CYBER RISK INSIGHTS CONFERENCE

10 FEBRUARY 2015 | LONDON

ADVISEN Insurance Intelligence

Welcome to the 2015 Cyber Risk Insights Conference!

@Advisen #CyberRisk

Welcoming Remarks

Bill Keogh
CEO
Advisen

Thank you to our Sponsors

ZURICH

Swiss Re Corporate Solutions

AIG

Willis

Paragon

XL

LEWIS BRISBOIS BISGAARD & SMITH LLP ATTORNEYS

epiq SYSTEMS

beazley

BITSIGHT

cfc Underwriting

22 countries are represented by our audience today!

This is the **largest** Cyber Risk conference for P&C professionals in the UK or Continental Europe.

385 people have registered for today's event!

Leading the way to smarter and more efficient risk and insurance communities.

Advisen delivers:

the **right** information into
the **right** hands at
the **right** time

to *power* performance.

Opening Remarks from our Conference Chair

Graeme Newman
Director
CFC Underwriting

Keynote Address

Brian Lord
Managing Director
PGI Cyber

Cyber Market Metrics

Jim Blinn
Executive Vice President
Advisen

CYBER RISK INSIGHTS CONFERENCE

10 FEBRUARY 2015 | LONDON

ADVISEN Insurance Intelligence

ADVISEN CYBER RISK NETWORK

Insurance Intelligence for the Cyber Community

Slides from the Cyber Market Metrics session are available to members of the Cyber Risk Network Only

For more information or to subscribe contact Jim Delaney at jdelaney@advisen.com

"The Survey Says"

Jeremy Smith
Head of Technology and Security & Privacy
Zurich

2015 Network Security & Cyber Risk Management Survey

The Fourth Annual Survey of Enterprise-wide Cyber Risk Management Practices in Europe
Sponsored by Zurich

Presented by Jeremy Smith
Head of Technology PI and S & P
Zurich

Survey Scope:

- **Aim of the survey is to gain insight into the current state and ongoing trends in cyber risk management in Europe.**
- **Completed by risk managers, insurance buyers and other risk professionals.**
- **61% were from the UK, 37% Europe, and 2% North America.**
- **The majority of respondents came from multinational enterprises.**
- **Weighted towards larger companies with 76% having turnovers in excess of £1bn.**
- **58% have excess of 5,000 employees.**
- **An array of industries are represented.**

Perception of Cyber Risk

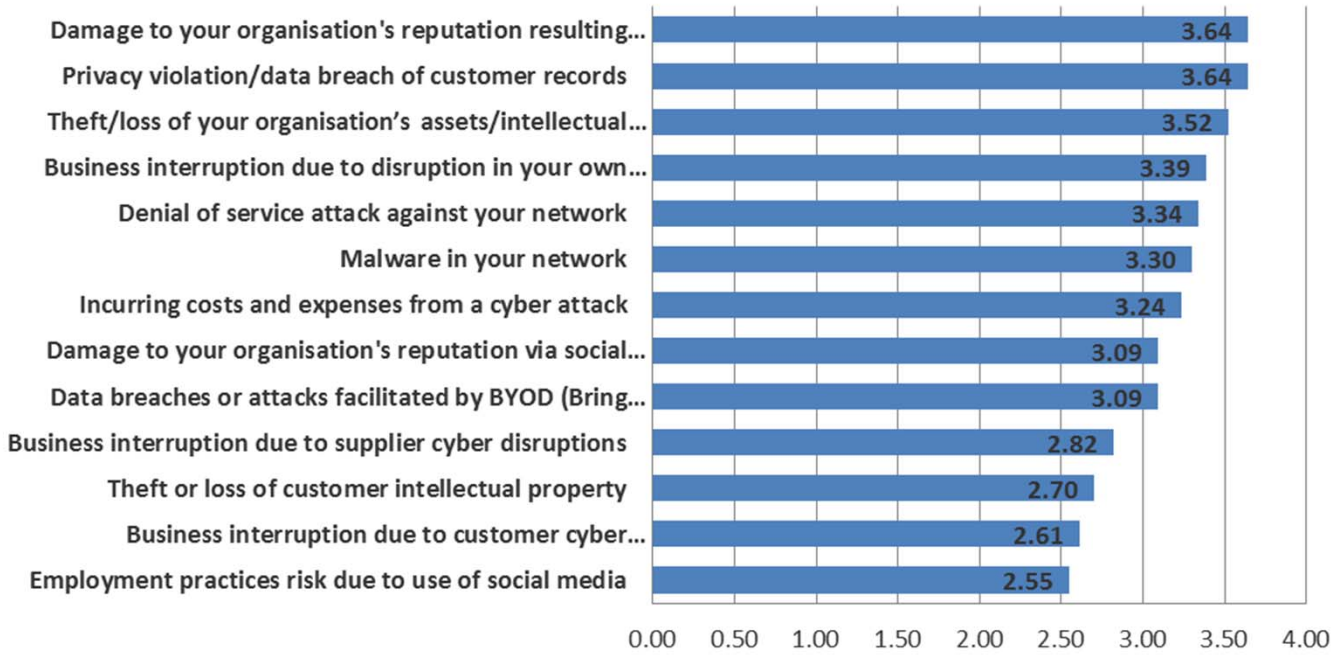
- **89 percent believe cyber risks pose at least a moderate threat,**

