RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: GRC-T09R

Bridging the Gap Between Threat Intelligence and Risk Management

Wade Baker

VP, Strategy & Risk Analytics
ThreatConnect
@wadebaker

#RSAC

Underlying assumption

Good **intelligence** makes smarter **models**;
Smarter models inform **decisions**;
Informed decisions drive better **practice**;
Better practice improves **risk** posture**;**
which, done efficiently,
Makes a successful security **program**.

Does your security program look like this?

Threat Intelligence

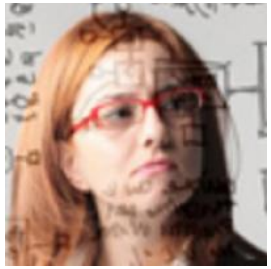
Risk Management

They have some issues dividing them...

Threat Intelligence

- “There’s way too much uncertainty around her. I live & die in binary world.”
- “I beat adversaries with STIX & detonate their remains. She plays with numbers.”
- “People say she’s “stochastic.” That explains a lot; she needs serious help.”
- “She doesn’t even cyber, bro! Need I say anything more?”

Risk Management



- “He’s intolerable. I assess he needs to be treated & transferred to a 3rd party.”
- “One look at his laptop makes me panic. It’s a giant audit finding with a keyboard.”
- “He never shares with coworkers. I swear, if he TLP-Red’s us one more time…”
- “What’s his deal with China, anyway? It’s an HR liability if you ask me.”

…but they'd make such a great team.

Agenda

- Bridging Risk & IR in Verizon's DBIR.
- Building Understanding
- Finding Common Ground
- Bridging the Gap
- Crossing the Divide (Apply)

Bridging Risk and IR in Verizon's DBIR

Bridging Risk and IR in the DBIR

Frequency of incident classification patterns per victim industry

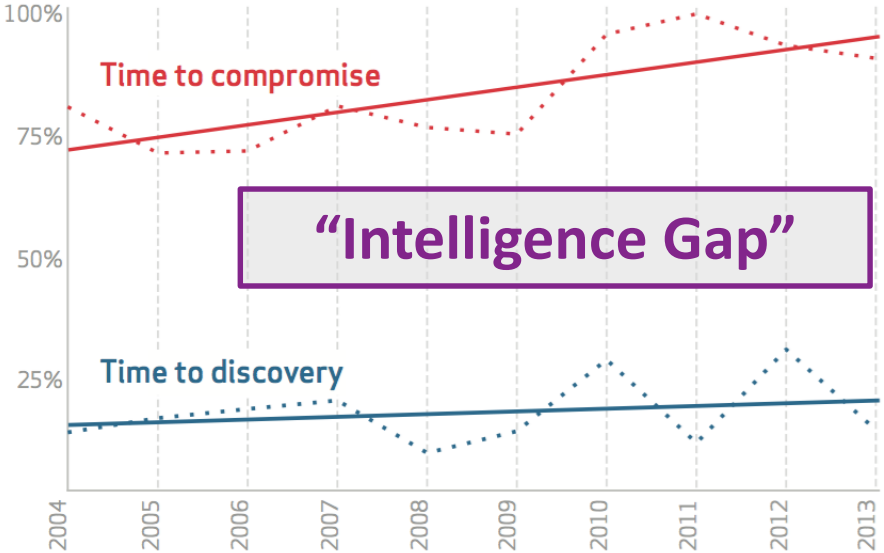
INDUSTRY	POS INTRUS-ION	WEB APP ATTACK	INSIDER MISUSE	THEFT/ LOSS	MISC. ERROR	CRIME-WARE	PAYMENT CARD SKIMMER	DENIAL OF SERVICE	CYBER ESPION-AGE	EVERY-THING ELSE
Accommodation [72]	75%	1%	8%	1%	1%	1%	<1%	10%		4%
Administrative [56]		8%	27%	12%	43%	1%		1%	1%	7%
Construction [23]	7%		13%	13%	7%	33%			13%	13%
Education [61]	<1%	19%	8%	15%	20%	6%	<1%	6%	2%	22%
Entertainment [71]	7%	22%	10%	7%	12%	2%	2%	32%		5%
Finance [52]	<1%	27%	7%	3%	5%	4%	22%	26%	<1%	6%
Healthcare [62]	9%	3%	15%	46%	12%	3%	<1%	2%	<1%	10%
Information [51]	<1%	41%	1%	1%	1%	31%	<1%	9%	1%	16%
Management [55]		11%	6%	6%	6%		11%	44%	11%	6%
Manufacturing [31,32,33]		14%	8%	4%	2%	9%		24%	30%	9%
Mining [21]			25%	10%	5%	5%	5%	5%	40%	5%
Professional [54]	<1%	9%	6%	4%	3%	3%		37%	29%	8%
Public [92]		<1%	24%	19%	34%	21%		<1%	<1%	2%
Real Estate [53]		10%	37%	13%	20%	7%			3%	10%
Retail [44,45]	31%	10%	4%	2%	2%	2%	6%	33%	<1%	10%

