

RSA[®]Conference2015

Singapore | 22-24 July | Marina Bay Sands

SESSION ID: GRM-F03

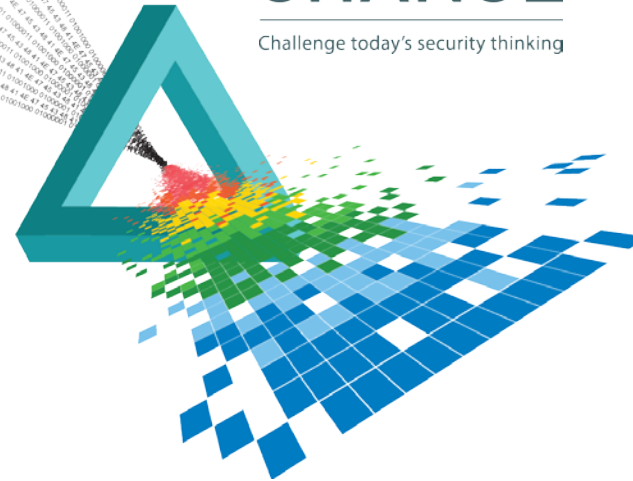
The Enemy You Know

Ted Harrington

Executive Partner
Independent Security Evaluators
@ISEsecurity

CHANGE

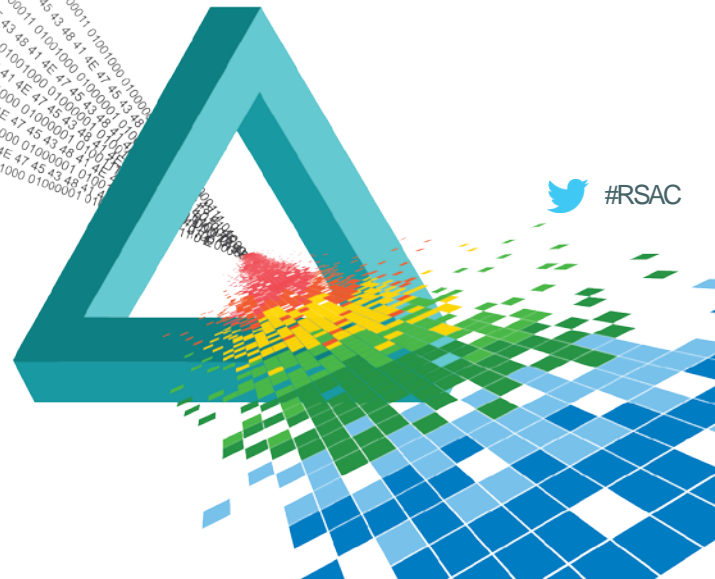
Challenge today's security thinking

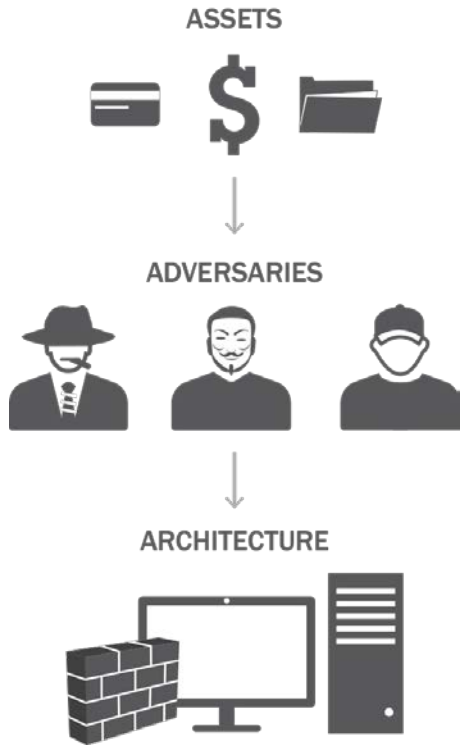


RSA[®]Conference2015

Singapore | 22-24 July | Marina Bay Sands

Why is this important?