Europe's Perception in cyber risks is in-line with North America @ 88%.

More specifically *Cyber risks are continued to be viewed as a significant risk by senior management and the board:*

- **74 percent say senior management view them as a significant threat,**
- **69 percent say board members view cyber risks as a significant threat**

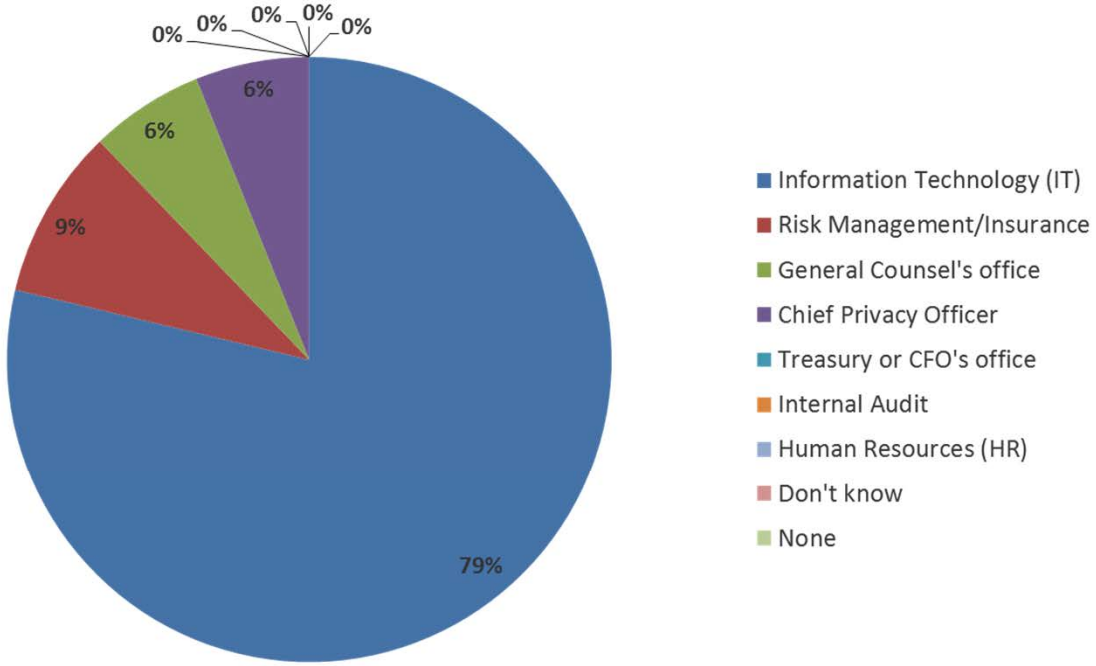
Top Risks for Organsiations: *"From the perspective of your organisation, please rank the following on a scale of 1 to 5, with 5 as very high risk and 1 as very low risk"*



Data Breach Response:

- 58% of businesses have data breach response plans.
- This remains lower than the US although the gap is closing. Last year there was a 17% point difference now it is just 4%.
- 85% include network interruption in their BCPs.
- If it was determined that customers should be notified of a breach, the department most responsible for this task was PR at 33% and GC at 20%.

