

TECHNOLOGY

COMPLIANCE WORKSHOP FALL 2015

Wes Brinkley

wbrinkley@maynardcooper.com

(205) 254-1845



Presentation Overview

- ▼ **Cybersecurity**
- ▼ **Cloud Recordkeeping**
- ▼ **Email Surveillance**
- ▼ **Disaster Recovery Plans**

Cybersecurity

▼ **Gramm-Leach-Bliley Act**

▼ **Regulation S-P**

▼ **Regulation S-ID**

January
2014

- The Office of Compliance Inspections and Examinations (“OCIE”) includes a focus on technology and cybersecurity preparedness in its exam priorities.

April 2014

- OCIE issues risk alert on its cybersecurity initiative and announces sweep exams.

February
2015

- OCIE issues initial observations from sweep exams.
- FINRA issues report on cybersecurity policies.

April 2015

- Division of Investment Management (“IM”) issues cybersecurity guidance update.

September
2015

- OCIE issues second risk alert on its cybersecurity examination initiative and announces second round of sweep exams.
- SEC releases first cybersecurity related enforcement action.

OCIE Guidance

▼ Items OCIE may request during an examination:

- ▼ Inventory of devices
- ▼ Inventory of software platforms and applications
- ▼ Maps of network resources, connections, and data flows (including where customer data is housed)
- ▼ Resources (hardware, data, software) prioritized for protection based on sensitivity and business value
- ▼ Written information security policy
- ▼ Details regarding periodic risk assessments to identify cybersecurity threats, vulnerabilities and potential business consequences
- ▼ Written business continuity plan that addresses cybersecurity incidents and recovery from such incidents
- ▼ Insurance policies that specifically cover losses and expenses attributable to cybersecurity incidents

IM Guidance

- ▼ **Written cybersecurity policy and rapid response plan tailored for the nature and scope of the adviser's business**
 - ▼ **Appoint a Security Manager**
 - ▼ **Identify sensitive data**
 - ▼ **Prioritize critical needs**
 - ▼ **Access rights and controls**
 - ▼ **Data loss prevention**
 - ▼ **Vendor management**
 - ▼ **Training**

- ▼ **Cybersecurity embedded into the firm's compliance policies**
 - ▼ **Identity theft**
 - ▼ **Data protection**
 - ▼ **Fraud**
 - ▼ **Business continuity**

What are the primary causes of BREACHES?

Common reasons include:

- 46% A lost or stolen computing device
- 42% Employee mistakes or unintentional actions
- 42% Third party snafus
- 33% Criminal attack
- 31% Technical systems glitch
- 14% Malicious insider
- 8% Intentional non-malicious employee action



These breaches were discovered by:

52%
audit/
assessment



47%
employee
detected



36%
patient
complaint



SOURCES: Third Annual Benchmark Study on Patient Privacy & Data Security
| medicalnewstoday.com | huffingtonpost.com

Information provided by: <http://www.backgroundcheck.org/>

 **BACKGROUNDCHECK.ORG**

MAYNARD
COOPER GALE

Insurance Considerations

- ▼ Only 21% of advisers examined as part of the OCIE's National Examination Program maintained insurance that would cover losses and expenses attributable to cybersecurity incidents.
- ▼ Cyber insurance can take two primary forms:
 - ▼ First party coverage protects a company from costs that it incurs in handling a data breach (credit monitoring, forensic investigation and analysis).
 - ▼ Third party coverage protects a company from claims by third parties, typically clients who may have been affected by the breach (legal defense, settlements, liability to banks for re-issuing credit cards, responding to regulatory inquiries).


Insurance Considerations

- ▼ Consider whether the terms of a commercial general liability policy would cover claims involving cyber-attacks and loss of electronic data.
- ▼ Carefully review any exclusions or conditions that may impact cyber coverage.
- ▼ Negotiate for the narrowest definition of “war” possible.
 - ▼ Attacks by a foreign government?
 - ▼ What if the U.S. government declares the attack an act of terror?
- ▼ Consider if acts of god are covered in cyber or CGL policies.
 - ▼ Data loss due to tornado, lightening, etc.

