RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Adventures in Insurance Land: Weaknesses in Risk Pricing & Alternatives

SESSION ID: GRC-W01

Tim West

Senior Consultant
Accuvant Advisory Services
@west_tim

Jamie Gamble

Principal Consultant
Accuvant LABS
@bitgamble

What’s this talk About?

Cyber insurance! but really *measuring risk*

- Review of how it all works
- A critique of how the Insurance industry approaches information risk
- A discussion of ideas for improving pricing techniques

Why do we personally care about a topic with the word ‘Cyber’ in it?

- The core of this business is measuring risk…

and ***it’s big, serious, business***

What’s This Talk NOT About?

- A sales pitch on buying selling, or otherwise
- Anything more than a superficial view of actuarial science

Personally, we don’t care if or how much insurance you buy.

We don’t sell it or do any associated business!

Why Might this Talk Interest You?

- Recent breaches show tangible value to CFO
- Insurance has been touted (academically) as a market-based alternative to compliance
- Field has been dominated by insurance professionals; our experience as practitioners and consultants provides an outsiders look

The Key Question

Ponder this:

- If you had to bet a million dollars on who in the S&P 500 will and won’t get hacked, what information would you want on each company?
- If all companies were willing, how could this data be acquired?

“How should financially motivated outsiders judge the security of a network?”

Agenda

Cyber Risk Insurance Primer

Insurance from Three Facets

- Sales Process – Broken from the Beginning
- Underwriting – God Throwing Dice?
- Claims – Not so Pleasant

Musings

Recommendations

Cyber Insurance Primer

Cyber Insurance Market Stats

- Revenue: $2 Billion in 2013
- Penetration Rate:
  - 31% of companies have policies
  - 39% of companies are planning to buy in the near future
- Growth Rate: 11.8% from 2008 to 2013
- Global Market Diversity: Top player only has 1.6% market, 276 players tracked by IBISWorld, market research firm

Policy Coverage Areas

First Party – Protection for direct costs from the breach

- Consultants
- Business interruption
- Notifying third party victims

Third Party – Liability protection for harm to others

- Legal liability
- Fines
- Law suits

Just like other insurance, but Cyber

Public Breach Costs

Direct Costs:

- Lawyer fees
- Outside Consultants - Detection, forensics, etc…
- Crisis Management – aka Public Relation firms
- Fines – state, federal, etc…
- Cost of mandatory notification & fraud monitoring services

Indirect Costs:

- Internal time - Cleanup of machines, root cause solutions, etc…
- Loss of data and intellectual property – poorly quantified & tracked*

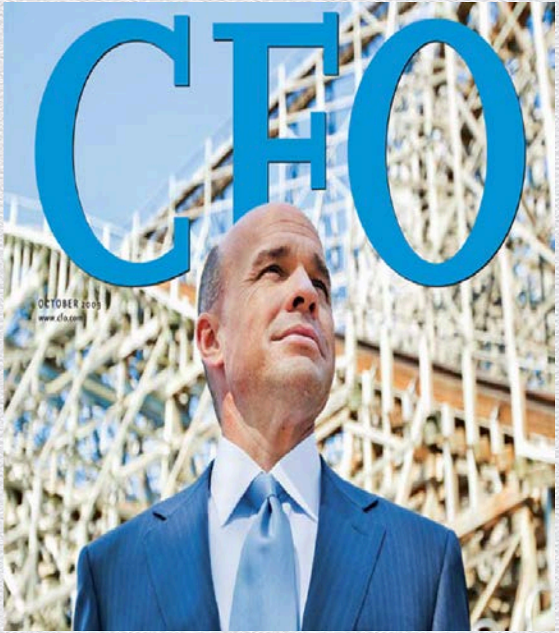
Are the Coverage's Offered Enough?

Answer: It depends

- $10K - $35K Annual Premium per $1M in coverage (annual)
- Sublimits exist for policy lines
- Coverage's for individual notification and fraud monitoring services can provide business justification with large data sets

The Dance:
Let’s talk about the Sales Process

Meet Your Typical Buyer



None of these people know how secure the enterprise is.

