RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

One Failure Leads to Another: Developing Leading Indicators for Security Threats and Risks

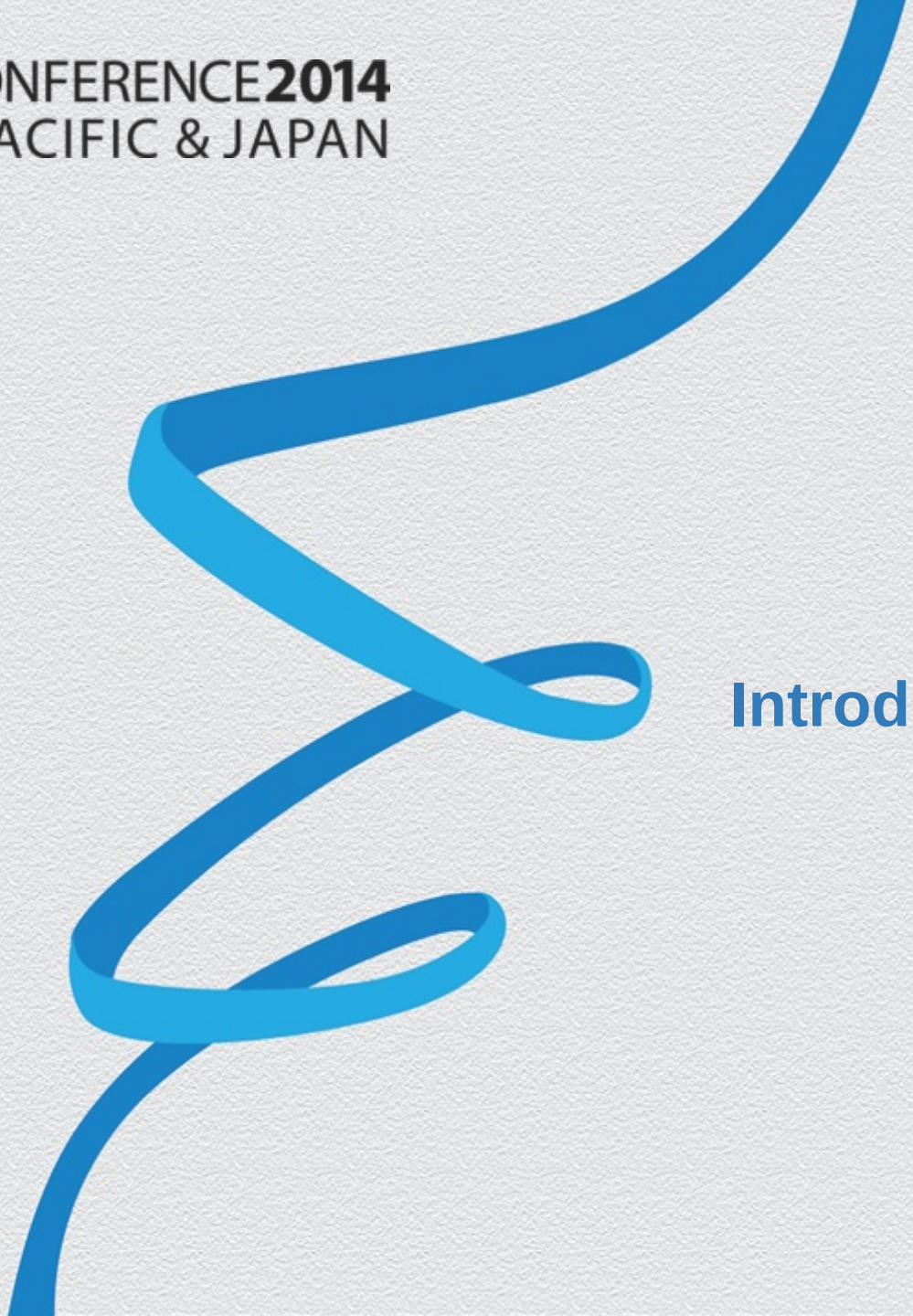
SESSION ID: TRM-W07

Dr. Lance Hayden

Solutions Architect & Information Scientist
Cisco Global Security Services
@hay_lance