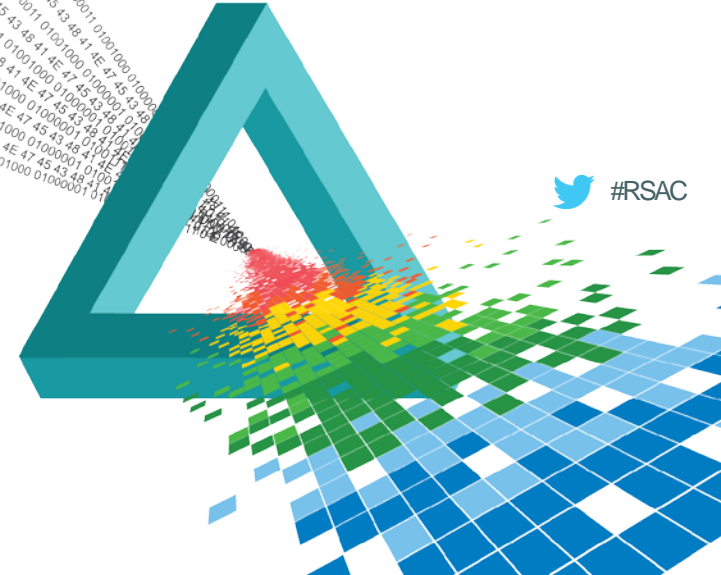




RSA[®]Conference2015

Singapore | 22-24 July | Marina Bay Sands

External Adversaries



External Adversaries



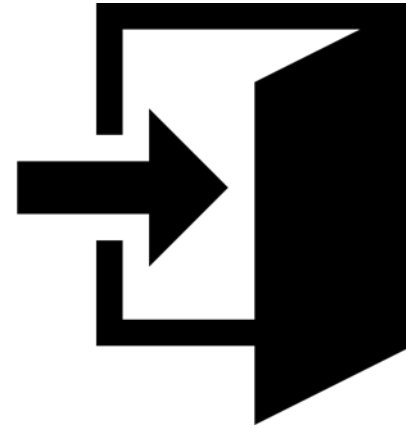
RSA[®]Conference2015

Singapore | 22-24 July | Marina Bay Sands

Internal Adversaries



Internal Vs. External?



