RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking

SESSION ID: CRWD-R04

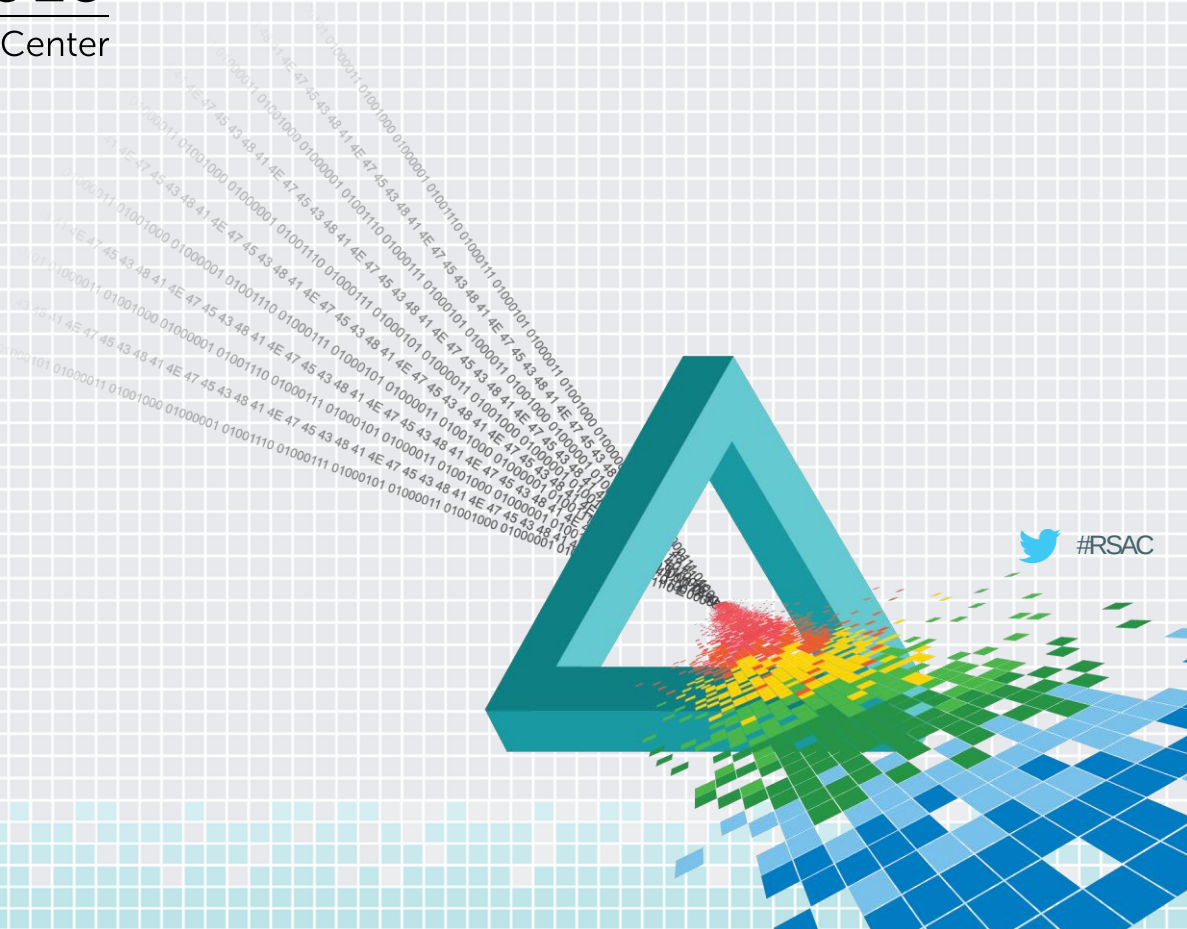
Evolution of Hackers and Reverse Incident Response

Alex Holden

Chief Information Security Officer
Hold Security, LLC
@HoldSecurity

Goal: Typical problem, different perspective

Evolution



Hackers – Learning To Be Different

- Learning new things – survival techniques
  - Technologies
  - Language barriers
  - Geopolitical drivers

