Massachusetts Risk Insurance Management Society

RIMS

January Meeting

Norwood Massachusetts
Welcome
Presenters: Eddie Molloy & Dan Aloï

Advent Cat Risk
RISK MANAGEMENT CONSULTANTS

specializing in catastrophic risk protection
WWW.ADVENTCATRISK.COM
TODAY'S TOPIC: NEW AND EMERGING CYBER RISK
ABOUT US

We are a Risk Management consulting practice with over 30 years of successful experience at managing corporate risk programs such as – enterprise Insurance including cat risk management, crisis management, business continuity, and cyber attack preparedness and response.

We have successfully provided these services to the Engineering, Public Utility, Commercial Nuclear Power Generation and Health Care sectors.

We help companies develop effective insurance placements, plans, procedures and training programs which enable senior management to lead their organization through tough times and survive on the other side.
SOURCES OF INFORMATION

The Ponemon Institute @ http://www.ponemon.org/ - “The Ponemon Institute conducts independent research on privacy, data protection and information security policy.”


HHS – Listing of Cyber attacks on health care operations @ http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

Hackmageddon – Good source of new cyber risks and how affected parties @ http://hackmageddon.com/
RISK MANAGERS AND THEIR CHALLENGES

HIGH PROFILE NOW

SHAREHOLDER SUITS, D&Os, etc.
PROPERTY LOSS
MERGERS AND ACQUISITIONS
CONTRACTING & COUNTER PARTY RISKS

THE FUTURE TOP PRIORITIES

CYBER RISK
INTELLECTUAL PROPERTY RISKS
FINANCIAL GUARANTEES
MORE RELIANCE ON DATA

Projected Annual Datacenter Construction Size (billions of $)

- Global
- US

Source: C. Belady
Historical National Big Picture
Cost & Defense for Attacks

Cost of Attack Capability

Availability of Capability

1945
Invasion

1955
Strategic Nuclear Weapons

1960
Missiles ICBM & SLBM

1970
Cruise Missile

1975
Precision Guided Munitions

1985

Today

Computer

Source: FEDERAL BUREAU OF INVESTIGATION
Cyber Division FBIHQ

Cyber Attacks: The Next Frontier
Gen. Keith Alexander is the director of the National Security Agency and oversees U.S. Cyber Command.

"the theft of intellectual property costs American companies $250 billion a year." He also mentioned a McAfee estimate that the global cost of cybercrime is $1 trillion.
CYBER RISK COSTS

Average annualized cost by industry sector

<table>
<thead>
<tr>
<th>Industry Sector</th>
<th>FY 2010</th>
<th>FY 2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defense</td>
<td>$16.31</td>
<td>$19.93</td>
</tr>
<tr>
<td>Utilities &amp; energy</td>
<td>$4.64</td>
<td>$15.63</td>
</tr>
<tr>
<td>Financial services</td>
<td>$5.28</td>
<td>$12.37</td>
</tr>
<tr>
<td>Technology</td>
<td>$2.68</td>
<td>$9.29</td>
</tr>
<tr>
<td>Communications</td>
<td>$2.86</td>
<td>$8.09</td>
</tr>
<tr>
<td>Services</td>
<td>$4.58</td>
<td>$5.05</td>
</tr>
<tr>
<td>Healthcare *</td>
<td>$3.06</td>
<td>$4.02</td>
</tr>
<tr>
<td>Public sector</td>
<td>$5.36</td>
<td>$5.68</td>
</tr>
<tr>
<td>Transportation</td>
<td>$3.72</td>
<td>$5.24</td>
</tr>
<tr>
<td>Industrial</td>
<td>$2.77</td>
<td>$4.02</td>
</tr>
<tr>
<td>Consumer products</td>
<td>$3.60</td>
<td>$3.60</td>
</tr>
<tr>
<td>Hospitality *</td>
<td>$2.99</td>
<td>$3.60</td>
</tr>
<tr>
<td>Retail</td>
<td>$2.77</td>
<td>$2.99</td>
</tr>
</tbody>
</table>

*Industry was not represented in the FY2010 benchmark sample.

Ponemon Report 2012
A CYBER ATTACK TIMELINE

South Carolina’s Revenue agency - 2012:

Aug. 13: A phishing email went to multiple Revenue employees.

Aug. 27: The attacker logged into Revenue’s remote access service using legitimate credentials.
Aug. 29: The attacker executed utilities designed to obtain user account passwords on six servers.
Sept. 2: The attacker interacted with 21 servers.

Sept. 12: The attacker copied database backup files to a staging directory.

