Top Threats to Cloud Computing

Sean Heide M.S.c | CCSK
Research Analyst

Agenda

- Purpose of the document
- How threats are identified
- How to utilize the findings
- Deep Dive Document
- Threat Modeling
- Moving into the future

Before We Begin

- 95% of cybersecurity breaches are caused by human error. (Cybint)
- 68% of business leaders feel their cybersecurity risks are increasing. (Accenture)
- On average, only 5% of companies' folders are properly protected. (Varonis)
- Data breaches exposed 36 billion records in the first half of 2020. (RiskBased)

Purpose of Top Threats

Identify the last few years major breaches to raise awareness of threats, risks, and vulnerabilities in the cloud enterprise space.

Provide a means for logical threat analysis that incorporates mitigation techniques

There is no limitation to its use

How Are Threats Identified

- Collaboration of the working group
- Identifying the main security flaws and appropriately categorizing them
- Top Threats Survey report
  - Gives the enterprise a say in what they have seen
  - Brings together the same ideologies and forecasts

How Are Threats Identified

The latest report highlights the *Egregious Eleven* ranked in order of significance per survey results (with applicable previous rankings):

1. Data Breaches (1)
2. Misconfiguration and Inadequate Change Control
3. Lack of Cloud Security Architecture and Strategy
4. Insufficient Identity, Credential, Access and Key Management
5. Account Hijacking (5)
6. Insider Threat (6)
7. Insecure Interfaces and APIs (3)
8. Weak Control Plane
9. Metastructure and Applistructure Failures
10. Limited Cloud Usage Visibility
11. Abuse and Nefarious Use of Cloud Services (10)

Utilize The findings

1. Security Issue: Data Breaches

A data breach is a cybersecurity incident where sensitive, protected or confidential information is released, viewed, stolen or used by an unauthorized individual. A data breach may be the primary objective of a targeted attack or merely the result of human error, application vulnerabilities or inadequate security practices. A data breach involves any kind of information that was not intended for public release, including—but not limited to—personal health information, financial information, personally identifiable information (PII), trade secrets and intellectual property.

HISTORY OF RANKING

Top Threat 1 ⟷ Top Threat 1

SECURITY RESPONSIBILITY

- Customer
- Cloud Service Provider
- Both

ARCHITECTURE

- Appli
- Info
- Meta
- Infra

CLOUD SERVICE MODEL

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

Business Impact

Negative consequences of a data breach may include:

1. Impact to reputation and trust of customers or partners
2. Loss of intellectual property (IP) to competitors, which may impact products release
3. Regulatory implications that may result in monetary loss
4. Brand impact which may cause a market value decrease due to previously listed reasons
5. Legal and contractual liabilities
6. Financial expenses incurred due to incident response and forensics

There are cases of data breaches being undetected until months after the compromise. In such incidents, the implications might not be immediately apparent (e.g., IP theft). For example, the United States Office of Personnel Management (OPM) and Sony Pictures breach both had a dwell time of approximately one year[1].

CSA Security Guidance

Domain 2: Governance and Enterprise Risk Management
Domain 3: Legal Issues, Contracts and Electronic Discovery
Domain 4: Compliance and Audit Management
Domain 5: Information Governance
Domain 6: Management Plane and Business Continuity
Domain 9: Incident Response
Domain 11: Data Security and Encryption
Domain 12: Identity Entitlement and Access Management
Domain 14: Related Technologies

CCM Controls

AIS Application and Interface Security
AIS-01: Application Security
AIS-02: Customer Access Requirements
AIS-03: Data Integrity
AIS-04: Data Security / Integrity

CCC Change Control and Configuration Management
CCC-05: Production Changes

DSI Data Security and Information Lifecycle Management
DSI-01: Classification
DSI-02: Data Inventory / Flows
DSI-03: Ecommerce Transactions
DSI-04: Handling / Labeling / Security Policy
DSI-05: Non-Production Data
DSI-07: Secure Disposal