Hackers – Learning To Make Money

- Sharing knowledge = Innovation
- Business schemes
- Technology innovations
- Payout

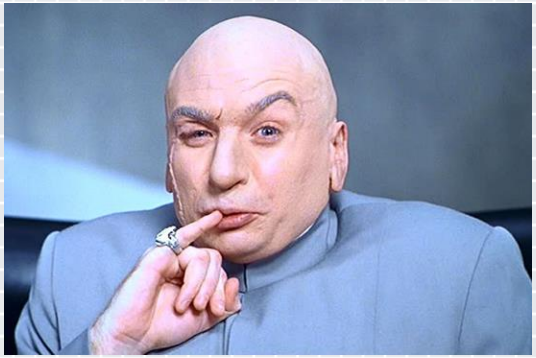
Hackers – Learning To Organize

- Gang life ideology
- Structure
- Turf
- Weaknesses

"I'm fighting a holy war against the West… They drive their Rolls Royces and go home to their million-dollar houses, while people here are struggling. I will never harm my fellow Slavs; but America, Europe, and Australia deserve it."

- aqua (jabberzeus gang)

Modern Actors - Transformation



Modern Actors – Transformation (Take 2)

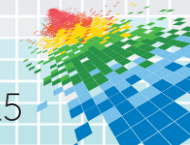
- Не говорит по-английски
- Semi-educated
- Lazy
- Money-hungry
- Addicted to drugs, alcohol, gambling

Modern Actors – Transformation (Cont'd)

- 99% of hackers fail in their careers
- On the run from the law
- On the run from competition
- On the run from street gangs

Black Market – Specialization

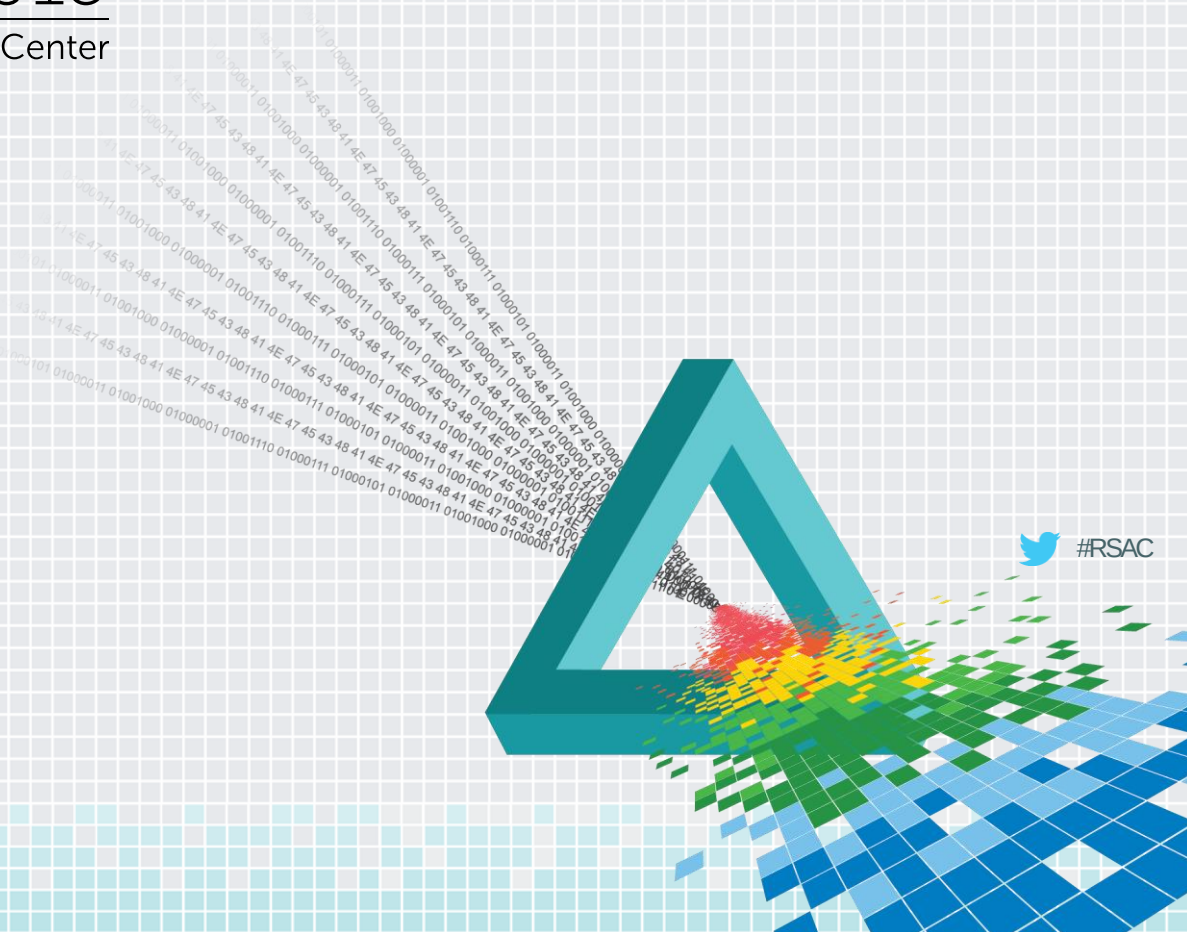
- Break complex processes into small tasks
- Hacker professions
- Marketing
- Community education