"Which department is responsible for spearheading the information or network security risk management effort?"



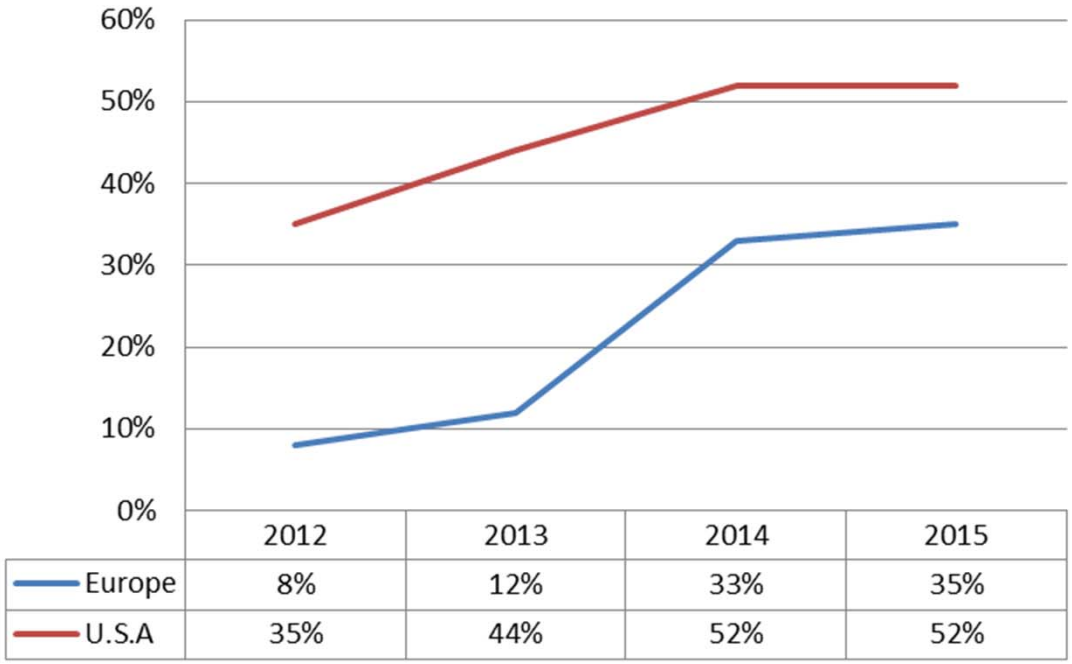
- **IT is still acknowledged as the front line defense against information losses and other cyber risks**
- **45 % of respondents take a multi-departmental approach to cyber risk management.**
- **The functions most likely to be represented on the cyber risk management committee is IT, GC & Risk Mngt.**

Other Headlines:

- 75 % have a written social media policy
- 79% have a mobile security policy
- 75% have a BYOD policy (up 12 points from last year)
- 59% include the assessment of vulnerabilities from cloud services as part of their cyber risk management program
- Smaller companies (annual turnover less than £1 billion) view cyber threats less seriously than large companies (annual turnover greater than £1 billion)

Cyber Insurance:

- **35% purchase cyber cover (up by 2 points from last year)**

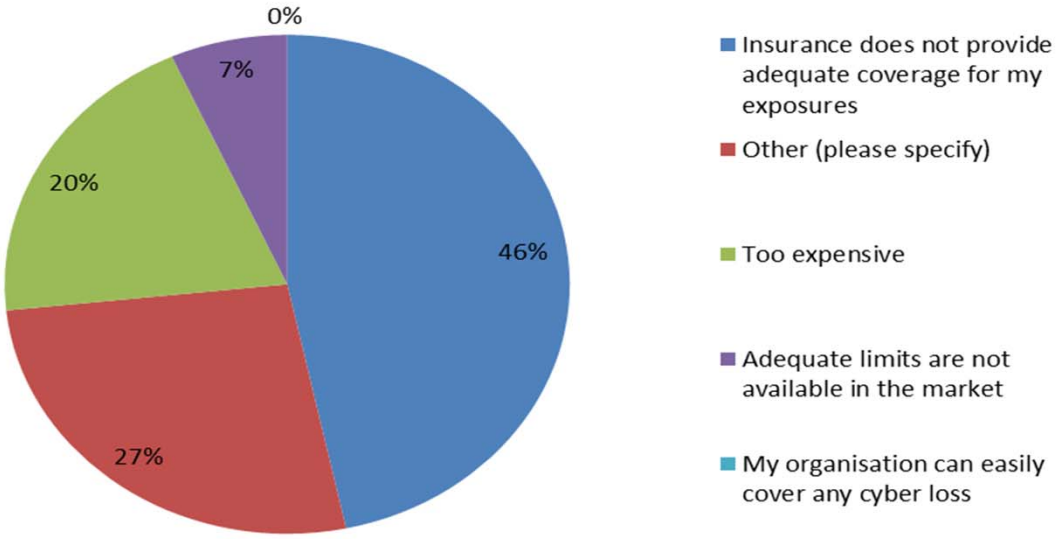


	2012	2013	2014	2015
Europe	8%	12%	33%	35%
U.S.A	35%	44%	52%	52%

- **88% purchase a standalone policy, 12% buy as part of another policy.**

- **None have ever had a cyber claim.**

"Why has your organisation chosen not to purchase cyber insurance?"



"Is the Insurance industry doing enough to address cyber risks with current products"?

26% said YES, 65 % said NO, 9% ?????

In Conclusion:

- Cyber risks continued to be increasingly recognised risk management focus.
- Insurance continues to play a bigger role in the cyber risk management strategy of more organisations.
- **“Can do better”…….**

The Risk Management Perspective

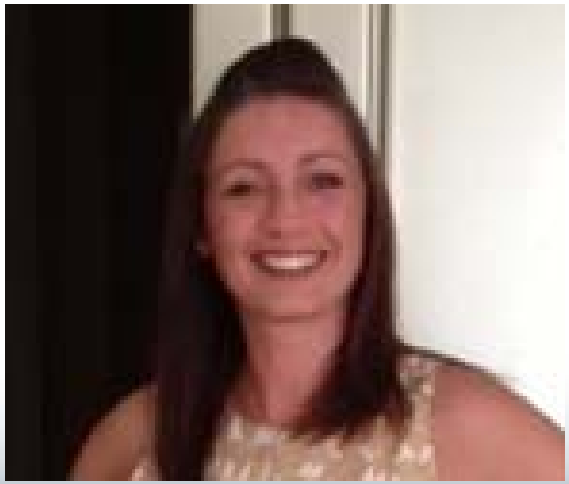
The Risk Management Perspective

Jimaan Sane
International Underwriter of Specialty Lines, Beazley
Moderator

The Risk Management Perspective

- **Jimaan Sane,** International Underwriter of Specialty Lines, Beazley (Moderator)
- **Jonathan Armstrong**, Partner, Cordery
- **Alan Jenkins**, MD & Principal Consultant, Cyber Security Pilotage Ltd
- **Ali Murphy**, Manager Operational Risk – Insurable Risk, TSB Bank

The Risk Management Perspective



Insurance Coverage and Coverage Issues

Insurance Coverage and Coverage Issues

Stephen Wares
Cyber Risk Practice Leader, EMEA, Marsh
Moderator

Insurance Coverage and Coverage Issues

- **Stephen Wares**, Cyber Risk Practice Leader, EMEA, Marsh (Moderator)
- **François Brisson**, Head of Cyber Technology, Director, Products & Global Markets, Swiss Re Corporate Solutions
- **Lisa Hansford-Smith**, Senior Underwriter, Professional Indemnity, XL
- **William Wright**, Senior Vice President, Paragon

Insurance Coverage and Coverage Issues

Regulatory Landscape Update

Regulatory Landscape Update

Steve Wright
Chief Privacy Officer
Unilever

Bridget Treacy
Partner
Hunton & Williams

Business Interruption

Business Interruption

Graeme Newman
Director, CFC Underwriting
Moderator [2015 Conference Chair]

Business Interruption

- **Graeme Newman**, Director, CFC Underwriting (Moderator)
- **Mark Bannon**, Senior Underwriter, Technology and S&P, Zurich
- **Ben Beeson**, Vice President, Cybersecurity and Privacy, Lockton
- **Mark Camillo**, Head of Cyber, EMEA, AIG
- **Vijay Rathour**, Vice President, Stroz Friedbergr, Hunton & Williams

Business Interruption





"Who goes there?!"