Bridging Risk and IR in the DBIR

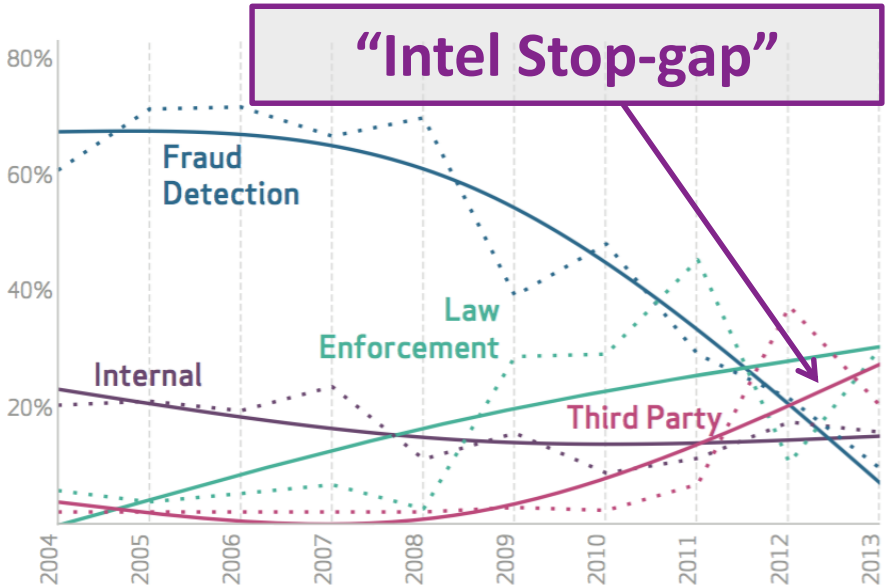
The Intelligence Gap

**All figures from Verizon DBIR

Percent of breaches where time to compromise (red)/time to discovery (blue) was days or less



Breach discovery methods over time



Building Understanding

What is threat intelligence?

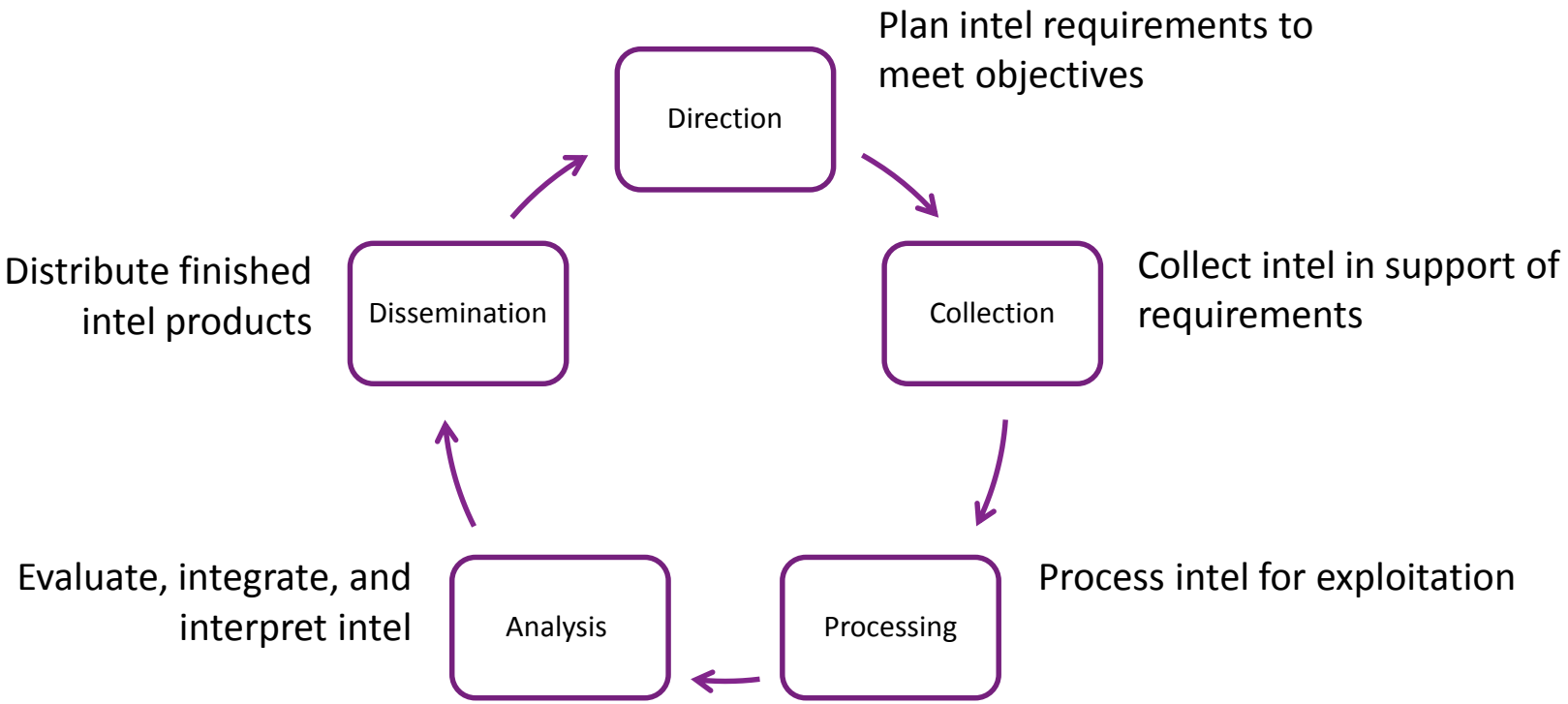
"Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."

Gartner

"The details of the motivations, intent, and capabilities of internal and external threat actors. Threat intelligence includes specifics on the tactics, techniques, and procedures of these adversaries. Threat intelligence's primary purpose is to inform business decisions regarding the risks and implications associated with threats."