Exclusions

B. This Policy does not directly or indirectly cover:

1. loss not reported to the COMPANY in writing within sixty (60) days after termination of this Policy as an entirety,
2. loss due to riot or civil commotion, outside the United States of America or Canada, or any loss due to military, naval or usurped power, war or insurrection. However, this Exclusion shall not apply to loss which occurs in transit, provided that when such transit was initiated, there was no knowledge on the part of any person acting for the INSURED of such riot, civil commotion, military, naval or usurped power, war or insurrection,



III. EXCLUSIONS

A. EXCLUSIONS APPLICABLE TO ALL INSURING AGREEMENTS

1. This **CyberRisk Policy** will not apply to any **Claim** or **Single First Party Insured Event** based upon or arising out of any nuclear reaction, nuclear radiation, radioactive contamination, biological or chemical contamination or to any related act or incident.
2. This **CyberRisk Policy** will not apply to any **Claim** or **Single First Party Insured Event** based upon or arising out of war, invasion, acts of foreign enemies, hostilities (whether war is declared or not), civil war, rebellion, revolution, insurrection, military or usurped power, confiscation, nationalization, requisition, or destruction of, or damage to, property by or under the order of any government, public or local authority; provided that this exclusion will not apply to any “act of terrorism” as defined in the Terrorism Risk Insurance Act, as amended.
3. This **CyberRisk Policy** will not apply to any **Claim** or **Single First Party Insured Event** based upon or arising out of damage to, or destruction of, loss of, or loss of use of, any tangible property including damage to, destruction of, loss of, or loss of use of, tangible property that results from inadequate or insufficient protection from soil or ground water movement, soil subsidence, mold, toxic mold, spores, mildew, fungus, or wet or dry rot.
4. This **CyberRisk Policy** will not apply to any **Claim** or **Single First Party Insured Event** for any actual or alleged bodily injury, sickness, disease, death, loss of consortium, emotional distress, mental anguish, humiliation or loss of reputation; provided that this exclusion will not apply to that portion of any **Claim** for a **Communications and Media Wrongful Act** seeking **Loss** for emotional distress, mental anguish, humiliation or loss of reputation.

**Vendors are responsible
for 20% of all data breaches.**

(Ponemon Institute 2014 Cost of Data Breach Study: United States)

Three Pillars of Vendor Management

Perform data security assessment of the vendor.

Negotiate contract to minimize risk.

Train, monitor, audit, remediate.

Third Party Vendor Considerations

- **Industry Specific Experience**
- **Retention and Disposal of Data**
- **Cybersecurity Policies and Procedures**
- **Insurance Coverage (Consider asking to be named a third party beneficiary on your vendor's policy)**
- **Allocation of liability**
- **Internal Controls**
- **Disaster Recover Plan**
- **Breach Notification**
- **Privacy Policy**

Sample Terms of Service

Limitation of Liability

TO THE FULLEST EXTENT PERMITTED BY LAW, EXCEPT FOR ANY LIABILITY FOR [REDACTED]S OR ITS AFFILIATES' FRAUD, FRAUDULENT MISREPRESENTATION, OR GROSS NEGLIGENCE, IN NO EVENT WILL [REDACTED] ITS AFFILIATES, SUPPLIERS OR DISTRIBUTORS BE LIABLE FOR:

(A) ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR

(B) ANY LOSS OF USE, DATA, BUSINESS, OR PROFITS, REGARDLESS OF LEGAL THEORY.

THIS WILL BE REGARDLESS OF WHETHER OR NOT [REDACTED] OR ANY OF ITS AFFILIATES HAS BEEN WARNED OF THE POSSIBILITY OF SUCH DAMAGES, AND EVEN IF A REMEDY FAILS OF ITS ESSENTIAL PURPOSE.

ADDITIONALLY, [REDACTED] ITS AFFILIATES, SUPPLIERS AND DISTRIBUTORS WILL NOT BE LIABLE FOR AGGREGATE LIABILITY FOR ALL CLAIMS RELATING TO THE SERVICES FOR MORE THAN THE GREATER OF \$20 OR THE AMOUNTS PAID BY YOU TO [REDACTED] FOR THE PAST 12 MONTHS OF THE SERVICES IN QUESTION.

Some places don't allow the types of limitations in this paragraph, so they may not apply to you.



Cybersecurity Information Sharing Act of 2015 (“CISA”)

- ▼ Cyber threats like malware and phishing will often attack many targets at once.
- ▼ CISA promotes information sharing among private companies and between private companies and the federal government. The goal is to encourage companies to share information in real time regarding cyber threat indicators.
- ▼ Protecting consumers’ personal and financial information has been an underlying concern.
- ▼ Companies have been hesitant to share information regarding cyber threats for fear of violating privacy regulations. CISA would provide safe harbors to protect participating companies from litigation stemming from voluntarily sharing of information.

