Issues, Dilemmas, and New Direction in Information Security

Meng-Chow Kang, PhD, CISSP
Director, Information Security, Cisco Systems

Agenda

- Dichotomy of Information Security
- Circular Problem of Information Security Principles
- Responsive Security

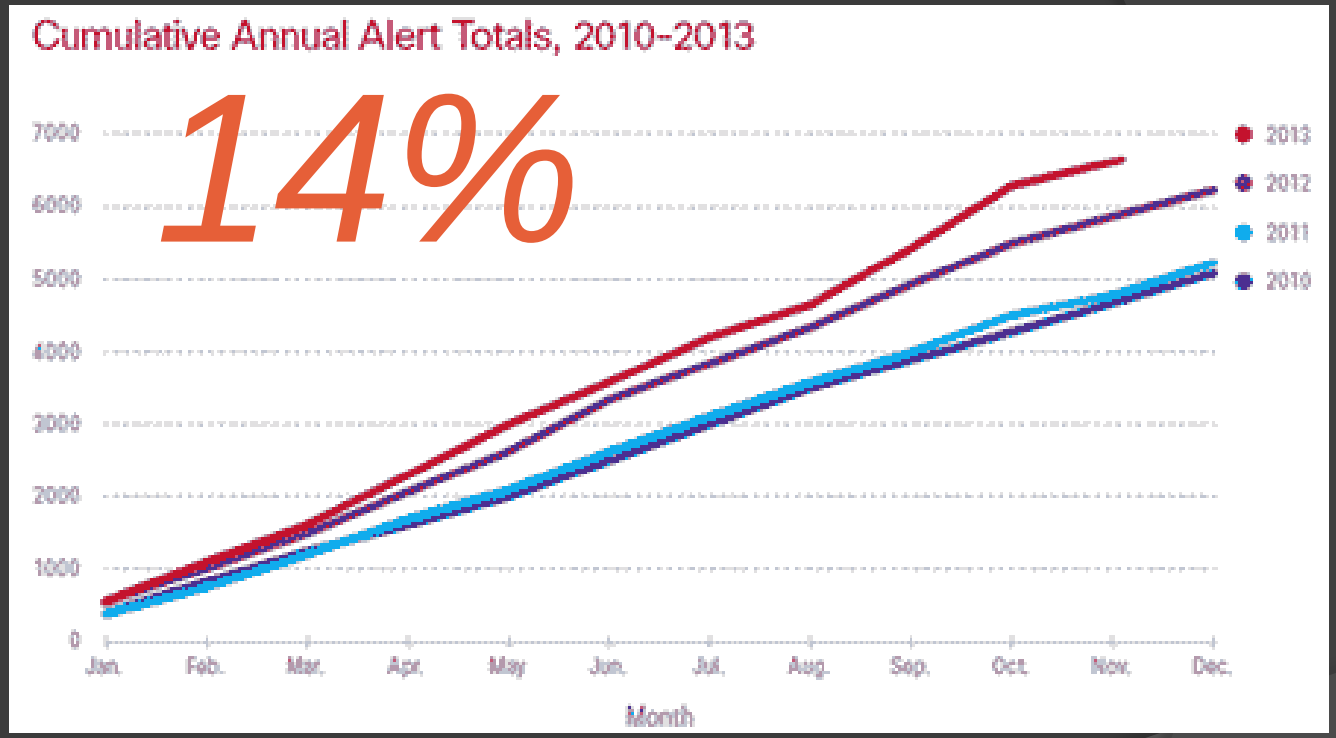
Dichotomy of information security

- Outcome of good security – what does it look like?
- How about the outcome of insecurity?

