

# Advancing Information Risk Practices

Start Time	Title	Presenter
1:00 PM	Practical Quantitative Risk Analysis	David Musselwhite
1:55 PM	An Inside Look at Cyber Insurance	Jake Kouns
2:45 PM	BREAK	
3:00 PM	Metrics That Matter	Evan Wheeler, Scott Borg, Alex Hutton, Kymberlee Price, Michael Werneburg
3:40 PM	Leveraging Threat Analysis Techniques	Mark Clancy

# **RSA**®Conference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: SEM-M03

## Practical Quantitative Risk Analysis

**David Musselwhite**

---

Team Leader, Enterprise Risk Management  
Quicken Loans, Inc.

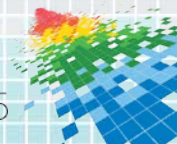
# CHANGE

Challenge today's security thinking



# About Quicken Loans

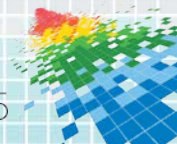
- ◆ Second largest retail home mortgage lender in the nation
- ◆ Based in Detroit, MI and a driving force in the city's resurgence
- ◆ Closed \$140 billion of mortgage volume in 2013-2014.
- ◆ “Highest in Customer Satisfaction for Primary Mortgage Origination” by J.D. Power for the past five years
- ◆ Among the top 30 companies in FORTUNE Magazine's annual “100 Best Companies to Work For” for the last 12 years

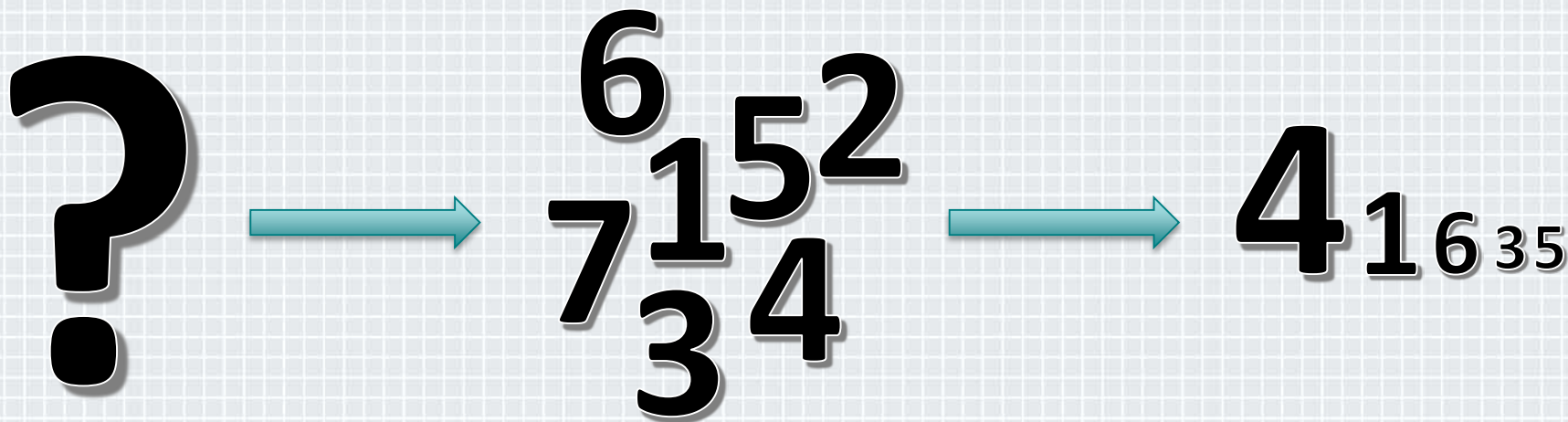




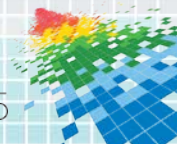
# When I Say Quantitative...

- ◆ There is no such thing as a risk; there are scenarios with associated amounts of risk.
- ◆ risk : dollars :: weight : pounds :: distance : miles
- ◆ Expressed in ranges with varying levels of confidence
- ◆ *“The probable frequency and probable magnitude of future loss,”* or “how many times over the next year is this bad thing likely to happen, and how much is it likely to cost us each time it does.”
- ◆ Likelihood x impact = risk is not quantitative risk analysis



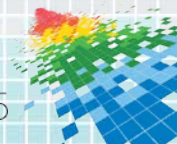


## The Risk Analyst's Task



# What Quantitative ERM Does

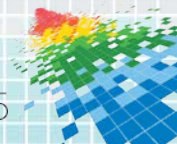
- ◆ Provide, in as close to real-time as possible, high-quality, evidence-based, and actionable information on risks facing the Company
  - ◆ Estimates of future losses
  - ◆ What can we influence and what can we not – what lever to pull
  - ◆ Regular monitoring of key risk indicators
  - ◆ Alerts of failed control testing results





# Quantitative Risk Assessment Process

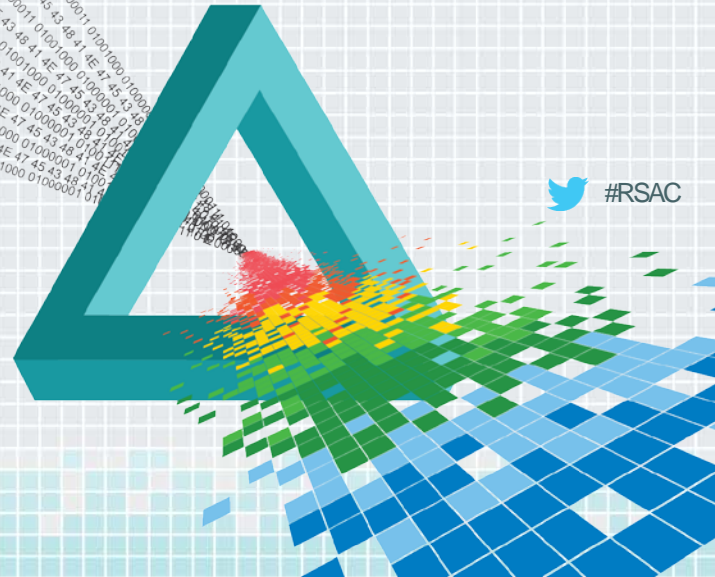
- ◆ Risk Identification
- ◆ Risk Analysis
- ◆ Risk Evaluation
- ◆ Risk Treatment
- ◆ Ongoing Monitoring



# RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

## Case Study

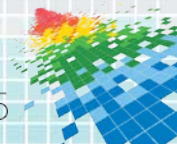




# Risk Identification

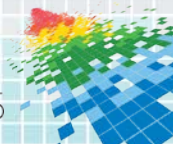
- ◆ What business processes do you execute?
- ◆ What is the successful outcome of each process?
- ◆ How does each process work, step by step?
- ◆ What vendors or information assets, if any, support this process?
- ◆ What sensitive information is handled in this process?

**Failure to respond to FHA “binder requests” in a timely manner.**



# Risk Analysis

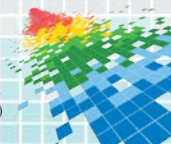
- ◆ FAIR Framework
- ◆ How many times over the next year is this likely to happen?
- ◆ How much might it cost us each time?
- ◆ Gather estimates and run Monte Carlo simulations
  - ◆ Palisades' @Risk, OpenPERT, FairIQ



Context-Specific Question	Minimum	Most Likely	Maximum	Confidence
Over the next year, how many FHA or VA binder requests do you expect Quicken Loans will receive?	1,000	1,800	2,400	Medium
Over the next year, what percentage of binder requests do you estimate will not be fulfilled within ten days of receiving the request?	0%	.05%	.1%	High
Given the current percentage of binder requests that are not fulfilled on time, what is the likelihood of FHA removing our ability to insure our loans using their automated systems?	0%	0%	0.5%	Very High
If FHA were to remove our ability to insure our loans using their automated systems, how much loss would we expect over the next year from having to pay team members to manually execute this process?	\$1,000,000	\$2,500,000	\$4,000,000	Medium

Note: numbers on this slide are dummy values.

**\$0 to \$12,000 of exposure over the next year.**





Most likely annualized risk

One-time maximum loss

**1. Risk Scenario: QL fails to respond to FHA binder requests in a timely manner**

QL regularly receives requests from FHA for full loan files for their QC process. QL has ten days to provide each requested file. If we were to fail to provide these files in a timely manner, FHA could revoke our ability to insure FHA loans using automated submission methods, resulting in loss to the Company from having to pay team members to insure loans using manual processes.



Mar 2015



Estimated Risk Results	Minimum	Most Likely	Maximum
Requests fulfilled late in next year	0	.9	2.4
Probability FHA revokes automation	0%	0%	0.5%
Cost to manually insure FHA loans	\$1,000,000	\$2,500,000	<b>\$4,000,000</b>
<b>Annualized Risk</b>	<b>\$0</b>	<b>\$1,500</b>	<b>\$12,000</b>

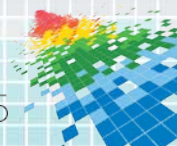
**a. Action Item:** If the business chose to take any actions to further remediate the risk from this scenario, a one or two sentence description would go here.

**CONN:** Who's responsible for completion of this action item?

**Status:** An update on the status of the action item would appear here each month until completion.

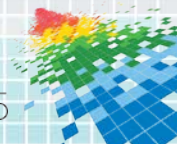
**Target Due Date:** mm/dd/yyyy|

**Estimated Risk After Completion:** Here we'd put information about which variable would be reduced by the action item, and how much estimated risk we'll have after it's completed. This helps the business determine if the juice is worth the squeeze.



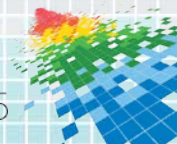
# Risk Evaluation/Treatment

- ◆ Is this too much risk to accept from this scenario?
- ◆ What could we do to reduce exposure, and by how much?
- ◆ Business compares current and future-state risk results
- ◆ Document accept/remediate decision
  - ◆ If any remediation is warranted, track action items to completion



# Ongoing Monitoring

- ◆ Framing a scenario with FAIR makes monitoring easier
- ◆ Key Risk Indicators
  - ◆ # of binder requests fulfilled late in last quarter
  - ◆ Binder requests received / number of team members
- ◆ Key Controls
  - ◆ Verify that all requests were immediately logged
  - ◆ Verify that aging reports are accurate

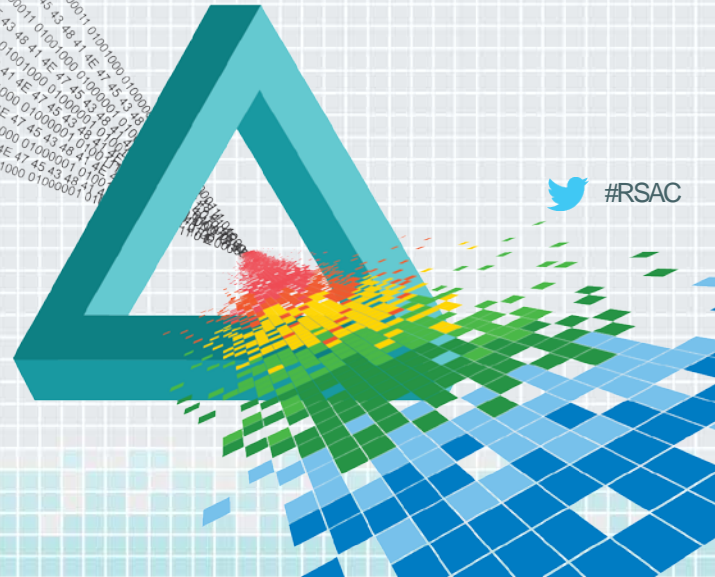




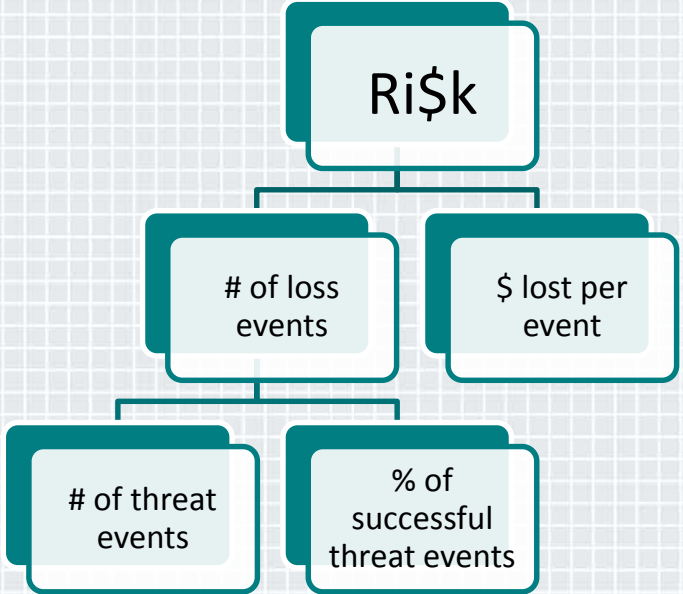
# RSA<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

## Hypothetical Discussion



# Scenario



Privileged team member compromises data on a shared file location resulting in fines against the Company and media coverage/reputation damage

What control changes could we make and how would they impact our risk exposure?



