With Great Power Comes Great Responsibility

The Challenge of Maintaining Security in the Cloud

October 6, 2020
Legal Disclaimer

Although the information provided by Clearwater Compliance may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

All materials contained within this document are protected by United States copyright law and may not be reproduced, distributed, transmitted, displayed, published, or broadcast without the prior, express written permission of Clearwater Compliance LLC. You may not alter or remove any copyright or other notice from copies of this content.

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Compliance LLC.
Introduction to Clearwater

- Founded in Nashville in 2009, colleagues in 20+ states, growing rapidly
- Portfolio company of Altaris Capital Partners, a healthcare PE firm with $4.8B under management
- Leading provider of cyber risk management and HIPAA compliance software and solutions for healthcare
- Approximately 400 customers, including 68 IDNs, many with multi-year enterprise programs
- 100% success rate when deliverables submitted to the Office For Civil Rights (OCR)
Webinar Logistics

✓ Slide materials – Link will be in the chat box
✓ All attendees are in “Listen Only Mode”
✓ Please ask content related questions in “Q&A”
✓ In the event of technical issues, check “Chat”
✓ Please complete the Exit Survey when you leave the webinar
✓ Recorded version, final slides, & Certificate of Attendance will be shared with you within 48 hours
Today’s Presenter

Jon Moore, MS, JD, HCISPP
Chief Risk Officer & SVP, Consulting Services

- 25+ Years Executive Leadership, Technology Consulting and Law
- 14+ Years Data Privacy & Security
- 10+ Years Healthcare
- Former PwC Federal Healthcare Leadership Team
- Former IT Operational Leader PwC Federal Practice
- BA Economics Haverford College, MS E-Commerce Carnegie Mellon University, JD Dickinson Law Penn State University, HCISPP
- Speaker and Published Author on Security, Privacy, IT Strategy and Impact of Emerging Technologies
Agenda

- Buckets of Trouble
- Cloud Defined
- Healthcare in the Cloud
- 7 Specific Concerns
- Recommendations
- Coming Attractions
- Questions
The Case of the Bucket of Health Records

Researchers contact DataBreach.net to inform of misconfigured Amazon S3 Bucket with 61K Medical Records.

DataBreach.net and Researchers contract BioTel and SplashRx as potential owners of the Bucket.

August 5, 2020.
Researchers contact DataBreach.net again reach out to BioTel and SplashRx and again get no response.

August 8, 2020.
Researchers contact Amazon Abuse team to notify of Bucket and ask notify owners.

August 9, 2020.
Bucket locked down.

October 6, 2020.
No evidence of either entity reporting this as a breach or of any other entity reporting this incident.
A Pattern

- 2017, records on 150K patients found by researchers in unsecure AWS S3 bucket.

- Two occasions in 2018 MedCall neglected to secure ePHI in AWS S3 storage buckets.

- Aug 2018. 90K records exposed due to misconfigured AWS S3 bucket.

- Patient Home Monitoring Corp
- MedCall
- Sunshine Behavioral Health
Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. - NIST
Definitional Model

- Broad Network Access
- Rapid Elasticity
- Measured Service
- On-Demand Self-Service

Resource Pooling

- SaaS (Software as a Service)
- PaaS (Platform as a Service)
- IaaS (Infrastructure as a Service)

Public
Private
Hybrid
Community

Service Models

Deployment Models
Shared security model defined at the high level by service model.
Service Models

Cloud Security Alliance – Security Guidance v4
2019 NetWrix Survey of 750 organizations:

- 32% healthcare organizations store all ePHI in cloud
- 74% of healthcare organizations store some ePHI in cloud
- 30% say lack sufficient budget to secure information
- 26% of organizations had cloud security incident in past year

https://www.netwrix.com/2019cloudsecurityreport.html
Benefits of the Cloud

**Scalability**

The cloud offers scalability and flexibility in deploying assets.

**Cost**

Only using what you need and paying for what you use offers cost savings.

**Security?**

Is the cloud more secure? It depends on what cloud we are talking about and what we are comparing it to.
Concern 1 – Storage/Containers/Virtual Machines (VM)

**ISSUE – Insecure Configuration**

Containers/VMs are easy to create and if developers don’t secure them or misconfigure them.

**IMPACT**

Containers and contents are discoverable using tools like Shodan and the contents accessible to the public.

**RECOMMENDATIONS**

1. Maintain current inventory of assets
2. Implement and enforce configuration management policies and procedures.
5. Test regularly and use tools like Shodan to see what others see.
Concern 2 – Multi-Factor Authentication

**ISSUE – Identity and Access Control**

With single factor authentication if credentials are compromised and attacker may gain access to all resources to which the user has access.

**IMPACT**

Getting access to a user’s credentials, particularly recently with phishing attacks may lead to exfiltration of data, ransomware and other malicious acts.