Typical Buy Scenario: Cluster 101

Typical Buyer

- Owns Budget & Decision Maker
- Little / No Understanding of Security Posture
- Doesn’t understand “the Data”
- Buy Can Fail…
  - as a “Add On” to other Policies
  - as a “Random Coverage Amount”
  - without internal due diligence

Impacted: CIO/CSO/CTO

- Limited Engagement in Buy or Scoping Exercises
- Considered an Admission of Failure or Poor Management
- Investing in Risk Management But Investments May Not Impact Premiums

“But don’t we have brokers for that?”

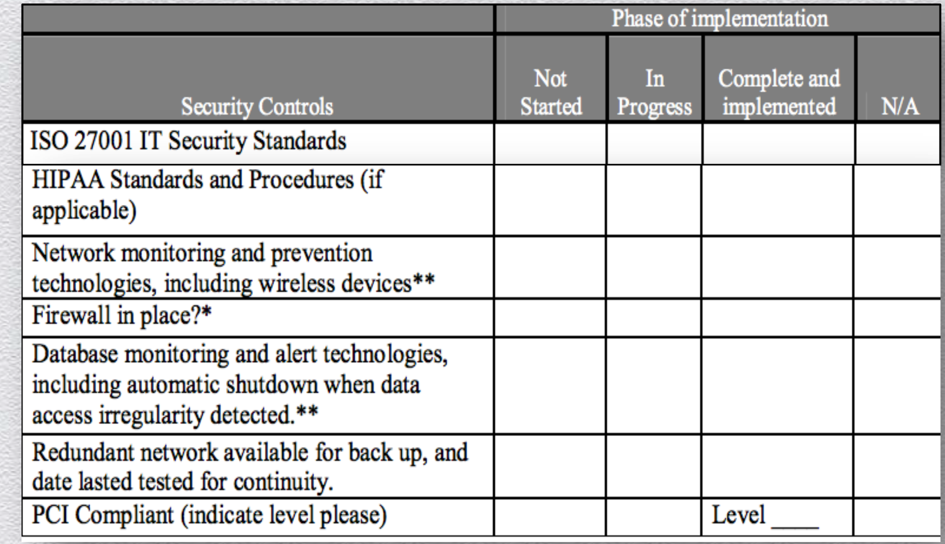
- Cyber insurance is often an add-on on other corporate insurance policies
- Brokers are not security people, and have no idea what the risks you need to insure against are. They do know what other people are buying and what is sold and trends in policies, claims, and the market.
- No, we don’t know which brokers you should talk to…

(…but if you know of a good one we’d love to hear your experiences)

Qualifying for Cyber Insurance

- Data is gathered about your security program from questionnaires without validation; typically a ‘call’
  - No third party evaluation
  - Technical questions very diverse
  - Specific implementations of technical controls are rare*

**maybe device encryption but specific implementation (laptops, phones, email, etc… or validation not detailed*



	Phase of implementation			
Security Controls	Not Started	In Progress	Complete and implemented	N/A
ISO 27001 IT Security Standards				
HIPAA Standards and Procedures (if applicable)				
Network monitoring and prevention technologies, including wireless devices**				
Firewall in place?*				
Database monitoring and alert technologies, including automatic shutdown when data access irregularity detected.**				
Redundant network available for back up, and date lasted tested for continuity.				
PCI Compliant (indicate level please)			Level ____	

Policy Underwriting

Assumptions made by the Industry

- A questionnaire is a valid approach to baseline risk
- Insurers methods are fairly static & policies last years (does your risk?)
- Past event data regarding losses is indicative of future events
- Claims will be distributed without large spikes
- Don’t Forget!
  - The least secure companies are fundamentally bad at internally detecting intrusions
  - If you do not want to make the event public, you can’t claim insurance

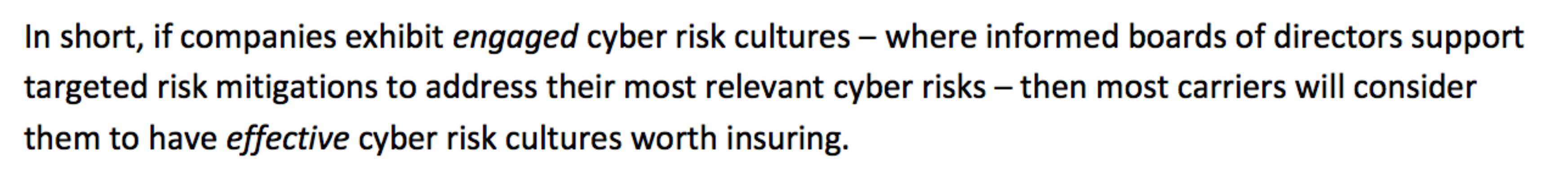
Underwriting "Principles"