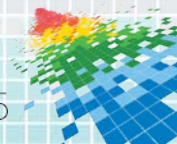
# Contact Information



Quicken Loans, Inc.  
ATTN: David Musselwhite  
1050 Woodward Avenue  
Detroit, MI 48226

[davidmusselwhite@quickenloans.com](mailto:davidmusselwhite@quickenloans.com)

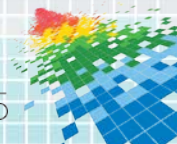
<https://www.linkedin.com/in/riskguydavid>





# Advancing Information Risk Practices

Start Time	Title	Presenter
1:00 PM	Practical Quantitative Risk Analysis	David Musselwhite
1:55 PM	An Inside Look at Cyber Insurance	Jake Kouns
2:45 PM	BREAK	
3:00 PM	Metrics That Matter	Evan Wheeler, Scott Borg, Alex Hutton, Kymberlee Price, Michael Werneburg
3:40 PM	Leveraging Threat Analysis Techniques	Mark Clancy



# **RSA**®Conference2015

San Francisco | April 20-24 | Moscone Center

## **CHANGE**

Challenge today's security thinking

SESSION ID: SEM-M03

# An Inside Look at Cyber Insurance

**Jake Kouns**

---

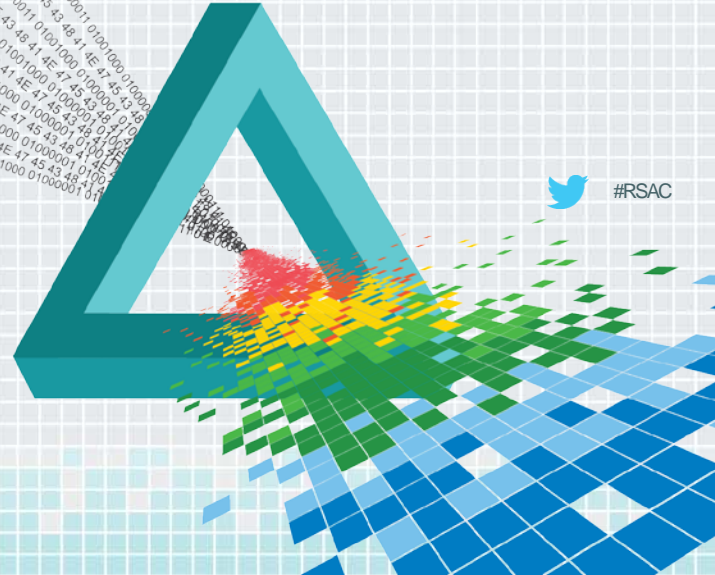
CISO  
Risk Based Security  
@jkouns



# RSA<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

# State Of Security



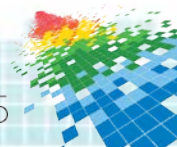




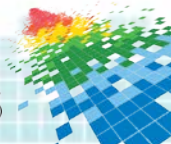
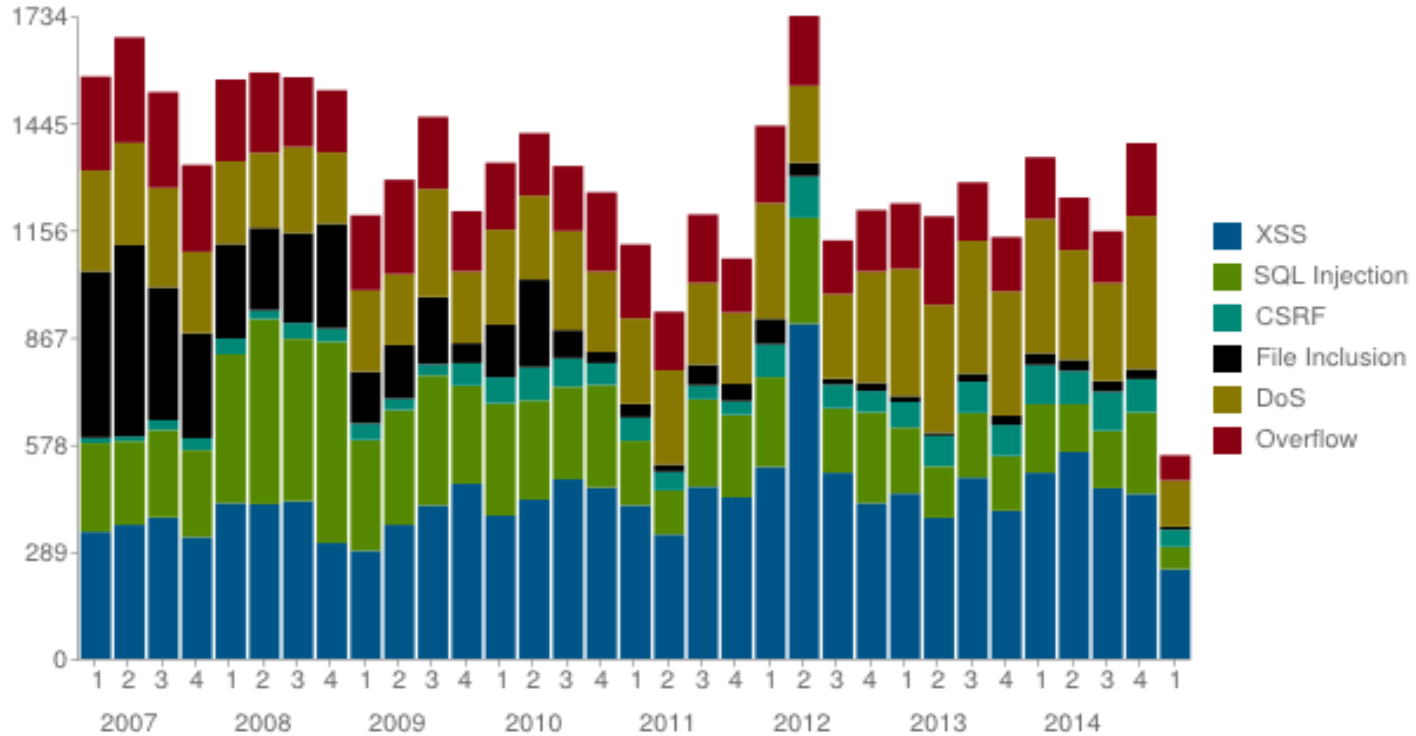
## Buying Into the Bias: Why Vulnerability Statistics Suck



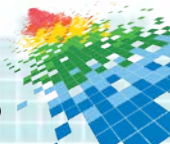
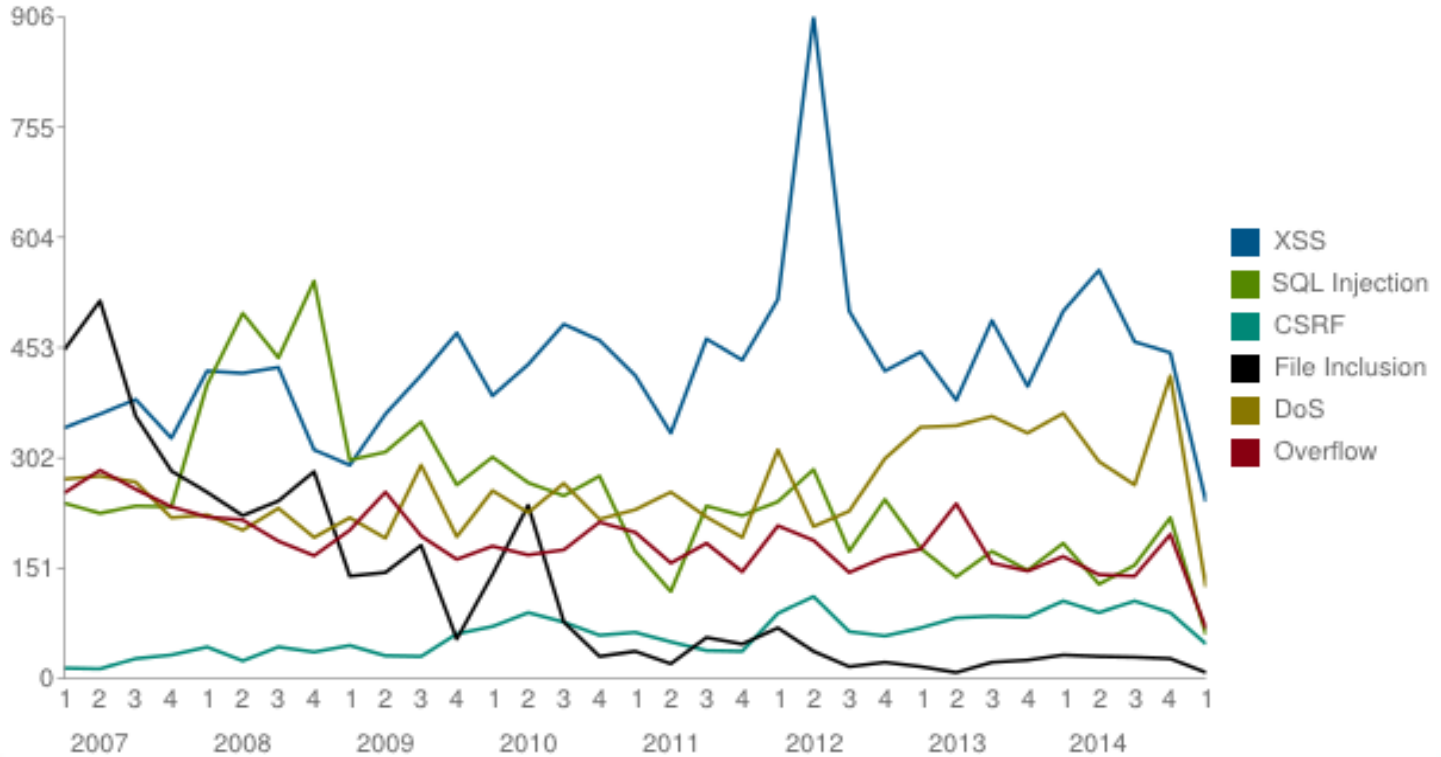
Steve Christey (MITRE) & Brian Martin (OSF)



## Vulnerabilities in OSVDB by Quarter by Type

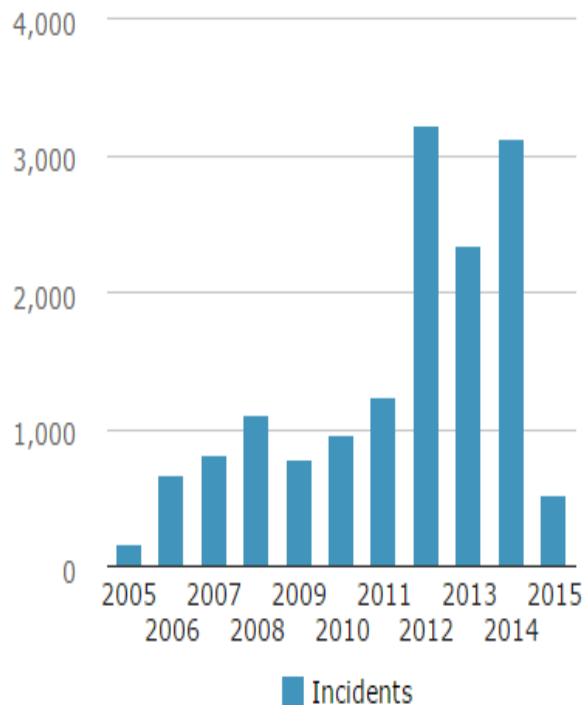


## Vulnerabilities in OSVDB by Quarter by Type

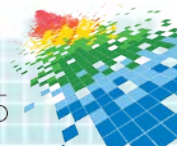
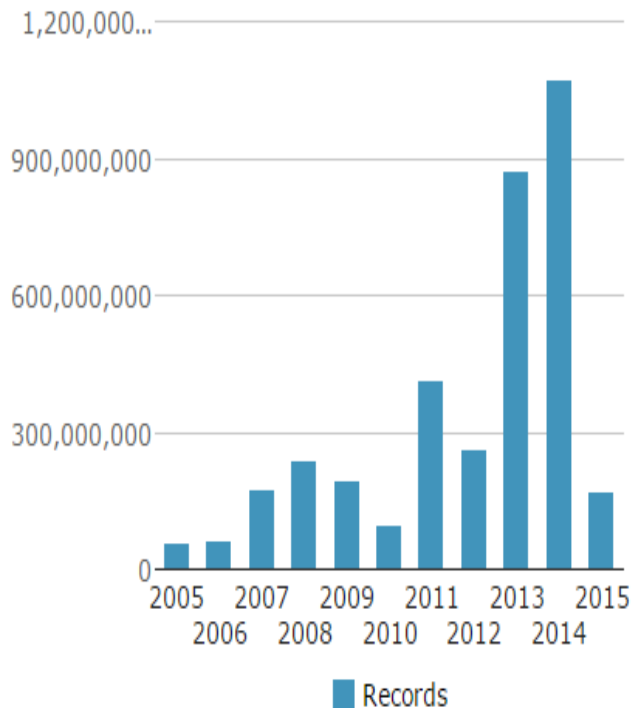




## # Of Incidents Over Time

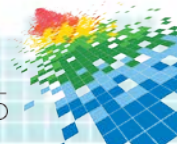


## # Of Records Lost Over Time



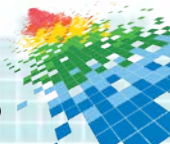


Only a matter of when for most organizations?