EKM Encryption and Key Management
EKM-01: Entitlement
EKM-02: Key Generation
EKM-03: Sensitive Data Protection
EKM-04: Storage and Access

GRM Governance and Risk Management
GRM-02: Data Focus Risk Assessments
GRM-06: Policy
GRM-10: Risk Assessments

IAM Identity and Access Management
IAM-01: Audit Tools Access
IAM-04: Policies and Procedures

Utilize The Findings

CCM™ CLOUD CONTROLS MATRIX v4.0.3

Control Domain	Control Title	Control ID	Control Specification	Implementation Guidelines
Audit & Assurance - A&A				
Application & Interface Security	Application Security Metrics	**AIS-03**	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.	Actionable metrics should be defined with consideration to business goals, the criticality of service, security requirements, and compliance obligations. Example technical metrics include: • Count or percentage of vulnerabilities by weakness. • Count or percentage of vulnerabilities by severity. • Count or percentage of vulnerabilities by detection source (design review, code review, SAST, DAST, penetration test, VDP, or bug bounty). • Count or percentage of vulnerabilities by environment detected (pre-production vs. production). • Average time to resolution. • Count exceeding remediation service level objectives (SLOs). Example operational metrics include: • Count or percentage of applications using automated security testing by test type (SAST, DAST, SCA). • Count or percentage of applications have completed penetration testing in the last "n" months. • Count or percentage of development teams or individuals who have completed application security training in the last "n" months. • Count of proactive engagements by development and business teams. • Results from surveys delivered to application security customers, such as business and development teams. Reporting:

The Fun Part- Deep Dive

- Usage spans from architects, engineers, and analysts +
- Combines the Top Threats with a granular look at 9 examples of real-world attacks and breaches
- A means for use in threat comparative analysis, understanding threat vectors, and mitigation techniques

The Fun Part- Deep Dive

cloud security alliance®

Top Threats EE:DD Analysis

'Top Threats' Coverage by Case Study

Top Threats Item #	Capital One	Disney+	Dow Jones	Github	Imperva	Ring	Tesco	Tesla	Zoom
EE 1									
EE 2									
EE 3									
EE 4									
EE 5									
EE 6									
EE 7									
EE 8									
EE 9									
EE 10									
EE 11									

Observations

The nine Deep Dive case studies cover all elements of the Egregious Eleven (EE:DD).

Deep Dive Cont.

Case Study CCM Control Coverage Frequency

CCM Control	Capital One	Disney+	Dow Jones	Github	Imperva	Ring	Tesco	Tesla	Zoom
IAM	3	2	2		1	1	1	1	4
SEF	4	1	1	2		4	1	2	2
TVM	1	1			1	1	1	2	2
HRS	1	1	1				2	1	1
IVS	3	1		2	4			1	1
CCC	1				1	1	1	2	
AAC			2	2		1	1		
GRM	2	1			1				1
STA			2			4	3		
AIS		1			1		1		
DSI	1				1				
EKM					1		1	1	
BCR		1		1					
DCS									
IPY									
MOS									
Total Controls	16	9	8	7	11		12	10	11

Observations

The domains in the chart above are sorted according to how often controls in those domains are relevant as a mitigation control.

Deep Dive Cont.