What We'll Cover Today

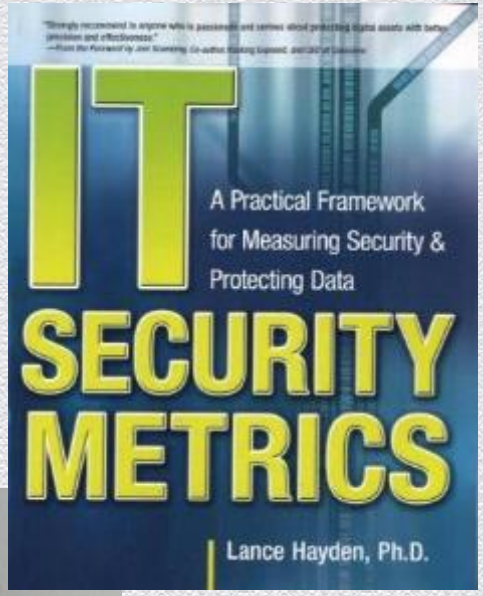
- Introductions
- Measures, Metrics and Indicators
- Leading Indicators in Security
- Examples
- Developing Leading Indicators in Your Security Program
- Concluding Remarks and Open for Questions



Introductions

Introducing Myself

Dr. Lance Hayden
CISSP, CISM, CRISC
lhayden@cisco.com
www.linkedin.com/in/drhayden
www.amazon.com/author/drhayden