- Insurers look for 'engaged' cyber cultures
- Companies rewarded for 'talking to' cyber risk
- Not due diligence, talk.
- Substitute for lack of actual data

Cyber Risk Culture Roundtable Readout Report

National Protection and Programs Directorate
Department of Homeland Security

May 2013



In short, if companies exhibit *engaged* cyber risk cultures – where informed boards of directors support targeted risk mitigations to address their most relevant cyber risks – then most carriers will consider them to have *effective* cyber risk cultures worth insuring.

Questionnaires and Checklists

- Comparable to data points within a maturity model *
- Asking hard questions results in fewer sales
  - E.g. malware protections…
- Early market application processes were more robust but pushed typical customers away

* A maturity model from the 90's.

Defining Security

As an industry, we need better rules for what makes a network more or less secure.

But what should they be??

Think back to what we asked you earlier, what data would you want on companies before betting on which will be hacked and which won't be?

What would we want to know?

Breaks down into 3 general questions

1) How easy is it for an attacker to get a foot hold on your network?
2) How prepared are you to notice the attack?
3) How easy is it for an attacker to move laterally on your network?

Where is this information?

- Vulnerability / configuration flaws that go beyond scanner results
- Pen test results, and the limitations placed on testers
- Firewall rule sets and the “real” network topology
- Network trust relationships
- Trust relationships between user accounts

There is an absence of metrics and models to quantify this data.

Is that all?

- No.
- Some products can provide views of this data, but a comprehensive solution is still a few years out, at best
- There is very little good research on what makes a network more or less secure

Please reread that last sentence. Isn’t that crazy?!

RSACONFERENCE2014

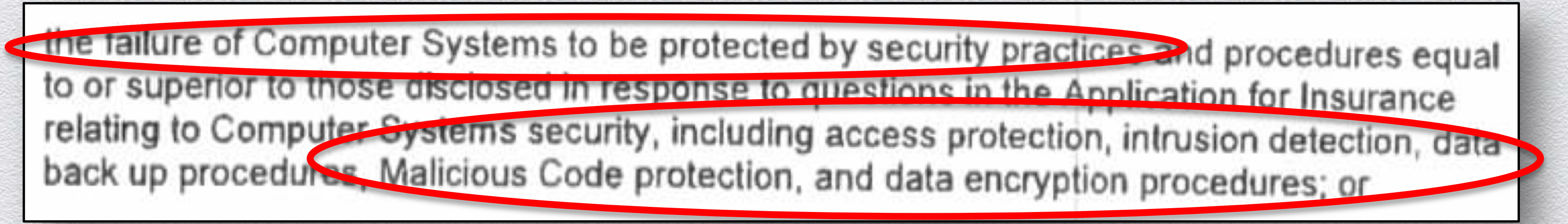
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Claims

“Minor” Exclusion Clauses

Common language could exempt **most** from making a successful claim.

This policy exempts payments if…:

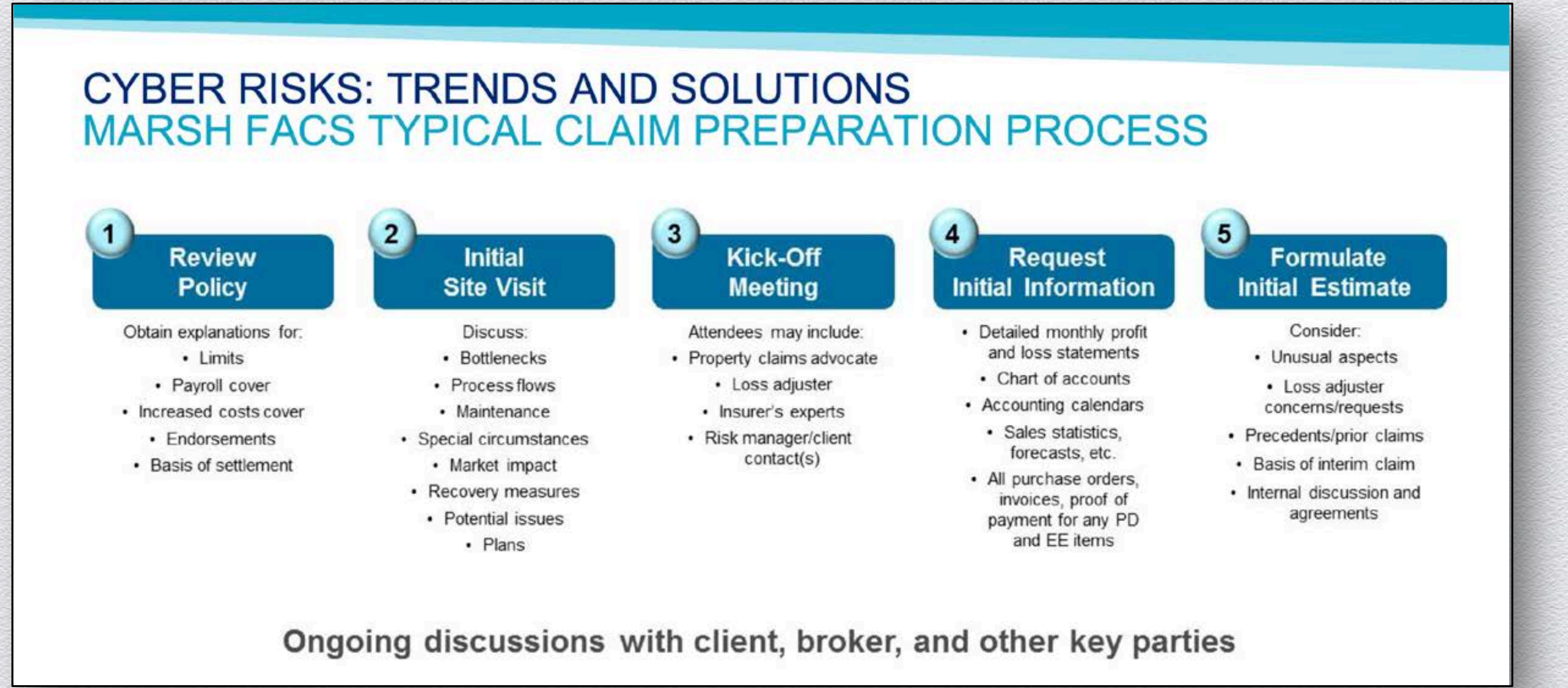


the failure of Computer Systems to be protected by security practices and procedures equal to or superior to those disclosed in response to questions in the Application for Insurance relating to Computer Systems security, including access protection, intrusion detection, data back up procedures, Malicious Code protection, and data encryption procedures; or

Or

“The ***failure to install available software product updates*** or releases, ***or patches***, to computers or Computer System”

Claims Process



CYBER RISKS: TRENDS AND SOLUTIONS

MARSH FACS TYPICAL CLAIM PREPARATION PROCESS

1 Review Policy

Obtain explanations for:

- Limits
- Payroll cover
- Increased costs cover
- Endorsements
- Basis of settlement

2 Initial Site Visit

Discuss:

- Bottlenecks
- Process flows
- Maintenance
- Special circumstances
- Market impact
- Recovery measures
- Potential issues
- Plans

3 Kick-Off Meeting

Attendees may include:

- Property claims advocate
- Loss adjuster
- Insurer's experts
- Risk manager/client contact(s)

4 Request Initial Information

- Detailed monthly profit and loss statements
- Chart of accounts
- Accounting calendars
- Sales statistics, forecasts, etc.
- All purchase orders, invoices, proof of payment for any PD and EE items