## Data Breaches cost organizations money?

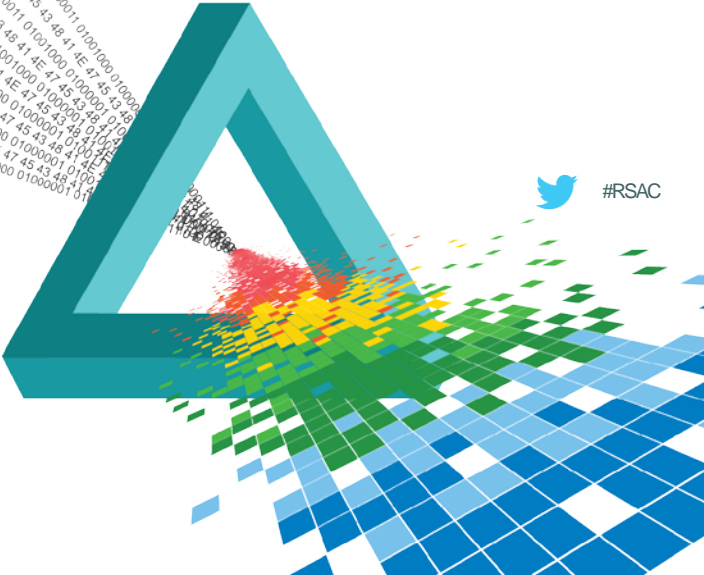




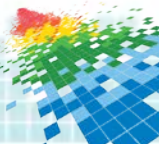
# RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

# Risk Management

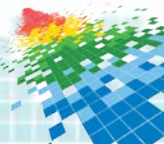


## Perfect Security?

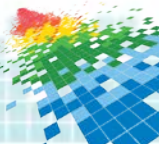
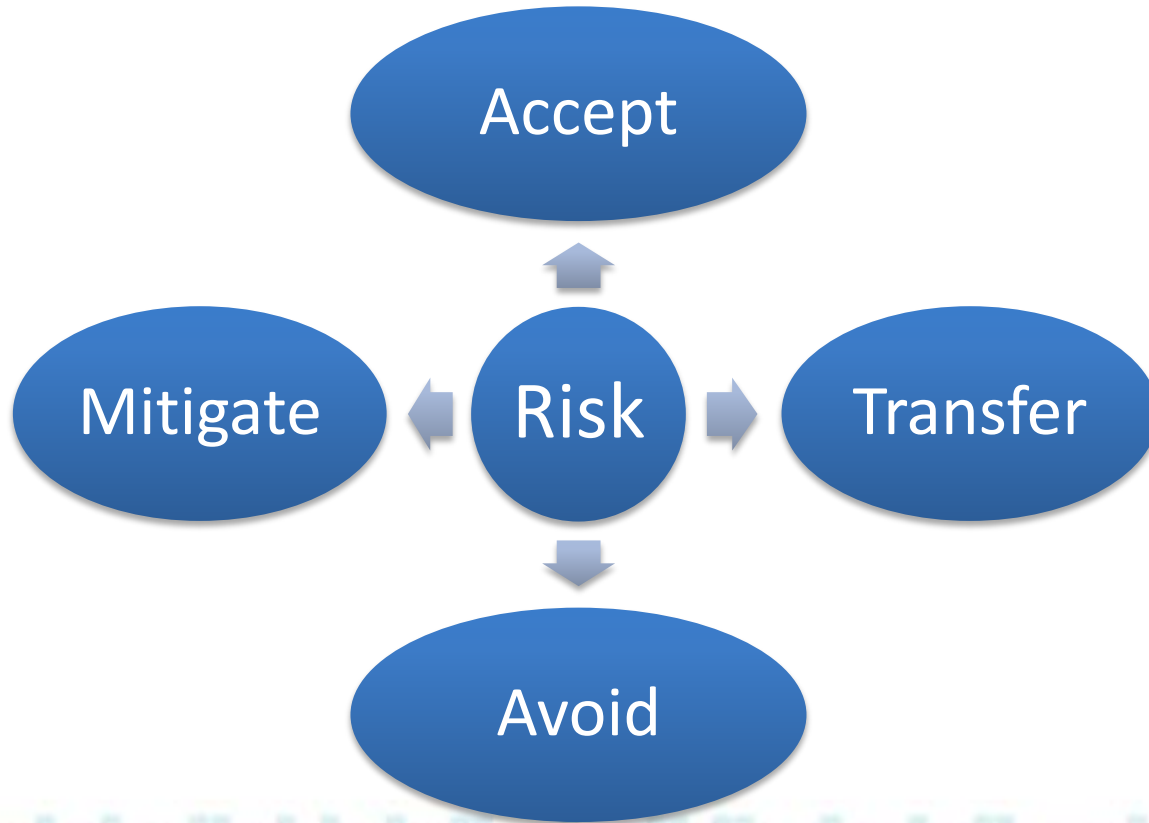


## Law of Diminishing Returns

$$\frac{1}{X} \sum_{i=1}^x \frac{1}{2^{i-1}} = D$$

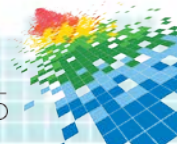






# Transfer Options

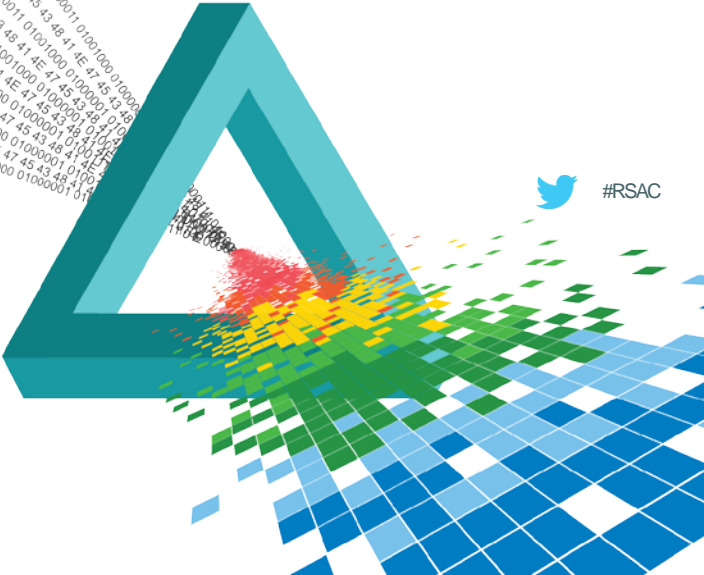
- Outsourcing
  - Contracts & Agreements
  - Insurance



# RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

# Insurance

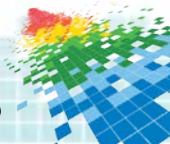


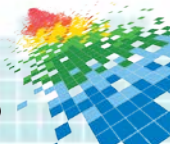
#RSAC



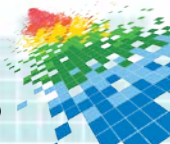
- Insurance is purchased for numerous reasons:
  - Reducing liability
  - Loss recovery
  - Legal requirements
  - Securing loans and/or investments
  - Improving business image and stability
  - Peace of mind
- Typically purchased for most valuable assets

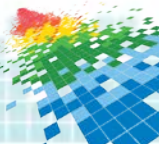






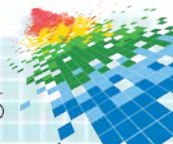






## Why haven't more organizations bought Cyber Liability?:

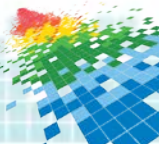
- They have “unbreakable” security controls?
- They think the coverage won't last or respond?
- They don't believe its a good spend of budget?
- They are not aware of the market?
- Something else?
- Perhaps, organizations don't truly understand it?





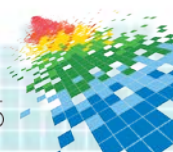
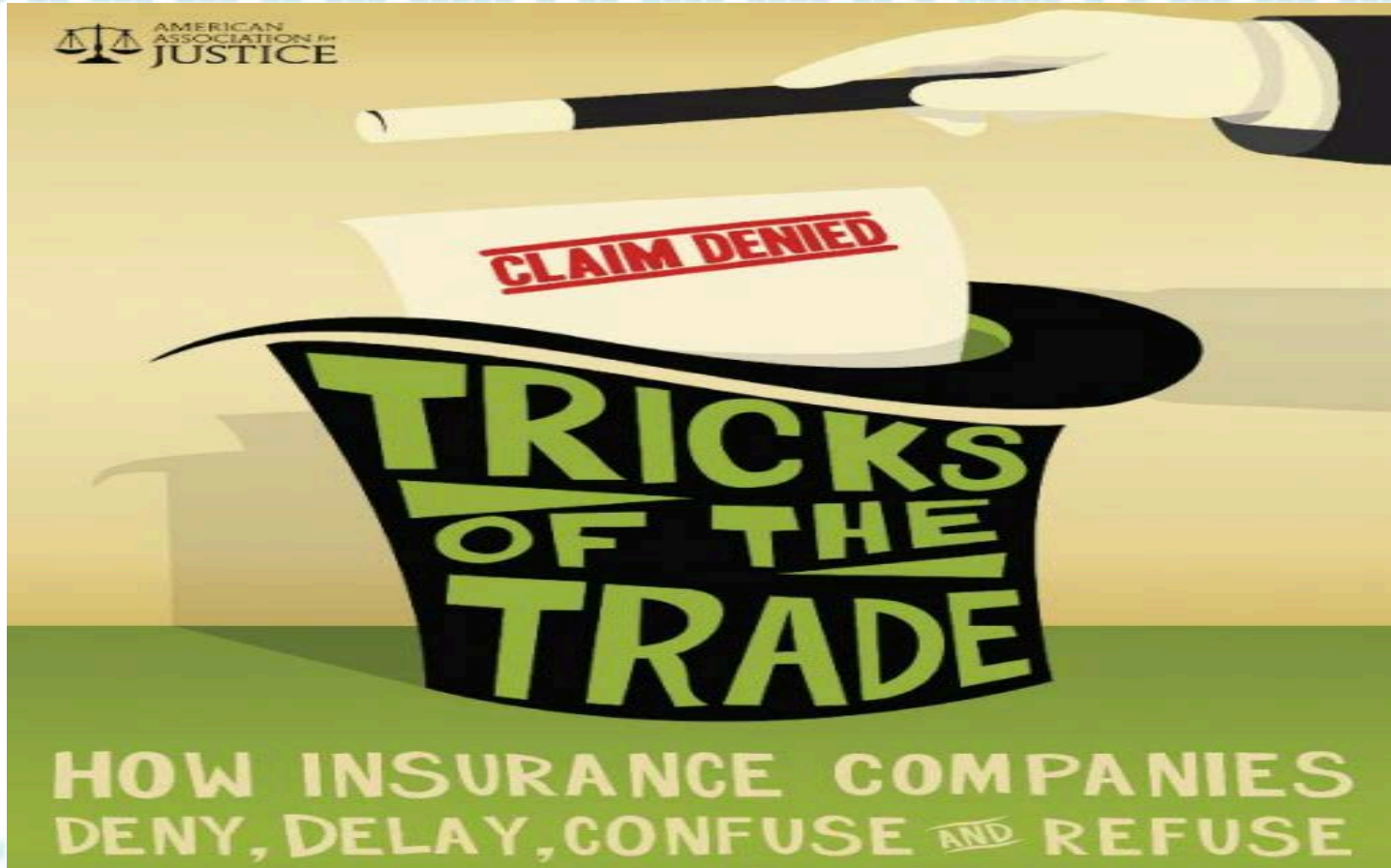
Trust The Salesman!

#RSAC



But is it well deserved?

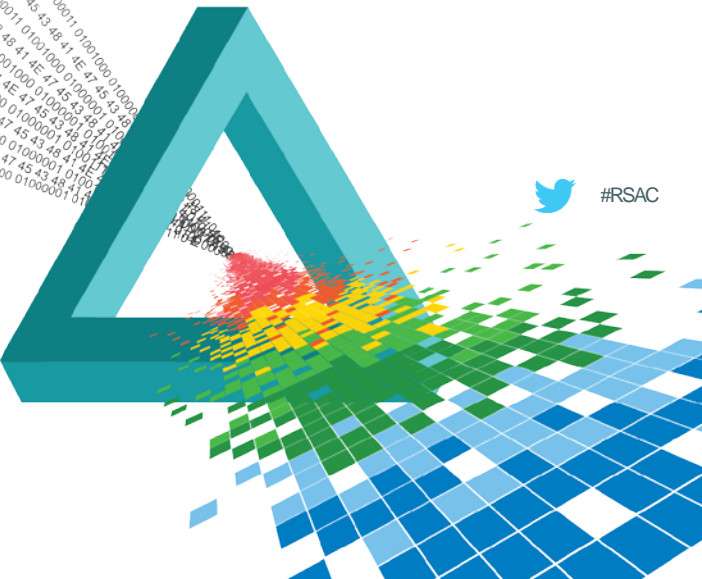
#RSAC



# RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

# Cyber Liability Insurance



- Two forms of distribution, P&C insurance industry
- Wholesale
  - Carrier -> Broker -> Agent -> End Insured
- Retail
  - Carrier -> Agent -> End Insured
  - Carrier -> End Insured
- Pricing: Admitted or Non-Admitted



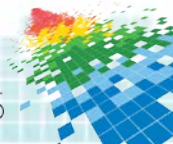


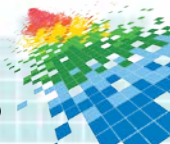
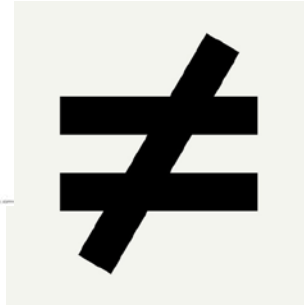
## Many Names, Little Commonality

- Cyber Liability
- Privacy Injury Liability
- Network Security Liability
- Data Privacy
- Theft of Digital Identification
- Cyber Extortion
- Internet Liability



- **Annual premium volume information about the U.S. Cyber Risk market is hard to come by,**
  - Estimated annual gross written premium is in the **\$2 Billion range** (up from \$1.3 Billion in last year's report).
  - Betterly Report June 2014
- **40+ Carriers have a stand alone Cyber Liability Product**
  - Many, many more with packaged policy or excess
- **Commonly called the next EPLI**





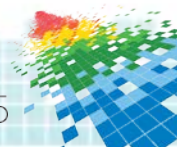
## First Party

Pays to fix the things  
we own when  
damaged

## Third Party

Pays others when our  
actions (or inaction)  
causes harm

As a result of a security event including data  
compromise

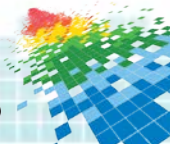




## Third Party



## First Party



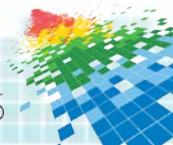
## Why does this matter?