FORRESTER®

Classic intelligence cycle

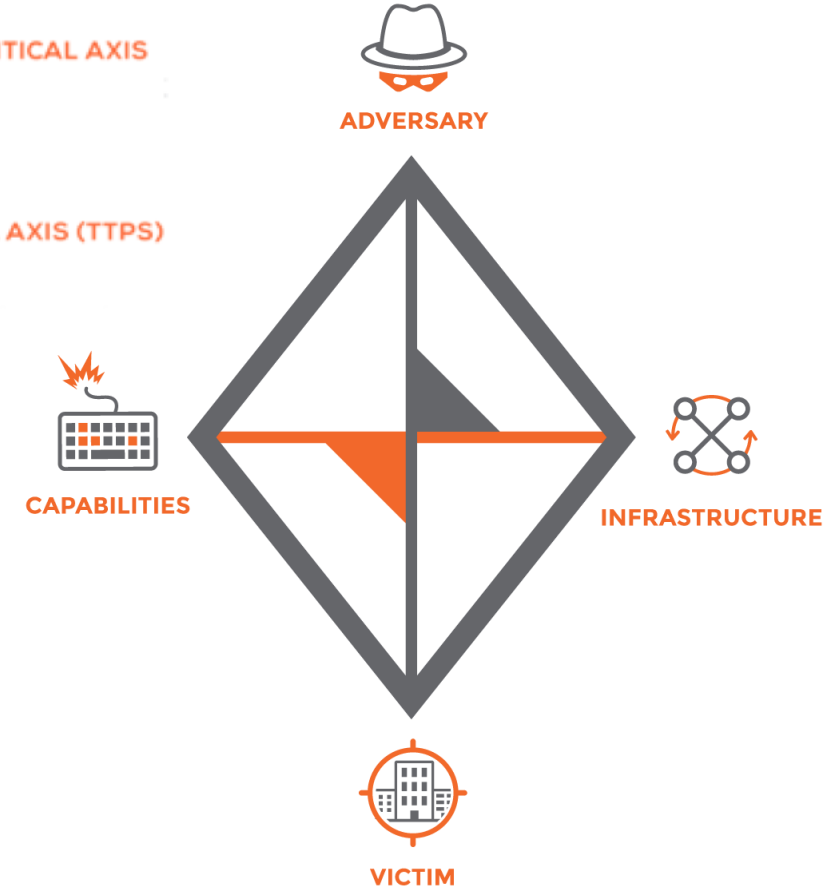


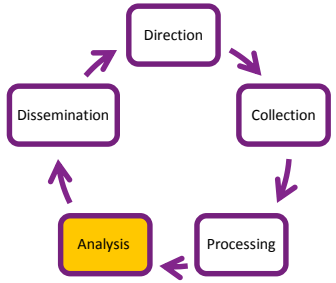
Threat intelligence process

The Diamond Model of Intrusion Analysis

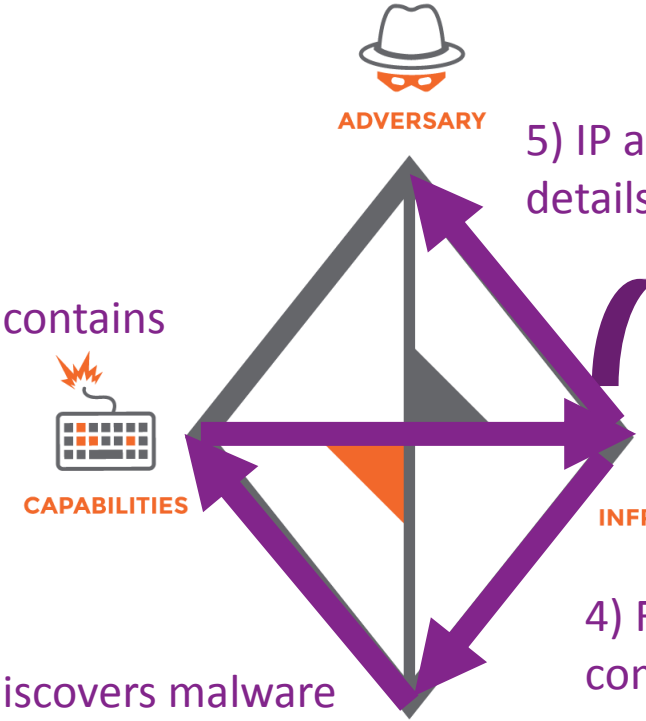
1 SOCIO-POLITICAL AXIS

2 TECHNICAL AXIS (TTPS)





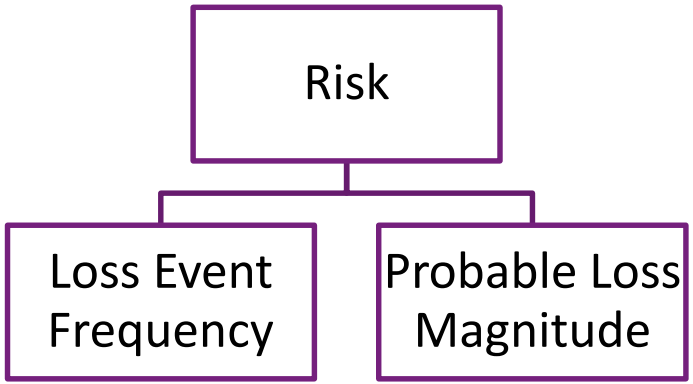
Threat intelligence process



What is risk?

"The probable frequency and probable magnitude of future loss"

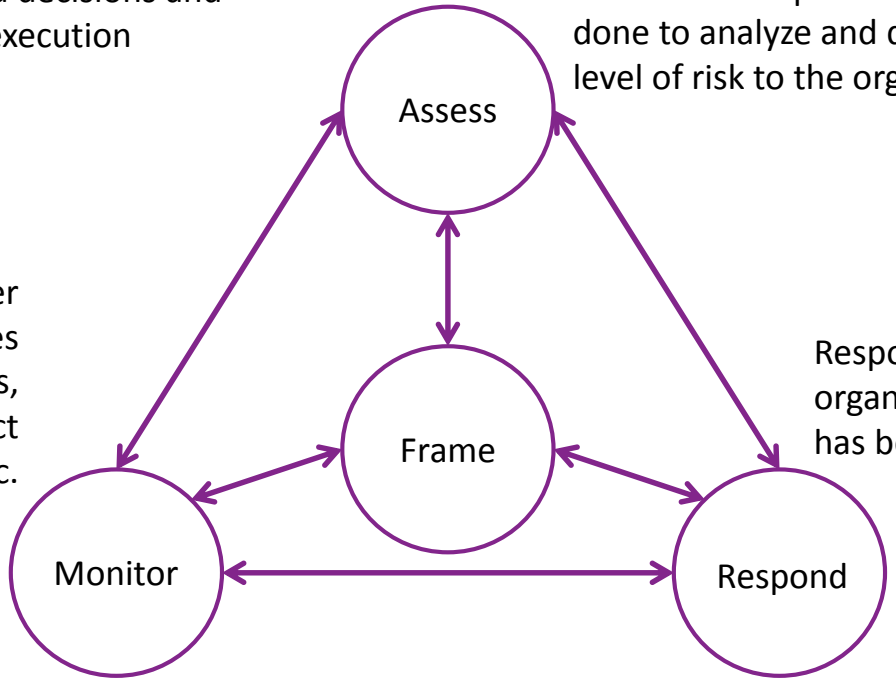
- Factor Analysis of Information Risk (FAIR)