1.5 million

Monitored cyber attacks in the United States in 2013

IBM Security Services 2014 Cyber Security Intelligence Index, April 2014



Source: Cisco Annual Security Report 2014

Total Breaches

253

2013

+62%

Total Identities Exposed

552 Million

2013

+493%

Source: Maryam Runiassy, Sep 19, 2014: http://prezi.com/pflqhvvpb2nm/important-cybersecurity-incidents-and-statistics/

Lost Revenue

Forensic Investigation

Reputation

Trust

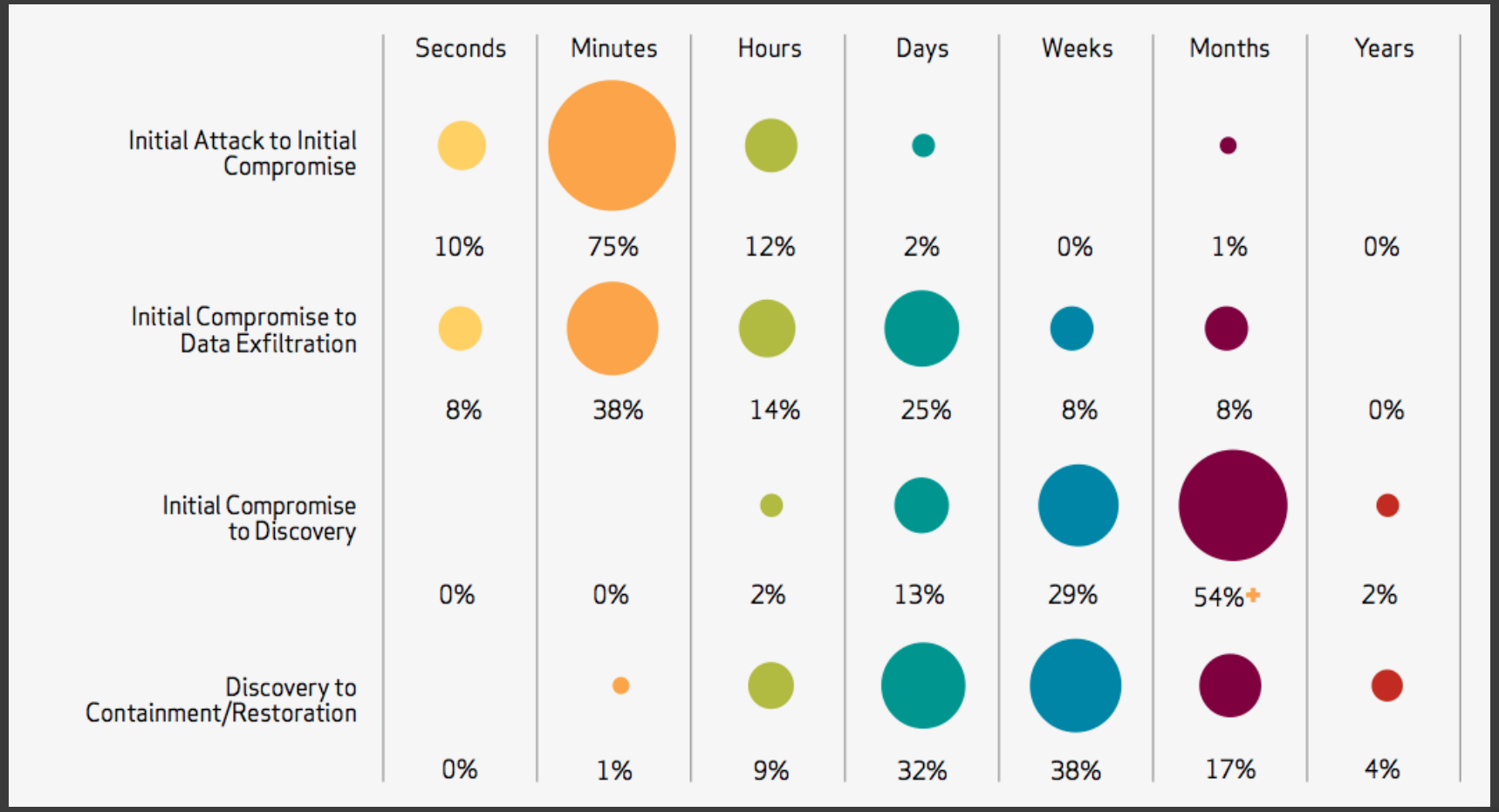
Brand Damage

Lost Productivity

Technical Support

Regulatory Compliance

Timespan of events by percent of breaches