Internal Adversaries



DETERMINED

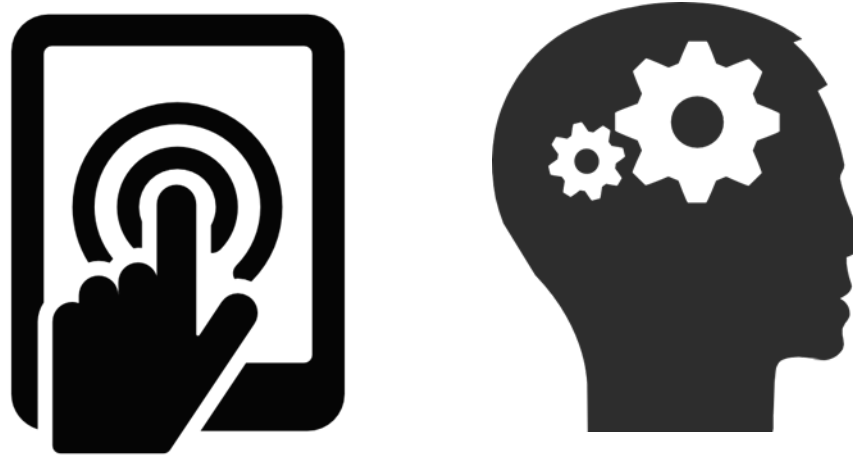


OPPORTUNISTIC



ACCIDENTAL

Defence Measures



PREVENTION | DETECTION | MITIGATION

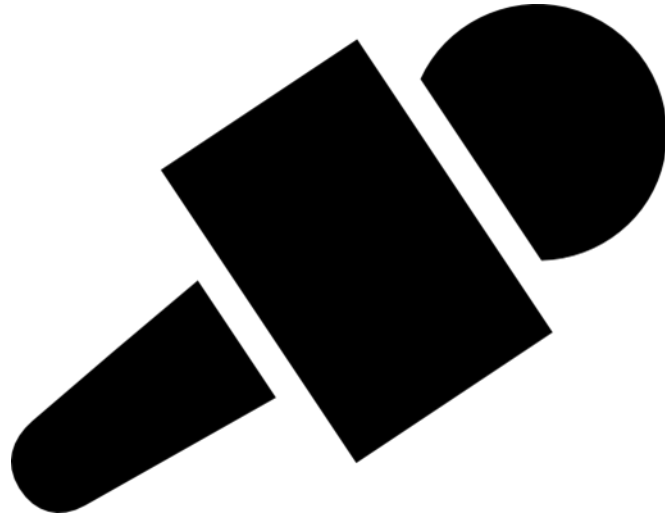
Internal Adversaries



Accidental Insider

Internal Adversaries





Passwords 2014

1.123456

2.Password

3.12345

4.12345678

5.Qwerty

6.2345678

7.1234

8.Baseball

9.Dragon

10.Football

11.1234567

