WEBINAR

aws

HALL RENDER
ADVISORY SERVICES

Holding Health Care Ransom

How to Reduce the Threat

Cory Brennan
Hall Render

Mark Branstetter
Hall Render
Advisory Services

Hector Rodriguez
Amazon Web
Services

Mark Swearingen
Hall Render

HALL
RENDER
KILLIAN HEATH & LYMAN

Introductions

Cory Brennan

Attorney, Advisor

Hall Render & Hall Render Advisory Services

Mark Branstetter

Advisor

Hall Render Advisory Services

Hector Rodriguez

Principal Industry Specialist

Amazon Web Services

Mark Swearingen

Attorney

Hall Render

Agenda

- Overview
- Anatomy of a Ransomware Attack
- Legal Implications
- Operational Impact and Recovery
- Practical and Proactive Approaches to Mitigation

Overview

- Ransomware attacks continue to increase in frequency and severity.
  - Threat actors have adapted their tactics over time.
- Healthcare organizations are popular targets.
  - Rich, valuable and sensitive data
  - Regulatory pressures
- Implications are various and significant:
  - Operational
  - Legal
  - Financial
  - Reputational

Anatomy of a Ransomware Attack

- What is ransomware?
- Types of ransomware
  - Scareware
  - Screen lockers
  - Encrypting ransomware
- Ransomware **typically** infects victim machines in one of three ways:
  - Through phishing emails containing a malicious attachment or link
  - Exploiting known vulnerabilities
  - By viewing an advertisement containing malware (malvertising)

An Expanding Attack Surface

- Health care provides “low hanging fruit”
  - Electronic health records (EHRs)
  - Wireless medical devices
  - Legacy devices
  - Telemedicine and remote work
    - Remote desktop protocols (RDPs) and remote access VPNs
  - Flat networks
  - Third-party security risks in healthcare IT

How Ransomware Has Evolved

- Nature and intent of the typical ransomware attack has evolved over time
  - Ransomware goes mainstream
  - Data leakage extortion
  - More complex encryption techniques
  - Ransomware-as-a-Service

Legal Implications

- A ransomware attack can trigger numerous time-sensitive legal obligations:
  - Notification to individuals
  - Notification to regulators
  - Notification to contractual parties
  - Notification to other potentially impacted parties
  - Notification to insurance carriers
- Delicate balance between remediating the attack, fact gathering, and timely reporting.

Legal Implications

- A ransomware attack can have significant legal impacts:
  - Regulatory investigations and penalties
    - HIPAA; state laws; industry standards (e.g., PCI-DSS)
  - Lawsuits
    - Individual suits and class actions
      - Violation of Privacy
      - Breach of Contract
      - Personal injury/Malpractice
    - Plaintiff or defendant
  - Indemnity/Insurance
    - Address proactively in contracts to the extent possible

Legal Implications

- Keys to the legal analysis of a ransomware attack:
  - Type and amount of information involved
    - Form and location
  - Was data exfiltrated?
  - Nature of access to data:
    - Interactive vs. Programmatic
    - Alteration/deletion
    - Duration of access
  - Attacker's motive
    - Monetization vs. Data theft

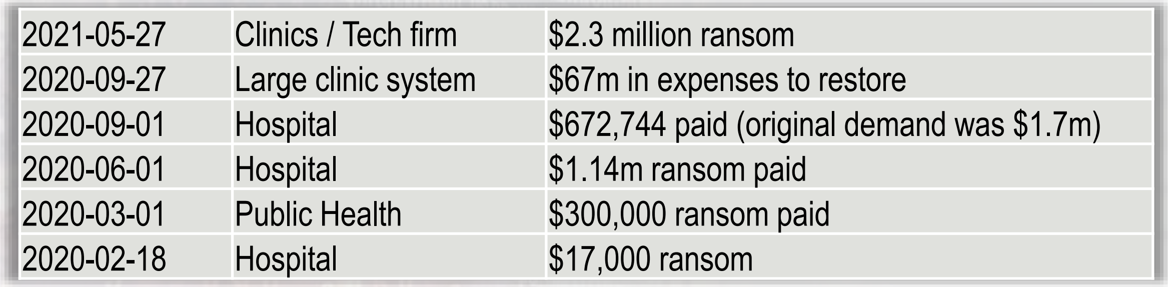
Legal Implications

- Keys to an effective legal response:
  - Early involvement of experienced counsel to manage the incident response
  - A comprehensive and rehearsed plan
  - Timely, thorough and detailed review from an experienced IT forensic firm
    - Attorney-client privilege
  - Complete transparency and cooperation

Big Payouts/Expenses – Event Response

- Event response: Prepare to recover fast (RPO/RTO)
  - Recovery Point Objective: How often do you backup?
  - Recovery Time Objective: How fast can you recover data?
  - Exposure consideration: Will PHI be revealed by bad actors?
    - Is your data encrypted in transit and at rest?
      - Picture a safe inside of a safe…