5 Formulate Initial Estimate

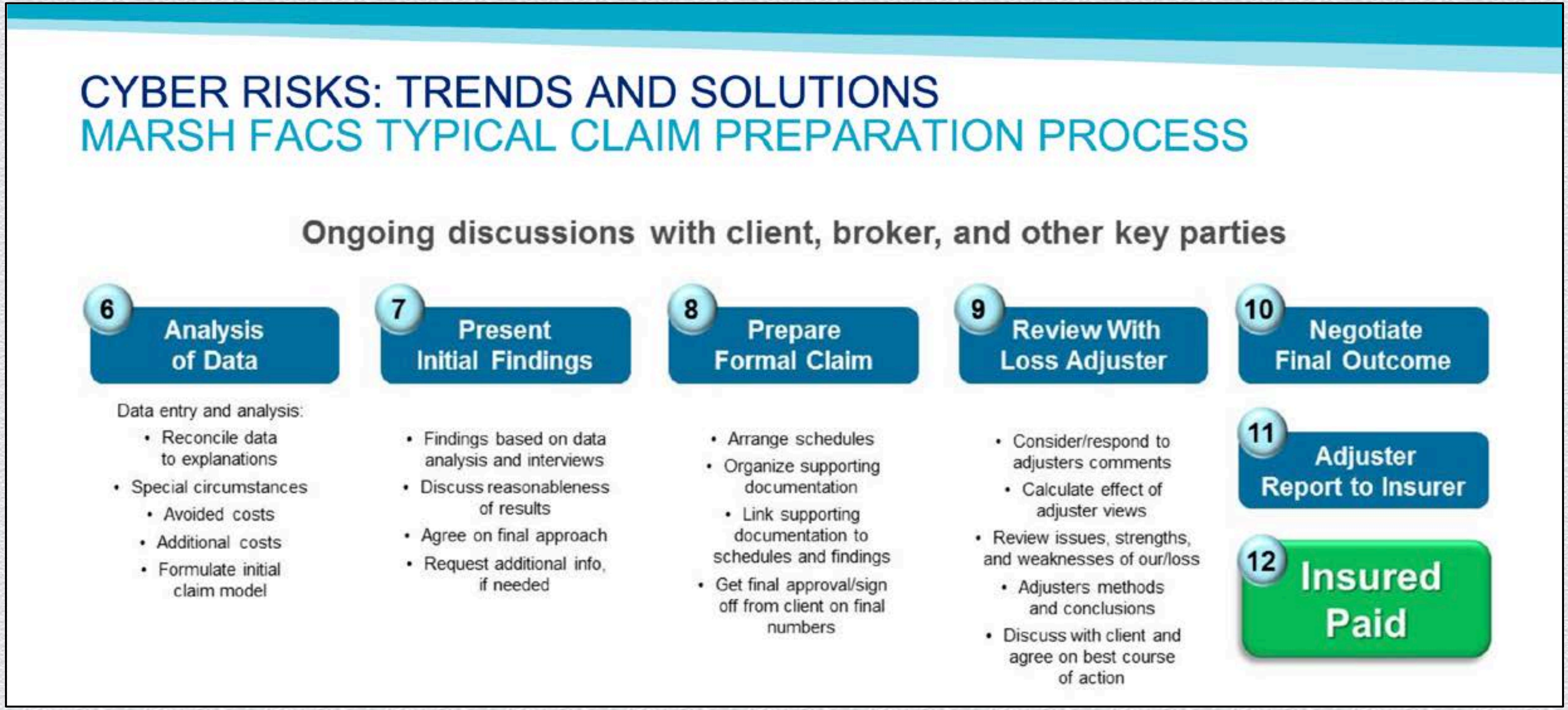
Consider:

- Unusual aspects
- Loss adjuster concerns/requests
- Precedents/prior claims
- Basis of interim claim
- Internal discussion and agreements

Ongoing discussions with client, broker, and other key parties

Per "Marsh NROR September 2013 Report"
Major US Cyber Insurance Broker

12 Step Program Continued



CYBER RISKS: TRENDS AND SOLUTIONS
MARSH FACS TYPICAL CLAIM PREPARATION PROCESS

Ongoing discussions with client, broker, and other key parties

6 Analysis of Data

Data entry and analysis:
- Reconcile data to explanations
- Special circumstances
- Avoided costs
- Additional costs
- Formulate initial claim model

7 Present Initial Findings

- Findings based on data analysis and interviews
- Discuss reasonableness of results
- Agree on final approach
- Request additional info, if needed

8 Prepare Formal Claim

- Arrange schedules
- Organize supporting documentation
- Link supporting documentation to schedules and findings
- Get final approval/sign off from client on final numbers

9 Review With Loss Adjuster

- Consider/respond to adjusters comments
- Calculate effect of adjuster views
- Review issues, strengths, and weaknesses of our/loss
- Adjusters methods and conclusions
- Discuss with client and agree on best course of action