12.monkey

13.Letmein

14.Abc123

15.111111

16.Mustang

17.Access

18.Shadow

19.Master

20.Michael

21.Superman

22.696969

23.123123

23.Batman

24.trustno1

Remediation: Accidental Insider

PREVENT



Encryption
2-Factor Authentication



Training

Internal Adversaries



Opportunistic Insider

Internal Adversaries



Remediation: Opportunistic Insider

DETER

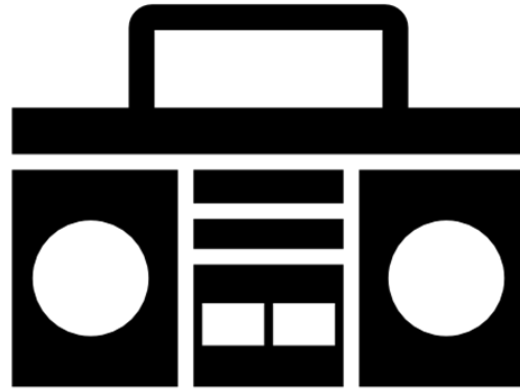


Logging
Monitoring
Digital Rights Management



Awareness

Context: Opportunistic Insider



Internal Adversaries



Determined Insider

Internal Adversaries



NASA

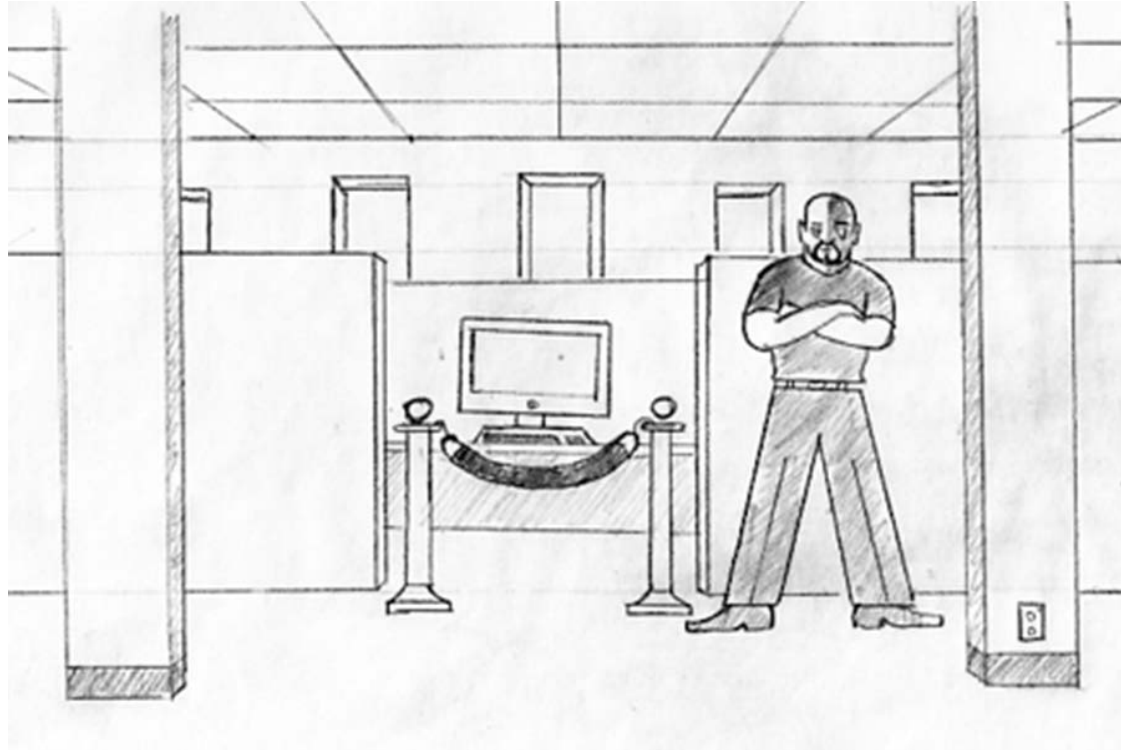
Remediation: Determined Insider

MITIGATE



Defense in Depth
Least Privilege

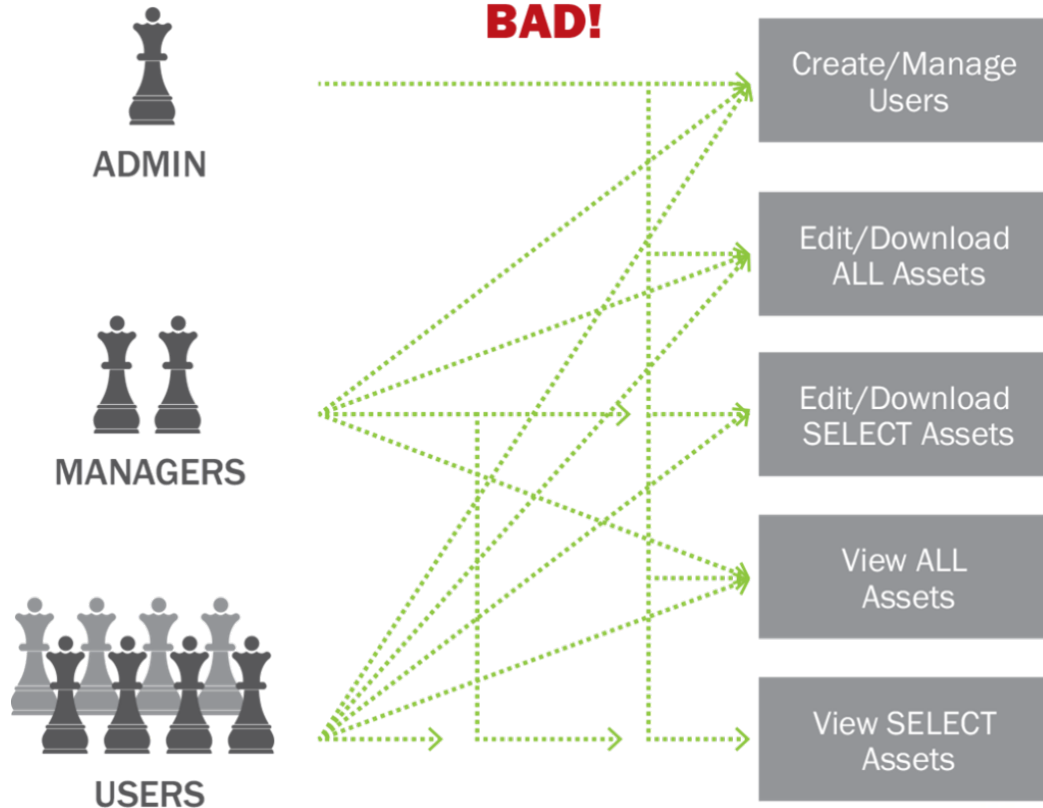
Remediation: Determined Insider



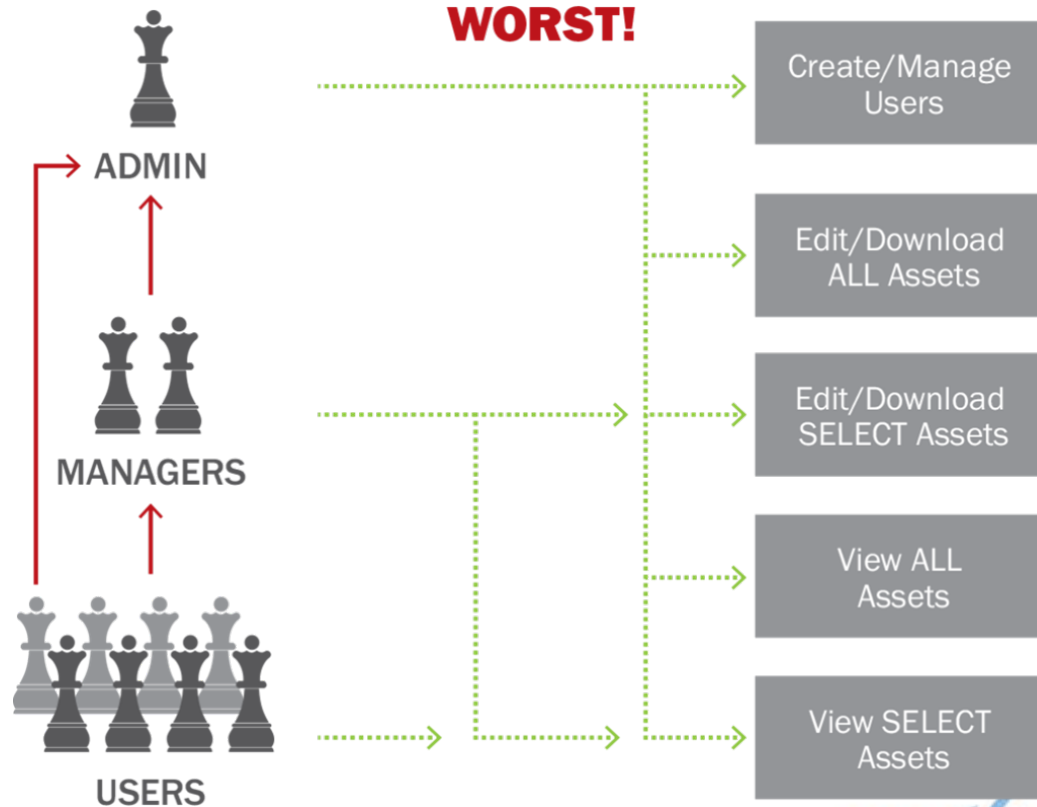