Risk management process (NIST 800-39)

Frame: establishes the context for risk-based decisions and strategy for execution

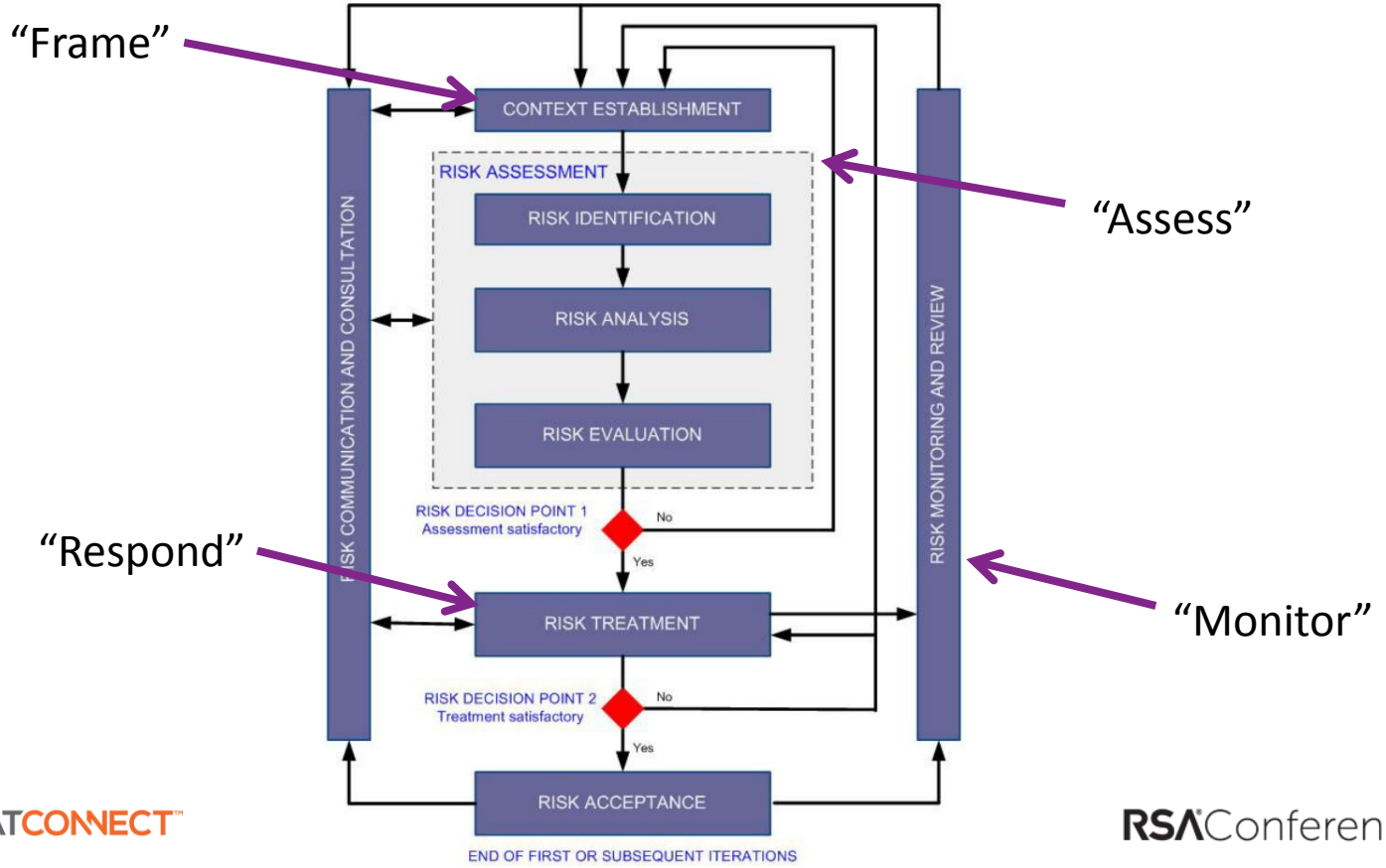
Assess: encompasses everything done to analyze and determine the level of risk to the organization.



Monitor: verifies proper implementation, measures ongoing effectiveness, tracks changes that impact effectiveness or risk, etc.

Respond: addresses what organizations choose to do once risk has been assessed and determined

Risk management process (ISO 27005)



Finding Common Ground

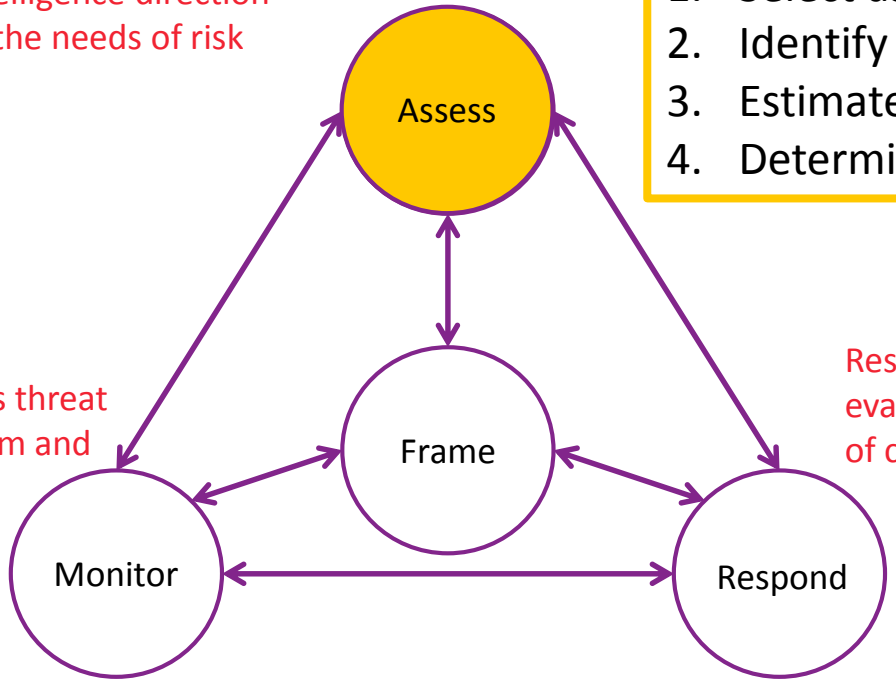
Risky questions needing intelligent answers

