“Legal Issues of Forensics in the Cloud”

OWASP

The Open Web Application Security Project

About Me

- Owner, Titan Info Security Group, LLC

  "A Risk Management and Cyber Security Law Firm"

- Partner, OnlineIntell, LLC

  "Protecting online brands and reputation while providing corporate intelligence and Active Defense"

- Want to know more? Just ask.

OWASP
The Open Web Application Security Project

- Breach!

Some or all data in the cloud?

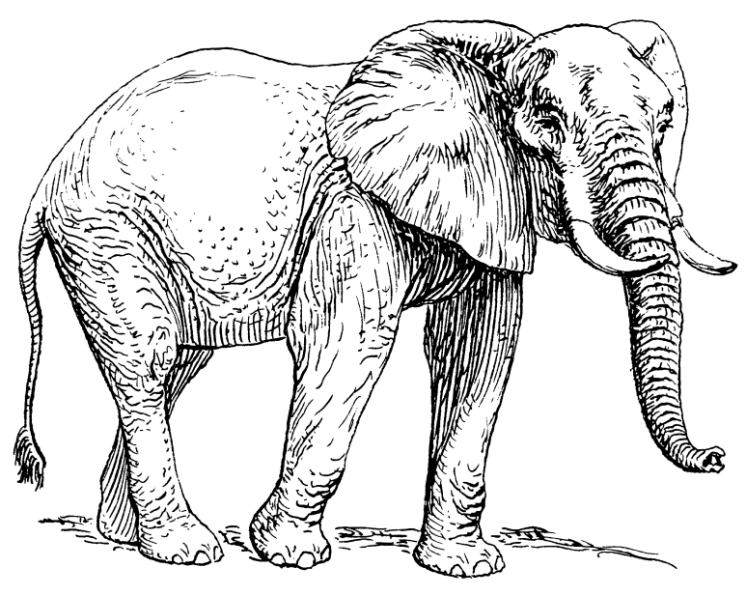
Forensic Investigation

Legal Issues

Perspective

OWASP
The Open Web Application Security Project

1. **You are a forensic examiner**



Or

2. **The Cloud customer**

(suffered an incident and need to conduct forensics)

Definition

OWASP
The Open Web Application Security Project

Computer or Digital Forensics

- Specialized practice of investigating computer media;
- for the purpose of discovering and analyzing available, deleted, or hidden information;
- that may serve as useful evidence in legal or other matters.

What is the Cloud?

OWASP
The Open Web Application Security Project

Characteristics:

1. On-demand Self-service
2. Rapid Elasticity
3. Location Independence
4. Data Replication

What is the Cloud?