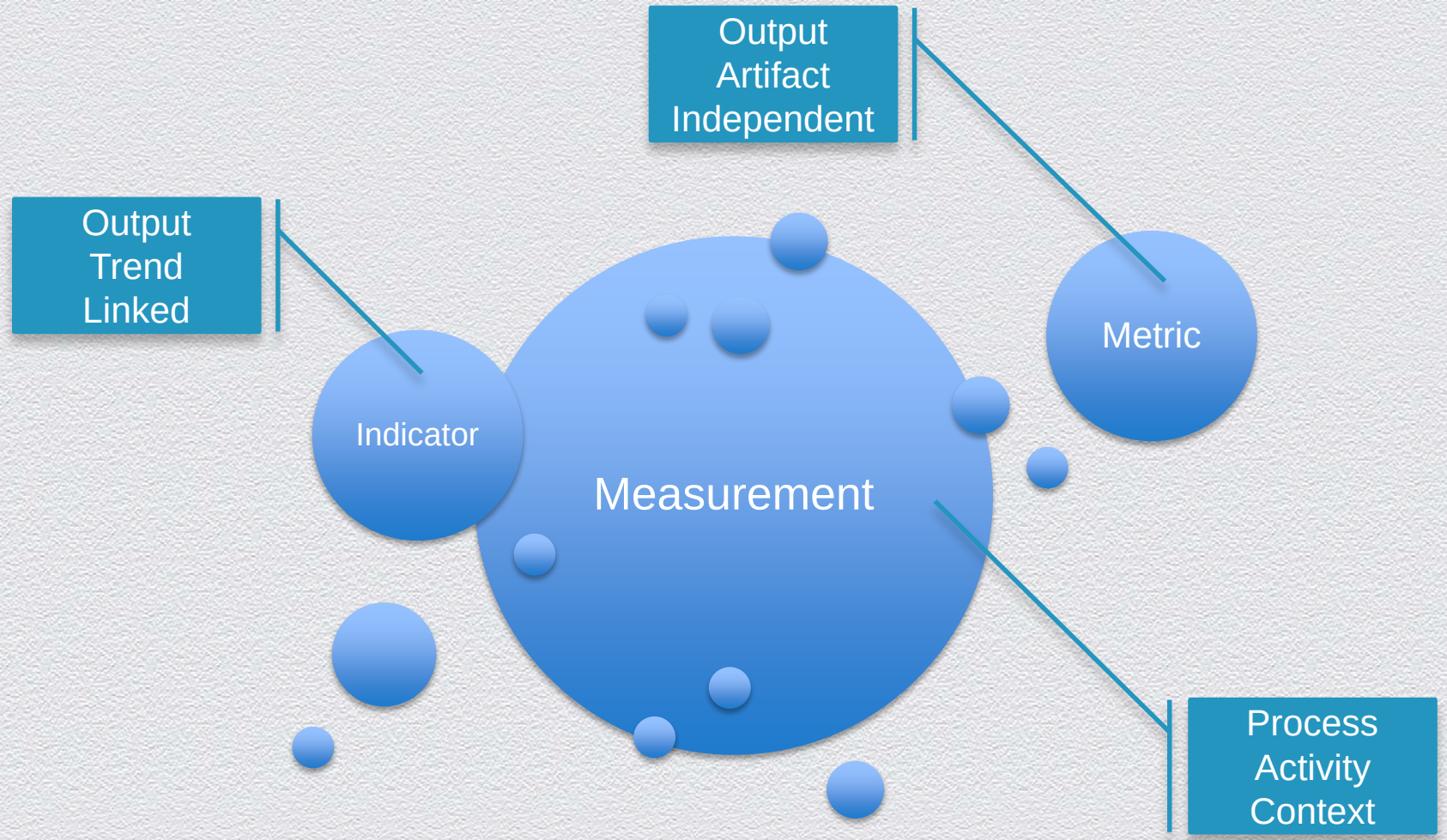
Measures, Metrics and Indicators

Measures, Metrics and Indicators

What does it mean to measure?

- “[To] ascertain the size, amount, or degree of (something) by using an instrument or device marked in standard units or by comparing it with an object of known size”
- “[To] estimate or assess the importance, quality, value, or effect of (something)”
- “[To] judge someone or something by comparison with (a certain standard)”[1]

Measures, Metrics and Indicators



Measures, Metrics and Indicators

Leading and Lagging Indicators

- Concept borrowed from economics
  - Use of indicators dates back to 1930's
  - National Bureau of Economic Research (NBER)
- Metrics involving "economic processes found to be important in business cycles"[2]
- Types of indicators include:
  - Leading – indicators that anticipate future cycles and events
  - Coincident – indicators that describe current state
  - Lagging – indicators that are evidence of past cycles and events

Measures, Metrics and Indicators

Examples of Economic Indicators

- Lagging Indicators
  - GDP drop for two consecutive quarters indicates recession
  - Unemployment rising indicates economy has fared poorly
- Coincident Indicators
  - Income and wages
- Leading Indicators
  - Stock prices
  - Retail sales
  - Building permits

Measures, Metrics and Indicators

“It’s very difficult to make predictions, especially about the future…”[3]

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Leading Indicators in Security