**RECOMMENDATIONS**

1. Determine your goals for MFA.
2. Determine the best solution to meet your goals (Every time, certain situations, risk based).
3. Implement the solution.
Concern 3 – Keeping Secrets Secret

**ISSUE – Managing Secrets, Keys, Certificates**

Keys, Secrets, Certificates are not managed and secured and may be encoded in software.

**IMPACT**

If an attacker gains access to the secret or key, he/she has access to everything it unlocks.

**RECOMMENDATIONS**

1. Find and remove any hard-coded keys
2. Implement policy and procedures to prevent hard coding.
3. Change hard coded keys.
4. Implement secure key management solution. (Secrets Manager, Key Vault)
5. Manage secrets on an ongoing basis.
6. Limit access to root
Concern 4 – Encryption

**ISSUE – Encrypting Data**

Data at rest and/or in motion is not encrypted.

**IMPACT**

If an intruder gains access to a VM or the network and the data is not encrypted, he will be able to read that data.

**RECOMMENDATIONS**

1. Apply disk encryption to VMs
2. Secure access from on prem to cloud (VPN)
Concern 5 - Web Application Firewall

ISSUE – Web Attacks

Web applications often have flaws in their software like SQL injection and cross site scripting that when exploited allow an attacker to gain access to the application and its data.

IMPACT

If an intruder gains access to an application, he likely also has access to any data used by the application.

RECOMMENDATIONS

1. Develop requirements.
2. Consider managed or unmanaged.
3. Identify vendors.
4. Evaluate vendors.
5. Select vendor.
## Concern 6 - Logging

<table>
<thead>
<tr>
<th>ISSUE – Lack of Logs or Log Review</th>
<th>RECOMMENDATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not keeping or reviewing logs.</td>
<td>1. Turn on event logging</td>
</tr>
<tr>
<td></td>
<td>2. Establish policy and procedures</td>
</tr>
<tr>
<td></td>
<td>3. Regularly review logs</td>
</tr>
<tr>
<td></td>
<td>4. Consider investment in a SIEM</td>
</tr>
</tbody>
</table>

### IMPACT

Failure to review logs may result in a failure to identify an intrusion or other malicious activity resulting in an ongoing breach and data exfiltration.
## Concern 7 – Patching/Software Updates

### ISSUE – Unpatched, Deprecated, Unsupported Software

Software is often released with vulnerabilities. As the vulnerabilities are identified companies created patches for the vulnerabilities. If not applied, the software remains vulnerable to attack..

### IMPACT

Failing to regularly patch systems results in an ever-expanding list of technical vulnerabilities. The longer a vulnerability goes unpatched the more likely an attacker will exploit it.

### RECOMMENDATIONS

1. Create and maintain inventory of software.
2. Prioritize systems/software.
3. Develop and implement patch management policies and procedures.
5. Test before applying patch.
6. Apply compensating controls until patches applied.
7. Apply patch as soon as possible.
General Recommendations

1. Understand your shared security responsibilities
2. Understand environment
3. Classify information
4. Implement baseline controls (NIST, CSA, CIS, FedRAMP)
5. Perform Risk Management
6. Test Controls
7. Monitor Systems
References


https://services.google.com/fh/files/misc/google-cloud-security-foundations-guide.pdf

https://cloudsecurityalliance.org/artifacts/security-guidance-v4/
Upcoming Clearwater Web Events...

**OCR-QUALITY® RISK ANALYSIS WORKING LAB**
Interactive.
Hands-on.
Five-weeks.
Every Wednesday.
1 hour Sessions.
Starting October 7.

Get a closer look at how Clearwater's Risk Analysis software IRM|Analysis® can help you minimize cyber risk exposures and meet compliance requirements.

**A PATIENT SAFETY - CYBER RISK DISCUSSION with**
Dr. Benoit Desjardins
Penn Medicine
&
Bob Chaput,
Clearwater

**Web Event**
Thursday, Oct 8 | 11am CT

**The Rise of Telehealth: Planning for the Future**
MIKAELA LEWIS, MSHCPM
Consultant, Clearwater
TRAPPER BROWN, CASP
Consultant, Clearwater

**WEBINAR**
Thursday, October 15
11am - 12pm CT

**IRM|Analysis®**
ENTERPRISE CYBER RISK MANAGEMENT SOFTWARE

**LIVE DEMONSTRATION**
Tuesday, Oct 27 @ 11am CT

Learn more and register for these webinars at [https://clearwatercompliance.com/upcoming-educational-events/](https://clearwatercompliance.com/upcoming-educational-events/)
Thank You & Questions

Jon Moore
Jon.moore@clearwatercompliance.com

Thank you for taking the time to complete the survey when you leave the session. We value and use your feedback!