Ransomware Events



2021-05-27	Clinics / Tech firm	$2.3 million ransom
2020-09-27	Large clinic system	$67m in expenses to restore
2020-09-01	Hospital	$672,744 paid (original demand was $1.7m)
2020-06-01	Hospital	$1.14m ransom paid
2020-03-01	Public Health	$300,000 ransom paid
2020-02-18	Hospital	$17,000 ransom

Healthcare Operational Impact (Cost*)

- Average data breach total cost for healthcare increased from $7.13 million in 2020 to $9.23 million in 2021, a 29.5% increase.
- Ransomware breaches nearly 10% costlier than typical breaches.
- 4 areas included in breach total cost calculation:
  - Detection and escalation
  - Lost business (highest percent 38%)
  - Notification
  - Post breach response
- Cost per record $161 (average across all industries)

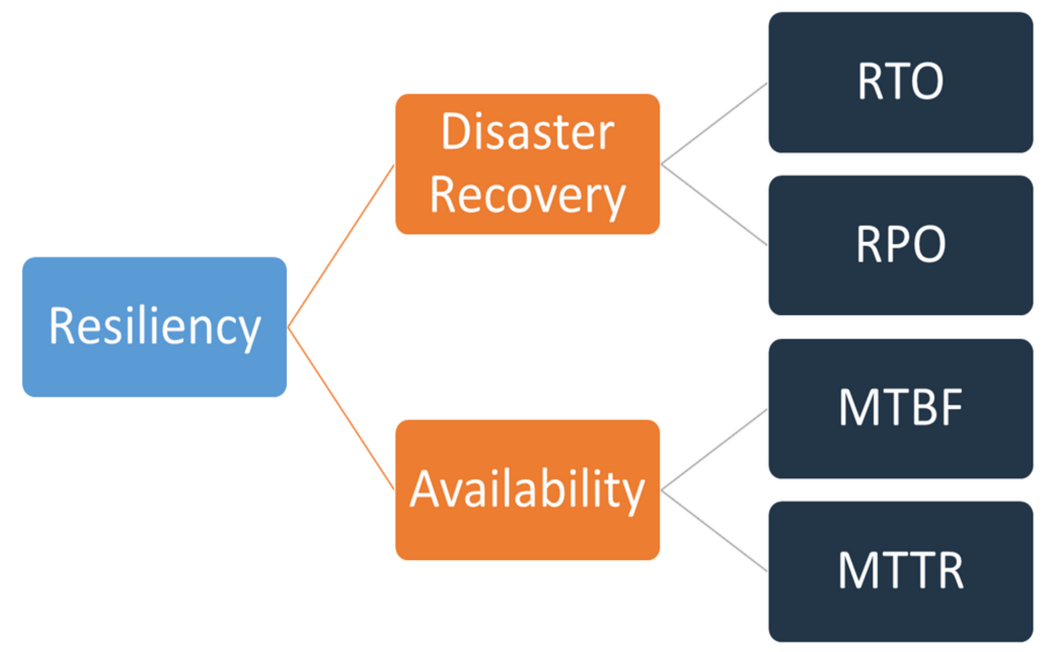
* IBM Cost of a Data Breach Report 2021

Practical & Proactive Approaches to Mitigation

Modernize and Measure your Readiness and Response

- Cybersecurity is everyone’s job – “Job zero”, “Top priority”
- Cybersecurity is a process - must be a strategic process
- Cybersecurity is a shared responsibility
- Strategy should focus on “resiliency” - ability to recover from infrastructure & service disruptions
- Resiliency includes both Disaster Recovery (DR) and Availability
- Intrusion Analysis is critical