- What types of threats exist?
- Which threats have occurred?
- How often do they occur?
- How is this changing over time?
- What threats affect my peers?
- Which threats could affect us?
- Are we already a victim?
- Who's behind these attacks?
- Would/could they attack us?
- Why would they attack us?
- Are we a target of choice?
- How would they attack us?
- Could we detect those attacks?
- Are we vulnerable to those attacks?
- Do our controls mitigate that vulnerability?
- Are we sure controls are properly configured?
- What happens if controls do fail?
- Would we know if controls failed?
- How would those failures impact the business?
- Are we prepared to mitigate those impacts?
- What's the best course of action?
- Were these actions effective?
- Will these actions remain effective?

Intel in the risk management process

Frame: adjust intelligence direction and ops to meet the needs of risk management

1. Select asset(s) at risk
2. Identify risk scenarios
3. Estimate risk factors
4. Determine risk level

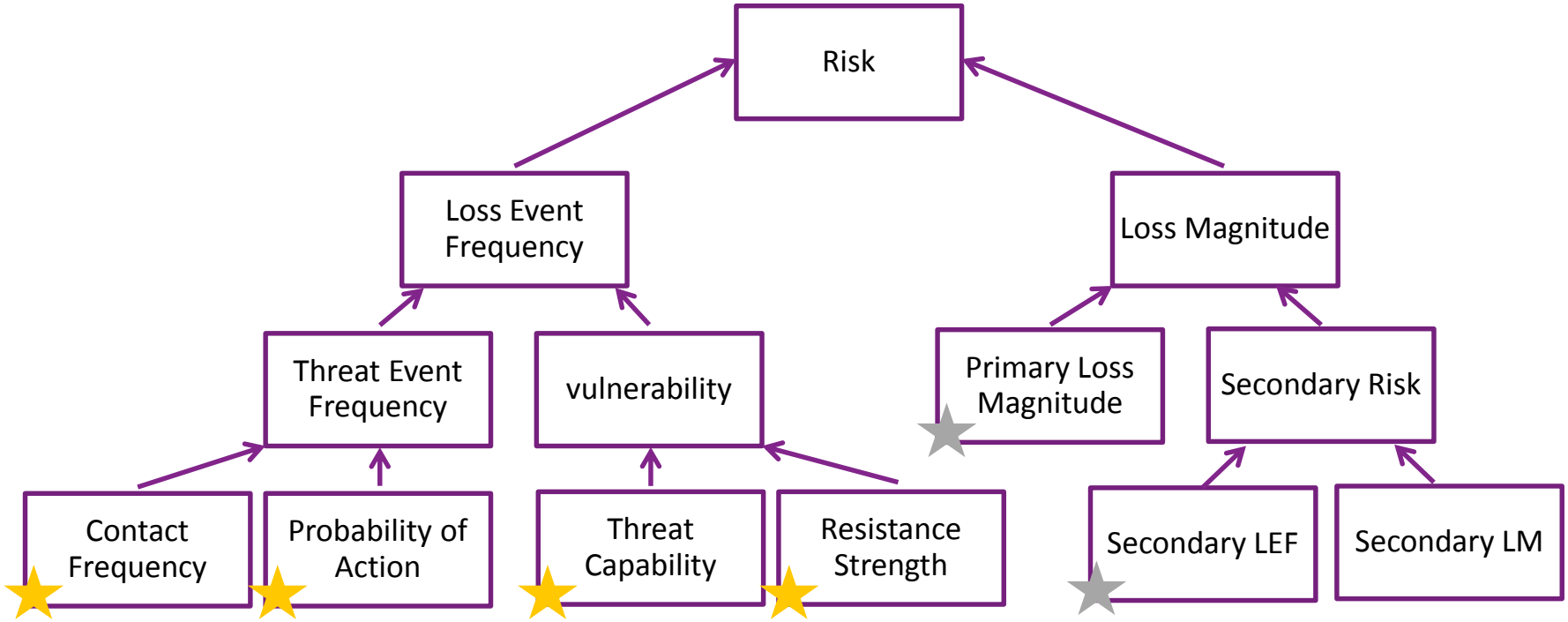


Monitor: intelligence tracks threat changes that warrant system and control changes

Respond: intelligence supports evaluation and implementation of courses of action

