MEASURING & PRICING THE COST DRIVERS OF A CYBER SECURITY RISK EVENT

PRESENTED BY
KEITH BURKHARDT, V.P. KRAUS-ANDERSON INSURANCE
Overview

I. Why are cyber security events occurring?
II. What are the financial variables that impact a company when a cyber security event occurs?
III. What are the estimates of a cyber event claim cost?
IV. How is cyber risk presently underwritten?
V. What current issues are companies addressing to improve their cyber risk?
I. WHY ARE CYBER SECURITY EVENTS OCCURRING?
“The Internet?  
We’re not interested.”

Bill Gates, Microsoft Founder, 1993
81% Percentage of Americans who are online

11 billion Total web searches per month in the U.S.

210 billion Total number of e-mails sent daily

1 in 8 Number of U.S. married couples who met online

28% Internet growth in content 2014-2015
Ronnie Biggs
The Great Train Robbery, 1963
Albert Gonzales
Heartland Hack, 2009
<table>
<thead>
<tr>
<th>Credit card info</th>
<th>Date of birth</th>
<th>Social Security number</th>
<th>Mother’s maiden name</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Credit card" /></td>
<td><img src="image2" alt="Date of birth" /></td>
<td><img src="image3" alt="Social Security number" /></td>
<td><img src="image4" alt="Mother’s maiden name" /></td>
</tr>
</tbody>
</table>

Health record
DATA BREACH STATS
The 2014 Verizon Data Breach Investigation Report Dispelled The “Only a Big Company is a Target” Myth

- 94% of attacks are on firms under 1000 employees
- All industries are vulnerable. Information & Professional services, financial organizations, consumer products & manufacturing.
- 76% of attacks used weak/stolen user credentials
- 92% of breaches originated from external parties not employees.
- 82% of breaches were discovered by a third party (vendor, customer, etc.).
- 75% of breaches took weeks to be “discovered” by the victim organization.
60% of breached small-medium sized organizations were OUT OF BUSINESS within 6 months of discovering a breach.
The 2015 Verizon Data Breach Investigation Report Focused in on Breach Tactics, Causes and Financial Impact

- 2014 trends & STATS continued at or near same levels.
- 70% of breaches where the motive was understood, were focused on a secondary victim/organization.
- 60% of the breaches the attackers infiltrated the victims systems within minutes.
The Report Confirms Leading Tactics to Breach an Organization Were:

- Phishing – 23% of receptionists open phishing messages.
- Common vulnerabilities & exposures (CVE). Poor patching strategies are 99.9% of the culprit is a breach or attack is via the system platform.
- Mobile devices are NOT a preference vector in data breaches (Android is strongest in this area).
- Malware – Over 50% of breaches in this area were discovered 35 days or more.
  - The #1 victim is Education
  - Insurance is #4
The 2015 report confirms 96% of all intrusions could be classified in 9 categories and the frequency could assist companies in reducing their cyber risk.

- **POS Intrusions**: 28.5%
- **CrimeWare**: 18.8%
- **Cyber-Espionage**: 18%
- **Insider Misuse**: 10.6%
- **Web App Attacks**: 9.4%
- **Miscellaneous Errors**: 8.1%
- **Physical Theft/Loss**: 3.3%
- **Payment Card Skimmers**: 3.1%
- **Denial of Service**: 0.1%

Frequency of incident classification patterns with confirmed data breaches.
II. WHAT HAPPENS TO A MID-SIDE COMPANY WHEN A CYBER BREACH OCCURS
2 Reports Attempt to Identify Cyber Costs

- 2015 Verizon Data Breach (79,000 Security Incidents)

- 2015 Ponemon 2015 Cost of Cyber Crime Study: Global – (252 Large Companies)
The Cost of a Breach

Notable breach costs/expense that are incurred include:

- Legal Advice/Defense Costs
- Notification to affected parties (customers, vendors, employees)
- ID Theft Monitoring
- Call Center
- Regulatory Fines & Penalties
- Forensic Investigation

- Business Interruption/Extra Expense
- Damage to Systems & Equipment
- Court Appearance Costs
- P.R. Expenses (Managing Opinion)
- Reputational Harm
Ponemon Report (10/2012)

Percentage cost for external consequences
Consolidated view, n= 252 separate companies

- Business disruption: 39%
- Information loss: 35%
- Revenue loss: 21%
- Equipment damages: 4%
- Other costs: 2%
Percentage cost by activities conducted to resolve a cyber attack
Consolidated view, n= 252 separate companies

Detection: 30%
Recovery: 23%
Containment: 16%
Investigation: 14%
Incident Mgmt: 9%
Ex-post response: 7%
III. CURRENT ESTIMATES OF A CYBER EVENT CLAIM
Two Opinions/Methodology

- Verizon calculates cost of a cyber event by number of records stolen

- Ponemon calculates cyber costs by enterprise seats (defined as number of direct connections to the network and enterprise systems)
Expected average loss by records lost