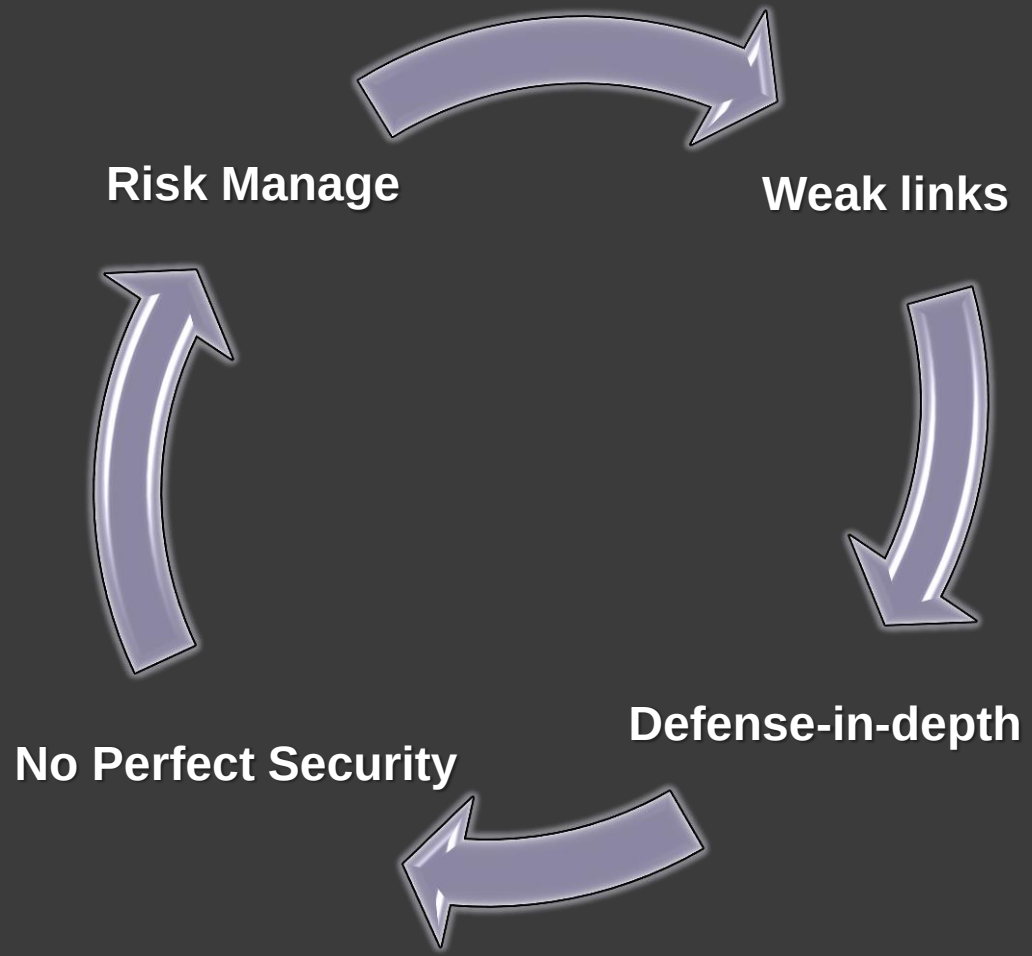


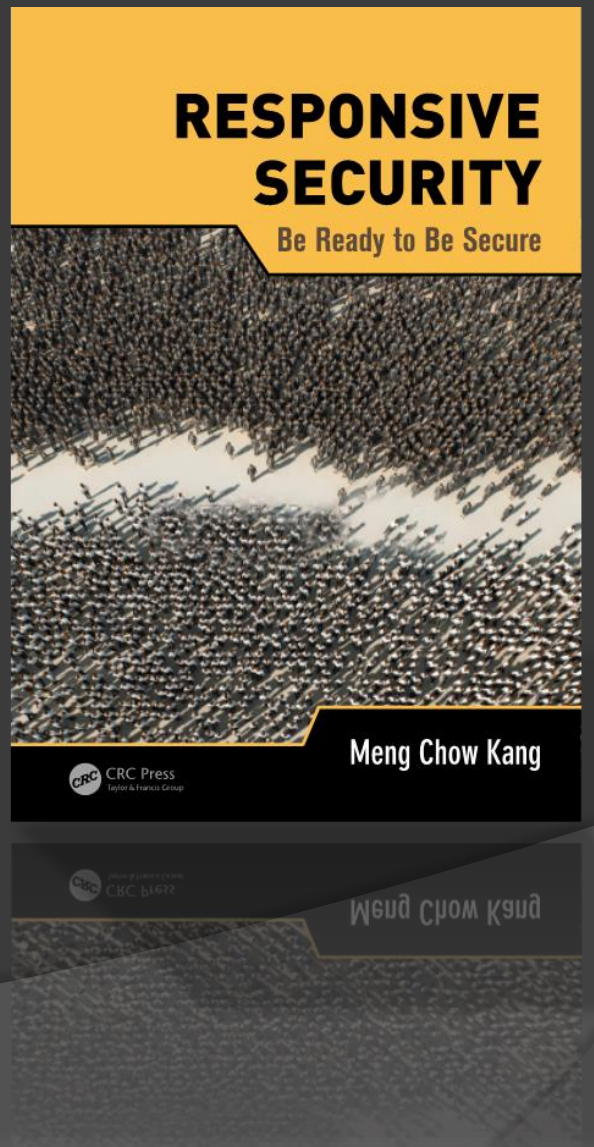
Source: Verizon Data Breach Investigation Report 2012

Imbalance of Investment impact ability to see what's happening

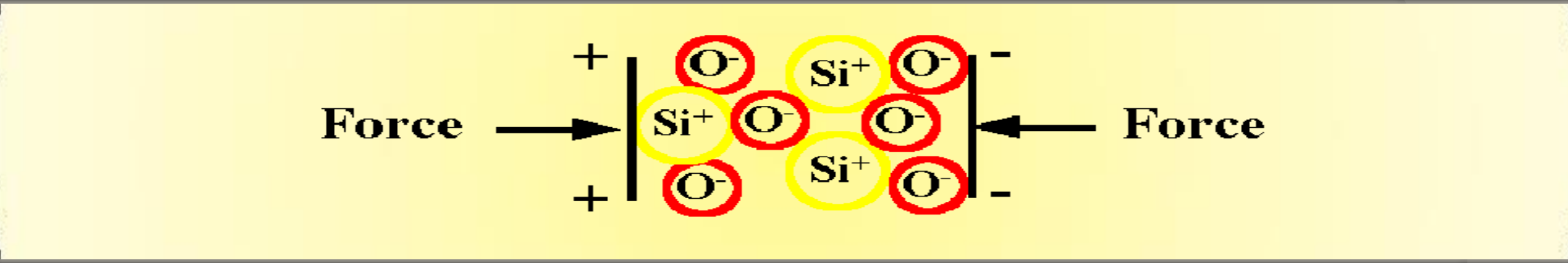
Lack of preparedness impact ability to contain emerging attacks and recover promptly.