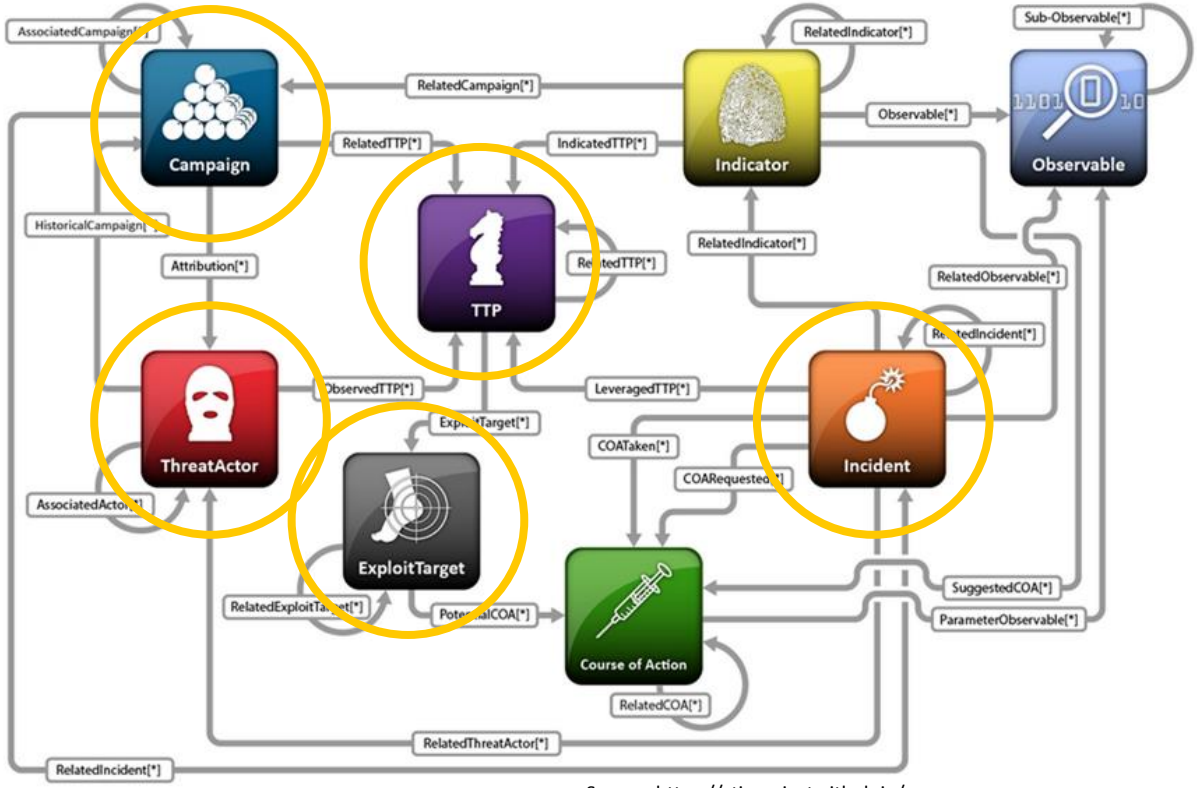
Finding some common ground

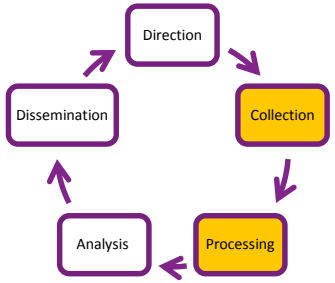
Factor Analysis of Information Risk (FAIR)



Finding some common ground

Structured Threat Information eXpression (STIX)



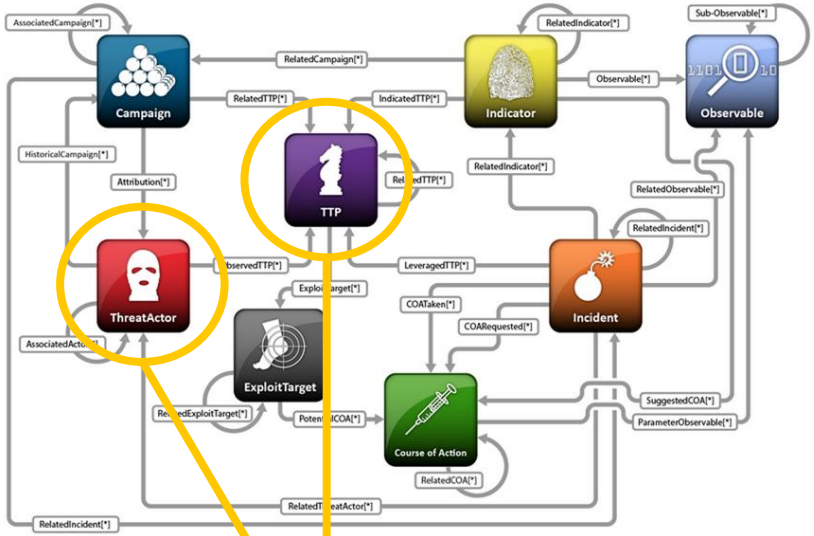


Source: https://stixproject.github.io/

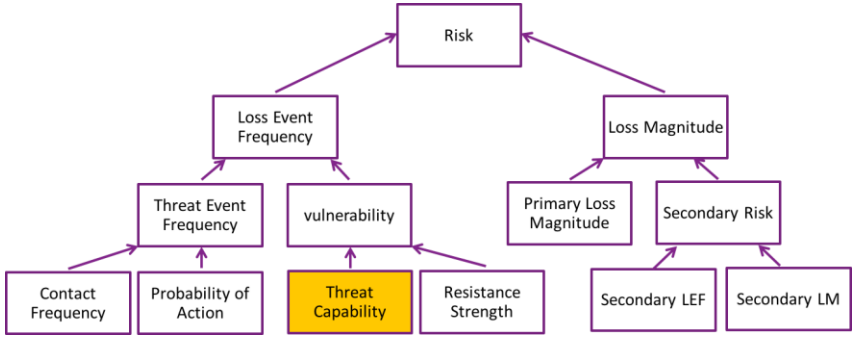
Finding some common ground

A FAIR-ly intelligence approach

Threat Intel (STIX)



Risk Analysis (FAIR)



- *Type*
- *Sophistication*
- *Kill_Chain_Phases*
- *Exploit_Target*
- *Observed_TTPs*

*Initial map: https://threatconnect.com/threat-intelligence-driven-risk-analysis/

Bridging the Gap

Example risk assessment project

"During a recent audit, it was discovered that there were active accounts in a customer service application with inappropriate access privileges. These accounts were for employees who still worked in the organization, but whose job responsibilities no longer required access to this information. Internal audit labeled this a high risk finding."