Ranges of expected loss by number of records

<table>
<thead>
<tr>
<th>RECORDS</th>
<th>PREDICTION (LOWER)</th>
<th>AVERAGE (LOWER)</th>
<th>EXPECTED</th>
<th>AVERAGE (UPPER)</th>
<th>PREDICTION (UPPER)</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>$1,170</td>
<td>$18,120</td>
<td>$25,450</td>
<td>$35,730</td>
<td>$55,660</td>
</tr>
<tr>
<td>1,000</td>
<td>$3,110</td>
<td>$52,260</td>
<td>$67,480</td>
<td>$87,140</td>
<td>$1,461,730</td>
</tr>
<tr>
<td>10,000</td>
<td>$8,280</td>
<td>$143,360</td>
<td>$178,960</td>
<td>$223,400</td>
<td>$3,866,400</td>
</tr>
<tr>
<td>100,000</td>
<td>$21,900</td>
<td>$366,500</td>
<td>$474,600</td>
<td>$614,600</td>
<td>$10,283,200</td>
</tr>
<tr>
<td>1,000,000</td>
<td>$57,600</td>
<td>$892,400</td>
<td>$1,258,670</td>
<td>$1,775,350</td>
<td>$27,500,090</td>
</tr>
<tr>
<td>10,000,000</td>
<td>$150,700</td>
<td>$2,125,900</td>
<td>$3,338,020</td>
<td>$5,241,300</td>
<td>$73,943,950</td>
</tr>
<tr>
<td>100,000,000</td>
<td>$392,000</td>
<td>$5,016,200</td>
<td>$8,852,540</td>
<td>$15,622,700</td>
<td>$199,895,100</td>
</tr>
</tbody>
</table>
### Table 1. Quartile analysis Cost expressed in US dollars

<table>
<thead>
<tr>
<th>Quartile</th>
<th>FY 2015 (n-252)</th>
<th>FY 2014 (n-252)</th>
<th>FY 2013 (n-252)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quartile 1 (Smallest)</td>
<td>$3,279,376</td>
<td>$2,967,723</td>
<td>$2,965,464</td>
</tr>
<tr>
<td>Quartile 2</td>
<td>$5,246,519</td>
<td>$5,107,532</td>
<td>$4,453,688</td>
</tr>
<tr>
<td>Quartile 3</td>
<td>$8,987,450</td>
<td>$8,321,024</td>
<td>$6,659,478</td>
</tr>
<tr>
<td>Quartile 4 (Largest)</td>
<td>$13,372,861</td>
<td>$13,805,529</td>
<td>$14,707,980</td>
</tr>
</tbody>
</table>

### Table 2. Quartile analysis Cost expressed in US dollars

<table>
<thead>
<tr>
<th>Quartile</th>
<th>2015 Cost per seat</th>
<th>2014 Cost per seat</th>
<th>2013 Cost per seat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quartile 1 (Smallest)</td>
<td>$1,555</td>
<td>$1,601</td>
<td>$1,388</td>
</tr>
<tr>
<td>Quartile 2</td>
<td>$878</td>
<td>$962</td>
<td>$710</td>
</tr>
<tr>
<td>Quartile 3</td>
<td>$709</td>
<td>$726</td>
<td>$532</td>
</tr>
<tr>
<td>Quartile 4 (Largest)</td>
<td>$368</td>
<td>$437</td>
<td>$431</td>
</tr>
</tbody>
</table>
IV. HOW IS CYBER RISK PRESENTLY UNDERWRITTEN?
Multiple Methods of Underwriting

- Can be Generally grouped into 3 Theories:
  
  I. Selective Underwriting
  
  II. Collateral Customer Underwriting
  
  III. The Law of Large Numbers Underwriting
The Selective Underwriting Process

- Long application forms
- Warranty app wording
- Highly detailed review of Customer’s IT Systems
- Narrow number of applicants qualify
- Quotes manage risk by limiting the policy offerings: limits, deductibles, coverage based on Underwriting appetite of domicile, industry, size of risk, and app info
The Collateral Customer Underwriting Process

- Add Cyber extensions to the customer’s current policy
- Additional premium is calculated as percent of policy premium
The Law of Large Numbers Underwriting Process

- Premise is based on Macro data number of potential businesses creating a large pool of insureds & predictability
- 85mm possible insured entities vs. 250,000 (est.) cyber incidents
- Remove barriers of purchase:
  - Simple application
  - Broad coverage rating based on domicile, industry, revenue and number of employees
  - Streamlined claims process & payment (focused on cyber time vs. natural time)
Law of Large #s Method sets Policy limits within an insurers risked based capital model
V. WHAT CURRENT ISSUES ARE COMPANIES ADDRESSING TO IMPROVE THEIR CYBER RISK?
Are you “Cyber Resilient”?

» Data is the new currency
» 94% of cyber-attacks are on small-mid sized firms

Questions to Develop Answers*

» Has your firm gone through the data mapping process?
» What’s your data disposal process?
» When are you engaged in the IT procurement process?
» When/how does IT fit in to the process of bringing a new product to market?
» Do you have the resources you need?

*Via CyberSmart Law & Kraus-Anderson Insurance
Be Prepared for a Security Incident

» Do you have a complete list of all accounts and services that you use?
» Would you know who to contact for any account or service that appears to have been compromised?
» Can you identify the types of sensitive data you are storing, and know where it is being stored?
» Have you developed a tiered response plan to react to incidents of varying different degrees?
» Do you have a plan for an alternate form of communication, in case email is compromised?
» Have you organized and/or standardized where all documentation is stored to minimalize the potential of having secure data stored in unknown locations?
» Do you have a data retention plan?
» Have you determine security breaches financial impact on your company and know how to finance it?
Sources

» Verizon 2015 Data breach investigation report (verizonenterprise.com)
» RSM (McGladrey’s) : Anatomy of a Breach (mcgladrey.com)
» CFCUnderwriting.com
» Beazley.com
» Infraguard.org
» CyberSmart Law (dukelawoffice.com/cybersmart-law)
» Brian Krebs (krebsonsecurity.com)