Remediation: Determined Insider



Remediation: Determined Insider



Remediation: Determined Insider



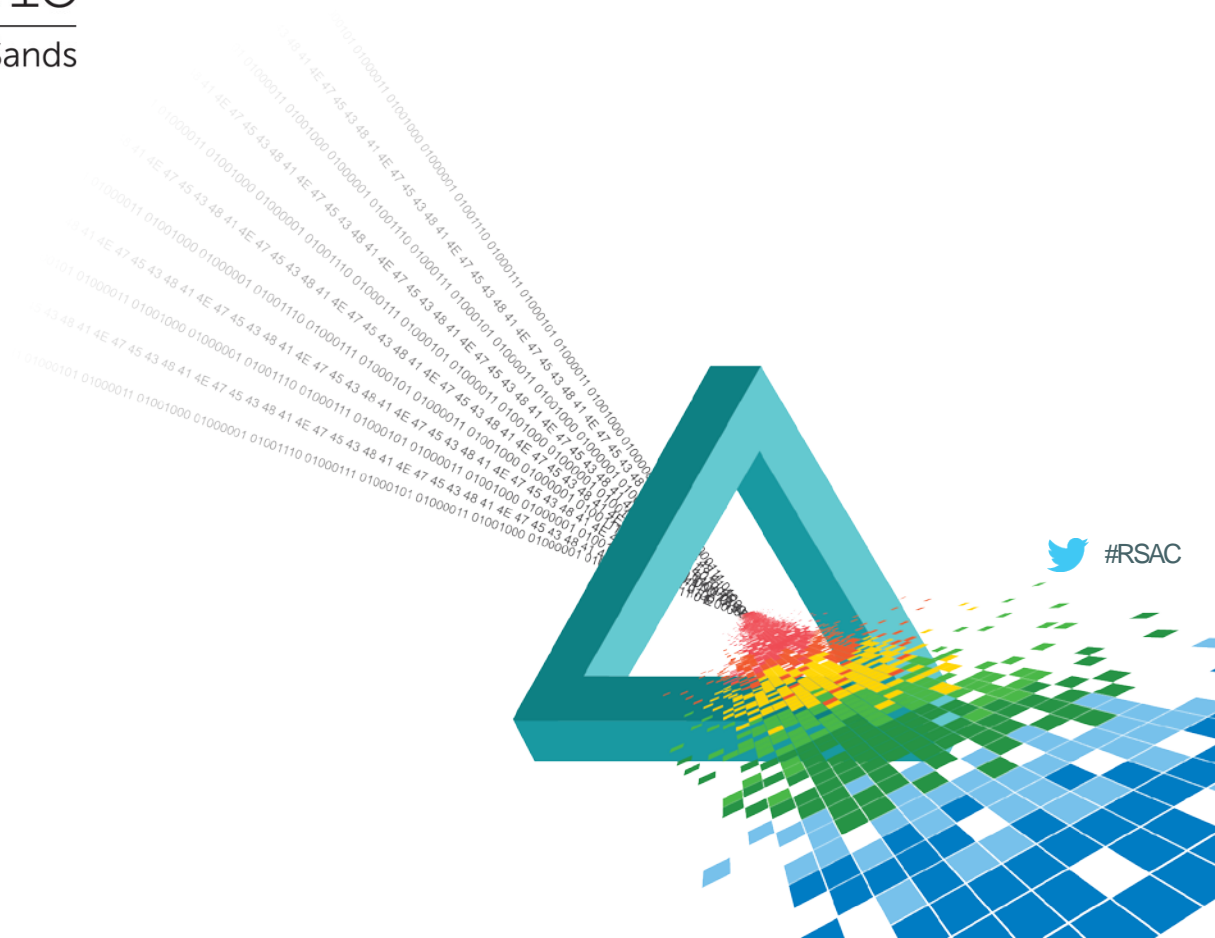
Remediation: Determined Insider



RSA[®]Conference2015

Singapore | 22-24 July | Marina Bay Sands

Recap



Recap



DETERMINED. OPPORTUNISTIC. ACCIDENTAL.

- Least Privilege
- Defense in Depth
- Encryption
- 2 Factor Auth.
- Logging
- Monitoring
- Awareness
- Training