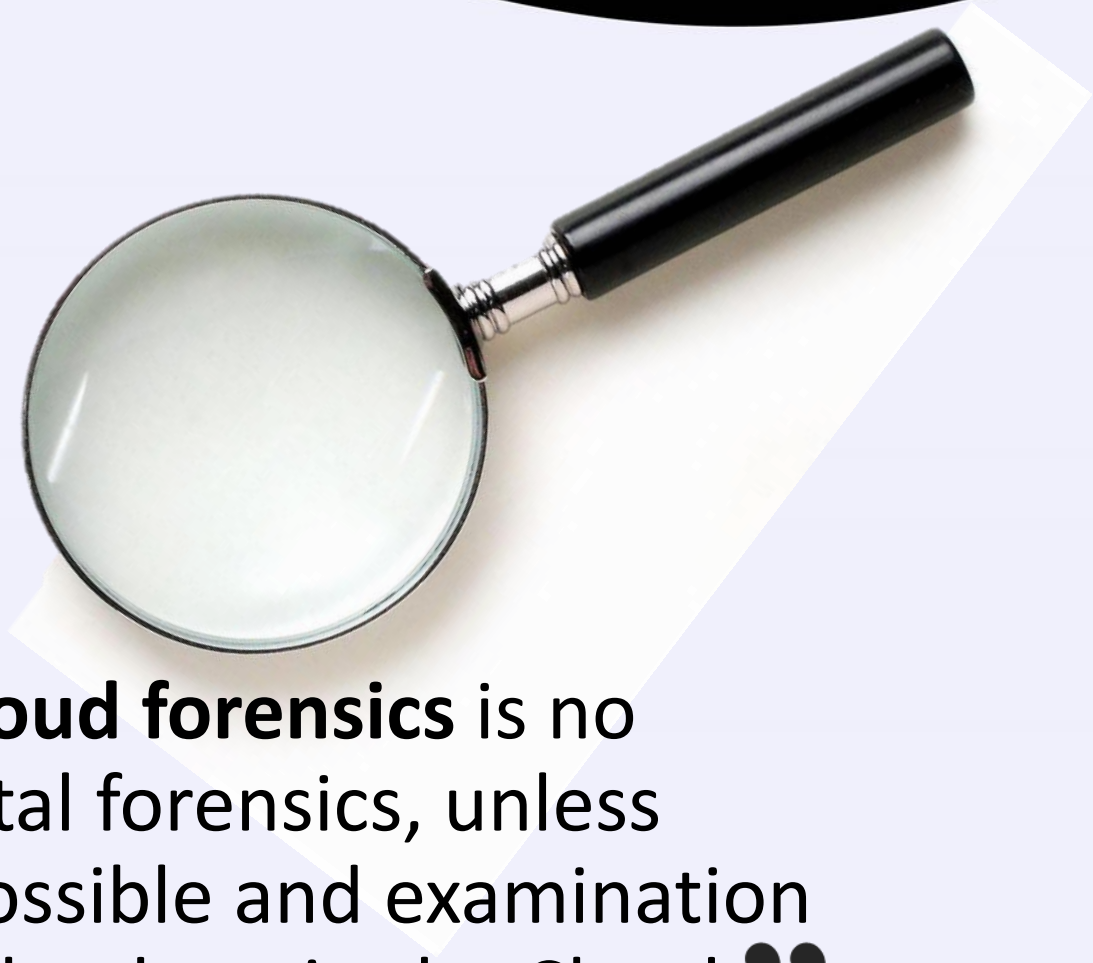
OWASP
The Open Web Application Security Project

- Service Delivery
  - Infrastructure
  - Platform
  - Software
- Customer Billed
- Advertiser Funded

Forensic Process

OWASP
The Open Web Application Security Project

1. Collection
2. Examination
3. Analysis
4. Reporting



"Once collected, **Cloud forensics** is no different than digital forensics, unless collection is not possible and examination and analysis must be done in the Cloud."

Issues

OWASP
The Open Web Application Security Project

1. Where's *My* Data?

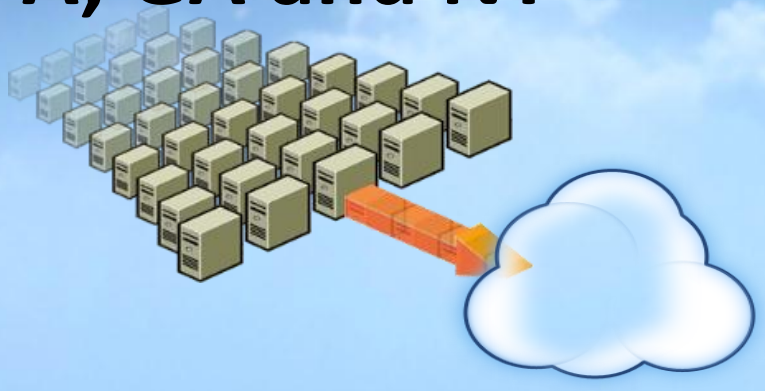
2. Legal Tools
   For compelling disclosure (e.g. subpoena)

3. Breach Strategy
   Pre & Post

Example Scenario

OWASP
The Open Web Application Security Project

- You/company/data owner located in California
- Cloud Provider incorporated in Maryland
- Cloud servers in PA, GA and NY
- Scattered Data