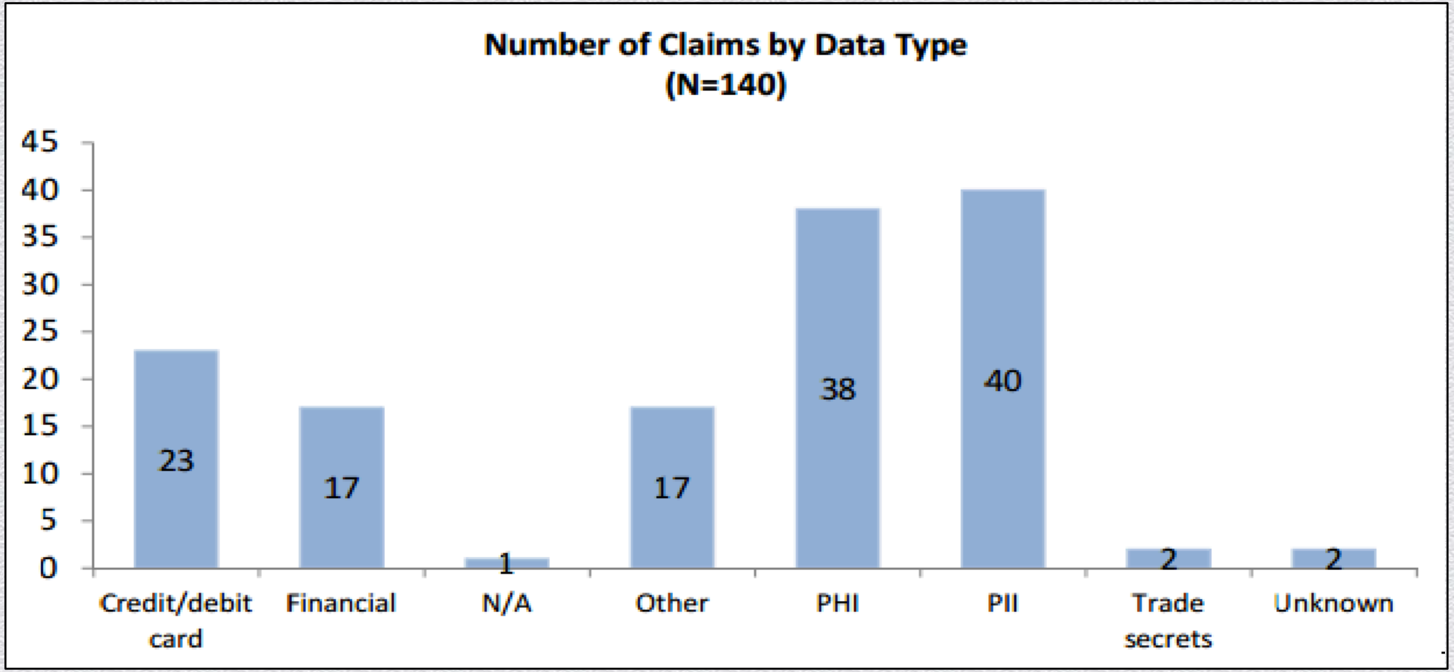
10 Negotiate Final Outcome

11 Adjuster Report to Insurer

12 Insured Paid

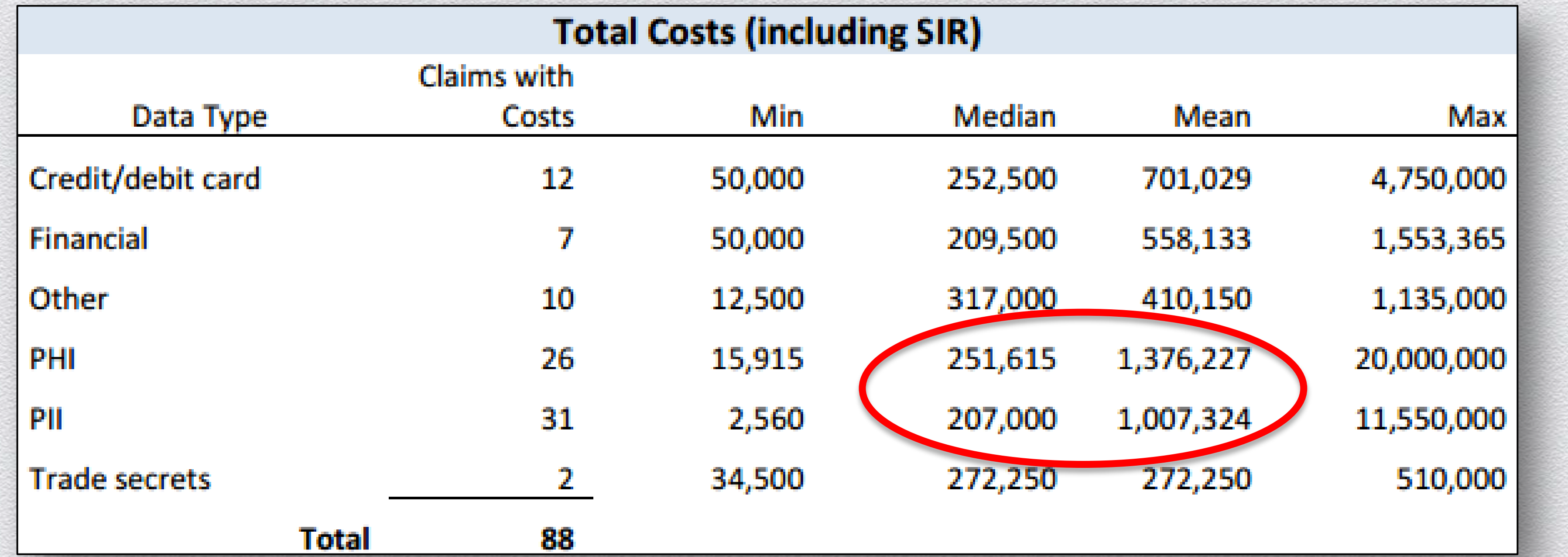
Per "Marsh NROR September 2013 Report"
Major US Cyber Insurance Broker

Actual 2013 Claims Data



Per "NetDiligence 2013 Cyber Liability &
Data Breach Insurance Claims Report"
Data from Underwriters, total n=140, cost data n=88

Actual Claims Cost



Total Costs (including SIR)					
Data Type	Claims with Costs	Min	Median	Mean	Max
Credit/debit card	12	50,000	252,500	701,029	4,750,000
Financial	7	50,000	209,500	558,133	1,553,365
Other	10	12,500	317,000	410,150	1,135,000
PHI	26	15,915	251,615	1,376,227	20,000,000
PII	31	2,560	207,000	1,007,324	11,550,000
Trade secrets	2	34,500	272,250	272,250	510,000
Total	88				

Per NetDiligence 2013 Cyber Liability & Data Breach Insurance Claims Report

Now that we’ve explained how it works works…

Our Musings

At a high level

- To keep everyone honest, due diligence of work should occur prior to the insurance sale, rather than prior to the claim
- There is a serious need for research to quantify the following:
  - How to measure / model the security of a network
  - Define and measure factors that influence security

Can Insurance be an Alternative to Compliance?

Idea: Insurance can be used as a free market alternative to compliance regimes

Assumption: Premiums reflect a security level

Proponents: Academics, theorists, some government policy people; quote DHS & White House Policy docs

- Compliance systems can be very flawed, but in it’s current state using insurance for this is a step backwards

Rethinking Questioners

- Biggest complaint: Questions indicate that definitions of maturity are old
- Maturity models attempt to plot the maturity of a process to that of a defined set of maturity levels
  - Capability Maturity Model is the popular choice
- The value of each question can be weighed and valued however an insurance company likes
- Overtime results applications from different companies should show interesting changes in the industry. Shifts in maturity, differences by sector, etc

Currently, Only Lagging Indicators are used

- Incident detection rates
- Average cost of claims and trends
- Volume of hacking activity
- Previous claims per industry vertical
- Potential loss valuation by industry vertical - PHI loss, PII loss, network disruption

Flaws:

- All aggregate data!
- Intrusion rates will change as new hacking techniques, targets, motivations, and data valuation change?

Leading Indicators? Not there Yet…

What useful data can we measure?