Sept. 13-14: The attacker compressed the database backup files into 14 encrypted archives, then moved those from the database server to another server and sent the data to an Internet system. The backup files and archives were then deleted.

Sept. 15: The attacker interacted with 10 systems using a compromised account.

Oct. 17: The attacker checked connectivity to a server using the back door previously installed on Sept. 1, but there’s no evidence of additional activity.

Oct. 19-20: Revenue removes the attacker’.
SAN FRANCISCO — The antivirus industry has a dirty little secret: its products are often not very good at stopping viruses. Consumers and businesses spend billions of dollars every year on antivirus software. But these programs rarely, if ever, block freshly minted computer viruses, experts say, because the virus creators move too quickly. .......A new study by Imperva, a data security firm in Redwood City, Calif..... collected and analyzed 82 new computer viruses and put them up against more than 40 antivirus products, made by top companies like Microsoft, Symantec, McAfee and Kaspersky Lab..... **They found that the initial detection rate was less than 5 percent.**
CYBER RISK TRENDS HISTORY
<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Target</th>
<th>Description</th>
<th>Attack</th>
<th>Target Category</th>
<th>Attack Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nov 16</td>
<td>@DARWINARE</td>
<td>Minnesota United States Bankruptcy Court (mnb.uscourts.gov)</td>
<td>@DARWINARE hacks the Minnesota United States Bankruptcy Court (mnb.uscourts.gov) and dumps nearly 1,300 accounts with usernames and hashed passwords.¹</td>
<td>SQLi</td>
<td>Government</td>
<td>Cyber Crime</td>
</tr>
<tr>
<td>Nov 17</td>
<td>Môle</td>
<td>Fuel Up to Play 60 (fueluptoplay60.com)</td>
<td>A hacker called Môle hacks Fuel Up to Play 60 (fueluptoplay60.com) and dumps 100,000 credentials with first and last names, emails and clear text passwords.²</td>
<td>SQLi</td>
<td>Organization: Education</td>
<td>Cyber Crime</td>
</tr>
<tr>
<td>Nov 17</td>
<td>i0Illusion</td>
<td>Animal Legal Defense Fund (aldf.org)</td>
<td>i0Illusion hacks the Animal Legal Defense Fund (aldf.org) and dumps 4,000 records with full personal details such as usernames, names, phones, address and emails.³</td>
<td>SQLi</td>
<td>Organization: Cyber Crime</td>
<td>Cyber Crime</td>
</tr>
<tr>
<td>Nov 17</td>
<td>?</td>
<td>FreeBSD.org</td>
<td>FreeBSD.org announces that on Sunday 11th of November, an intrusion was detected on two machines within the FreeBSD.org cluster. The affected machines were taken offline for analysis. The intrusion happened via SSH authentication key and login credentials stolen from a developer. No evidence is found of any modifications that would put any end user at risk.⁴</td>
<td>Account Hijacking</td>
<td>Organization: Computer Software</td>
<td>Cyber Crime</td>
</tr>
<tr>
<td>Nov 17</td>
<td>YeZeta</td>
<td>Zacatecas Government</td>
<td>YeZeta hacks the web portal of Zacatecas Government (Portal de Gobierno de Zacatecas: zacatecas.gob.mx) and dumps nearly 500 records with personal information.⁵</td>
<td>SQLi</td>
<td>Government</td>
<td>Cyber Crime</td>
</tr>
<tr>
<td>Nov 17</td>
<td>YeZeta</td>
<td>PCMDI</td>
<td>YeZeta hacks the website of PCMDI (Program for Climate Model Diagnosis and Intercomparison: www-pcmdi.llnl.gov) and dumps nearly 300 records with personal information.⁶</td>
<td>SQLi</td>
<td>Government</td>
<td>Cyber Crime</td>
</tr>
<tr>
<td>Nov 17</td>
<td>YeZeta</td>
<td>Secretaría De Educación Pública</td>
<td>YeZeta hacks the website of sep.gob.mx (Secretaría De Educación Pública) and dumps 215 records with personal information.⁷</td>
<td>SQLi</td>
<td>Government</td>
<td>Cyber Crime</td>
</tr>
<tr>
<td>Nov 18</td>
<td>@ThisIsGameOver</td>
<td>myWoWArmory.com</td>
<td>@ThisIsGameOver hacks myWoWArmory.com (a World Of Warcraft community) and dumps 2,800 records with usernames and clear text passwords.⁸</td>
<td>SQLi</td>
<td>Game Community</td>
<td>Cyber Crime</td>
</tr>
<tr>
<td>Nov 18</td>
<td>@ThisIsGameOver</td>
<td>Ducat India</td>
<td>@ThisIsGameOver hacks Ducat India (ducatindia.com) and dumps more than 900 records containing personal information.⁹</td>
<td>SQLi</td>
<td>Industry: IT Training</td>
<td>Cyber Crime</td>
</tr>
</tbody>
</table>