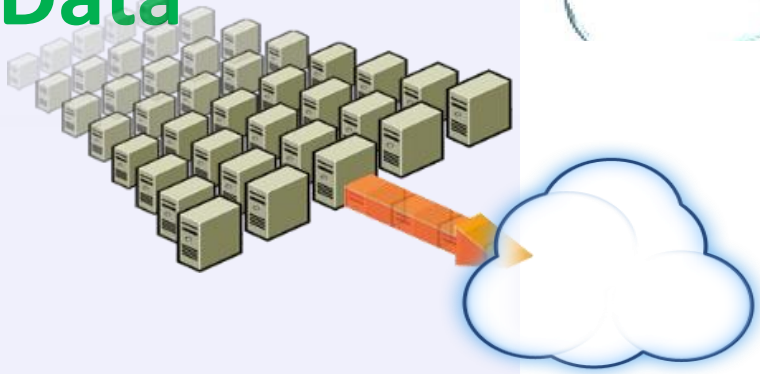


Technical Dilemmas

OWASP
The Open Web Application Security Project

- Can you seize a cloud?
- Do you have to seize it?

Scattered Data

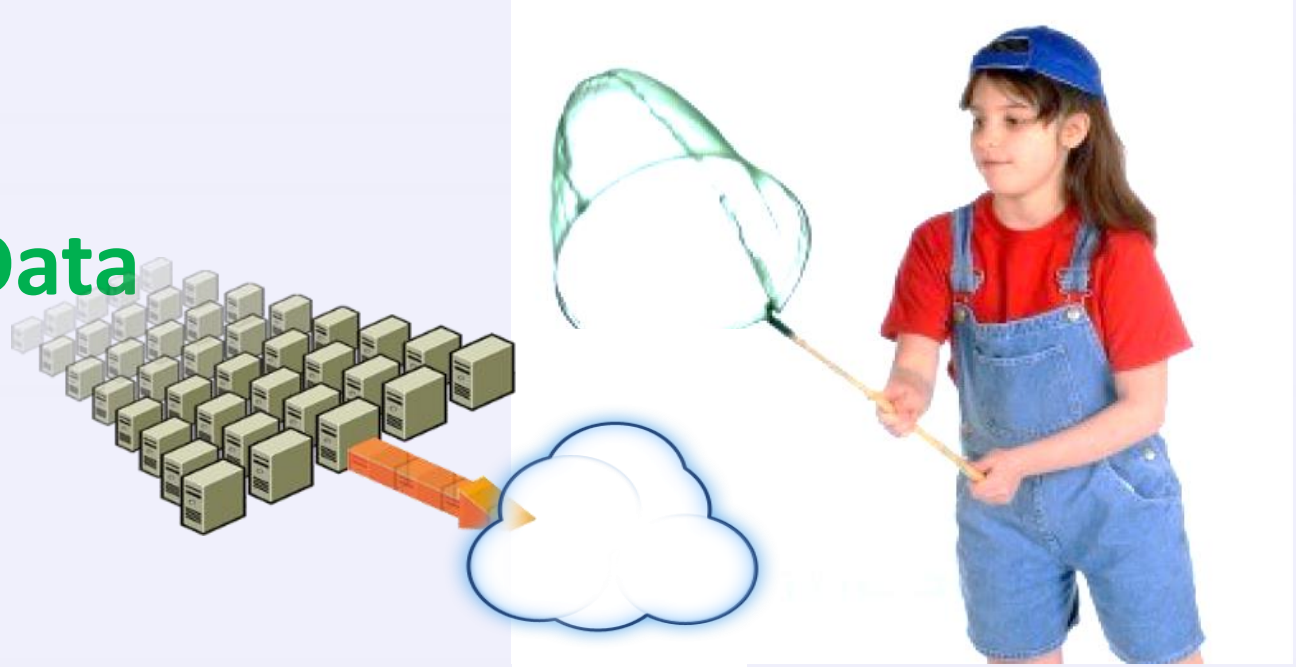


Technical Dilemmas

OWASP
The Open Web Application Security Project

- How much should be collected?
- What methods are available to collect it?