Because it means organizations can buy a policy that can cover *both*

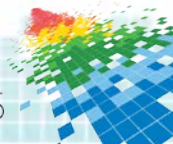
➤ Security event recovery costs

&

➤ Protection from lawsuits arising out of a data compromise

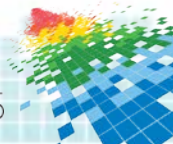


- **3<sup>rd</sup> Party Liability (Claims Made)**
  - Transmission of malicious code to other networks
  - Use of your network to harm other 3<sup>rd</sup> parties
  - Cost to reissue credit & debit cards
- **1<sup>st</sup> Party Exposures (Occurrence)**
  - Notify affected individuals & credit monitoring
  - Restoration of the system & extra expense to remain functional
  - Security consultants, legal notices
  - Payment of extortion demands, lost time, lost monies, lost business
- **Website Liability**
  - Intellectual property risk from the look, feel and content
  - Liability from defamatory content on your site, intensified by the search potential of the Internet
  - Usage of Social Media



## Unauthorized Access To Named Insured’s System

- Access gained as the result of fraud or deception
- Authorized user for unauthorized purposes
- Introduction of fraudulent or destructive code
- The threat to initiate malware for the purpose of extorting money or other valuable consideration
- Loss of a laptop or other digital storage device
- Whether or not for profit or gain

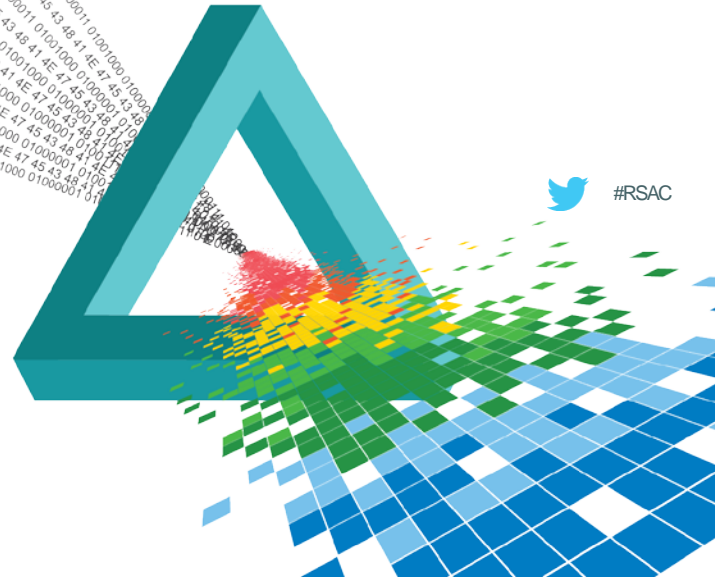




# RSA® Conference 2015

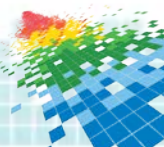
San Francisco | April 20-24 | Moscone Center

# Cyber Liability “Gotchas”



#RSAC

But I buy GL or  
professional  
liability  
insurance, so  
I'm covered for  
all this stuff,  
aren't I?



[SC Magazine](#) > [News](#) > Zurich seeking immunity from covering Sony over breach

## Zurich seeking immunity from covering Sony over breach

Dan Kaplan July 22, 2011

 PRINT  EMAIL  REPRINT  PERMISSIONS TEXT: [A](#) | [A](#) | [A](#)

 Tweet

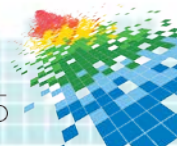
22

Sony's insurer is contesting any obligation to cover the electronics giant for costs related to lawsuits filed over its massive [PlayStation Network](#) breach earlier this year.

In a complaint filed with the state Supreme Court in New York, Zurich American Insurance Co. is seeking "declaratory relief" from having to defend and possibly compensate Sony over class-action lawsuits or state attorneys general actions filed in response to the breach.

### RELATED ARTICLE

- [Sony faces new PSN hack](#)
- [Sony expects to \\$171 million ov](#)
- [Sony PlayStation online after intru](#)
- [Anonymous sp](#)  
[Sony hack: "It w](#)





Home News & Commentary Authors Slideshows Video Radio Reports White Papers Events

ATTACKS/BREACHES

APP SEC

CLOUD

ENDPOINT

MOBILE

PERIMETER

RISK

## ATTACKS/BREACHES

10/20/2014  
07:30 AM



Ericka  
Chickowski  
News

Connect Directly



6 COMMENTS

[COMMENT NOW](#)

Login



50%



50%



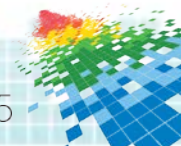
63

# Why You Shouldn't Count On General Liability To Cover Cyber Risk

**Travelers Insurance's legal spat with P.F. Chang's over who'll pay breach costs will likely illustrate why enterprises shouldn't think of their general liability policies as backstops for cyber risk.**

As the legal troubles for P.F. Chang's restaurant chain kept piling up over the [breach discovered this summer](#) affecting 33 of its locations, its legal team made an insurance end-around play that many enterprises try after a breach. It filed a claim for coverage under its comprehensive general liability (CGL) policy. But a lawsuit filed earlier this month from its general liability insurer, Travelers Insurance, offers a good lesson to organizations on why this play rarely works.

Travelers asked the US District Court in Connecticut to clear it of any obligation to defend or indemnify the restaurant company during breach litigation. Its argument to the court: that not only is a breach like this not covered in its general policy definitions, but that even if it were, the restaurant company hadn't met a \$250,000 basement floor limit up to which the firm needed to self-insure for covered events.





# Discovery of 13-Year Hacking Scheme Highlights Questions About Cyber Insurance Coverage

Posted on September 11, 2014

Hunton & Williams [Insurance Litigation & Counseling](#) partner [Lon Berk](#) reports:

An Israeli security firm recently uncovered a hacking operation that had been active for more than a decade. Over that period, hackers breached government servers, banks and corporations in Germany, Switzerland and Austria by using over 800 phony front companies (which all had the same IP address) to deliver unique malware to victims' systems. The hackers purchased digital security certificates for each phony company to make the sites appear legitimate to visitors. Data reportedly stolen included studies on biological warfare and nuclear physics, plans for key infrastructure, and bank account and credit card data.

The attack highlights concerns, not only about cybersecurity, but also about the extent to which such breaches are covered by specialty cyber insurance policies. These policies typically are written on a claims-made basis; that is, a policy responds to a claim made during its policy period. However, the policies also restrict coverage to events occurring on or after a "retroactive date." Given that these types of breaches sometimes result from events stretching over years, even decades, and a breach may not be discovered for years, the retroactive date may limit the available coverage. If coverage for a loss related to a data breach is blocked by a cyber policy's retroactive date, it may be necessary to look to standard general liability policies for coverage.



## STAY CONNECTED



✉ Subscribe by Email



## TOPICS

## ARCHIVES

## RECENT UPDATES

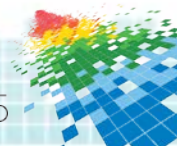
Video: In Depth – Sotto Details Who, What, Why of Today's Cyber Threat Landscape

2015

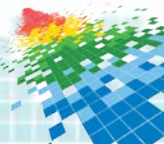
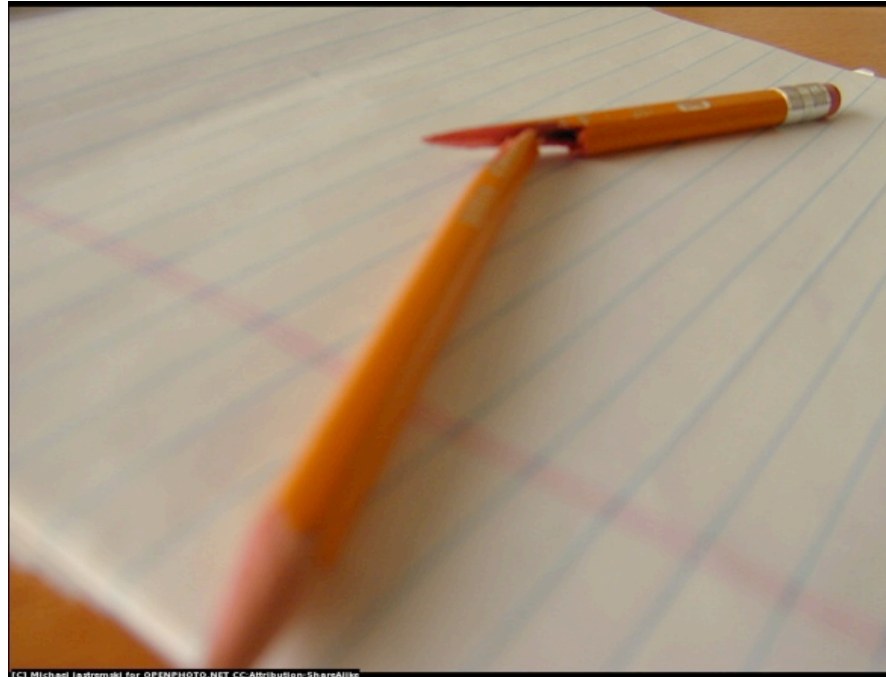




**As helpful as some of these policies can be,  
expect some things not to be covered**



# Reputation Damage

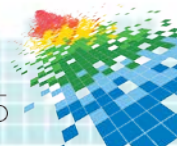




Regular maintenance

Upgrades

Fixes

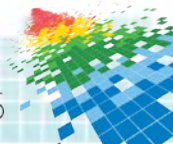




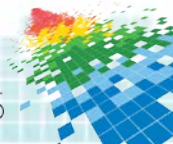
The economic  
value of data



Data or systems in  
the care, custody or  
control of others

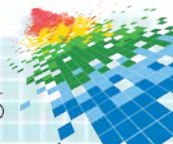


- Failure to encrypt data (typically portable devices)
- Failure to maintain or take reasonable steps to maintain security
- Coverage limited to web site and Internet activities only
- Widespread virus / Spyware
- Failure to comply with PCI standards
- Wireless
- Cloud / SaaS
- Business Income Loss





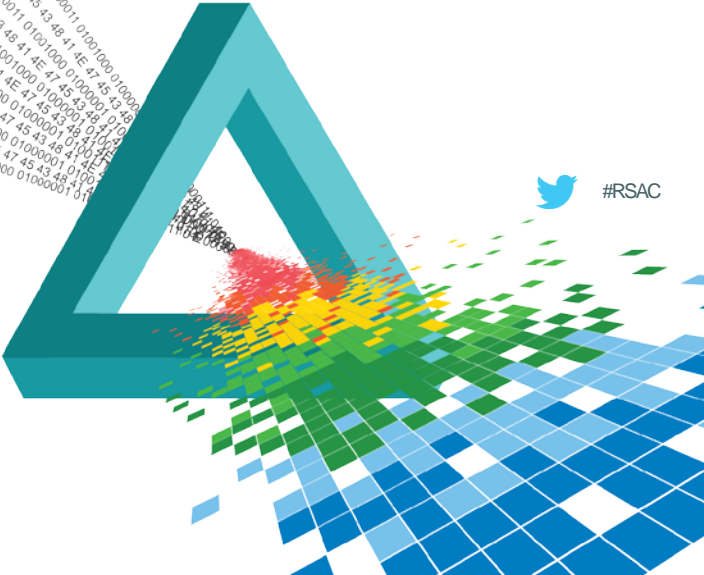
- Notification Costs
- Credit Monitoring
- Public Relations Expenses
- Forensic Costs
- Extortion Costs
- Reward Reimbursement



# RSA<sup>®</sup>Conference2015

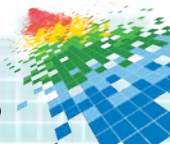
San Francisco | April 20-24 | Moscone Center

# Underwriting and Pricing



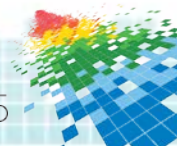
 #RSAC





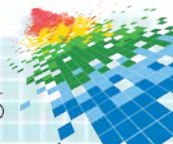
## Applications can be 1 page or run up to 12 pages and require input from multiple departments

4. Does the Applicant have :		
A. a disaster recovery plan?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
B. a business continuity plan?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
C. an incident response plan for network intrusions and virus incidents?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
How often are such plans tested? _____		
5. Does the Applicant have a program in place to test or audit security controls on an annual or more frequent basis?		
	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If yes, please summarize the scope of such audits and/or tests: _____		
6. Does the Applicant terminate all associated computer access and user accounts as part of the regular exit process when an employee leaves the company?		
	<input type="checkbox"/> Yes	<input type="checkbox"/> No
7. Is all valuable/sensitive data backed-up by the Applicant on a daily basis?		
	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If no, please describe exceptions: _____		
8. Is at least one complete back-up file generation stored and secured off-site separate from the Applicant's main operations in a restricted area?		
	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If no, describe the procedure used by the Applicant, if any, to store or secure copies of valuable/sensitive data off-site? _____		
9. Does the Applicant have and enforce policies concerning when internal and external communication should be encrypted?		
	<input type="checkbox"/> Yes	<input type="checkbox"/> No
A. Does the Applicant encrypt data stored on laptop computers and portable media?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
B. Does the Applicant encrypt data stored on back-up tapes?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
C. Does the Applicant encrypt data "at rest" within computer databases?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
10. Does the Applicant enforce a software update process including installation of software "patches"?		
	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If Yes, are critical patches installed within thirty (30) days of release?		
	<input type="checkbox"/> Yes	<input type="checkbox"/> No