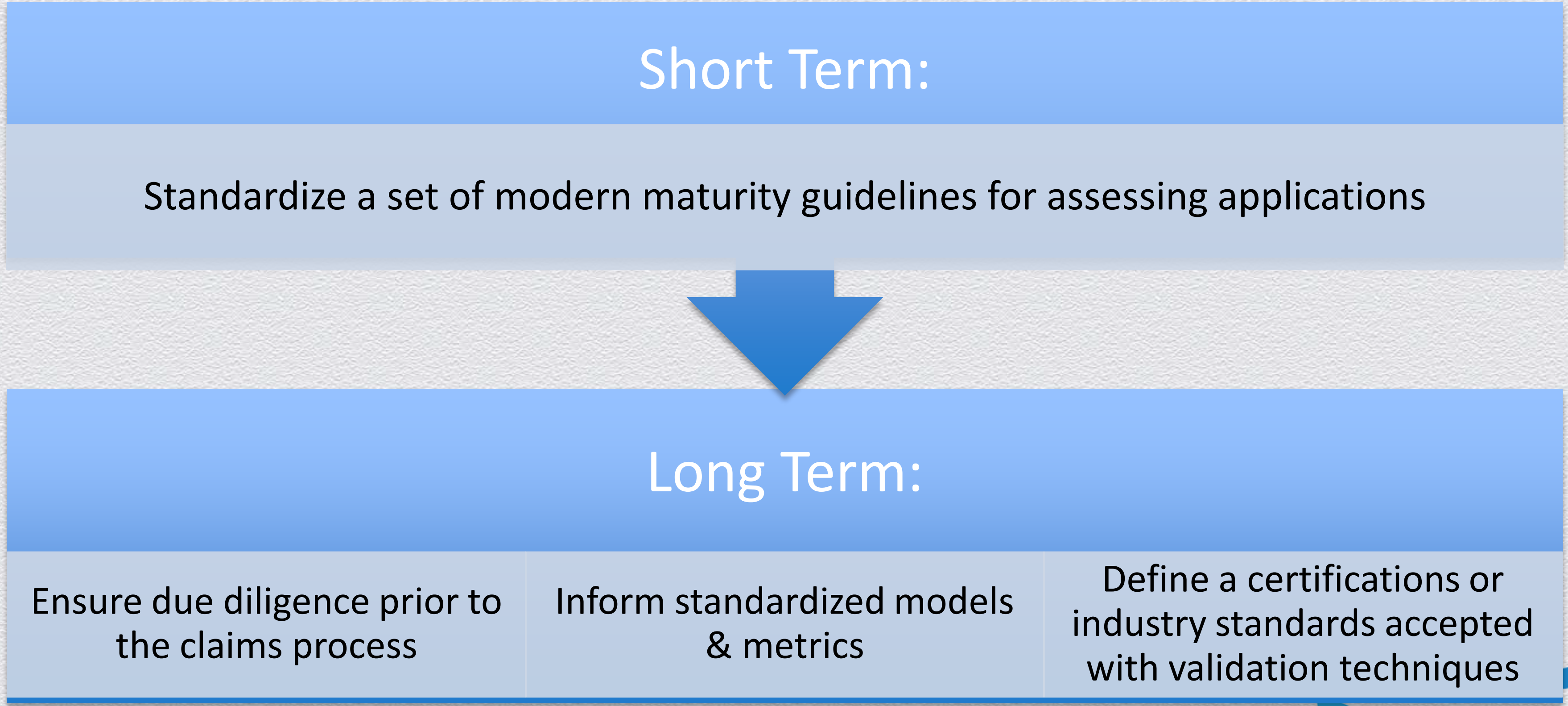
- Maturity comparisons between companies
- Resilience to loss triggers
  - Safe harbor achievements
  - Network security capabilities
  - Detection & response capabilities

Recommendations

Advice for buyers

- Shop around!
- Involve security people that understand the company's security posture in the buy process
- Understanding only comes by digging in and reading the fine print
- Work with a broker to understand what is being insured
- Analyze your policy options & use gaps to inform your security strategy
- Posture your strengths in strategy and risk management practices to negotiate your premiums!

Practical Recommendations for Insurers



Short Term:

Standardize a set of modern maturity guidelines for assessing applications

Long Term:

Ensure due diligence prior to the claims process	Inform standardized models & metrics	Define a certifications or industry standards accepted with validation techniques

Next steps

Defensive research

- More work is needed to determine effectiveness of defensive strategies
- We would love to chat with you about this – the insured & insurers

Publish a maturity model application

- Targeting release of a maturity model based application for April 1st
- Watch the Accuvant Blog

Tim West

@west_tim

twest@accuvant.com

Jamie Gamble

@bitgamble

jgamble@accuvant.com