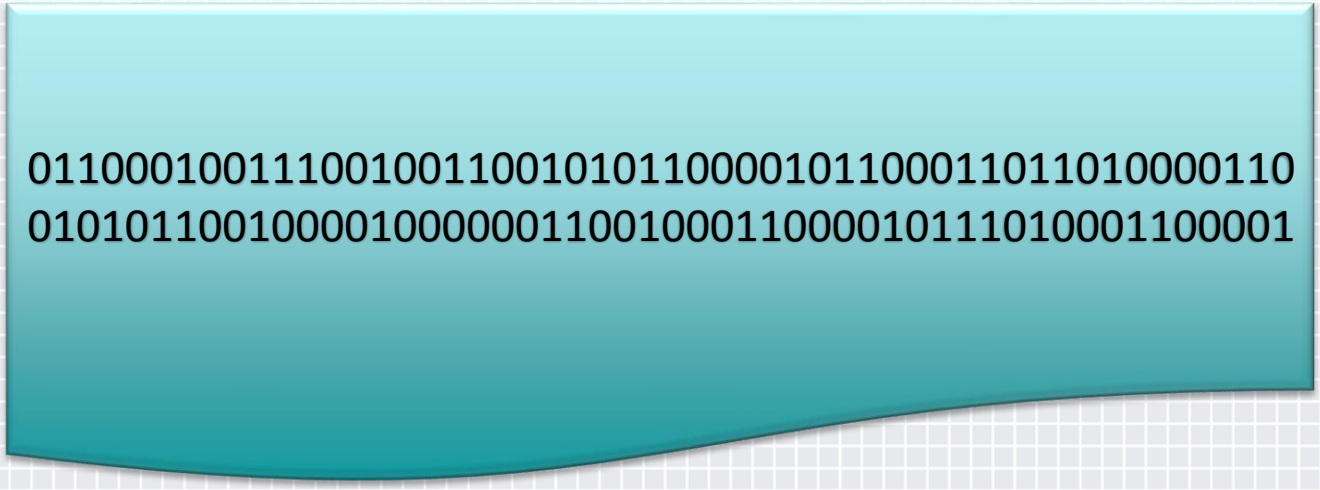
RSAConference2015

San Francisco | April 20-24 | Moscone Center

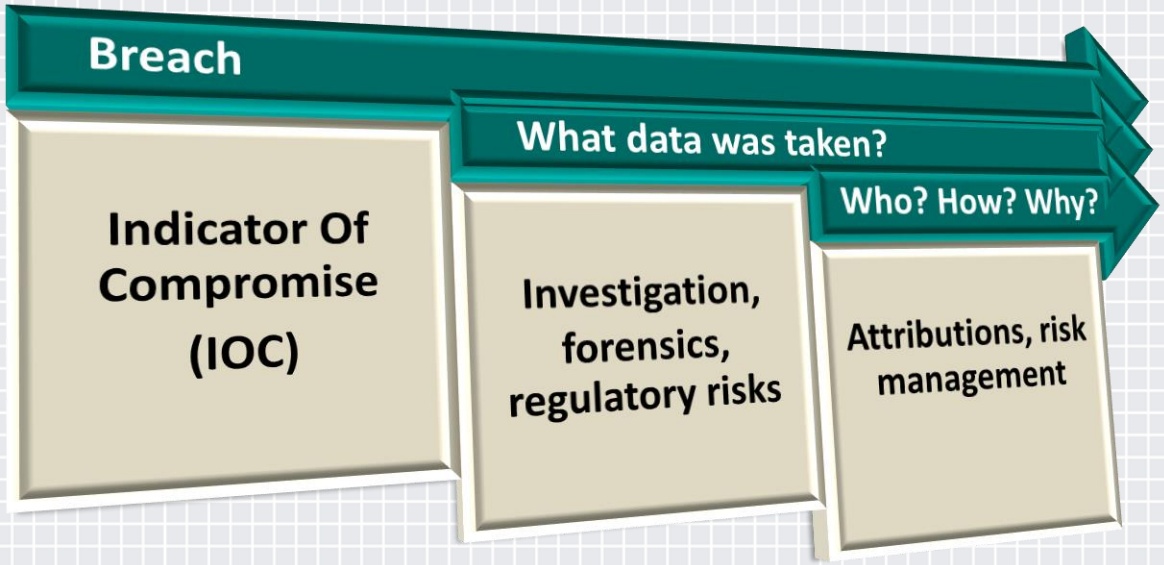
Incidents
Breaches
Opportunities



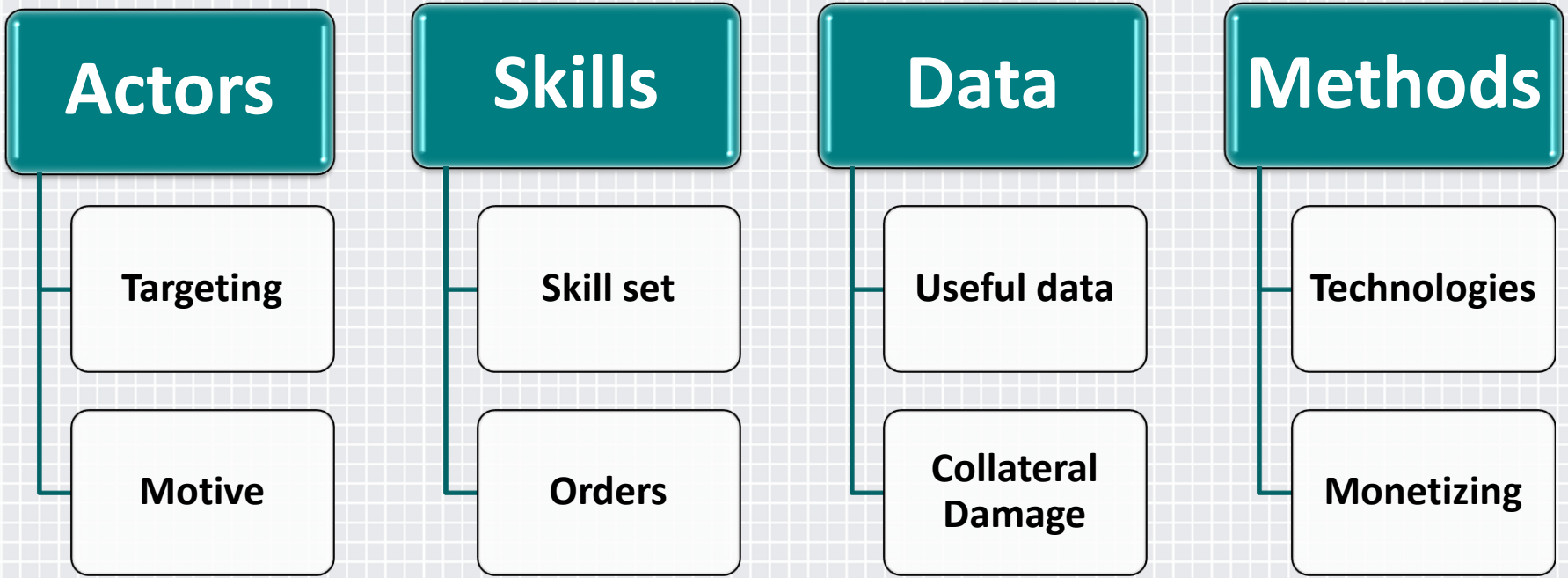
Reverse Incident Response



Incident Response