"Who goes there?!"

Rebecca Bole
Director of Editorial Strategy & Products, Advisen
Moderator

"Who goes there?!"

- **Rebecca Bole,** Director of Editorial Strategy & Products, Advisen (Moderator)
- **Erik Matson**, Partner—Global Head of Insurance & Co-Head of Cyber Practice, Boyden Global Executive Search
- **Eric Qualkenbush**, Member of the Board of Directors, BlackOps Partners

"Who goes there?!"

How big is the cyber security problem?

- ✓Over $500B of innovation and trade secrets are secretly stolen each year

- ✓The equivalent of $5 Trillion in total economic value is removed from the U.S. economy each year *(USA 2013 GDP: approx. $17 Trillion)*

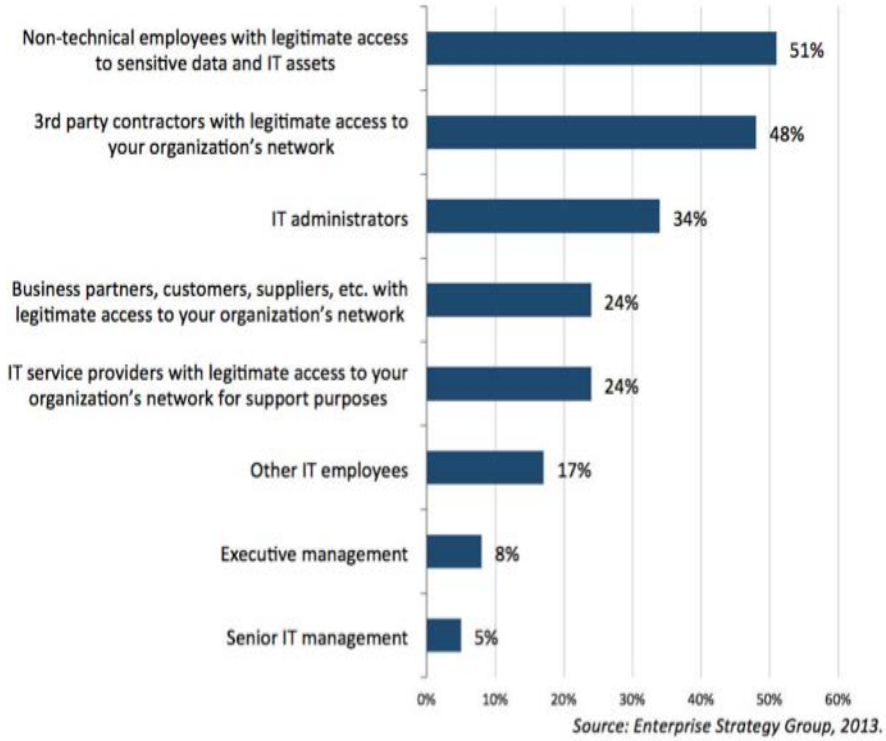
- ✓During the 'Cold War," the focus was on stealing state secrets; today, the focus is on economic information to give economic advantage

- ✓*"The U.S. economy has changed over the past 20 years. Intellectual capital rather than physical assets now represent the bulk of a U.S. corporation's value. This shift has made corporate assets far more susceptible to espionage." - (Protecting Key Assets: A Corporate Counterintelligence Guide, Office of the National Counterintelligence Executive, 2013)*

Who are the main actors?

- ✓China has roughly 250,000 “cyber-soldiers” devoted to its state sponsored effort
- ✓Russia has a major state sponsored effort to steal trade secrets and it makes little or no effort to thwart cyber criminals operating from its soil
- ✓The media have portrayed the hacker - either state sponsored, or criminals, or anarchist “hactivists” – as the main enemy. They are only opportunists who know how to exploit persons with legal access to an information system..

Types of Insiders who pose the biggest threat to organizations



Source: Enterprise Strategy Group, 2013.

The main problem is Insider Threat

- ✓95% of cyber-attacks are facilitated by human intervention; most often by unwitting employees of the targeted company who have legal access to the system.