2012

ATTACKS INCREASED ON:
- GOVERNMENT
- HACKTAVISTS
- DDoS ON FINANCIAL SERVICES (Wells Fargo, Chase, JPM)
CYBER LAWS

Cyber Laws:

Privacy, Fraud, Health Information and Various Crimes (e.g. stalking)

Federal and State Laws (note: 2011 SEC reporting guidance & insurance information)

Global Laws

Good Resource: Global Cyber Law Database @ http://cyberlawdb.com/main/
EXAMPLES OF CYBER ATTACKS ON COMPANIES

“Cyber attacks pose the biggest threats to national security and now by impacting our economy though businesses by proxy”, says former Department of Homeland Security Secretary Michael Chertoff.

TJX - $250MM

Sony - $1Bn+

Hannaford Brothers - $250MM

Health Care Breaches -
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
Financial Effects of Various Cyber Events

- Business Interruption: Hundreds of $MMs to $BNs
- Unintended Records Dissemination: $MMs to Hundreds of $MMs
- Loss of Control of Devices: $MMs to Hundreds of $MMs
- Denial of Services: $MMs to Hundreds of $MMs
- Phishing, Virus Attacks, etc.

Note: Probability is moving to the right and consequences are moving up at an alarming rate
SOME GOOD NEWS

- Organizational alignment
- Encryption use is increasing
- Insider risks are decreasing
- Decreasing risks from virtual computing environments
- More defense in depth of data environments
Any electronic based threat which can adversely affect operations, compromise information privacy and/or deteriorate customer service and relationships and, depending on severity can have major financial impacts and regulatory sanctions.

<table>
<thead>
<tr>
<th>VULNERABILITY</th>
<th>THREAT</th>
<th>EFFECT</th>
<th>CONSEQUENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security</td>
<td>• Hackers</td>
<td>Mostly financial and isolable.</td>
<td>• Customer relations</td>
</tr>
<tr>
<td></td>
<td>• Lost storage devices</td>
<td></td>
<td>• Regulatory</td>
</tr>
<tr>
<td></td>
<td>• Failure to follow industry protocol</td>
<td></td>
<td>• Board review</td>
</tr>
<tr>
<td>Business Interruption</td>
<td>• Purposeful attack</td>
<td>Major financial</td>
<td>• Customer financial impact</td>
</tr>
<tr>
<td></td>
<td>• Errors and Omissions by employees or contractors</td>
<td></td>
<td>• Regulatory and Board Involvement</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Litigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Infrastructure impact</td>
</tr>
<tr>
<td>Intellectual Property</td>
<td>• Allegations of theft and litigation</td>
<td>Major financial and major collateral damage to partners and customers</td>
<td>• Large dollar litigation</td>
</tr>
<tr>
<td></td>
<td>• Compromised property</td>
<td></td>
<td>• Major effect on enterprise</td>
</tr>
<tr>
<td>Effect from stakeholders</td>
<td>• Interruption from contractors and/or data breaches</td>
<td>Customer impact, lawsuits, discovery and forensic costs</td>
<td>• Regulatory involvement</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Costs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Relationships</td>
</tr>
</tbody>
</table>
HYPOTHETICAL SCENARIO AFFECTING YOUR COMPANY

- You are the Chief Risk Officer or CFO
- Your CEO was alerted that a highly credible and ultra sophisticated cyber attack is in progress at your company – Ransomware (DDoS)
- The purpose of the attack is to extort $150 MM in order to avoid major business disruption set for five days from today
- A letter is expected spelling out the terms of the money transfer
- There is little hope of thwarting it in time
- Your CEO wants you to prepare a plan of action with multiple options for he and the Board of Directors to consider
- The FBI will support you with some forensic information but your IT teams will need to do the bulk of the work to “fix it”
QUESTIONS FOR YOU

- How do you assess the materiality of the risk?
- Should you pay the extortion demands? How?
- Are you insured for extortion? Business Interruption? How much coverage do you have for all damages?
- How would you project manage this Crisis?
- How long of a disruption would it take to have a significant financial impact?
- Once the news leaks out, what would you expect this to do to market share, stock price and sales?
AHEAD OF TIME

