess Risks: Minimize Use	0	0	0	0
1	Section 2 - Identify and Assess Risks: Minimize Use	0	0	0	0
1	Section 2 - Identify and Assess Risks: Minimize Use	0	0	0	0
1	Section 2 - Identify and Assess Risks: Minimize Use	0	0	0	0
1	Section 2 - Identify and Assess Risks: Minimize Use	0	0	0	0
2	Section 3 - Identify and Assess Risks: Third Party	0	0	0	0
2	Section 3 - Identify and Assess Risks: Third Party	0	0	0	0
2	Section 3 - Identify and Assess Risks: Third Party	0	0	0	0
2	Section 3 - Identify and Assess Risks: Third Party	0	0	0	0
2	Section 3 - Identify and Assess Risks: Third Party	0	0	0	0
2	Section 3 - Identify and Assess Risks: Third Party	0	0	0	0
2	Section 3 - Identify and Assess Risks: Third Party	0	0	0	0
2	Section 3 - Identify and Assess Risks: Third Party	0	0	0	0
2	Section 3 - Identify and Assess Risks: Third Party	0	0	0	0
2	Section 3 - Identify and Assess Risks: Third Party	0	0	0	0
3	Section 4 - Protect: Information Assets	Group Level Example: Customer Account Information	High	0	0

Source: FINRA, Alpha Architect

Summary Report tells you what you should fix / improve



ALPHA ARCHITECT, LLC

CYBERSECURITY POLICY AND PROCEDURES

Adopted Effective 08/20/2018; Replaces version effective 07/04/2017

A. Purpose

Alpha Architect, LLC ("Alpha" or "the Adviser"), as part of conducting its business in the ordinary course, obtains and uses personal information of customers ("Personal Information") and employs proprietary resources and technologies, such as investment planning tools, trading strategies and formulas, and financial and economic analyses, to service those clients ("Proprietary Technology"). "Personal Information" generally includes the full name of a customer and one or more of the following categories of non-public information in the possession of the Adviser: (i) the customer's Social Security number, (ii) the customer's driver's license number or state issued identification card number, (iii) the customer's bank, custodial, or brokerage account number combined with any security code, access code, personal identification number (PIN) or password needed to access such account. "Proprietary Technology" includes those systems developed or licensed by the Adviser, other than commercially available hardware and software, specifically designed to support Alpha's advisory business.

Personal Information and Proprietary Technology may be transmitted and retained in electronic and hardcopy form throughout the infrastructure maintained by Alpha, or may be licensed by or transmitted to the Adviser from certain third-party vendors. Alpha acknowledges that it faces the risk of unauthorized access to and use of Personal Information and Proprietary Technology maintained by Alpha and third-party vendors (e.g., "cyber-attack"). The threat of such unauthorized access and use requires the Adviser to identify and analyze the material risks to its business created by the use of such technology, and develop procedures for minimizing the risk, detecting unauthorized activity and remedying such unauthorized access and/or use.

As part of its assessment and analysis, Alpha has developed and implemented this information security policy (the "Policy"), taking into account the manner in which it operates its business, as well as any limitations on the scope of that business. The principal purposes of this Policy are:

1. Prevent unauthorized access and use of Personal Information and Proprietary Technology;
2. Detect and remedy unauthorized attempts to access Personal Information and Proprietary Technology; and
3. Eliminate substantial business interruptions due to cybersecurity threats.

The Policy complements Alpha's privacy policy and Business Continuity Plan (the "BCP"), particularly with respect to Alpha's obligation to safeguard Personal Information and recover

1

Source: Alpha Architect, FINRA

Be sure to update your cybersecurity manual too!

alpha architect

2017 © Alpha Architect. All Rights Reserved.

Step 5: Lots of low hanging fruit to help you!

Compliance Manual?	NIST Framework (Excel)
Risk Assessment?	FINRA Small Firm Checklist
Encryption?	Windows Bitlocker (on!!!)
2 Factor?	Google Suite (on!!!)
Updates / Patches?	Windows Defender (on!!!)
Cloud?	Google Drive (FedRamp'd!)
Network security?	Buy a new router!
Vendor Management	SOC-2? Ask helpdesk?
Network Map?	PowerPoint and elbow grease
Alerts?	DHS Cert Listserve

alpha architect

2017 © Alpha Architect. All Rights Reserved.