## Typical Underwriting Considerations

- Basic security controls
- Type of data processed, stored or transmitted
- Back up procedures for 1st party cover
- History of prior incidents



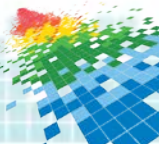
- Underwriting is far from a science
- Most underwriters are not security experts
- Typically written applications
- Model encourages less information not more
- Minimal security controls required are...  
**LOW**
- Typically no scans or audits performed



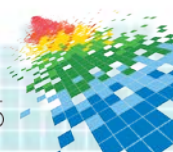
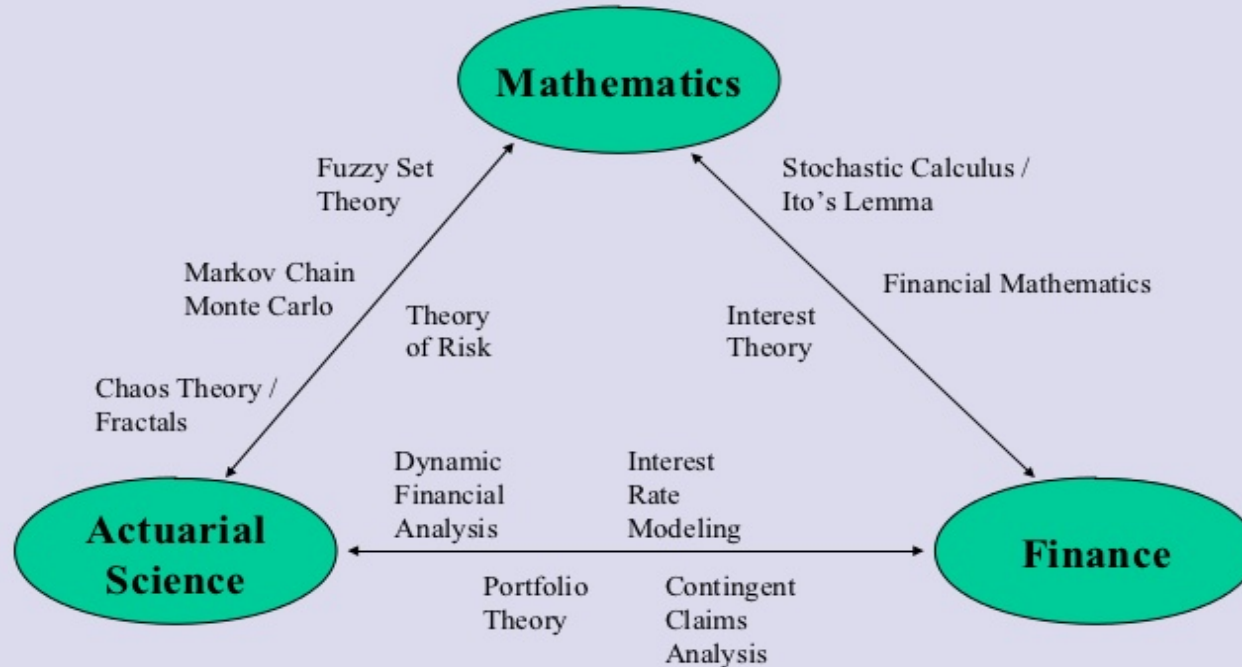


- Carriers do have prohibited classes/industries
- Most the market rates on revenues
- Prices currently vary wildly depending on:
  - Revenues
  - Class of business / industry
  - Records / Data types
  - Controls
- Price may not be appropriate for all organizations
- Deductibles can vary

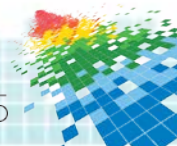




# The Actuarial Science Research Triangle



ACTUARIAL TRIANGLE										
	0	1	2	3	4	5	6	7	8	9
2003	4,788,143	4,302,761	4,180,630	4,422,967	4,489,386	4,486,796	4,513,650	4,515,277	4,509,693	4,513,958
2004	4,806,753	4,461,643	4,339,454	4,363,650	4,353,938	4,346,426	4,370,752	4,359,064	4,357,168	
2005	5,231,472	4,977,968	4,847,570	4,775,849	4,775,313	4,759,982	4,754,577	4,744,064		
2006	5,346,570	5,107,755	5,007,592	4,986,712	4,943,661	4,928,067	4,946,922			
2007	5,713,755	5,577,969	5,435,912	5,422,444	5,393,697	5,446,756				
2008	6,525,093	6,470,660	6,342,424	6,398,339	6,464,857					
2009	5,621,447	5,727,247	5,702,747	5,677,959						
2010	5,587,180	5,693,681	5,806,523							
2011	5,940,868	6,061,189								
2012	6,737,481									







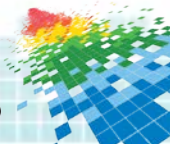
# Willis Fires First Salvo in the Cyber Risk Model Race

FEBRUARY 4, 2015



In announcing what it describes as the “insurance industry’s first cyber risk modeling tool,” **Willis Re**’s new product may be the first shot in a battle among reinsurers and modeling firms to measure and underwrite the growing field of cyber risk.

The new model – **PRISM-Re** – will offer an analysis of the susceptibility to data breach events across the insurer’s portfolio using a ‘common shock’ methodology to encompass the possibility of contagion behavior, according to a company statement issued yesterday. Based upon the latest exposure data, the model estimates the “frequency of data breaches and the potential severity of insured losses arising from those events.



## **CFO** What's the Cost of a Cyberattack?

A flurry of attempts to model the risk of a corporate cyberattack hasn't provided many answers.

### **Modeling Cyber Risk**

That, however, may be the easy part of the assessment. Much tougher is gauging the likelihood that a company's most valued data will be threatened—that is, how alluring a target is it for cybercriminals? To answer that question, a growing number of insurance-related firms are developing models of the risk fed by data on corporate cyber break-ins. The models represent a chance for finance chiefs and risk managers to get a better sense of their companies' risks of being hacked.

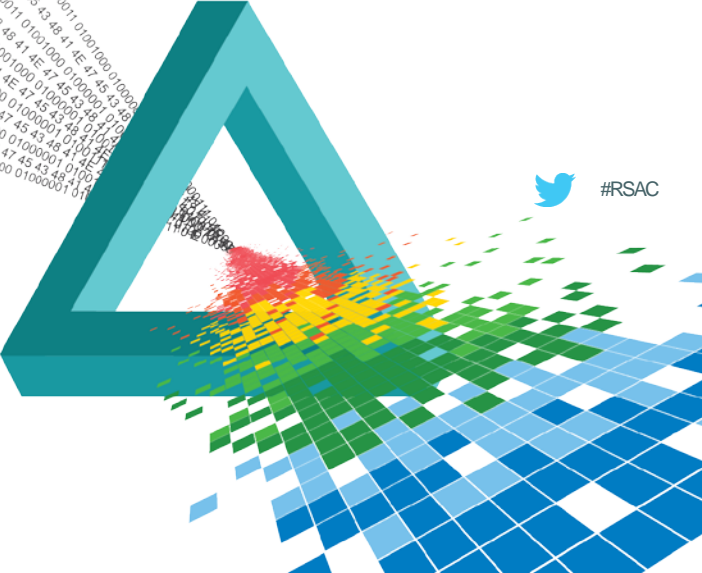
The history of cyberattacks is short, however, and information of which such events can cost a company is hard to come by. Relative to hazards like earthquakes, fires, and lawsuits—not to mention economic perils like capital-market volatility—the threat of bad actors breaking into computer systems and stealing vital information or creating havoc is in its infancy. Unlike, say, the knowledge amassed about hurricanes in the United States, which have been tracked for about 165 years, data about corporate cybercrime has only been recorded since the emergence of the Internet as a vehicle of commerce in the mid-1990s.



# RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

# Integrating Cyber Insurance



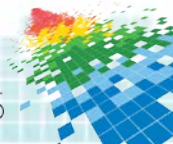
 #RSAC



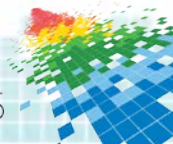
- Executives understand risk:
  - Avoid, Mitigate, Accept and Transfer
- Organizations understand the need to protect their most important assets and transfer risk already:
  - Property (Buildings)
  - Casualty Coverage (Accidents)
  - Employment Practices Liability & Workers Comp (People)
  - Professional Liability - Errors and Omissions
- Speak to executives in terms they understand



- Lets estimate costs for a security program for a small business (Approximately \$2-5M revenue)
  - Security Staff
  - Security Software / Hardware
    - Antivirus, Encryption, Firewall, IDS, DLP, Compliance, Scanners, etc.
  - Security Consulting
    - External Vuln Scans, Pen Tests, PCI compliance, Legal, Awareness, etc.



- For sake of argument.....
- Lets say it costs a business with \$2-5M in revenues spends approximately \$100,000/per year on security
- Not including initial investment costs
- This estimate is extremely low if they are to implement proper security
- Should they be spending more? Certain %?
- Does this ensure that they won't have a breach?



- Typical costs for Cyber Insurance are currently extremely reasonable
- Minimum premiums can be \$1,500 for \$1M in coverage
- Includes many Risk Management Services
- Pricing can change based on industry and controls
- Many smaller companies confused by security and are not yet doing anything

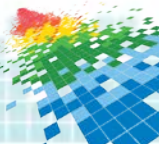





- Larger organizations can also get Cyber Insurance for a reasonable cost
- Large hospital with \$2B in revenues premium estimates:
  - \$100,000 for \$1M in coverage
  - \$200,000 for \$5M in coverage
- Can build towers with Limits are available up to \$250M
- Pricing can change based on industry & controls
- Larger organizations have not shown much interest thus far in actually using Risk Management Services








Despite the  
limitations, there is  
real value found in  
these policies.





## Homeland Security

Topics
How Do I?
Get Involved
News
About DHS

[Home](#) > [News](#) > [Publications](#) > **Cybersecurity Insurance**

Share / Email

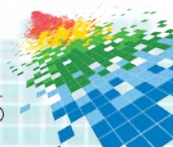
- News**
- [Blog](#)
- [Data](#)
- [Events](#)
- [Fact Sheets](#)
- [In Focus](#)
- [Media Contacts](#)
- [Multimedia](#)
- [National Terrorism Advisory System](#)

## Cybersecurity Insurance

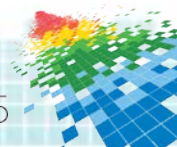
Cybersecurity insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage. A robust cybersecurity insurance market could help reduce the number of successful cyber attacks by: (1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection. Many companies forego available policies, however, citing as rationales the perceived high cost of those policies, confusion about what they cover, and uncertainty that their organizations will suffer a cyber attack.

In recent years, the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD) has brought together a diverse group of private and public sector stakeholders – including insurance carriers, risk managers, IT/cyber experts, critical infrastructure owners, and social scientists – to examine the current state of the cybersecurity insurance market and how to best advance its capacity to incentivize better cyber risk management.

Attachment	Size
 <a href="#">July 2014 Insurance Working Session Readout Report</a>	730.99 KB
 <a href="#">February 2014 Cyber Insurance Health Care Use Case Roundtable</a>	834.43 KB
 <a href="#">May 2013 Cyber Risk Culture Roundtable</a>	831.32 KB
 <a href="#">November 2012 Cybersecurity Insurance Workshop Readout Report</a>	943.02 KB



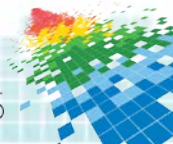
## Could insurance force uniform standards and increase security for all?



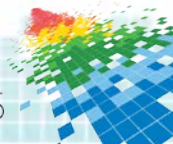


- Effective security programs cost \$\$\$
- Yet, can still be compromised
- Cyber Liability cheaper than most controls and provides serious financial coverage including security services
- While there are “gotchas”, there are legit policies out there
- If you are a CISO and you have a breach. What do you want to say?
  - Whoops? Sorry.
  - We are covered. Lets file a claim.