From: *Measuring and Managing Information Risk*
by Jack Freund and Jack Jones (p 123)

Example risk assessment project

FAIR analysis process flow

From: “Measuring and Managing Information Risk” by Jack Freund and Jack Jones (p 93)

Example risk assessment project

Scenarios associated with inappropriate access privileges

Asset at Risk	Threat Community	Threat Type	Effect
Customer PII	Privileged insiders	Malicious	Confidentiality
Customer PII	Privileged insiders	Snooping	Confidentiality
Customer PII	Privileged insiders	Malicious	Integrity
Customer PII	Cyber criminals	Malicious	Confidentiality

FAIR estimations relevant to the cyber criminal scenario

TEF Min	TEF M/L	TEF Max	TCap Min	TCap M/L	TCap Max
0.5 / year	2 / year	12 / year	70	85	95

From: "Measuring and Managing Information Risk" by Jack Freund and Jack Jones (p 127)

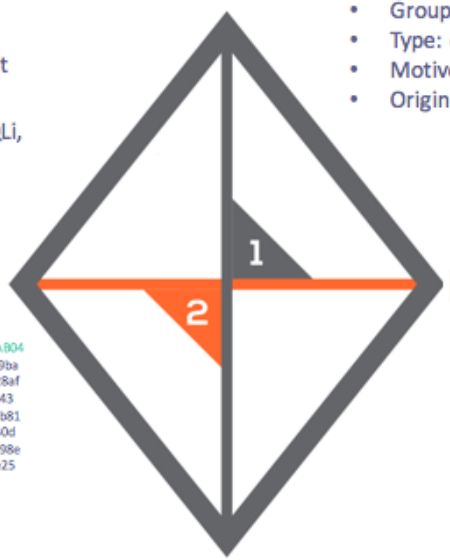
Example risk assessment project

Standard cyber criminal threat profile

Factor	Description
Motive	Financial, Intermediary
Primary intent	Engage in activities legal or illegal to maximize their profit.
Sponsorship	Non-state sponsored or recognized organizations (illegal organizations or gangs).
Targets	Financial services and retail organizations
Capability	Professional hackers. Well-funded, trained, and skilled.
Risk Tolerance	Relatively high; however, willing to abandon efforts that might expose them. Prefer to keep their identities hidden.
Methods	Malware, stealth attacks, and Botnet networks.

Example risk assessment project

Example intelligence-driven adversary profile



1 SOCIO-POLITICAL AXIS

- Intent: High
- Target Geo: US, RU
- Target Sector: FinSrv
- Timeline: 2014 to present

2 TECHNICAL AXIS (TTPS)

- Spear phishing, CSRF, SQLi, DNS hijack, Paremeter tampering
- ATM withdrawals

ADVERSARY

- Group: Anunak/Carbanak
- Type: eCrime
- Motive: Financial or economic
- Origin: Russia

CAPABILITIES

- Files
  - 6FF3AE58A4F9A312602C8D44A308A02AB0437378,58318739e970bafa3ef4567347a09ba3fe3f20b,833a8d88be11807bae966d56a28af7a3cc34dacd,fb434ba4f1eaf9f7f20fe6f49e4375e90fa98069,af7564ee7959142c3a0d9eb8129605c2ae582ca7,dcc932b878a374d47540d43a2dee97f37d68267f,32aa4911bc6a3b8098e496cd88790ff7147ec6ac3,3d1cd366ffe90e25c36c849d720ba6c7329dde7b
- VIRLOCK
- Exploits
  - CVE-2012-2539,CVE-2012-0158
- Tools
  - Mimikatz, MBR Eraser, Network Scanner, Cain & Abel, SSHD backdoor, Ammy Admin, Team Viewer

INFRASTRUCTURE

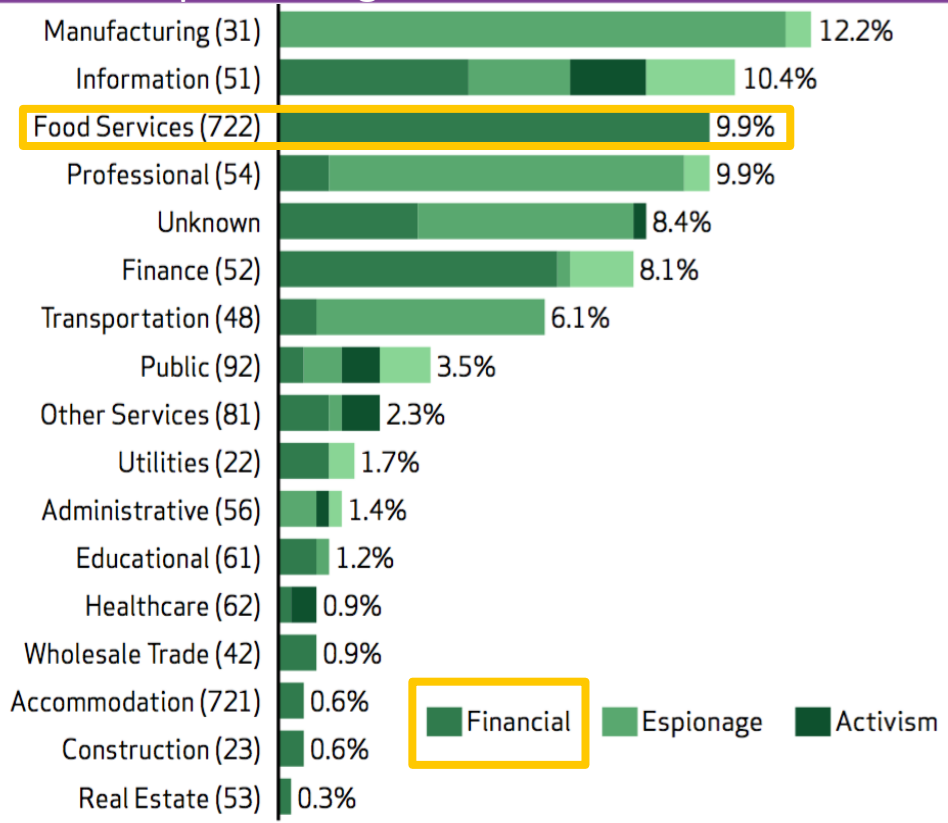
- IPs
  - 78.128.92[.]117
  - 176.31.157[.]62
- Hosts
  - login.collegefan[.]org
  - login.loginto[.]me
  - img.in-travelusa[.]com
- Known to rent adversary infr