Capital One

Threat actor	Threat	Vulnerabilities	Technical impacts	Business Impacts	Controls
Internal: Less Experienced Cloud Architects, Less Experienced Solutions Architect.	**EE1** *Data Breach:* Attacker exfiltrated sensitive information from 106M customer accounts.	**EE 2** *Misconfiguration and Inadequate Change Control* - ModSecurity Web Application Firewall allowed Server-Side Request Forgery (SSRF).	**EE9** *Metastructure and Applistructure Failures:* default hypervisor trust allows service discovery and interrogation	**Financial** - $150M Notification (est) - 6.9% Capital One stock price drop - Possible regulatory fines	**Preventive** - DSI-02 - GRM-01 - IAM-02 - IVS-13 - SEF-01
	EE11 *Abuse and Nefarious Use of Cloud Services:* VPN and anonymous network services used to manipulate identity.	**EE4** *Insufficient Identity and Credential Management* - overprovisioned EC2 and S3 roles for WAF and storage.	Over privileged cloud application exposes protected cloud storage and allows access to too much data.	**Operational** - Incident Response - Forensics Analysis - Informing affected parties	**Detective** - CCC-03 - GRM-02 - IAM-13 - IVS-01
External: *EE5 Insider Threat* - Former CSP Trusted Insider with intimate knowledge of AWS operations.	**Complicated Environment** Intimate knowledge requirements for correct implementation and configuration decisions.	**EE8** *Weak Control Plane* - AWS allows meta data interrogation.	PII from 106M consumer credit applications are exfiltrated.	**Compliance** - Sensitive Data Leakage - Class Action Lawsuits - Congressional Inquiry - $80M OCC Fine	**Corrective** - HRS-09 - IAM-07 - IVS-06 - SEF-02 - SEF-03 - SEF-04 - TVM-02
		EE10 *Limited Cloud Usage Visibility* - AWS IMDS v1 vulnerability to SSRF attack was unknown or not addressed.		**Reputational** - Cloud (CSP) Loss of Confidence - Long term stock price	

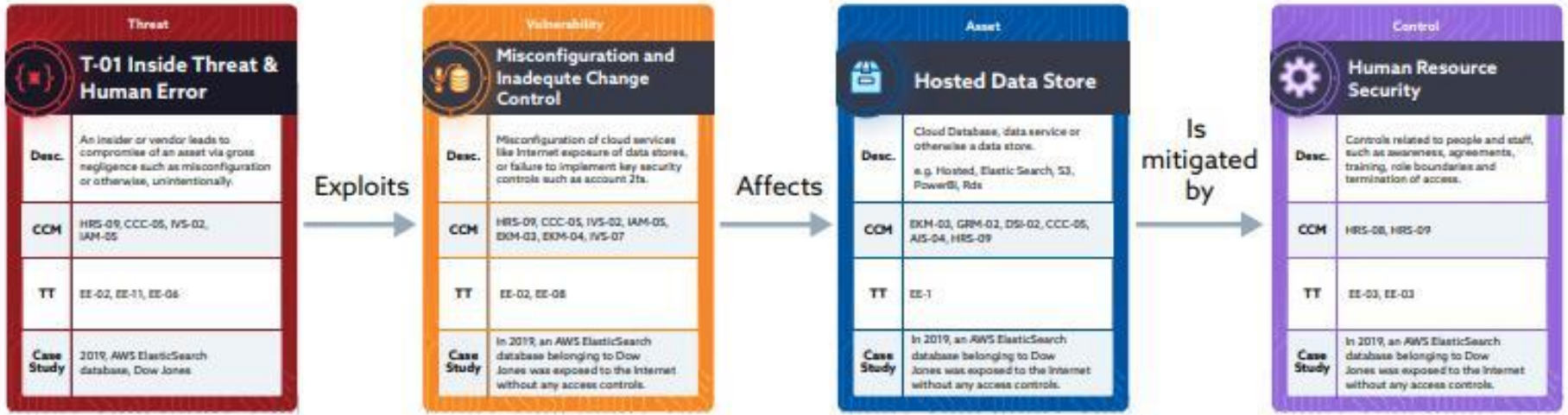
cloud security alliance®

Intro to Threat Modeling

Threat Modeling

- Identify threat modeling security objectives
- Set scope
- Identify and rate threats
- Identify system vulnerabilities
- Prioritize mitigations and controls
- Create a functional call to action for leadership

Threat Modeling



Preparing For The Future

- Threat based modeling
  - Utilizing CSA's Cloud Threat Modeling Template

- Researching new breaches and tactics
  - Log4j
  - SolarWinds

- Create an updated and consistent template that is timely to market

- Tabletop events
  - Seattle Chapter interest?

Join Us!

- https://circle.cloudsecurityalliance.org/

Questions?

sheide@cloudsecurityalliance.org