- Recommended Actions:
  - Continue to invest in the appropriate security controls
  - Define a response plan in case of a data breach
  - Understand your exposures
  - Understand your data and number of records



- Recommended Actions (cont):
  - Discuss transferring a portion of risk in the form of Cyber Liability insurance with management
  - Determine coverage that would be important to your organization
  - Determine amount of desired coverage
  - Obtain a Cyber Liability quote
  - If appropriate, integrate Cyber Liability into your risk management plan

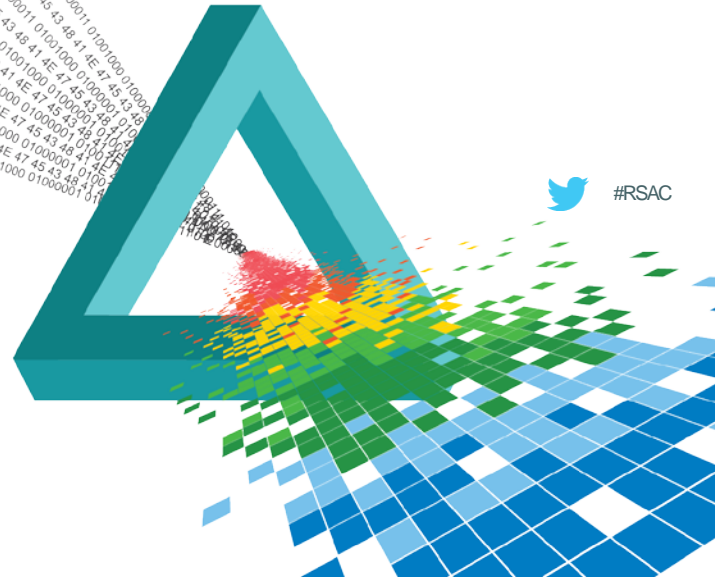




# RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

# Discussion!



# RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

## CHANGE

Challenge today's security thinking

SESSION ID: SEM-M03

# An Inside Look at Cyber Insurance

**Jake Kouns**

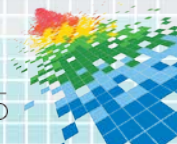
---

CISO  
Risk Based Security  
@jkouns



# Advancing Information Risk Practices

Start Time	Title	Presenter
1:00 PM	Practical Quantitative Risk Analysis	David Musselwhite
1:55 PM	An Inside Look at Cyber Insurance	Jake Kouns
2:45 PM	BREAK	
3:00 PM	Metrics That Matter	Evan Wheeler, Scott Borg, Alex Hutton, Kymberlee Price, Michael Werneburg
3:40 PM	Leveraging Threat Analysis Techniques	Mark Clancy



# RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: SEM-M03

## Metrics That Matter

# CHANGE

Challenge today's security thinking



**Evan Wheeler - Moderator**

**Scott Borg**

U.S. Cyber Consequences Unit

**Alex Hutton**

Large Financial Institution

**Michael Werneburg**

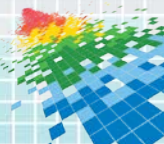
PortfolioAid

**Kymerlee Price**

Bugcrowd

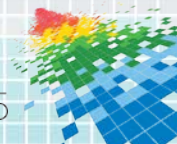






# Apply Slide

- ◆ Contextualize why it matters
- ◆ Understand your organization's tolerance
- ◆ There are different categories of metrics, can they can be misused
- ◆ It's not about fancy tools
- ◆ Look at other disciplines outside information security
- ◆ Ask yourself “so what?”



# Advancing Information Risk Practices

Start Time	Title	Presenter
1:00 PM	Practical Quantitative Risk Analysis	David Musselwhite
1:55 PM	An Inside Look at Cyber Insurance	Jake Kouns
2:45 PM	BREAK	
3:00 PM	Metrics That Matter	Evan Wheeler, Scott Borg, Alex Hutton, Kymberlee Price, Michael Werneburg
3:40 PM	Leveraging Threat Analysis Techniques	Mark Clancy



# RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: SEM-M03

## Leveraging Threat Analysis Techniques

**Mark Clancy**

CISO / CEO  
DTCC / Soltra

# CHANGE

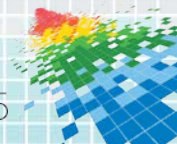
Challenge today's security thinking





# Outline

- ◆ Who are we worried about and why
- ◆ Analysis vs. Intelligence
- ◆ What do I want vs. What do I have...
- ◆ What does Cyber Threat Intelligence look like?
- ◆ How do I mature my capabilities?
- ◆ What is the “game changer”?



# Who are the adversaries?



## Criminals

- Money
- Money
- And more money
- Large number of groups
- Skills from basic to advanced
- Present in virtually every country
- Up to \$\$\$



## Hacktivists

- Protest
- Revenge
- Large number of groups
- Groups tend to have basic skills with a few 'standout' individuals with advanced technical and motivational skills"
- Up to \$ - \$\$\$



## Espionage

- Acquiring Secrets for national security or economic benefit
- Small but growing number of countries with capability
- Larger array of 'supported' or 'tolerated' groups
- Up to \$\$\$\$+



## War

- Motivation is to destroy, degrade, or deny capabilities of an adversary
- Politics by other means
- Small but growing number of countries with capability
- Non-state actors may utilize 'war' like approaches
- Up to \$\$\$\$ ?
- ...but, a lot less expensive than a nuclear weapon

\$ - Under thousands  
\$\$ - Tens to hundreds of thousands  
\$\$\$ - Millions  
\$\$\$\$ - Tens to hundreds of millions  
\$\$\$\$\$ - Billions



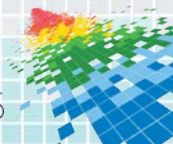
# Company Threat Intensity Map

	Overall	Division A	Division B	Division C	Division D	Division E	New Division 1	New Division 2
<b>Criminal</b>	▼▼	▼▼	▼	▼	▼	▼	▼▼	▼
<b>Hacktivist</b>	▼▼	▼▼	▼	▼	▼▼▼	▼	▼▼	▼
<b>Espionage</b>	▼▼	▼▼▼	-	▼▼▼	-	▼▼▼	▼▼	?
<b>War</b>	▼▼▼	▼▼	-	▼▼▼	-	▼	▼	?



# Analysis vs. Intelligence

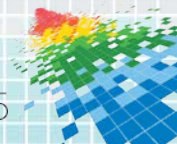
- ◆ Analysis
  - ◆ Looking at past or on going incidents to understand how adversaries are performing their attacks by observing the aftermath of the attack
  - ◆ Looking at sensor data \ forensic to identify attacks with known patterns
  - ◆ Looking at sensor data \ forensic to identify attacks with previously unknown patterns
- ◆ Intelligence
  - ◆ Observing the behaviors, actions, or communication of attackers as attacks are being contemplated, planned, organized, or executed
  - ◆ Projecting or Predicting adversary intentions, capabilities, and motivations along with the confidence level of those projections
- ◆ In the Information Security field we have merged these into “Cyber Threat Intelligence” for the working vocabulary, but recognize this imprecise
  - ◆ Most of the commercial world is “analysis” with a limited amount of “Intelligence”





# What do I want vs. What do I have...

- ◆ What do I want to know?
  - ◆ On April 30<sup>th</sup> at 11:00 UTC we will see 10Gbps/Sec of TCP Traffic mainsite.company.com which will last for 73 Minutes
  - ◆ The attacker is EvilBob aka John Doe who lives in Anytown, FL
  - ◆ He is upset we canceled his favorite TV show CSI Cyber
  - ◆ EvilBob controls 3 known BotNets he runs for a Pharma Spam ring based in Mexico. Attached is a list of all the known Command & Control nodes and the encryption key to the C2 traffic.
    - ◆ In the User Agent of the DoS tool, EvilDoS, there is a unique string of “EVIL-BOB-WANTS-HIS-CSI-CYBER”
    - ◆ Our DDoS mitigation provider can filter any traffic above 1Mbps from the attached sources or with the UA string
  - ◆ EvilBob rents his malware from VendorBob on the darknet forum Hire-a-Bob.nu and he paid \$999/mo per BotNet selecting the 2 hour SLA for support
- ◆ What do I have?
  - ◆ Our current web site traffic is 1 Gbps and our max capacity is 3 Gbps.
  - ◆ We see 1,000 sessions with unusual user agent strings that don't map to known browsers or search engines every month
  - ◆ We are running Apache 2.4.10 which is vulnerable to CVE-2014-3583, but we are upgrading on 3-May-15



# RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

## Cyber Threat Intelligence

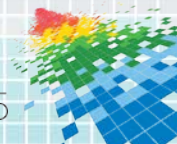




# What is cyber threat intelligence

## ◆ Information about cyber threats

- Bad people, things, or events
- Plans to attack victims
- Tactics used by bad people
- Actions to deal with bad events
- Weaknesses targeted by bad people



# Cyber threat Constructs

**Atomic**



What threat activity are we seeing?

**Tactical**



What threats should I look for on my networks and systems and why?

**Operational**



Where has this threat been seen?



What can I do about it?



What weaknesses does this threat exploit?

**Strategic**



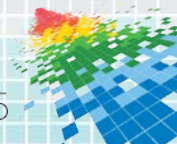
Who is responsible for this threat?



Why do they do this?



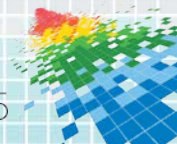
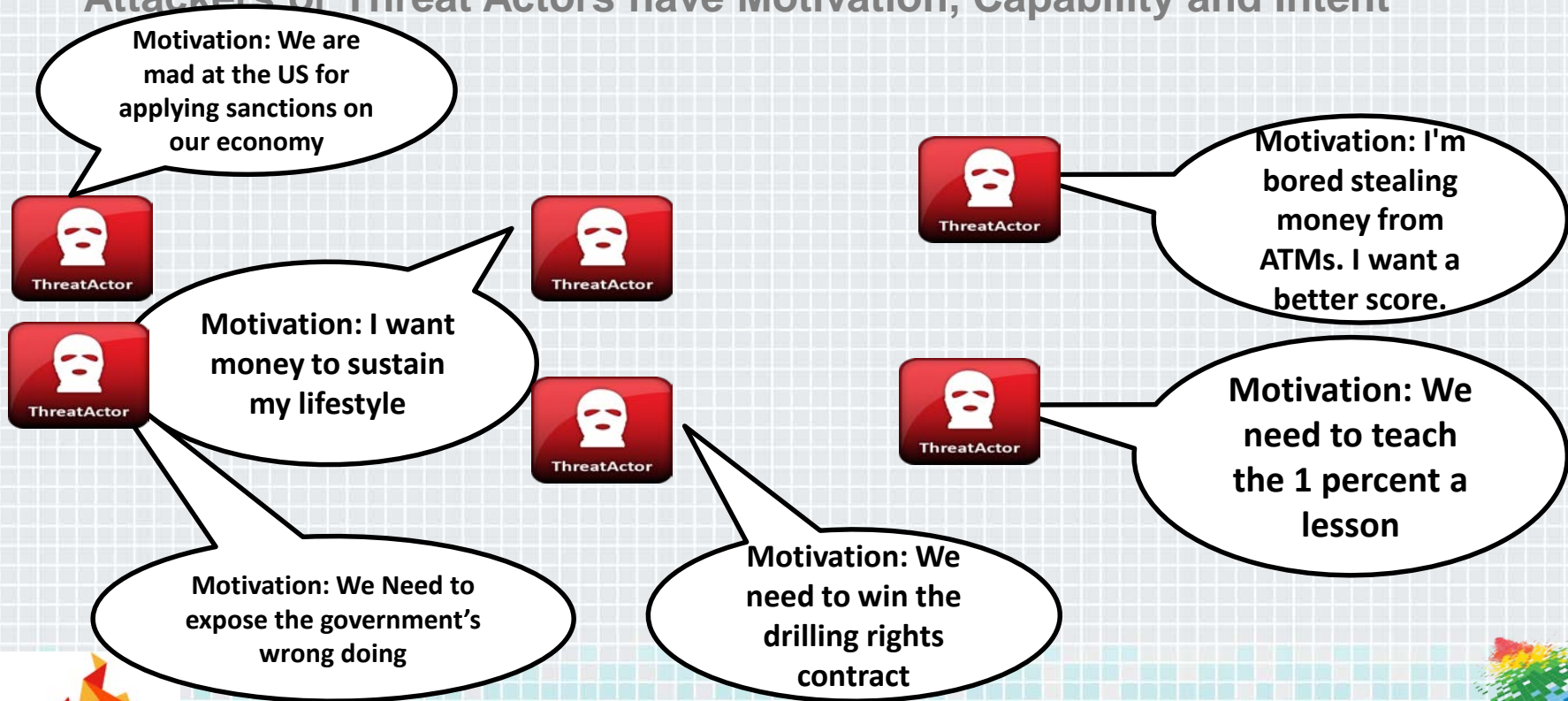
What do they do?





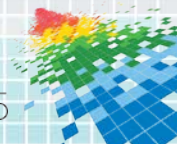
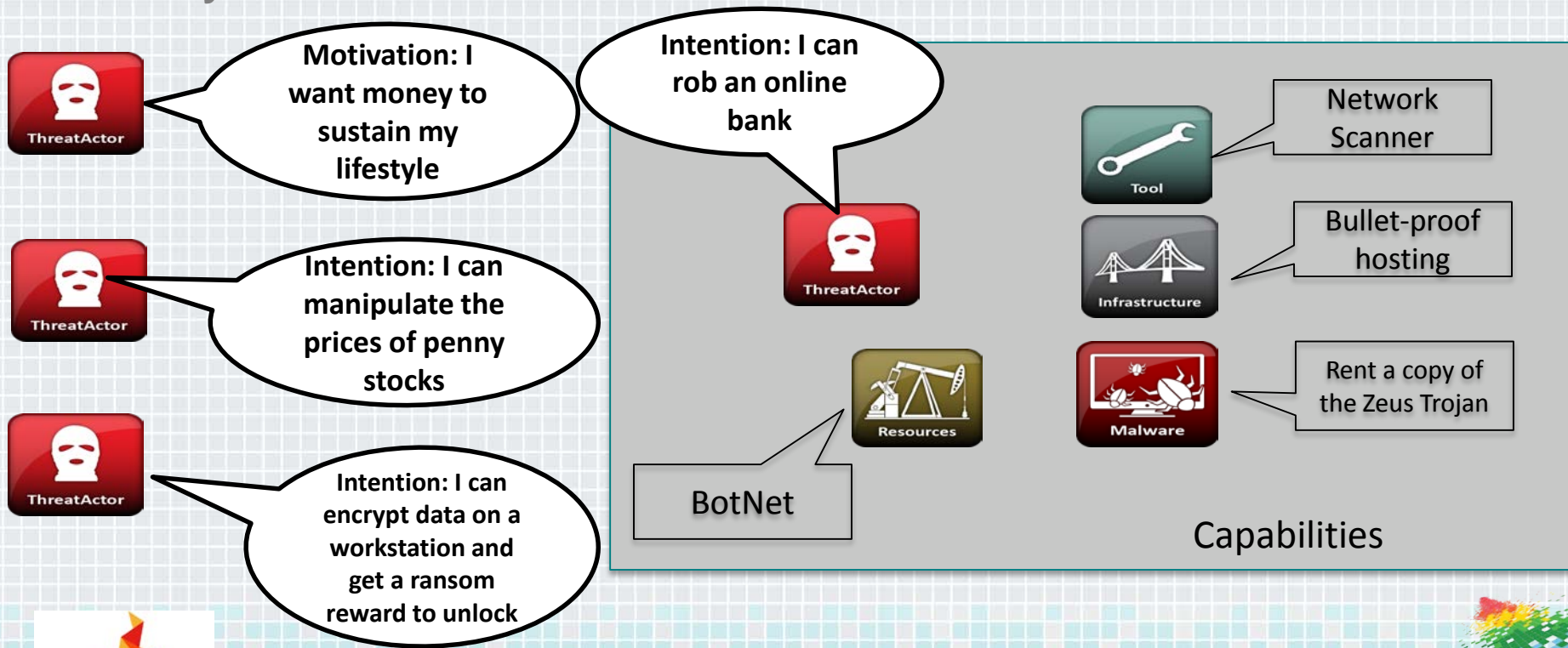
# Attackers workflow