Drift Model of Security Failure

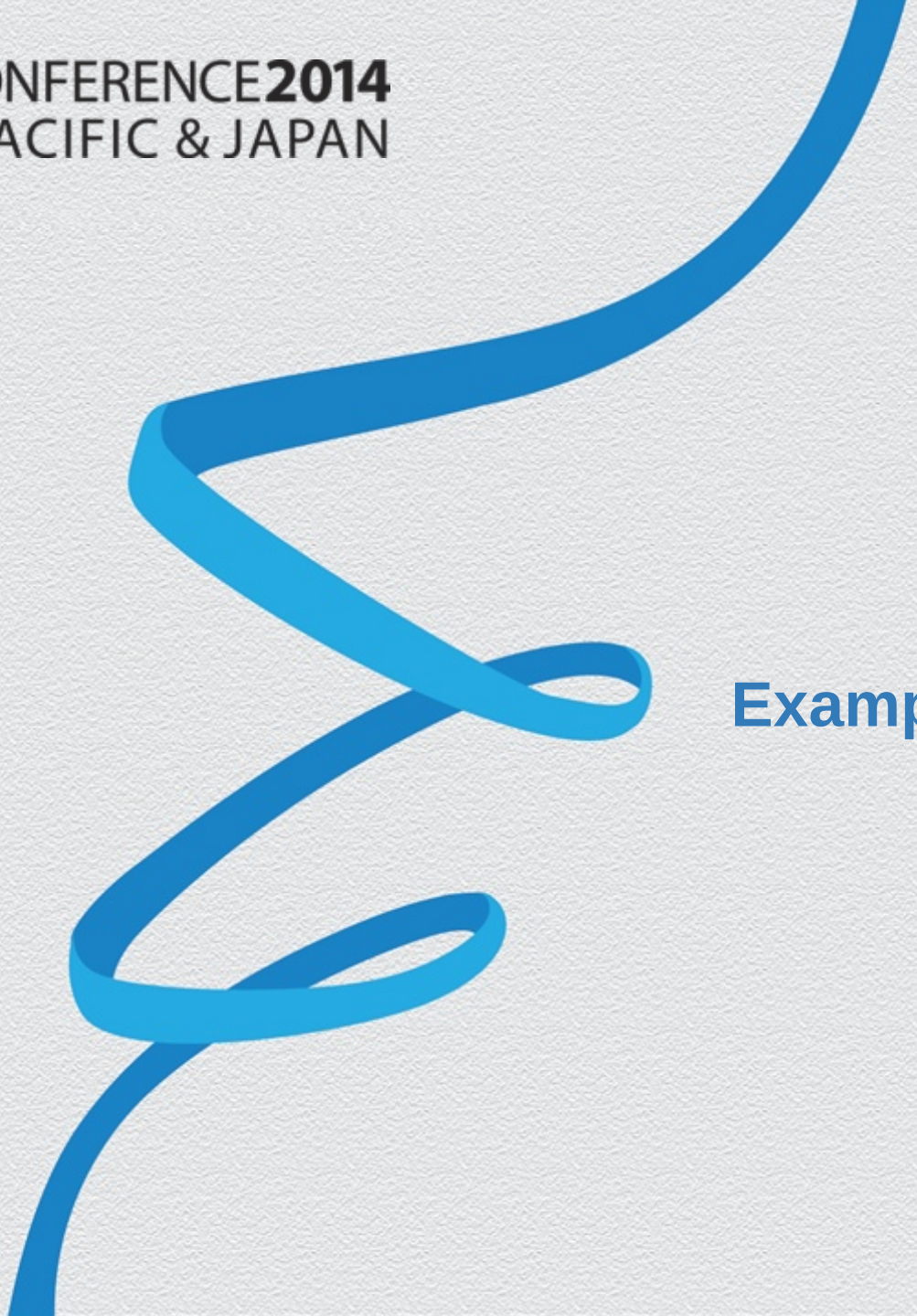
Leading Indicators in Security

- Security professionals understand the role of lagging and coincident indicators
  - Event counts (coincident)
  - Telemetry data (coincident)
  - Failed audits (lagging)
  - Security breaches (lagging)
- Today, security teams are looking for ways to anticipate threats and failures

Leading Indicators in Security

Requirements for leading security indicators are different

- Leading indicators require a different approach
  - Data collection prior to the cycle or event
  - Proactive rather than reactive vision
  - Creativity and imagination
- Leading indicators require different data sources
  - Exploratory rather than forensic data
  - Information investment against future insights
- Leading Indicators require different analysis
  - Linking past and future measurements
  - Looking for future trends in past data