A Real Crisis Plan in Place – ‘Ad hoc won’t work and is not enough’
- A real plan – a Fortune 100 company should spend at least $2-5M/yr on plans
- A place to go – a Corporate Emergency Response Center
- Command and Control by CEO and Directs
- Drilled monthly and exercised yearly

Measuring the Potential and Actual Losses - Insurance needs and effective claims management
- A prior scenario evaluation of losses and associated costs – helps with assessment and proof of loss – revenue, infrastructure restoration, performance guarantees, fines, damages, etc.
- A contracted IT forensic company to make a timely assessment
- Legal team in place with resources to make a determination of contractual damages

Pre-analysis of Risk Hedges
- Knowing the counterparties and protections – contracts, additional insured status, etc.
- Knowing the coverages and documenting scenarios with U/Ws ahead of a loss
- Executive summaries of insurance coverages
- Other hedges – reinsurance, captives, etc.
INSURANCE
TYPES & SCALE OF FINANCIAL IMPACT AND INSURANCE

Relative Financial Consequence

- Fines, Penalties, Punitives
- Revenue Loss
- Reputation Loss
- Business Impact (e.g. Shutdown, etc.)
- Damages to Partners
- Damages to Customers
- Shareholder Suits

Potential Insurance Coverages

- Director and Officer
- General Liability
- Property Business Interruption
- Cyber Liability
- Patent Infringement
- Errors and Omissions
## Tradional Insurance and Cyber Coverage

<table>
<thead>
<tr>
<th>Policy</th>
<th>Coverage</th>
<th>Considerations</th>
<th>Parties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property</td>
<td>Media/Business Interruption</td>
<td>Loss has to have covered 'proximate' causes</td>
<td>1&lt;sup&gt;st&lt;/sup&gt; and/or Additional Insureds</td>
</tr>
<tr>
<td>CGL</td>
<td>Physical Injury/Personal and Advertising</td>
<td>Am. Guar. Liab. Vs Ingram Micro - physical damage can include loss of use, access, functionality</td>
<td>3&lt;sup&gt;rd&lt;/sup&gt; party</td>
</tr>
<tr>
<td></td>
<td>Injury/Data Damage (?)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management Policies – D&amp;O's/E&amp;O's</td>
<td>At minimum, Defense and possibly indemnification of the loss; Investigations</td>
<td>For large companies - very customized</td>
<td>1&lt;sup&gt;st&lt;/sup&gt;, 3&lt;sup&gt;rd&lt;/sup&gt; Party and Shareholders</td>
</tr>
<tr>
<td>K&amp;R Policy</td>
<td>Investigation; BL; Extortion; Defense</td>
<td>Coverage maybe implied not specific</td>
<td>1&lt;sup&gt;st&lt;/sup&gt; and 3&lt;sup&gt;rd&lt;/sup&gt; Party</td>
</tr>
</tbody>
</table>
NEW WORLD OF CYBER COVERAGE

- Network Liability
- Technology E&O
- Cloud Computing
- Patent Infringement
- Special Cover – Remediation, Extortion, Loss of Use, Advertising
- Fidelity/Crime Coverage
CYBER COVERAGE

- Identity theft - credit monitoring of customers and loss costs
- Privacy loss damages
- Denial of service
- 3rd party (increasing 1st party) coverages for loss of use and business interruption
- Defense and related costs – e.g. forensics
- Content injury claims such as misuse or unauthorized use of copyrighted material
- Technology E&O coverages for damages through software development and installation
- Loss of digital media and assets
- Extortion and terrorism
THE STATE OF CYBER RISK INSURANCE MARKET

- There are about 26 insurers offering coverages
- World capacity ~ $250 Million and increasing
- Premiums are approximately $1 Billion in 2012 with premium growth averaging 20%/yr
- Pricing is flat
- The market is increasing in new sales but only 30% of publically traded companies are purchasing coverage
- Only a few companies are willing to manuscript coverages
- Policies are prone to sublimits and exclusions
- Coverages expanding for ‘cloud’ and E&O risks

LIST OF CYBER INSURERS
- Ace
- Admiral
- Allied World
- Arch
- Argo Pro
- Axis
- Beazley
- Berkley
- Brit
- CFC
- Chartis
- Chubb
- CNA
- Crum & Forster
- Digital Risk
- The Hartford
- Hiscox
- Ironshore
- Liberty International
- Markel
- NAS
- Navigators
- OneBeacon
- Philadelphia
- RLI
- Travelers XL
- Zurich
TYPICAL CYBER INSURANCE PROGRAMS

- Typically ‘off the shelf policy form’ with limited coverages
- Major limitations on coverages — e.g. defense, third party damages, risks covered
- No intellectual property coverage and no material Tech E&O coverages
- Many exclusions — punitive, etc.