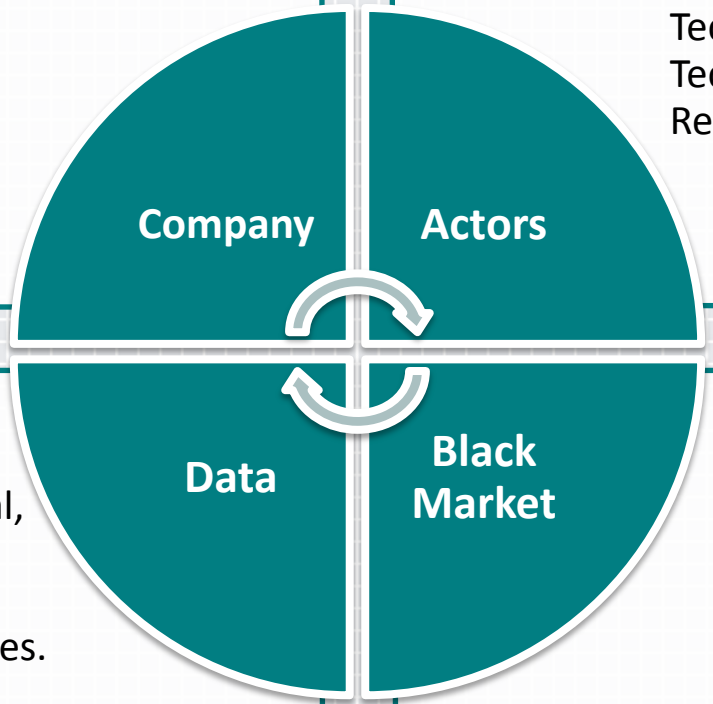
Breach In-The-Making



Incident Components

- IOC, Logs, Evidence, Data, Investigators, Regulators, Lawyers, Victims, Media.

- Motives, Opportunities, Technologies, Techniques, Relationships.

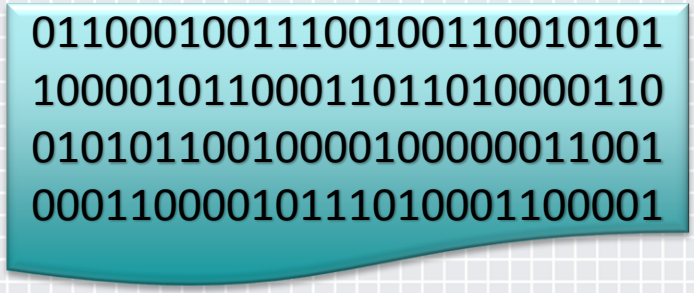


- Credentials, Financial, System, Blackmail, Partners, Vendors, Customers, Employees.

- Orders, Services, Forums, Chats, Debts, Cashing Out, Collateral Damages.

Reverse Incident

- Creating data connections
  - Is it credible?
  - Who has it?
  - Where did it come from?
  - What are the next steps?