Attackers or Threat Actors have Motivation, Capability and Intent



# Attacker's workflow

Many threat actors have the same Motivation but different Intentions



# How Attackers Engage a Target

Attackers have a development lifecycle they need to follow to conduct their attacks

Motivation,  
Capability and  
Intent



ThreatActor



VirtualTargeting

I should socially  
engineer  
somebody at the  
processor



TTP



AttackPatterns

I bet they have people  
who travel, so let me  
send fake airline  
notices to every email  
address I can find



Campaign



Behavior

When the link is  
clicked the malware  
gets installed from  
the BotNet

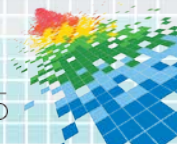


ExploitTarget

I should  
target an ATM  
card  
processor

I need to get from  
the office computer  
network to the  
transaction network

Joe in accounting  
clicked on the  
fake airline  
notice





# How defenders respond to incidents

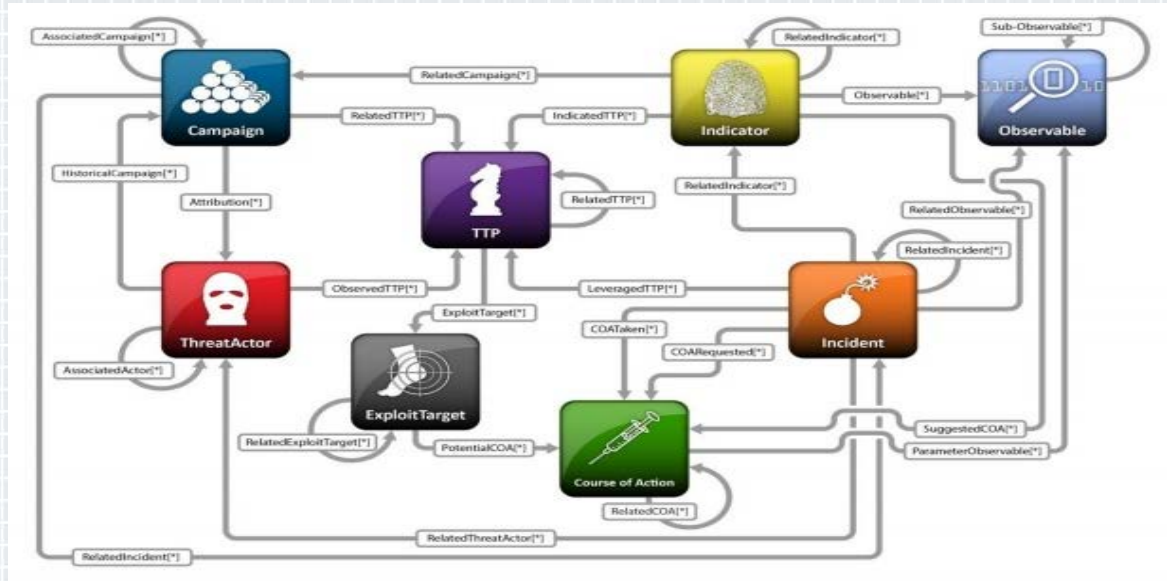
When an incident occurs the defender assesses damages and looks for the cause





# STIX Architecture

- ◆ The Power of Structured Intelligence
- ◆ Key to effective strategic cyber intelligence analysis and threat tracking
- ◆ Ability to pivot, view, analyze, and enrich complex relationships



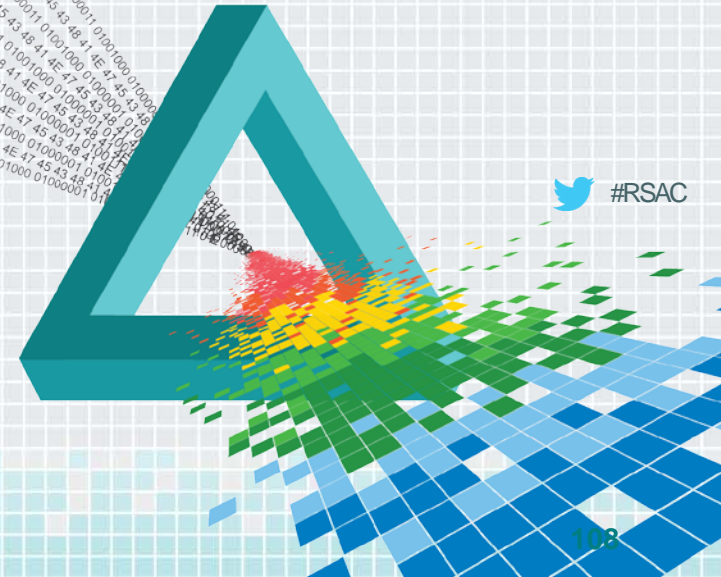
Graphic Source: Mitre



# RSA<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

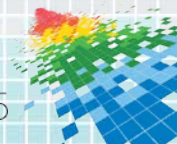
## Maturation



 #RSAC

# Cyber Threat Intelligence maturity

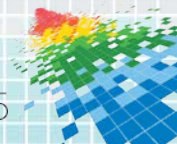
- ◆ Review public source materials for “news of the day”
- ◆ Consumption of threat data manually from public, commercial, or community sources in an ad hoc manner
- ◆ Publishing sightings of threats back to community based upon incidents or “punches”
- ◆ Publishing of new threat data back to community based upon incidents
- ◆ Consumption of all source threat data in an automated manner
- ◆ Publishing of threat data back to community based upon analytics
- ◆ Identification of potential victims prior to attack being launched
- ◆ Attribution of malicious activity to a specific threat actor group
- ◆ Prediction of future threat activity based upon Analysis and Intelligence





# How to Start

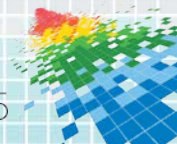
- ◆ Get data mainly about observables, indicators, and exploits
  - ◆ When you have 'stuff' to look for you will learn a lot about what you can see and what you can't see. This alone is helpful
- ◆ Figure out what kinds of data you can use and what you can't
  - ◆ Plan projects over time to add capabilities to address observable types you can not search for in your environment.
  - ◆ For me the first huge gap was windows workstation file names/ hashes
- ◆ Build efficiencies where ever possible
  - ◆ Standardize, Consolidate, and de-duplicate
- ◆ Make friends
  - ◆ Join community groups like ISACs, RSA Birds of a feather, etc





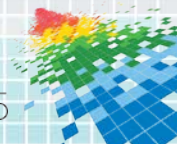
# Getting to the next level

- ◆ Keep Score
  - ◆ Track wins and losses using a model like Lockheed Martin's Cyber Kill Chain to know where controls work and fail
  - ◆ Track not just the incidents, but the attempts.
  - ◆ Organizing around Campaigns is a great consolidation point
- ◆ Give Back
  - ◆ Set a goal to share one item a week back to your community, even if it is just sighting information at first.
  - ◆ Ramp this up over time
- ◆ Develop analytic methods based not on keywords, but patterns



# Skills & Competencies for Threat Teams

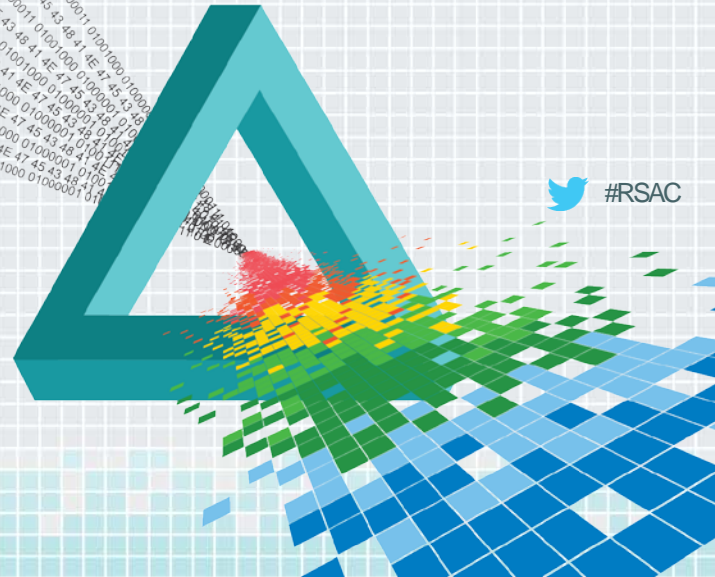
- ◆ Adversarial Mindset
- ◆ Curiosity
- ◆ Hands on keyboard
- ◆ Business context & process knowledge
- ◆ Organization and communications
- ◆ Social Networkers



# RSA<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

## Game Changer





# How it 'works' today

## All these sources, all this data, how do you process it efficiently?

Intelligence sources

-  FW
-  WLAN GW
-  IPS
-  WAF
-  SIM
-  email GW
-  Web GW
-  DAM
-  DLP
-  NAV

Untitled - Notepad

File Edit Format View Help

We have seen the below coming into our estate numbering into the 1000's.

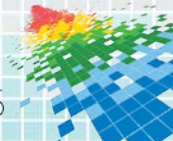
Sender: kshakong[at]Cashbuild.co[.]za  
 Attachment: SKMBT\_75114091015230.zip  
 Subject: ICopied invoices!

SKMBT\_75114091015230.zip  
 |146b388559cac0e9c5cfef5cb1778a29

2nd Stage payloads  
 acfnet[.]com[.]br/333[.]jpg  
 vistabuys[.]com/333[.]exe  
 musicacademymadras[.]in/333  
 golklopro[.]com/bitrix/modules[.]php  
 ethostraining[.]es/333[.]cab  
 cosjesgame[.]su/bitrix/modules[.]php

I have attached a sample of what we have received.

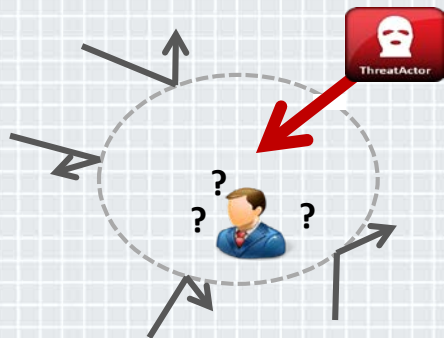
ter Research





# Evolution of Cyber Security Defense

## Yesterday's Security



### Network Awareness

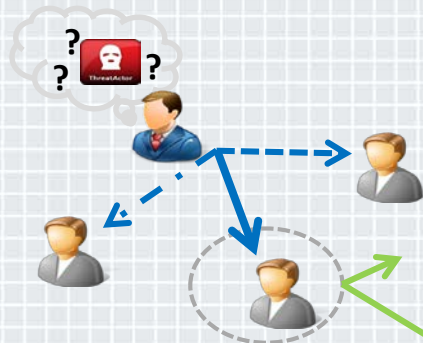
Protect the perimeter and patch the holes to keep out threats share knowledge internally.



### Increasing Cyber Risks

- Malicious actors have become much more sophisticated & money driven.
- Losses to US companies now in the tens of millions; WW hundreds of millions.
- Cyber Risks are now ranked #3 overall corporate risk on Lloyd's 2013 Risk Index.

## Present Day Problem



### Intelligence Sharing

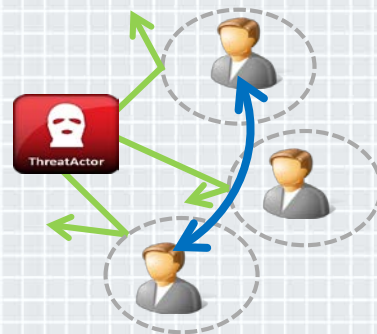
Identify and track threats, incorporate knowledge and **share what you know manually** to trusted others.



### Manually Sharing Ineffective

- Time consuming and ineffective in raising the costs to the attackers.
- Not all cyber intelligence is processed; probably less than 2% overall = high risk.
- No way to enforce cyber intelligence sharing policy = non-compliance.