Scattered Data



Legal Issues

Legal Issues

OWASP
The Open Web Application Security Project

- Can you get access to your data?
- Will provider collect data for you?
- Who exactly has access to your data?
- What will provider collect?

Legal Issues

OWASP
The Open Web Application Security Project

- Why are you collecting/gathering data?
- Can you determine goal(s) upfront?

(e.g. identify threat, prosecute attacker, calculate integrity loss, calculate confidentiality loss, etc.)

Know Your Expected End-State

This will guide how meticulous you need to be.

When in doubt assume you are going to court!

Legal Issues

OWASP
The Open Web Application Security Project

Location

- Jurisdiction: which applies?
- Law: Maryland

Legal Issues

OWASP
The Open Web Application Security Project

Ownership

Legal Issues

OWASP
The Open Web Application Security Project

0wnership after transfer to Cloud

- Who owns?
- Who controls?
- Do you really control your data? (Content v. meta data)

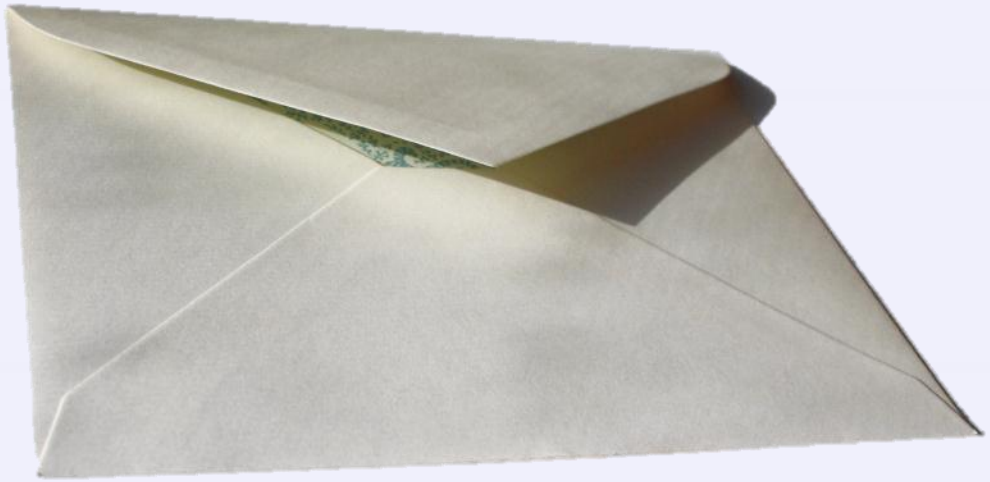
- SLA, SLA, SLA

- Taking & Seizing or Viewing & Copying?
- No deprivation of property

Legal Issues

Discovery Issues/Litigation Hold/Subpoenas

- Where do you send the subpoena?
- Does Cloud provider act as Agent of your data?
- Do you have proper authority from data owner to collect data?