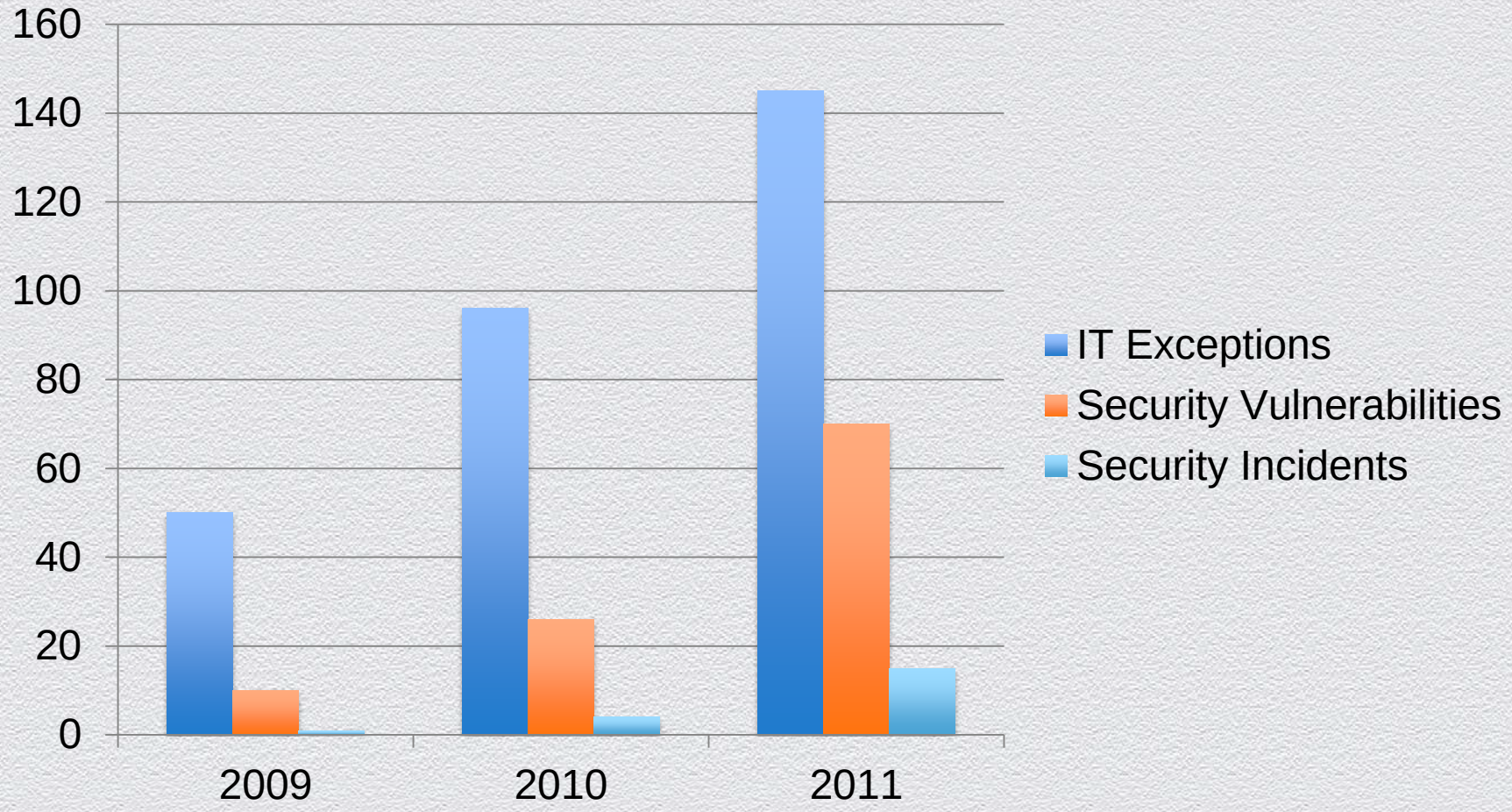


Examples

Example: Making an Exception

- Many organizations have standard security configurations
  - Deployment guides
  - Standard or secure build policies for production systems
- Many organizations also have exception processes
  - With approval, some systems may not have to “play by the rules”
  - Allows flexibility and agility
- A poorly managed exception process can be a leading indicator of security risk
- Source: exception process of large retail company