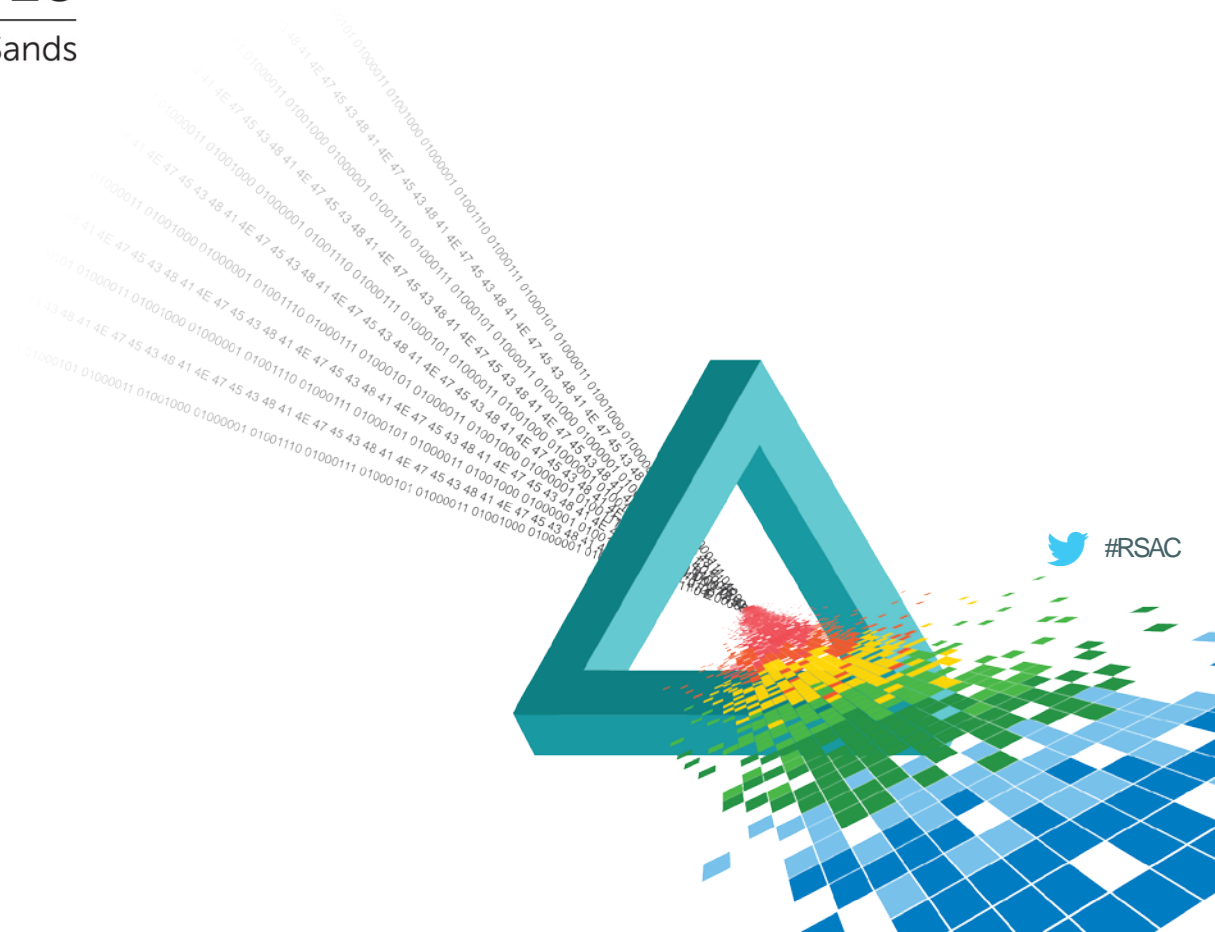
Recap

- ◆ Security is a business problem, not an IT problem.
- ◆ Security is about group dynamics.
- ◆ Different adversaries require different defense measures.

RSA[®]Conference2015

Singapore | 22-24 July | Marina Bay Sands

Apply



Apply What You Have Learned Today!

- ◆ Next week:
 - ◆ Create Threat Model
- ◆ In 3 Months:
 - ◆ Implement Mitigation program (Least Privilege, Defense in Depth)
 - ◆ Implement Prevention program (2FA, Encryption, etc)
 - ◆ Implement Deterrence program (Logging, Monitoring, Watermarking, etc)
- ◆ In 6 Months:
 - ◆ Implement Training program
 - ◆ Implement Awareness program