Circularity of Information Security Principles





Piezoelectric Theory



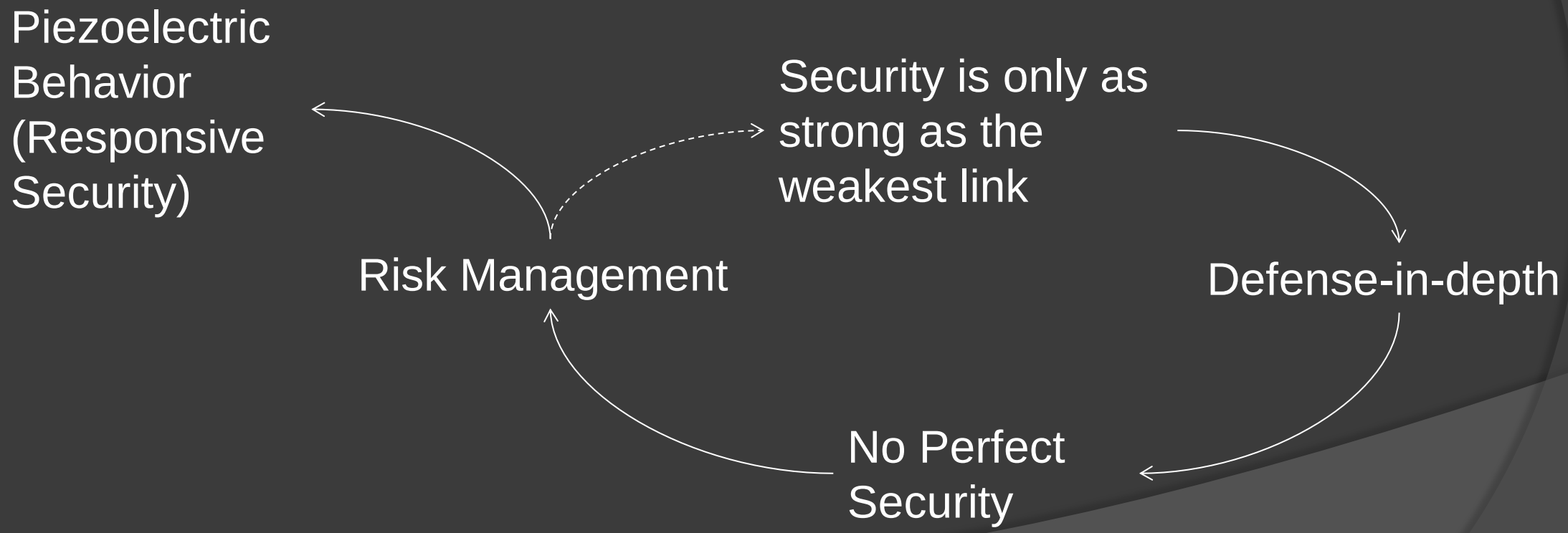
Squeeze/Relax → Trigger → Alignment

Piezoelectric Behavior

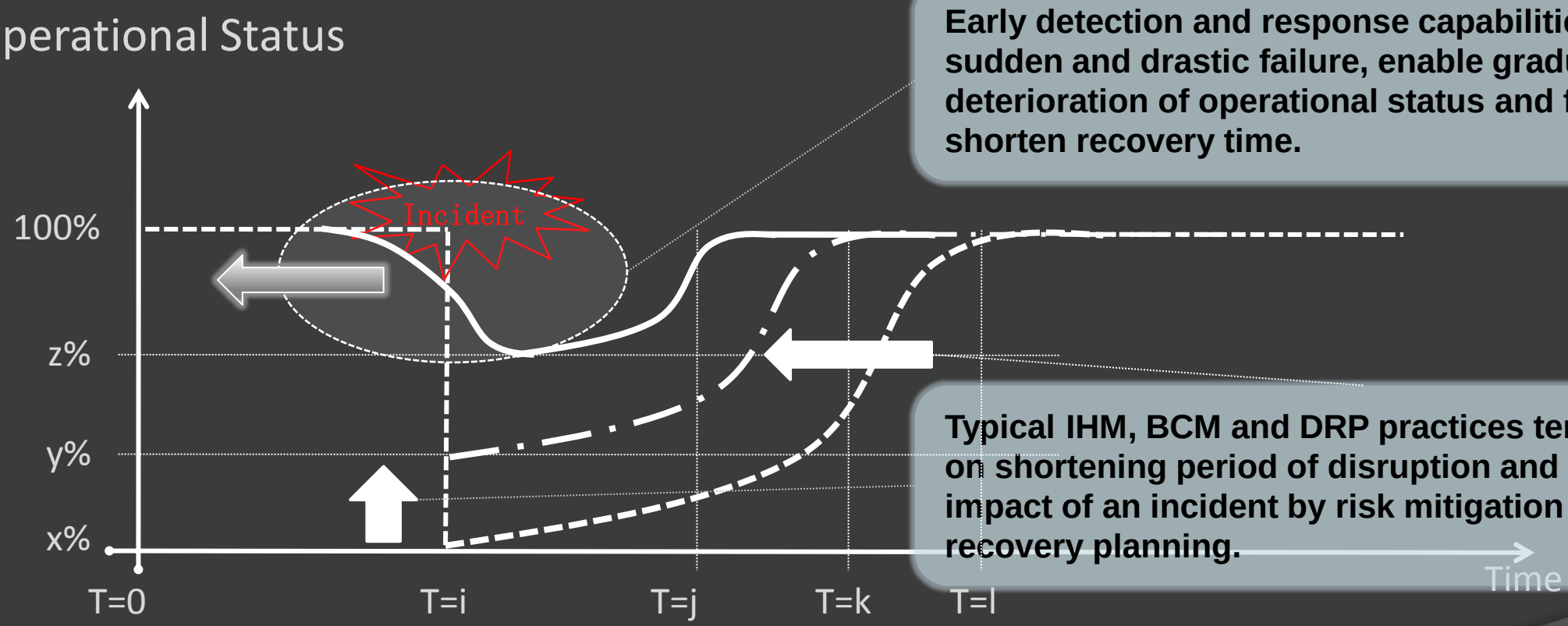
Responsive Behavior

Change Events → Situation Awareness → Critical Alignment

Breaking the circularity of Information Security Principles with Piezoelectric Behavior



Responsive Systems