Note: This example is for a Fortune 100 Company
CYBER INSURANCE EXCLUSIONS

- Bodily injury and physical damage
- May have geographical limitations
- No coverage for investigations, fines, etc. - Governmental
- Remediation and loss stop costs
- Claims - infringement of a patent, trade secret, copyright, trademark or service mark unless arising from electronic publishing activity
- “Beta” testing
- Claims arising from contractors
- Criminal acts (consider severability and “final adjudication” language)

CRIME POLICY EXCLUSIONS

- Collusion by D&Os
- Loss resulting directly or indirectly from the input of electronic data into a Computer System terminal device
- Loss from fraudulent modification of software
- Loss from unverified voice instruction
- Asset loss resulting from fraudulent source documentation used in the preparation of electronic instructions
- Losses from failures of EDP systems
- Fees, investigatory costs, global
ADEQUATE CYBER INSURANCE PROGRAM

- More limits ~
  - Depends on company risk tolerance
- Broadened coverages
- Customized to the needs
- Sub limits for additional insured
- Integration with other program insurance coverages
- International coverages
- Coverage certainty

<table>
<thead>
<tr>
<th>Level</th>
<th>Insurer</th>
<th>Limit (MM)</th>
<th>Level Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$231MM</td>
<td>E Insurer</td>
<td>$100 MM</td>
<td>(limits eroded by deductible and underlying)</td>
</tr>
<tr>
<td>$131MM</td>
<td>D Insurer</td>
<td>$50 MM</td>
<td>(limits eroded by deductible and underlying)</td>
</tr>
<tr>
<td>$61MM</td>
<td>C Insurer</td>
<td>$50 MM</td>
<td>(limits eroded by deductible and underlying)</td>
</tr>
<tr>
<td>$31MM</td>
<td>B Insurer</td>
<td>$25 MM</td>
<td>(limits eroded by deductible and underlying)</td>
</tr>
<tr>
<td>$6MM</td>
<td>A Insurer</td>
<td>$5MM / $5MM</td>
<td></td>
</tr>
<tr>
<td>$1MM</td>
<td>Self Insured Retention</td>
<td>$1MM / $10MM</td>
<td></td>
</tr>
</tbody>
</table>
CYBER RISK ASSESSMENT PROCESS

• Model the major vulnerabilities of your organization

• Establish a “what if” quantification of potential damages

• Aside from internal controls, can it be insured? Can it be measured post event? Can it be mitigated by a response plan

• Is there an Crisis Management Plan? Improvement costs?
PROGRAM DESIGN PROCESS

- Determine the cost/benefit of hedging options as insurance, reinsurance, risk transfer to partners

- Options available in today's financial markets

- Cost and resources to improve financial controls and improve the Crisis Response Plan
IMPLEMENTATION PROCESS

- Draw up a manuscripted insurance policy
- Ensure that coverages are integrated
- Market the program to risk takers
- Develop or enhance a Crisis Response Plan and forensic action plan
Crisis Response Plan Model
CRISIS PLANNING

Top Five Current Day Weaknesses

- Culture of Indifference & Avoidance - Cosmetic buy-in by BOD and CEO
- Lack of Clear Roles & Responsibilities
- Lack of Documented Plans & Procedures - Fractionation
- Lack of In-Place Resources
- Pre-planned Recovery Capability – Purchase Orders, Prior Approvals, etc.
CRISIS PLANNING

Attributes of Great Crisis Plans

- Enterprise Wide Policy
- Clear Organizational Roles & Command/Control & Resources
- Coordinated Plans & Procedures – “The 10 Page Plan”
- All Hazards Approach
- Qualified Emergency Response Team
- Drills & Exercises Conducted & Evaluated
- Corrective Action Program
CRISIS PLANNING

**Benefits of Great Crisis Plans**

- Save the Company (Think of J&J in 1982 (Tylenol) and NU in 1985 (Hurricane Gloria))
- Customer/Regulator Confidence - Costs and Distractions (Think of 2008 Defaults)
- Avoid Loss of Company Momentum
- Protect the Bottom Line (100 to 1 Payback)
WHAT ARE THE COSTS, TIMING & RESOURCES?

Costs:
- Insurance Rates on Line are anywhere from 3% to 15% depending on risk
- Project costs are highly variable and depend on current programs
- Going forward costs for additional controls

Timing:
- 2 to 6 months of design and implementation depends on risk and complexity of operations

Resources:
- Project lead - Risk Managers
- Legal - internal or external
- IT - internal
- Forensics - external
- Actuarial - external