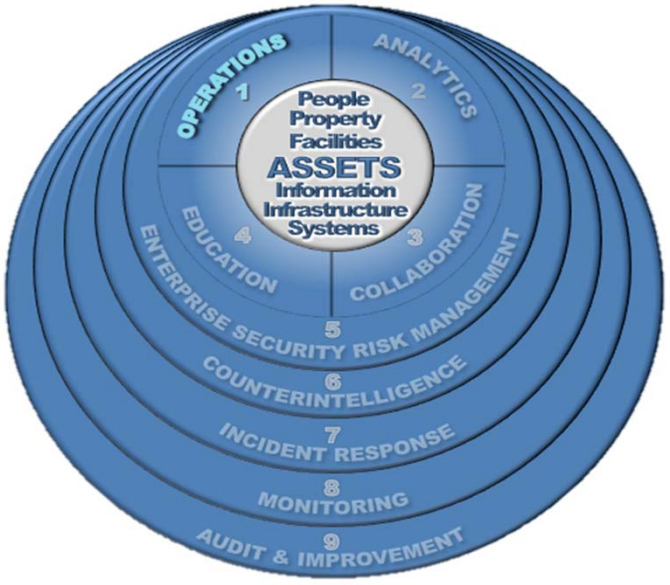
- ✓Weak links are not only **in** the organization. Contractors, vendors, suppliers, law firms have access to company information, company networks and they typically have poor security measures.

Information Security is a business problem, not just an IT problem

- When a breach occurs, the entire business is affected, from the stock and brand, to each employee
- 99% of U.S. companies have a “reactive” approach to Information Security. Less expensive up front but catastrophic to stock and brand in the aftermath. This approach offers zero options in the event of a breach. The total estimated cost of recent high-profile breaches exceeds $2B+ in long-term brand loss for each company.
- Current product-based IT approaches to Information Security are grossly inadequate.
- Once a breach occurs, your trade secrets are long gone. Many senior execs place a false reliance on law enforcement in an attempt to restore their pre-loss position but the trade secrets are permanently lost.

What can companies do to mitigate cyber risk?

- ✓Companies, senior executive teams and Boards must engage separate annual "unbiased" risk assessments to gauge true risk and gauge their true risk position. Intellectual property should be "inventoried" and then compartmented according to potential damage if lost.
- ✓Employees, new hires, interns and separated employees must continually be vetted. The company must show **everybody** that it is serious about Information Security through awareness and training programs.
- ✓A well-designed cyber liability policy with annual assessments through a major carrier should be a final step in your Information Security program.
- ✓Senior executives and Boards must annually plan for breaches and have a rehearsed response plan with an annual review. The plan must include law enforcement contacts, digital forensics, human forensics, physical forensics, customer, investor, legal, media and PR responses.



A Comprehensive Information Security Program Has Many Layers

THE HUMAN CAPITAL ELEMENT

Illustrative Factors to Consider

- What type of human capital experience and knowledge-set do we need to protect our assets?
- What are our efforts to neutralize insider threats – and where do we draw talent from outside the current organization to assess (to minimize being compromised)?
- What does this mean for your company and its ongoing viability to protect itself?
- How do you protect your trade secrets or maintain competitive advantage and not sacrifice shareholder value or employee creativity or innovativeness?
- What is your core strategic asset and what measures are you willing to protect this?

- Organizations must focus on the Human Capital element
  - Directly translates into minimizing theft risk, mitigated financial downside and senior management exposure
  - Intentions may vary from money to disruption and extortion, but the result is the same: your organization is left with having to mediate the damage and align the pieces back into a working entity.
  - The people you have dedicated to doing this will be the *difference*!

- Best practices to mitigate insider threats involve an organization's staff:
  - Management, human resources (HR), legal counsel, physical security, information technology (IT), and information assurance (IA), as well as data owners and software engineers.
  - Decision makers across the enterprise should understand the overall scope of the insider threat problem and communicate it to all the organization's employees.