Following Actors

- Profile
  - Specialties → Role
  - Acquaintances → Who else has this data
  - Footprint → Success rates
  - Locale → Monetization strategy

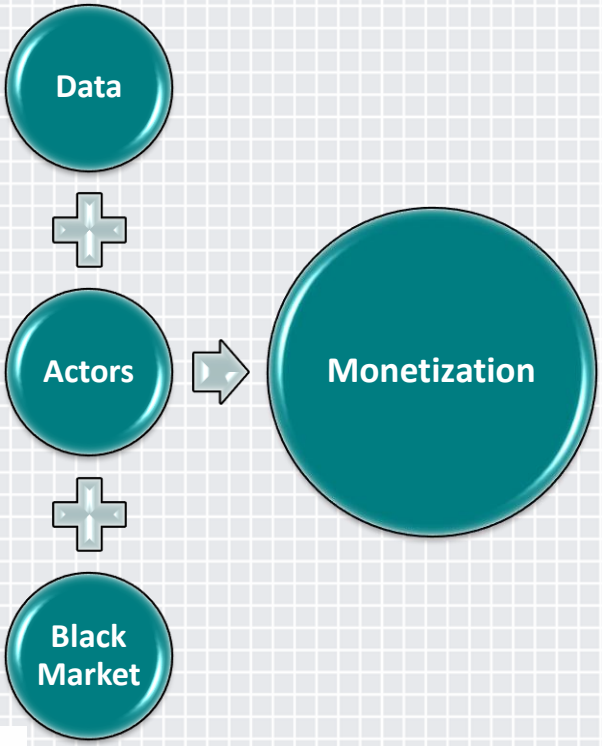
Following Data

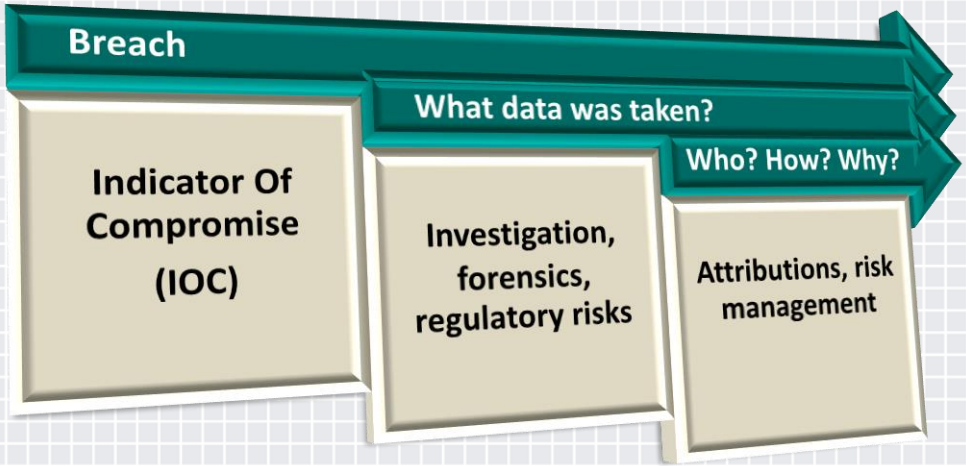
- Data types → Breach scope
- Locations seen → Distribution, intent
- Potential full data size → Victim profile
- Sophistication → Encryption and other defenses
- Primary purpose → Vectors of abuse
- Residual value → Future abuse

Correlations

- Vectors of compromise
- Black market value
- Link in a chain – other actors
- End goal – monetization, blackmail, etc.
- Similar data

Deep Web IOC To Data Breach





Advice - Learning Process

- Know your enemy
- Understand and classify your data
- Don’t assume that your organization is “hacker-proof”
- Get to know your “circle of friends” – vendors/partners/customers

Advice - Honeypots

- Honeypots are not only systems
  - Components
  - Credentials
  - Features

Advise - Quantitative Analysis

- How much of your data is transferred?
- What is normal? What is not?
- Learn to look at statistics

Advice - Look Around

- “Google” for your data, sometimes it is not that “deep” on the web
- Understand your enemies and keep up with current techniques
- Think outside the box

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Thank You!

Alex Holden

aholden@holdsecurity.com