Cloud Recordkeeping

- ▼ **Rule 204-2 under the Advisers Act allows advisers to maintain and preserve records on electronic storage media.**
- ▼ **Cloud computing is renting server space or access to software from a cloud service provider.**
- ▼ **Selection and management of Cloud service providers**
 - ▼ **Industry specific experience?**
 - ▼ **Experience with regulatory agencies?**
- ▼ **Advantages of Cloud recordkeeping**
 - ▼ **Cost savings**
 - ▼ **Accessibility**

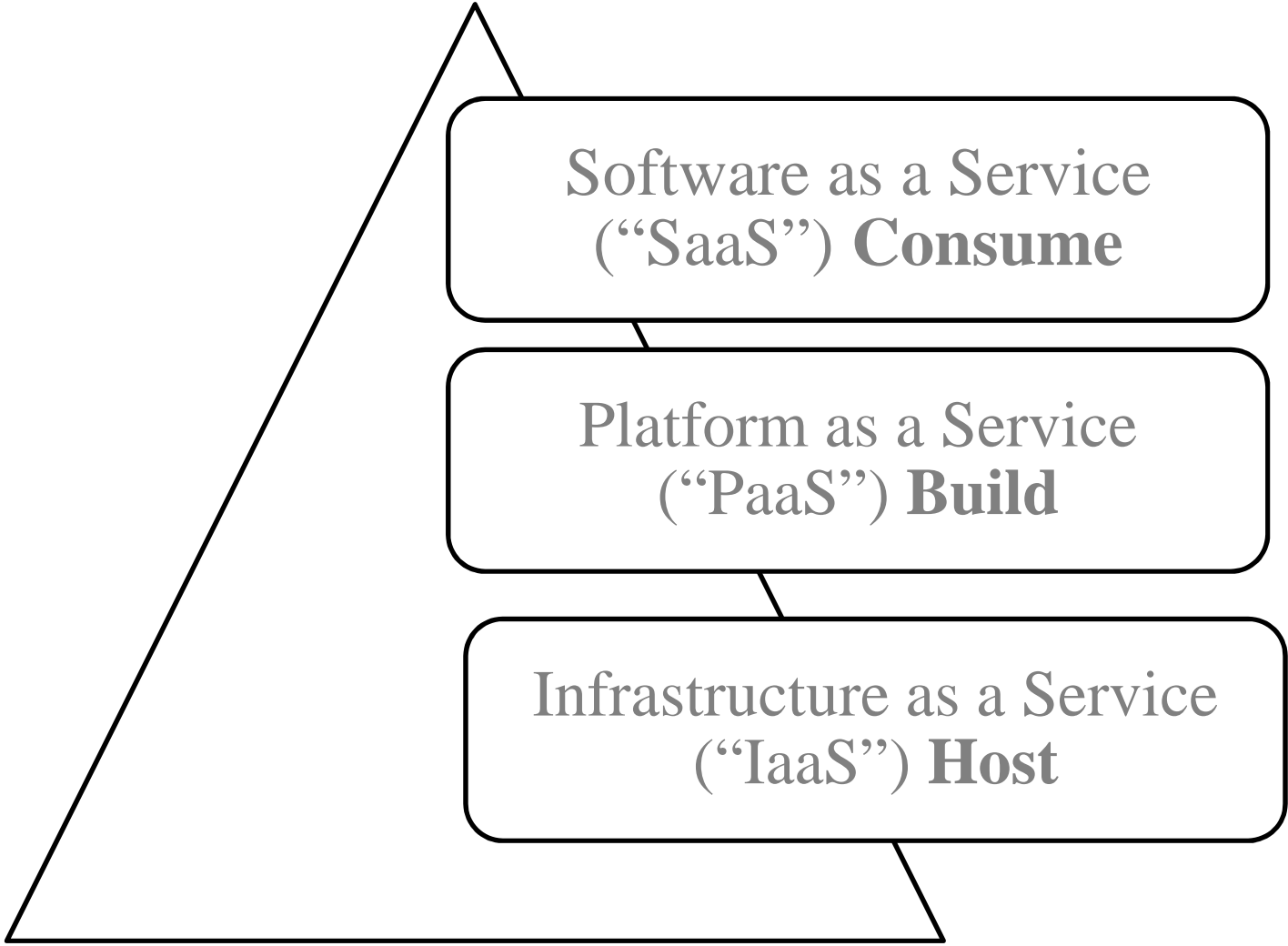
Cloud Computing

- ▼ **Public, private or hybrid Cloud computing**

- ▼ **Assess the security platform that is right for your business.**

- ▼ **Cloud Computing Categories**

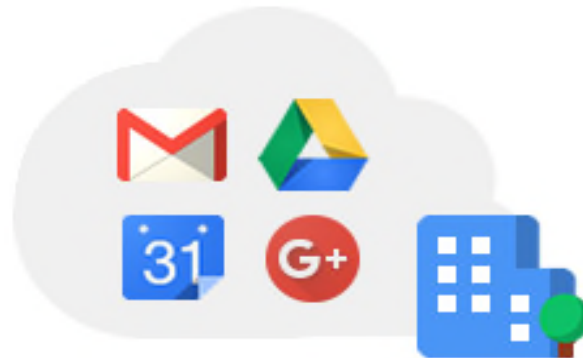
- ▼ **SaaS is a desktop application designed for end-users.**
- ▼ **PaaS provides a platform to develop, run and manage applications.**
- ▼ **IaaS is a virtual data center in the cloud that has access to many of the same technologies and resource capabilities of a traditional data center.**



Software as a Service
("SaaS") **Consume**

Platform as a Service
("PaaS") **Build**

Infrastructure as a Service
("IaaS") **Host**



Mail, Calendar, Drive, Docs,
and so much more

Google Apps is a cloud-based productivity
suite for your business that helps you get
work done from anywhere on any device.



APP ENGINE

A powerful platform to build web and mobile apps that scale automatically



Compute Engine

Run large-scale workloads on virtual machines hosted on Google's infrastructure. Choose a VM that fits your needs and gain the performance of Google's worldwide fiber network.

Cloud Recordkeeping

- ▼ **Cloud applications may introduce additional cyber risk because of the elevated access and privilege levels the application is given.**

- ▼ **Security Concerns**
 - ▼ **How will your stored data be handled?**
 - ▼ **Review privacy and cybersecurity policies**
 - ▼ **Information security requirements**
 - ▼ **Has the vendor had any breaches in the past?**
 - ▼ **What is the breach notification procedure?**

- ▼ **Ongoing monitoring**
 - ▼ **Reliability and access to stored information**

Email Surveillance

- ▼ **Written communications subject to recordkeeping requirements**
 - ▼ It may be difficult to archive and monitor certain activities, like text messages and personal email accounts, advisers may want to consider whether it should prohibit employees from using certain devices for business purposes.