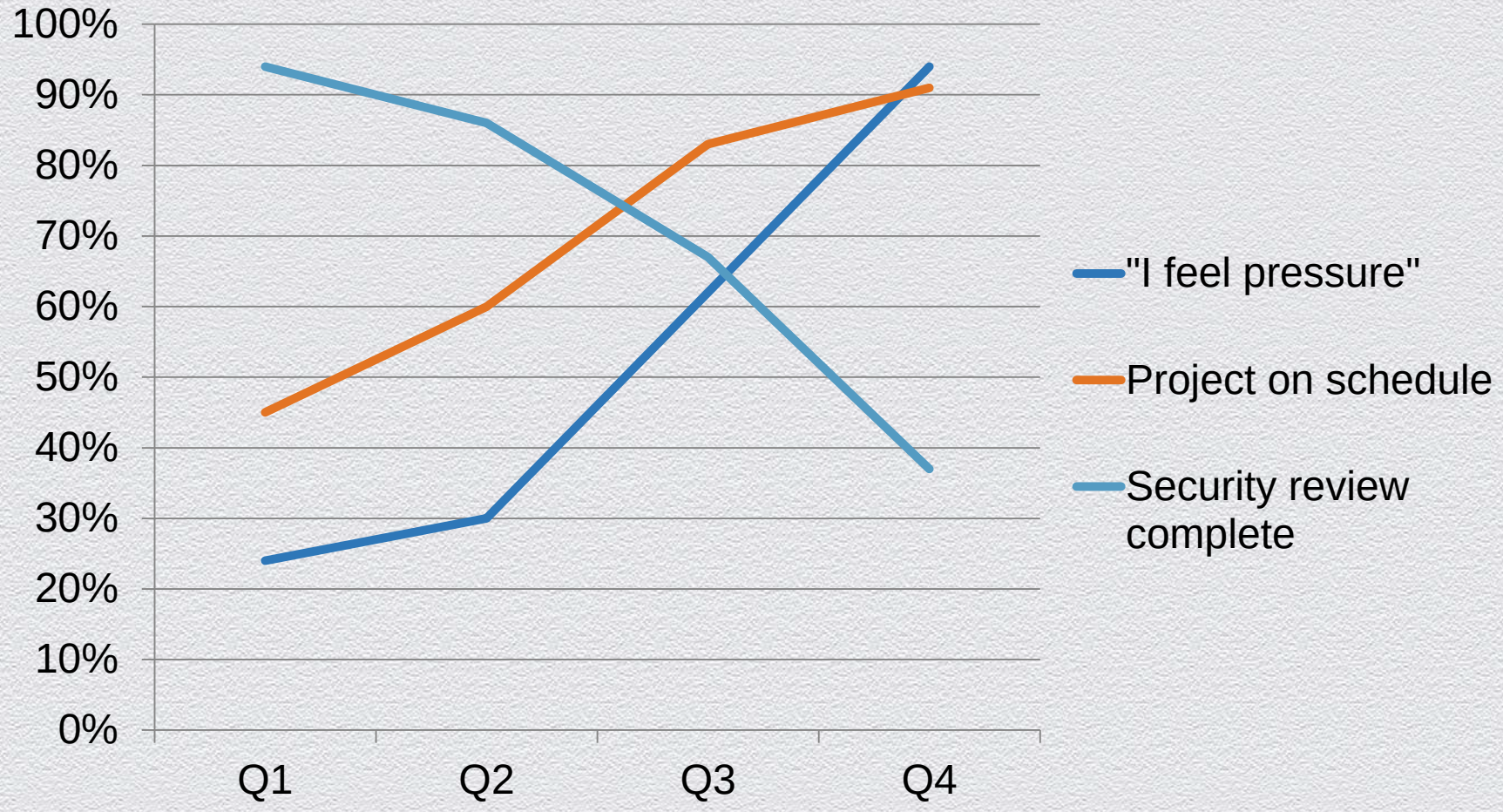
Example: Making an Exception



Example: Competing Priorities

- Security must compete with other enterprise priorities
  - Productivity targets
  - Revenue and cost pressures
- Habits and decisions, not policies, define security posture
  - If the choice is “secure” or “on time” which will be chosen?
  - Organizational culture defines what is truly important
- Changes in everyday decisions can be a leading indicator of increased security risks
- Source: survey responses & project data of medium ISP