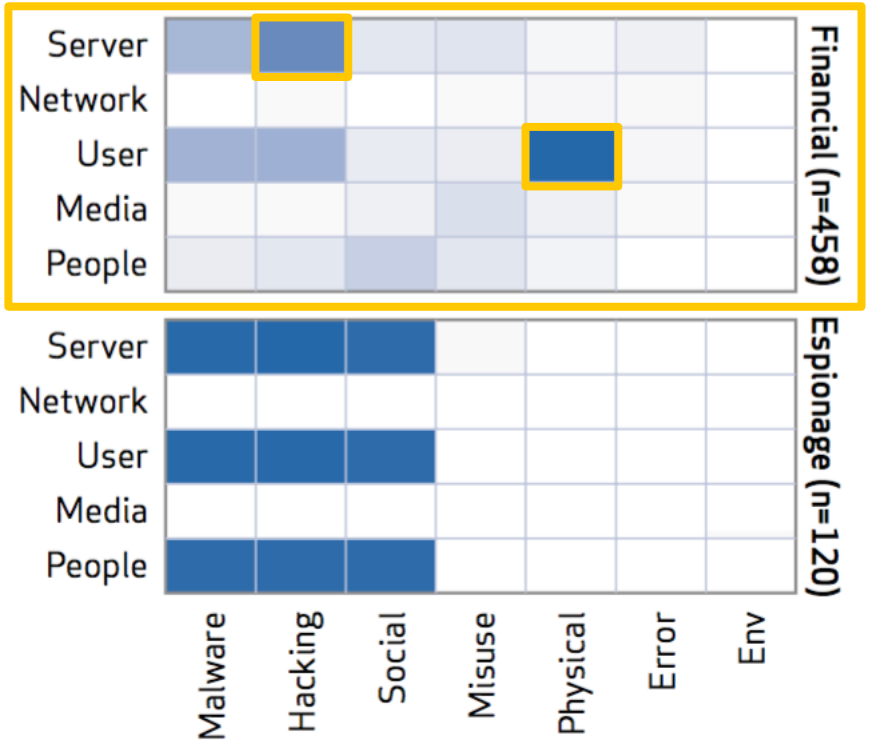
VICTIM

- Organizations: Acme Corp (that's us), 50 Russian banks, British bank
- Assets: Endpoints, servers, ATMs, SWIFT network

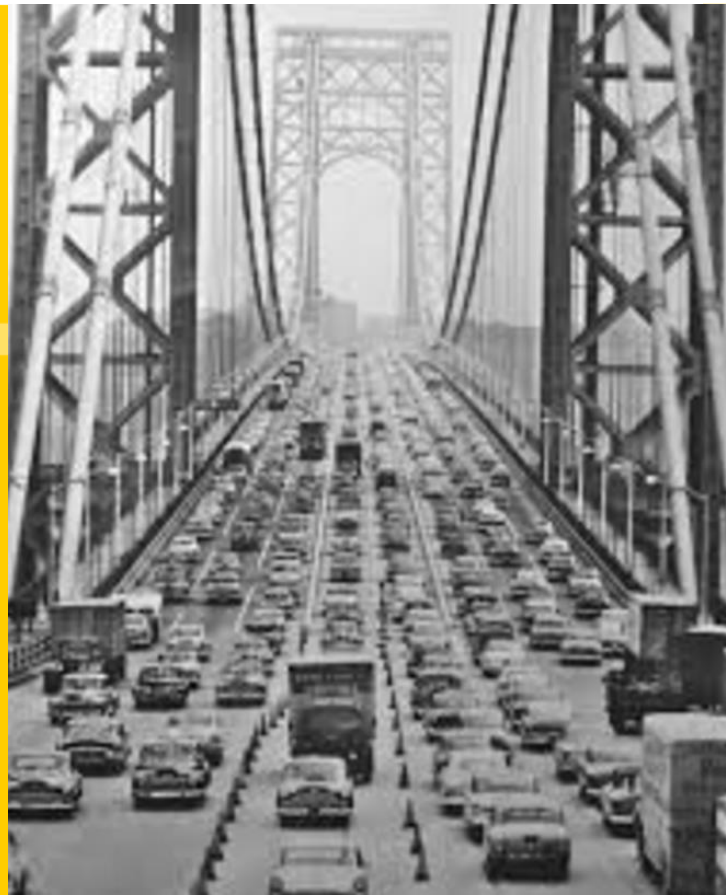
Example risk assessment project

Example intelligence-driven threat community profile...OVER TIME





Crossing the Divide



Making it work in your organization

1. Initiate communication between intel & risk teams
2. Orient intel processes & products around desired risk factors
3. Identify threat communities of interest and create profiles
4. Establish guidelines & procedures for risk assessment projects
5. Encourage ongoing coordination & collaboration
   - Create centralized tools/repositories

~~Underlying assumption~~
Motivating conviction

Good **intelligence** makes smarter **models**;
Smarter models inform **decisions**;
Informed decisions drive better **practice**;
Better practice improves **risk** posture**;**
which, done efficiently,
Makes a successful security **program**.

RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: GRC-T09R

Bridging the Gap Between Threat Intelligence and Risk Management

THANK YOU!!

Wade Baker

VP, Strategy & Risk Analytics
ThreatConnect
@wadebaker

#RSAC