Early detection and response capabilities to prevent sudden and drastic failure, enable gradual deterioration of operational status and further shorten recovery time.

Typical IHM, BCM and DRP practices tend to focus on shortening period of disruption and reducing the impact of an incident by risk mitigation and recovery planning.

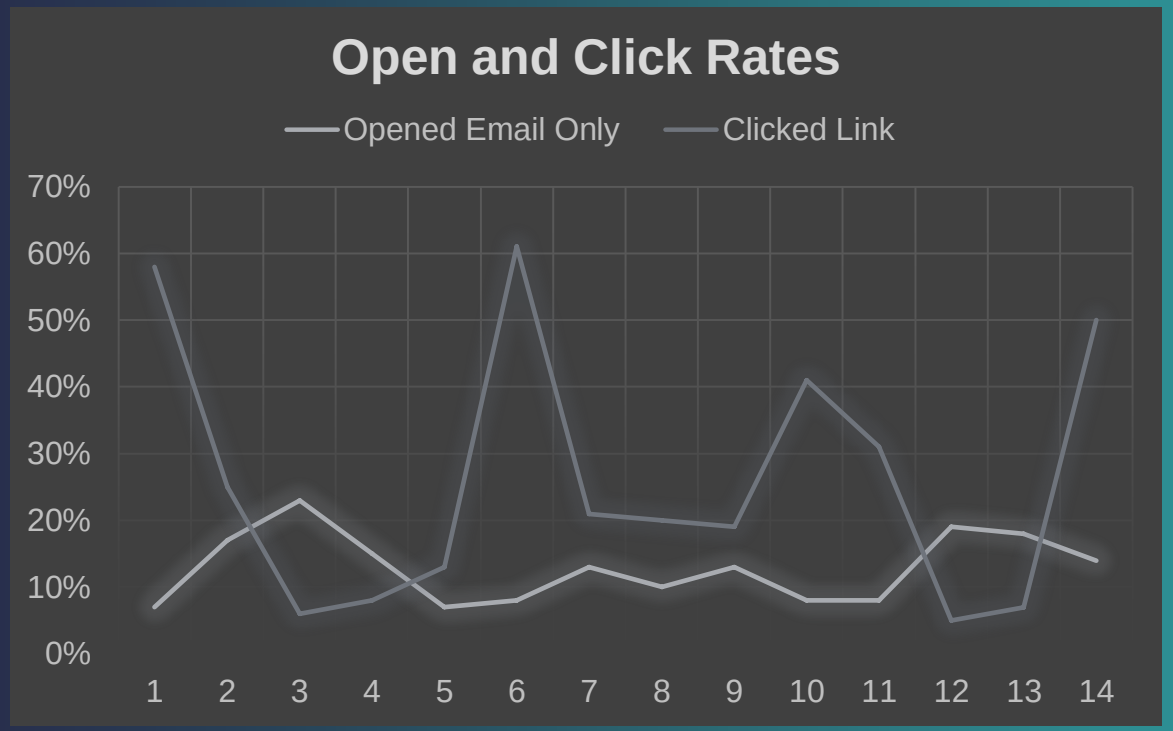
Before/weak implementation of IHM, BCM, and/or DRP