Step 6: Implement a simple process to carry out your manual

	Cybersecurity Compliance Tracker
✓	Q1 - Cybersecurity Compliance
✓	QUARTERLY TASKS - Q1
✓	Q2 - Cybersecurity Compliance
✓	QUARTERLY TASKS - Q2
✓	Q3 - Cybersecurity Compliance
✓	ANNUAL TASKS - Q3
✓	QUARTERLY TASKS - Q3
✓	Q4 - Cybersecurity Compliance
✓	QUARTERLY TASKS - Q4

Source: Alpha Architect, FINRA

I *Go through your manual, highlight key "to do" items*

II *Write down these steps, with calendar reminders*

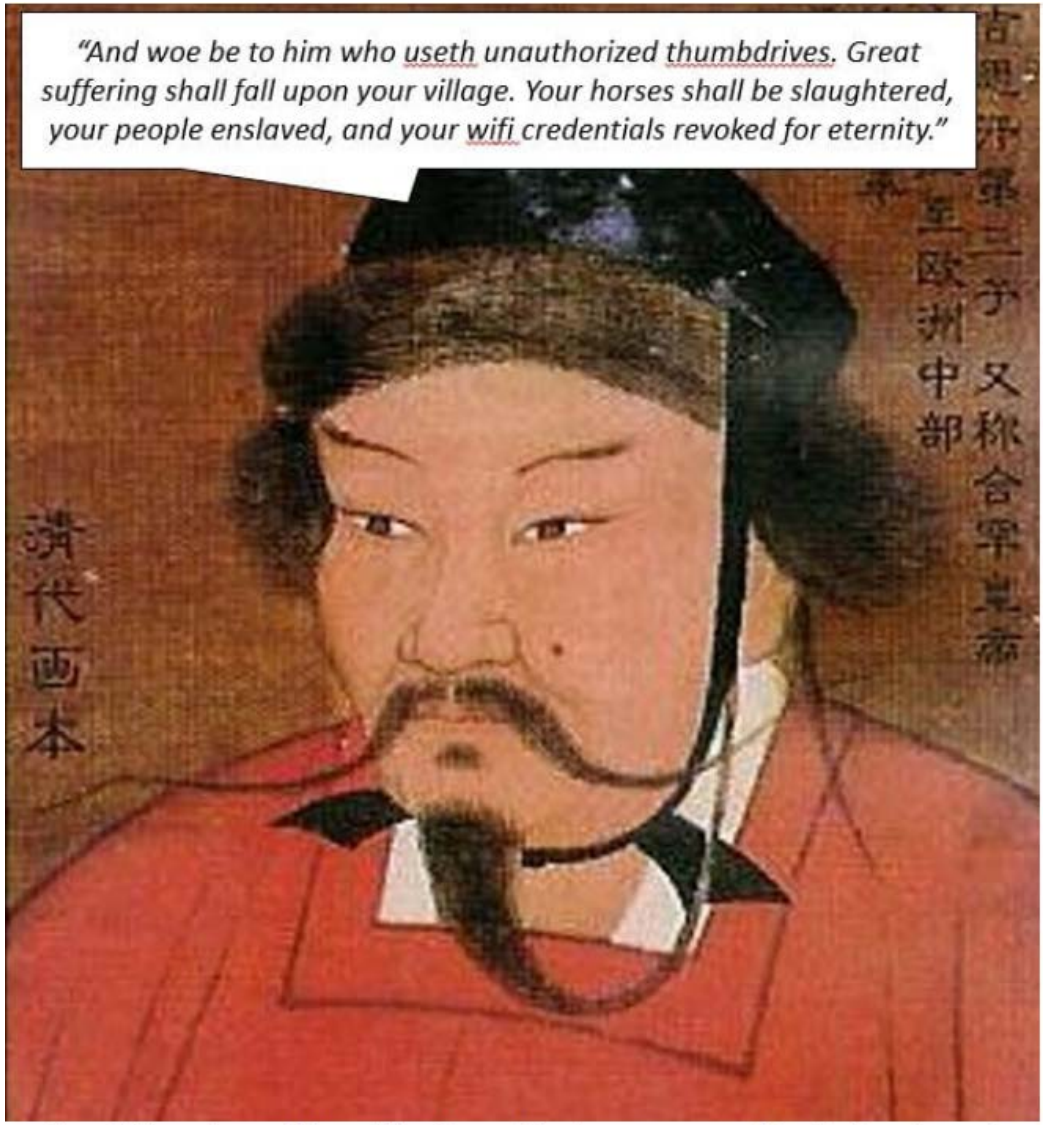
III *Have "sign-off" process to document completion*

This can be a high tech solution or low tech solution

alpha architect

2017 © Alpha Architect. All Rights Reserved.

Step 7: Train your employees!!!



Ogadai Khan, Second Khan of the Mongol Empire, conqueror of the Jin Dynasty, and Cybersecurity Overlord of All that is Living, pictured here during an annual cybersecurity training module given to Mongolian forces (c. 1231 AD).

Source: Wikipedia

alpha architect

2017 © Alpha Architect. All Rights Reserved.

A few blog posts to help

How to build an Investment Advisor Cybersecurity program

SEC Cybersecurity Requirements for RIAs

Vendor Management and Cybersecurity Compliance for RIAs

Penetration Testing for Financial Advisors

alpha architect

2017 © Alpha Architect. All Rights Reserved.

Key takeaways

Read the NIST framework – the SEC reads it too

Writing your manual = knowing your manual

Low hanging fruit can get 80% of the tech covered

Documentation of processes is critical

Use common sense – do you need an SSN for KYC?

Learning is cumulative. You don't need to be an expert day one

alpha architect

Emmet Peppers
epeppers@interactivebrokers.com
Sales Representative
Tel: +1 707 559 3258
West Coast Sales