Example: Competing Priorities

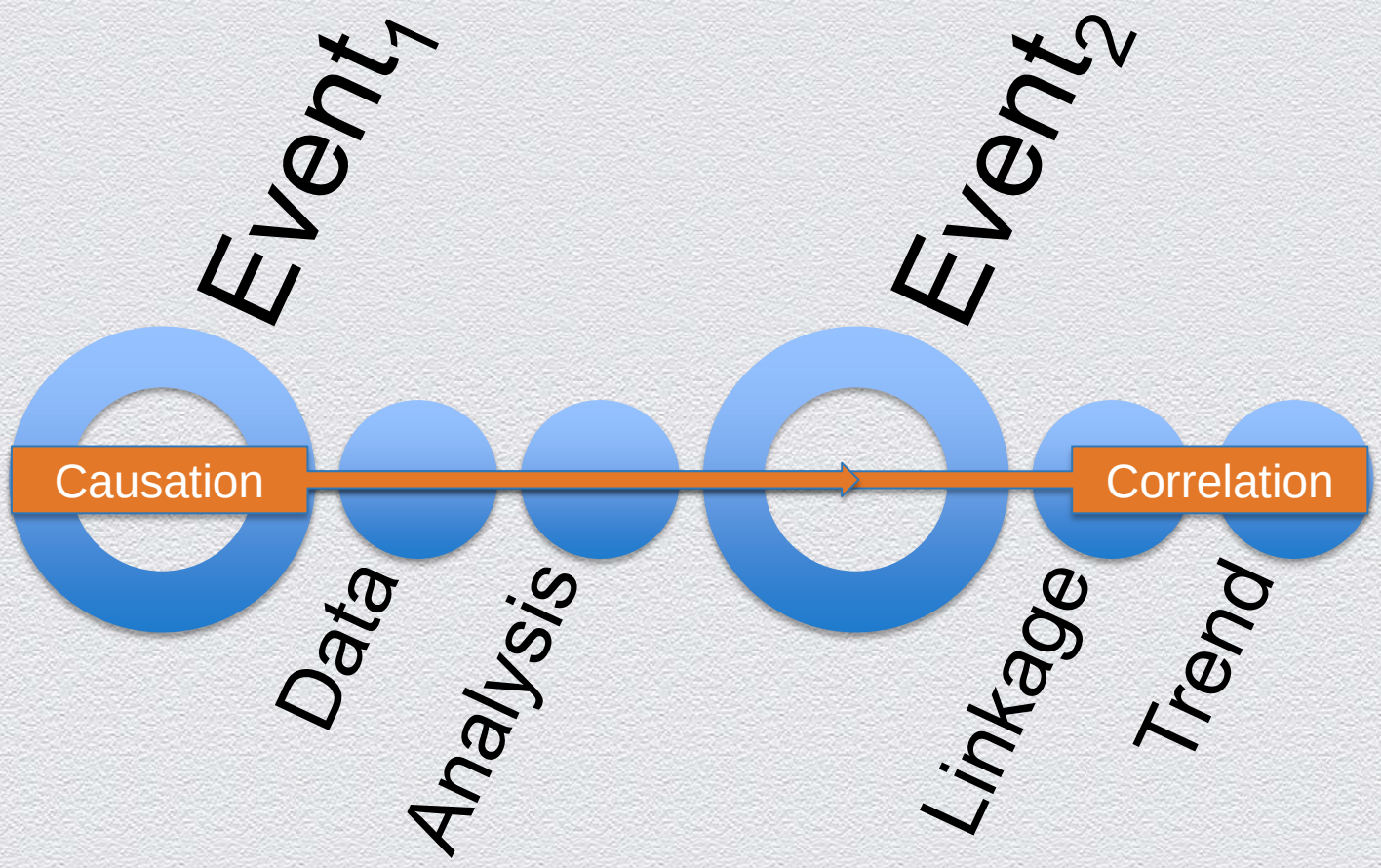


RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Developing Leading Indicators in Your Security Program

#RSAC

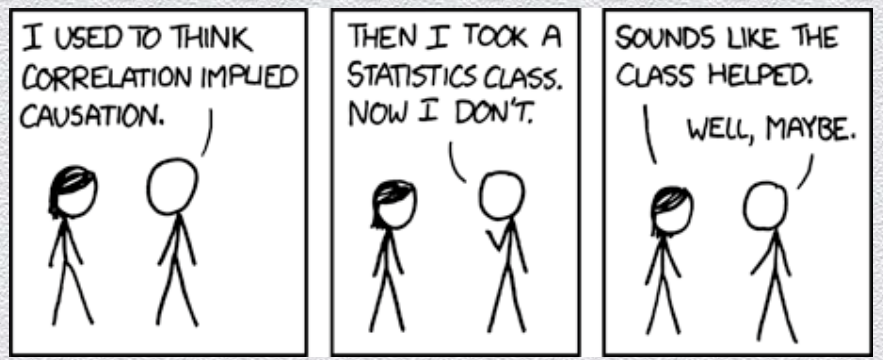
Developing Leading Indicators in Your Security Program



Developing Leading Indicators in Your Security Program

Five rules for leading security indicators

- One: Big events (almost) always follow small ones
- Two: Correlation is not causation
- Three: Patterns are not predictions
- Four: Analysis can't be (fully) automated
- Five: If you're sure, then you're sure to be wrong



http://xkcd.com/552/

Developing Leading Indicators in Your Security Program

Five tips for leading security indicators

- One: Work back from known events
- Two: Pay attention to small failures
- Three: Don’t let the perfect be the enemy of the good
- Four: Surveys make for great data
- Five: Don’t be afraid to experiment

Thinking Differently About Indicators

Let's examine a few examples

- Federal Reserve "Beige Book"[4]
  - Published eight times per year since 1970
  - Completely anecdotal data
- Consumer Confidence Indices (Various)
  - Survey-based data collection
  - Responses are variants of positive, neutral, or negative
- Ontario Leading Indicators Project (OLIP)
  - Designed to identify management practices that "improve health and safety performance before injuries and illnesses occur"
  - Again, survey based, categorical data collection

References

[1] Oxford English Dictionary

[2] NBER Working Paper No.941: *The Leading Indicator Approach to Economic Forecasting – Retrospect and Prospect*

[3] Variously attributed to Yogi Berra, Niels Bohr, and Mark Twain

[4] *Summary of Commentary on Current Economic Conditions by Federal Reserve District* (available at www.federalreserve.gov/monetarypolicy/beigebook/default.htm)