After implementation of IHM, BCM, and/or DRP

Desired effects of Responsive Security (focusing on Readiness)

How vulnerable are we?

- Target – 300 Dir/Mgrs/ICs in IT, launched at 10 am EST
- **Subject: Your request for Paid Time Off**



As of 4pm, out of 294 emails delivered, 125 (42.5%) were opened **AND** clicked on the link. 69 (23.5%) users clicked on the link in the first 15 minutes of the email campaign.

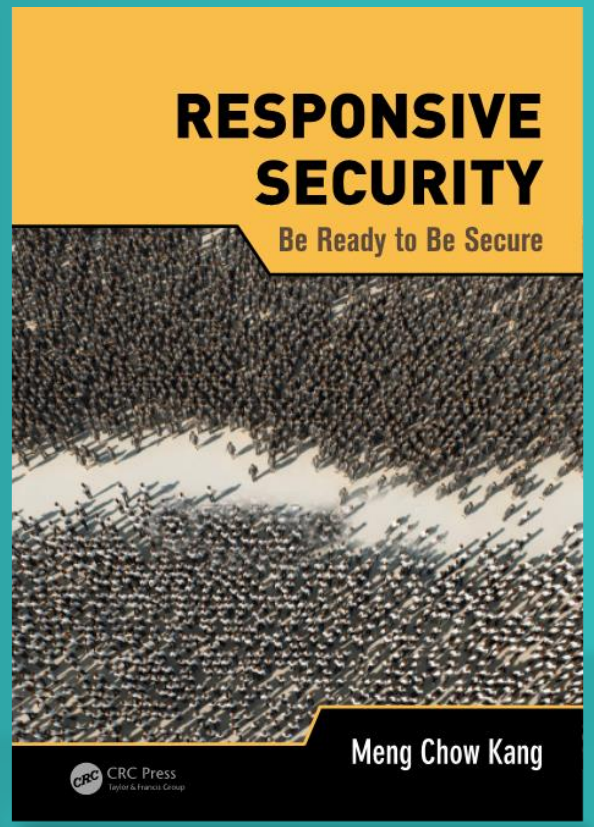
~20% of the users who clicked on the link were using a browser whose version was 4 years old or older.

Within 7 minutes of the campaign, CSIRT was notified and 5 minutes later the domain name was Black-holed.

Notification Mitigation

Towards Criticality Alignment

Intelligence	Visibility	Criticality Alignment
Knowledge	Awareness	Competence
	Capability	*Capacity*



“The most effortful forms of slow thinking are those that require you to think fast.”

– Daniel Kahneman in “Thinking, Fast and Slow”