- ▼ **Quality of Archive**
- ▼ **Monitor to detect risks, prevent and correct violations of their compliance programs**
 - ▼ Code of Ethics, advertising restrictions, cyber threats and possible client complaints
- ▼ **Run-key word searches periodically as well as flag certain terms or phrases**
 - ▼ “guaranteed performance,” “superior,” or “complaint”
- ▼ **Keep records of ongoing reviews and surveillance**

Disaster Recovery Plans

- ▼ **Rule 206(4)-7** requires each adviser to adopt and implement written policies and procedures reasonably designed to prevent the adviser from violating the federal securities laws. A disaster recover plan should be included in such policies and procedures.

- ▼ **Rule 204-2** includes a requirement that advisers maintain electronic storage media in a way that would reasonably safeguard such media from loss, alteration, or destruction.

Disaster Recovery Plan Considerations

- ▼ Address specific anticipated events
 - ▼ Cyber-attacks, electrical failure or loss of other utility services, like cable phones
- ▼ Pre-arrange relocation plans and lodging for key staff
- ▼ Evaluate disaster recover plans of service providers and maintain up to date contact information for such providers
- ▼ Data back up and recovery procedures
 - ▼ Remote servers, laptop computers, Internet access and online trading platforms?
 - ▼ Will someone have to physically retrieve the server from the firm's original office space in the days/weeks following the disaster?
- ▼ Client communications before, during and after business interruptions
- ▼ Insurance
- ▼ Ongoing reviews and testing of policies and procedures

FUND FORMATION & INVESTMENT MANAGEMENT

A SIMPLE SOLUTION TO A COMPLICATED SET OF ISSUES.

MAYNARDCOOPER.COM

Representing investment managers, consultants and fund sponsors on ▼
Structuring and forming private investment funds ▼ Other collective vehicles
▼ Preparation of offering memoranda and other fund documents ▼ Investment
adviser registration and exemptions ▼ CFTC registration and compliance ▼
Tax and ERISA matters ▼ Compliance policies and procedures ▼ Performance
Reporting ▼ Mock audits of SEC and state registered investment advisers

MAYNARD
COOPER GALE



Clark Goodwin

Greg Curran

Jessica McKinney

Wes Brinkley

Chris Harmon

Beth Beube

Hardwick Walthall

No representation is made that the quality of legal services to be performed is greater than the quality of legal services performed by other lawyers.