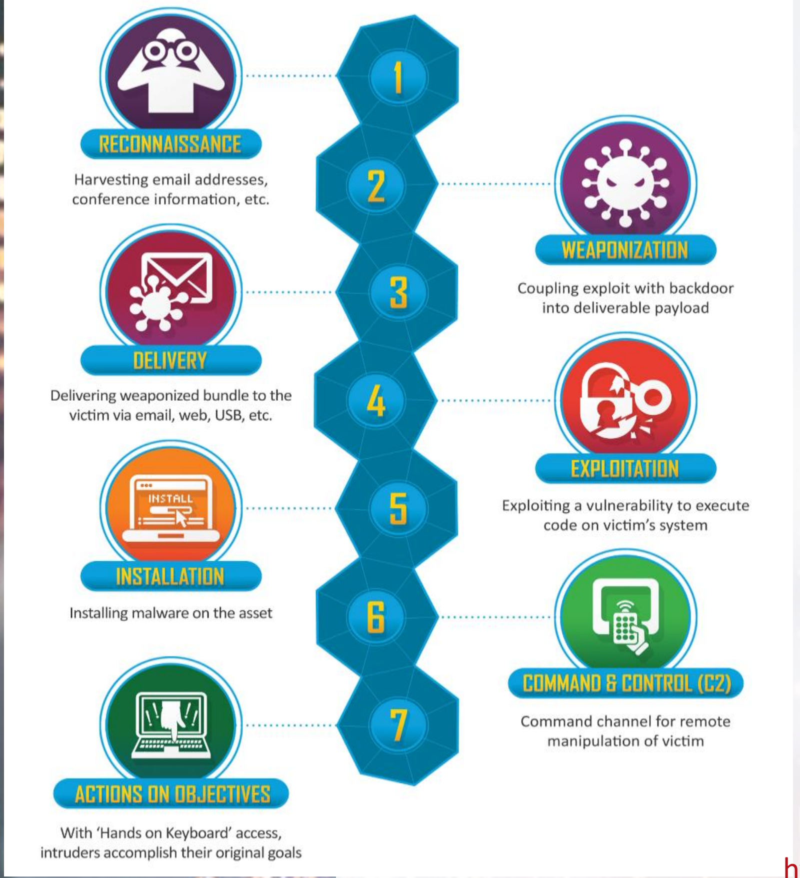
Disaster Recovery & Availability



- DR Focus: disaster events
- Availability Focus: smaller scale disruptions
- DR Objective: business continuity
- Availability Objective: maximize time that a workload is available
- Both should be part of resiliency strategy
- Measures are different

https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-workloads-on-aws.html

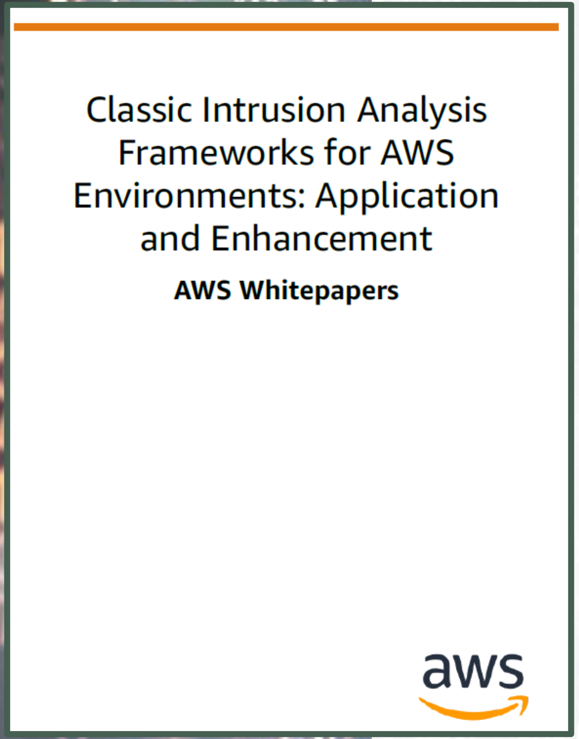
Intrusion Analysis is Critical


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

- Think like an "attacker"
- Process attackers use to conduct an attack can be analyzed as an intrusion kill chain
- Ransomware happens after successful intrusion
- Invest in upfront "courses of action" to detect, deny, disrupt, degrade, deceive, & destroy the process

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

White Paper Now Available



Classic Intrusion Analysis Frameworks for AWS Environments: Application and Enhancement

AWS Whitepapers

Abstract

Today, many Chief Information Security Officers (CISOs) and cybersecurity practitioners are looking for an effective cybersecurity methodology that will help them achieve measurably better security for their organization. One approach that has helped some organizations is to use classic intrusion analysis frameworks to analyze cybersecurity risks and provide methodologies and technologies for responding to attacks.

This paper provides background context on classic intrusion analysis frameworks, and shows how the transition to the cloud undermines some of its key premises, naturally disrupting modern attacker intrusion methods, i.e. “breaking intrusion kill chains”. This paper outlines how to use both the classic intrusion analysis framework and the AWS Cloud to address external threats to your AWS environment’s security.

https://aws.amazon.com/blogs/security/whitepaper-available-classic-intrusion-analysis-frameworks-for-aws-environments/

References & Resources

- The No More Ransom Portal - https://www.nomoreransom.org/en/prevention-advice.html
- Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf
- Defined in 2006 version of JP 3-13, as documented in Mitre, "Characterizing Effects on the Cyber Adversary, A Vocabulary for Analysis and Assessment", - https://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf
- Cloud Adoption Framework, Security Perspective - https://d0.awsstatic.com/whitepapers/AWS_CAF_Security_Perspective.pdf
- AWS Well-Architected framework - https://aws.amazon.com/architecture/well-architected/
- https://aws.amazon.com/security/
- https://aws.amazon.com/compliance/

This presentation is solely for educational purposes and the matters presented herein do not constitute legal advice with respect to your particular situation.

HALL RENDER
ADVISORY SERVICES

For more information on these topics visit hallrender.com.

Cory Brennan | cbrennan@hallrender.com

Mark Branstetter | mbranstetter@hallrenderas.com

Hector Rodriguez | hectormr@amazon.com

Mark Swearingen |mswearingen@hallrender.com