## Future Solution



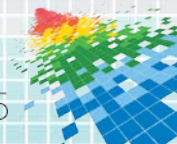
### Situational Awareness

**Automate sharing** – develop clearer picture from all observers' input and pro-actively mitigate.



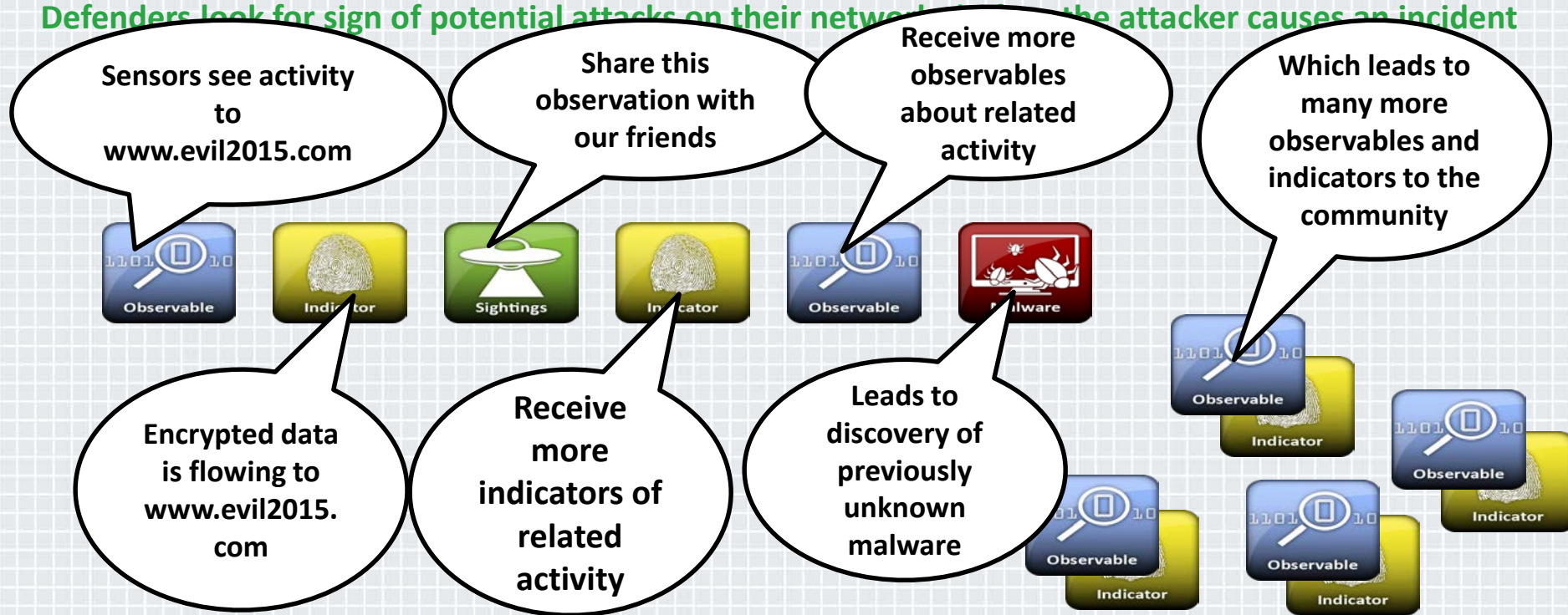
### Crowd Sourcing to solve the Problem

- Security standards are maturing
- ISAC's have become the trusted model for sharing industry threat intelligence.
- Use of automation is revolutionizing sharing and utilization of threat intelligence.



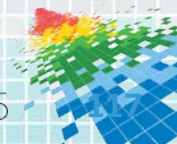
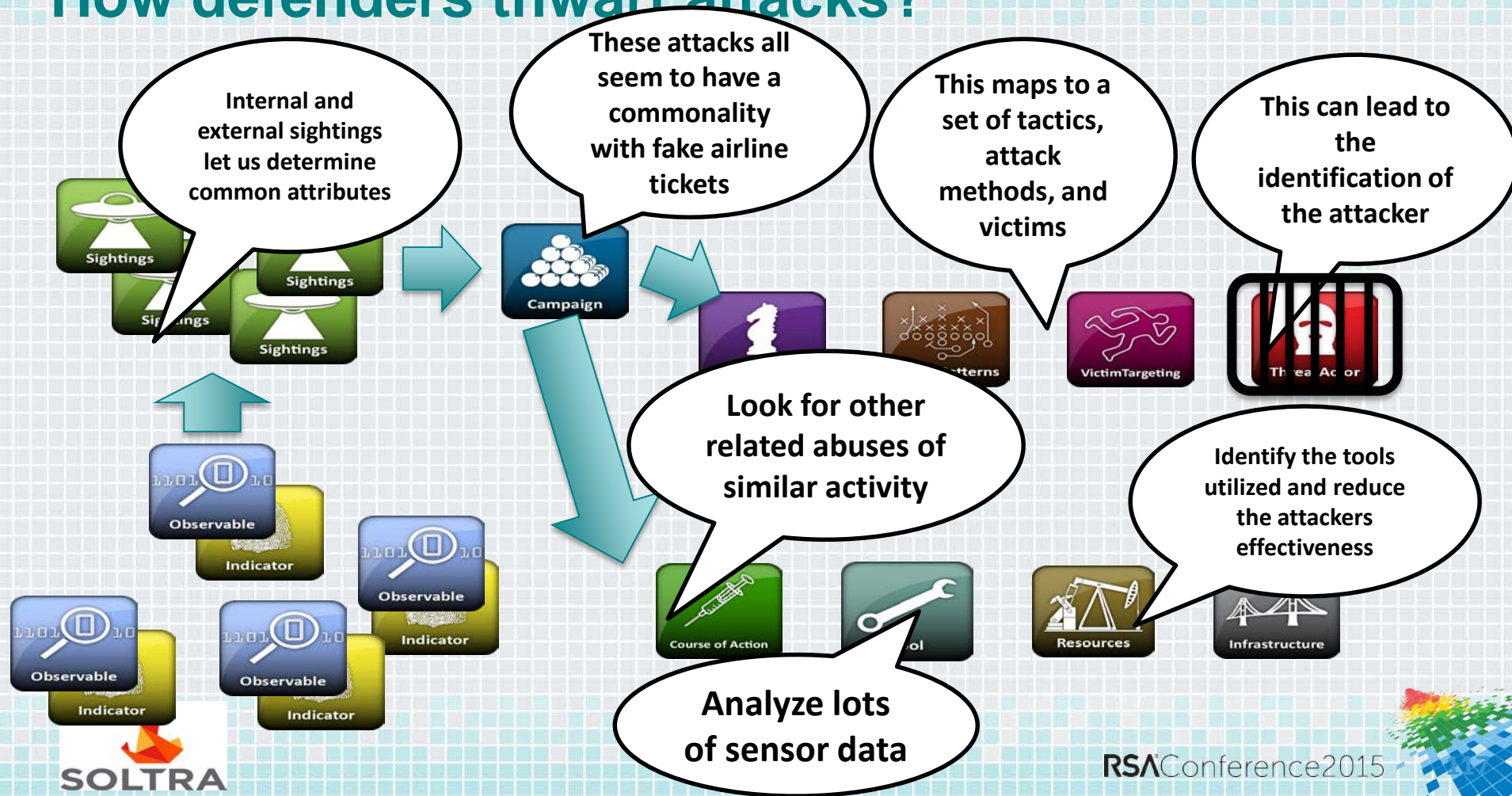
# How defenders thwart attacks?

Defenders look for sign of potential attacks on their network before the attacker causes an incident



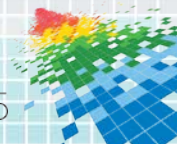
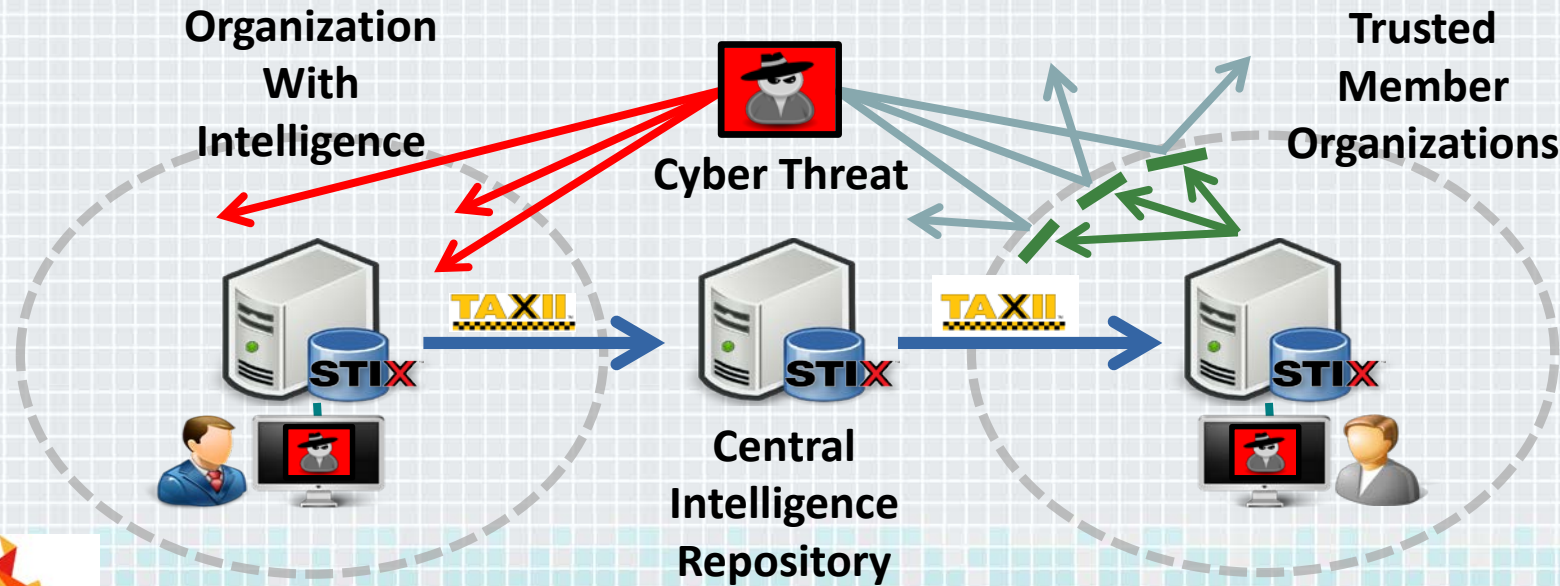


# How defenders thwart attacks?



# Intelligence Driven Community Defense

- ◆ Maturing An Intelligence Ecosystem
  - ◆ Standards-based Machine Speed Communication
  - ◆ End-to-End (Sensor to Control) Community Defense Model





# Changing the Economics

## Cost to Firms ↓

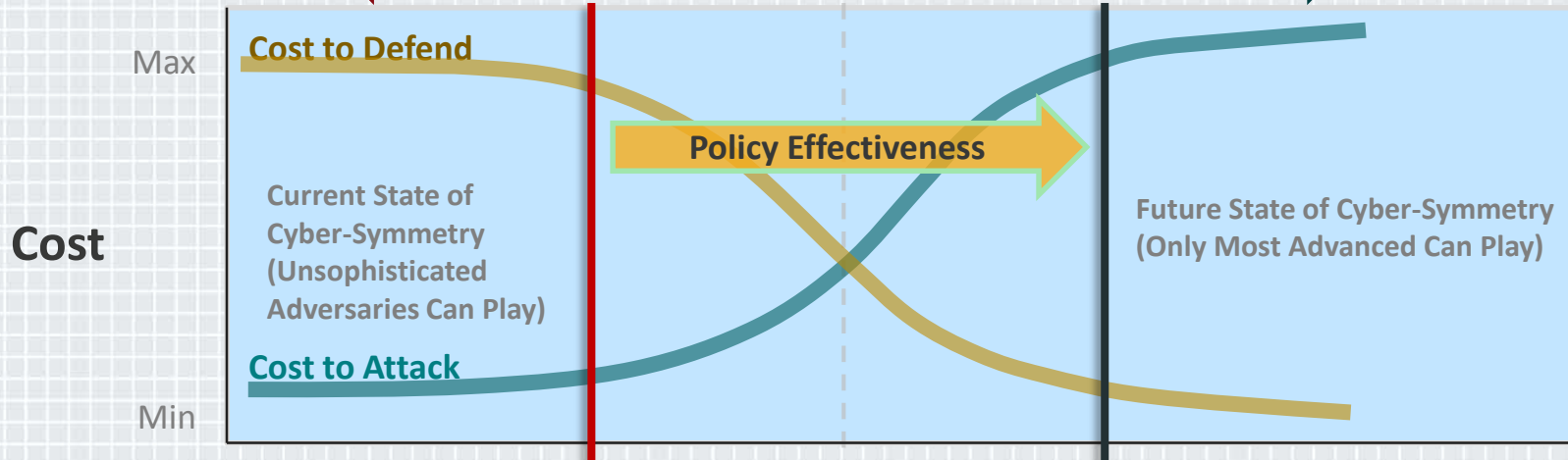
The current cost to process a single piece of intelligence is 7 hours. Equal to 2014 = \$100m; 2015 = \$1b; 2016 = \$4b

## Cost to Adversaries ↑

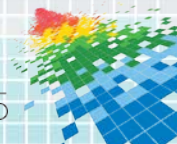
Adversaries must “re-tool” much more often and their exploits cause less damage

## Risks from Cyber Threats ↓

Frequency and impact of threats decrease while higher adoption leads to exponential benefits



Reducing asymmetry between attack and defense



# Apply What You Have Learned Today

- ◆ Next week you should:
  - ◆ Find an ISAC or Threat Sharing Community to join
  - ◆ Do an initial assessment for your companies exposure to C.H.E.W by business line
- ◆ In the first three months following this presentation you should:
  - ◆ Develop procedures to consume threat intelligence information and look for this activity in your environment
  - ◆ Develop a process to share information from your company to your community and execute it several times
- ◆ Within six months you should:
  - ◆ Identify opportunities to create efficiencies based upon the threat data you just can't process quickly enough
  - ◆ Bake this into your next year's budget requests in concert with threat intensity assessment and observed activity wins/losses