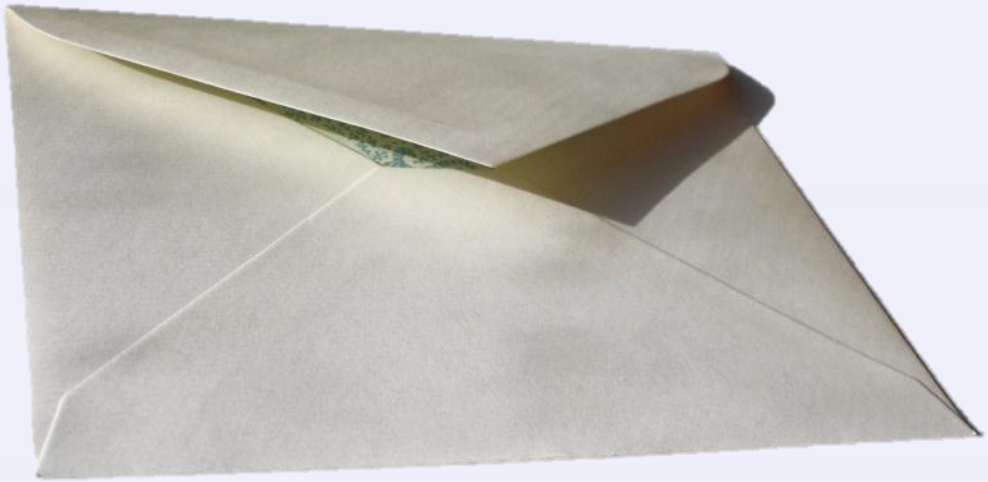


Legal Issues

OWASP
The Open Web Application Security Project

Litigation Hold

- Do first – Protect the Information
- Send Preservation Letter



Legal / Policy Issues

OWASP
The Open Web Application Security Project

Discovery / Subpoenas

- Rule 26 of the Fed. Rules of Civil Procedure
- Rule 34(a) FRCP

Legal / Policy Issues

Subpoenas

- Rule 45 of the Fed. Rules of Civil Procedure
- Subpoena service permitted in 3 instances
  1. Within the jurisdiction of the court that issues it;
  2. Within 100 miles of the place specified for trial, production, or inspection; and,
  3. Within the state of the trial, production, or inspection.

Legal / Policy Issues

OWASP
The Open Web Application Security Project

Strategy

- Develop processes
- Ensure policies and procedures in place
- Understand infrastructure of cloud provider
- Know where your data is at all times
- Legal documents in place to ensure necessary physical and legal control over your data
- *Zubulake*

Legal / Policy Issues

OWASP
The Open Web Application Security Project

Example Providers & SLAs

Windows Azure™

amazon web services™

rackspace®

Dropbox

Legal / Policy Issues

Trial = Who can convince jury or judge their story is the ***truth***

- A digital forensics plan is no different than plan and attempt to prevent a breach
- Put in place policies, procedures and processes

Two Rules (#2 relies on #1)

1. Show a process existed and was followed;
2. Show Integrity of data is sound

Legal / Policy Issues

OWASP
The Open Web Application Security Project

- Transactional metadata: data automatically generated by the computer or program in the normal course of use; may authenticate under FRE 901(b)(9)
- Embedded substantial data: data input into the computer or program – FRE 801(a), hearsay
- Show/describe a process or system used to produce a result and that it is accurate
- Forensic examiner may testify to the process and prove its accuracy (expert witness)

Legal / Policy Issue Conclusions

1. Customer must be provided service, access, and techniques by provider

2. Trust boundaries, responsibilities, and roles between customer and provider must be clearly defined during forensic investigation

3. Multi-jurisdictional forensic investigations, and multi-tenant environments, must address regulations including data confidentiality and privacy laws

Legal / Policy Issue Conclusions

Minimum 12 questions to answer:

1. Does breached company have a contract with cloud provider and what does it say?
2. Where is data right now?
3. What type of data is it?
4. What laws apply to data?

Legal / Policy Issue Conclusions

OWASP
The Open Web Application Security Project

5. Is metadata needed and is it accessible?
6. How was data safeguarded and how compromised?
7. Who had/has access to the data?
8. Who owns data, company or cloud provider; check the contract?

Legal / Policy Issue Conclusions

OWASP
The Open Web Application Security Project

9. Backup of the data and how often?
10. Is data on sole server or many?
11. Is company data only data on server(s) in question?
12. Is there a BYOD policy?

BYOD

OWASP
The Open Web Application Security Project

- What if your org. has allowed or implemented BYOD?
- How do you get the info off the user's device?
- What legal issues:
  - Privacy
  - Is there a BYOD and privacy policy?
  - What does BYOD and Privacy policy say?
  - What if you don't have one?

Thank You

OWASP
The Open Web Application Security Project

Proactive effort and pre-planning are key!

"By failing to prepare you are preparing to fail"

– Benjamin Franklin

OWASP
The Open Web Application Security Project

David Willson
Attorney at Law
CISSP, Security +

Titan Info Security Group, LLC
(www.titaninfosecuritygroup.com)
&
OnlineIntell, LLC
(www.onlineintell.com)