THE HUMAN CAPITAL ELEMENT

Illustrative Factors to Consider

- Internal Constituents
- External Constituents
- Core Strategy
- Design of Program
- Co-habitation with other programmatic efforts
- Links to Law Enforcement
- Links to Current Tools and Techniques
- Cooperative Partners – e.g., Blackhat Teams
- Links to Communication, Legal and Public/Shareholders

BEST PRACTICES TO CONSIDER

- Know your assets and what you need to protect so the insider team can add value to this effort (**people/team need mix of strategic and tactical acumen**)
- Consider hiring the team from outside the organization – minimizes the fox in the chicken coop setting (**understanding of advanced threat actors and/or typical techniques, tactics and procedures, as well as of Intelligence Community standards and directives for analytic tradecraft**
- Empowered the position to effectively report on what they find (**people/team need gravitas to communicate and analytical skills to report**)
- Invest in the role/initiative (**people have skills to create procedures/processes/training items/recommend action programs for organizational efficacy**)
- Identify the key partners internally for an insider team (**person/team must not reject the social DNA of the company so they can become highly effective -- insider teams must play nice in the sandbox to perform!**)

Reputational Risk – Real or Fallacy?

Reputational Risk – Real or Fallacy?

Rebecca Bole
Director of Editorial Strategy & Products, Advisen
Moderator

Reputational Risk – Real or Fallacy?

- **Rebecca Bole**, Director of Editorial Strategy & Products, Advisen (Moderator)
- **Jennifer Coughlin**, Partner, Lewis Brisbois
- **Melanie Dougherty Thomas**, CEO & Managing Director, Inform
- **Matthew Hogg**, Underwriting Manager, Strategic Assets division, Liberty Specialty Markets

Reputation as key strategic threat

- 87% rated reputation risk as "more important" or "much more important," than in previous years (Deloitte 2014 from 300 execs)
- 88% explicitly focusing on reputation risk as a key business challenge (Deloitte)
- 83% of companies will face a crisis that will negatively impact their share price between 20% and 30% during the next five years (Oxford Metrica)

Breach Nation

"There are two kinds of companies in America: those who've been breached and those who don't know they've been breached."

FBI Director James Comey
60 Minutes Interview
October 5, 2014

Attack of the Titans

- 43% of all companies in America have experienced a data breach, *USA Today*, 9/24/14
- 80% of breaches root cause is employee negligence, *USA Today*, 9/24/14
- 31.4 million people have had their protected health information compromised following a breach, HHS, 10/26/14

Impact of Crisis on Reputation

- Measured in lost contracts
- Decline in revenue
- Drop in stock price
- Lost confidence from consumers, partners, suppliers, government regulators, Wall Street, industry analysts, media
- Increased scrutiny, negative media & analyst coverage
- Leadership becomes vulnerable, dismissed
- Reputation is tarnished
- Brand is damaged

Pre-Breach

Historical behavior

- No or inadequate Incident Response Plan
- No or inadequate training
- Failure to appoint appropriate response team members
- Failure to prepare crisis scenario messaging.
- Reliance on internal generalists

CASE STUDY: CORPORATE BREACH

Scenario:

- The IT system of a highly visible division of a global conglomerate was infiltrated by bad actor, and confidential/sensitive/PI information posted on internet.
- Incident disclosed to employees before forensics involved.
- Employees leaked information to media. Media runs stories.
- Company issues statement based upon internal investigation, not conclusions of outside forensics.
- Significant media and regulatory scrutiny of executive team action and response.

CASE STUDY: CORPORATE BREACH

Post-Breach Analysis:

- Internal communication – content and timing.
- External communication – content and timing.
- Designated spokesperson – who delivers message, how, and when.
- Correcting misinformation reported in media.

Critical Next Step: Reputation Management Campaign

RM is a brand rehabilitation program, including:

- Messaging-moving forward
- Internal communications campaign-employee outreach
- Critical stakeholder engagement-partners, vendors, analyst, government-*Win them back!*
- Corporate social responsibility campaign-PSAs
- Media & analyst roadshow
- Op-eds, Letters to the Editors
- Earned media campaign shifting focus to positive corporate stories, programs and services
- Digital advertising campaign promoting the corporate brand

Move from the negative to the positive-remind the marketplace why they respected your brand prior to the incident

Critical Take-Away

- Have a current, tested and practiced Incident Response Plan in place to efficiently work through the incident response process.
- Have a current, tested and practiced Reputation Management Plan in place to restore the brand to pre-incident position as soon as possible.
- Identify and utilize outside public relations and outside privacy counsel resources from pre-incident, and have these resources work together.
- Create crisis messaging that fits within the brand guidelines, and have a brand rep available to ensure authenticity.
- Ensure message is clear, consistent and accurate – avoid confusion and control the story.

Reputational Risk – Real or Fallacy

Internet of Everything and More

Internet of Everything and More

Ken Munro
Partner
Pen Test Partners

Live Cyber Incident Simulation Exercise

What was the exercise?

On 9 February, Advisen hosted a cyber incident simulation exercise that saw a selected teams of experts – representing the various stakeholders in a real event – work through a mock cyber incident in real time.

An observation team critiqued the handling of the incident and now report back some best practices and key takeaways from the exercise.

CYBER RISK INSIGHTS CONFERENCE

10 FEBRUARY 2015 | LONDON

ADVISEN Insurance Intelligence

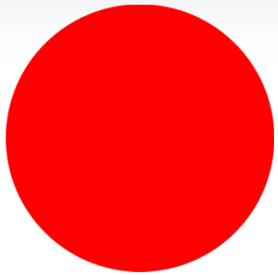
Who took part?

Red Team: A group of cyber security experts who devised the mock incident to be as realistic as possible and to test the 'corporation' to its limits.

Also acted as external resources to the Blue Team in crisis response

Blue Team: A select group representing the key cyber stakeholders within the corporation under attack. This team – made of board members and operations executives played roles on the day

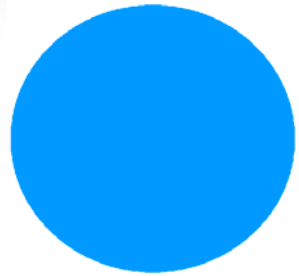
Live Cyber Incident Simulation Exercise



Red Team Participants

- Melanie Dougherty Thomas, Inform
- Chris Pogue, Nuix
- Stuart Quick, PGI
- Melissa Ventrone, Wilson Elser

Live Cyber Incident Simulation Exercise



Blue Team Participants

- Iain Ainslie, ACE
- Chris Cotterell, Safeonline
- Lara Forde, ePlace Solutions
- John Jolly, RedJack
- Sheelagh Keddie, Common Sense Privacy
- Randy Krause, ePlace Solutions
- Sarah Stephens, JLT Specialty

Observation Team

- **Cameron Azari**, Vice President, Epiq Systems
- **Peter Foster**, Executive Vice President of Cyber Practice, Willis
- **Matthew Hogg**, Vice President and Underwriting Manager, Liberty Specialty Markets
- **Cheryl Martin**, Partner, EMEIA Financial Services Advisory-Cyber Security, Ernst & Young LLP
- **Ira Scharf**, Chief Strategy Officer, BitSight Technologies
- **Melissa Ventrone**, Partner, Wilson Elser Moskowitz Edelman & Dicker LLP

The scenario

- Aston Maureen global car manufacturing company
- UK headquartered – dozens of worldwide locations
- 30,000 employees – 25 billion USD revenue
- Produces very high-end to commuter vehicles
- IT centrally managed, but data stored "all over the place"
- Provided with insurance coverage information and availability of legal on retainer
- Allowed to ask Red team any question they could think of

Pre-event pitfalls

Why would you be set up to fail?

Preparedness

- Have a plan
- Know how it works
- Understand where data is and how get access to it
- Understand legal and regulatory environment

CYBER RISK INSIGHTS CONFERENCE

10 FEBRUARY 2015 | LONDON

ADVISEN Insurance Intelligence

Post-event pitfalls:

How can your response let you down?

Challenges faced

- Consider leadership
  - Team
  - Delegation
  - Skills of a leader

- Prioritisation
  - When does incident become crisis?
  - Risk appetite and quantifying economic threat
  - Reputational harm

- Documentation of process

Key takeaways

- Preparedness
- The importance of assembling the proper team
- Establish a leader - delegate
- Practice your drill
- Understanding your internal procedures (data)
- Understanding legal and regulatory obligations
- Prioritize (during an event)
- Anticipate 3rd party responses
- Communicate to all stakeholders
- Document your response

CYBER RISK INSIGHTS CONFERENCE

10 FEBRUARY 2015 | LONDON

ADVISEN Insurance Intelligence

Thank you to our Sponsors

ZURICH

Swiss Re Corporate Solutions

AIG

Willis

Paragon

XL

LEWIS BRISBOIS BISGAARD & SMITH LLP ATTORNEYS

epiq SYSTEMS

beazley

BITSIGHT

cfc Underwriting