Risk Management Symposium 2015

Operational Risk in the New Age of Cybersecurity
Saturday, May 30, 2015
9:00am - 3:00pm
‘Between a Rock and a Hard Place’

incidit in scyllam cupiens vitare charybdim
Quick View

• Operational risk now includes data risk.
• Responsibility of the Board, Mgt. and staff.
• Cyber “mega” threats are increasing in volume, complexity and difficult to identify.
• Financial services, Insurance and retail are prime targets – Willy Sutton business model.
• Cyber threat actors: hackers, organized crime groups and nation states (no surprises here).
• Level 3 Tries to Waylay Hackers (5/29)
• Cyber Attacks Represent Top Risks, SEC Chief Says
• Theft of Debit-Card Data From ATMs Soars
• Cyber Insurance: One Element of Risk Management
• Regulators Altering Cyber Insurance Market
• Cyber Security Responsibility Falling to Boards
• What Happens If My Client Gets Hacked?
• World Economic Forum: Toward the Quantification of Cyber Risks (Deloitte)
THE WALL STREET JOURNAL.

RELATED NEWS

- Health Insurer CareFirst Says It Was Hacked (http://www.wsj.com/articles/health-insurer-carefirst-says-it-was-hacked-1432149975)
- Should Washington Allow Companies to Strike Back Against Hackers? (http://www.wsj.com/articles/should-washington-allow-companies-to-strike-back-against-hackers-1431022206)
Adult Dating Site Hack Exposes Millions of Users

Within hours of the data being leaked, hackers on the forum said they intended to hit victims with spam emails.

“While performing surveillance for a root9B client, the company discovered malware generally associated with nation state attacks,” root9B CEO Eric Hipkins wrote of the scheme, which he said was targeted financial institutions such as Bank of America, Regions Bank and TD Bank, among others.
Really?

• Russia and China Pledge Not to Hack Each Other...

May 8, 2015, 8:32 AM ET (WSJ)

...Russian hackers read President Barack Obama’s unclassified emails, according to senior U.S. officials. (NY Times).
Verizon DBIR

70 CONTRIBUTING ORGANIZATIONS

79,790 SECURITY INCIDENTS

2,122 CONFIRMED DATA BREACHES

61 COUNTRIES REPRESENTED"
Threat Actors

Source: Verizon DBIR
Threat Actions

Source: Verizon DBIR
Breach Discovery: hours, days, months?

Source: Verizon DBIR
The First Metric: cost per record?

Source: Verizon DBIR
Itemized

Cost of a Data Breach

- Direct Costs: $73
  - Notification
  - Call Center
  - Identity Monitoring
  - Identity Restoration
  - Discovery/Data
  - Forensics
  - Loss of Employee Productivity
- Indirect Costs: $141
  - Restitution
  - Additional Security and Audit Req’s
  - Lawsuits
  - Regulatory Fines
  - Loss of Consumer Confidence
  - Loss of Funding

Cost per Record: $214 (2010)

The Cost for Credit Unions

Cost Items Resulting from the Home Depot Breach

- Fraud: $4.89
- Card Reissuance: $2.64
- All Other Costs: $0.50
- Total Cost: $57.7 Million
- Cards Reissued: 7.2 Million
- Cost Per Card: $8.02

Source: Credit Union Natl. Assn. (CUNA), survey of credit unions Oct. 2014

Source: Ponemon Institute 2011 (sponsored by Symantec)
## Expected Loss by Number of Records

*(95% Confidence Level)*

<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>$555,660</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>

Source: Verizon DBIR
## Threat Classifications

<table>
<thead>
<tr>
<th>Classification</th>
<th>Most Affected Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. POS Intrusion</td>
<td>Accommodation, Entertainment retail</td>
</tr>
<tr>
<td>2. Payment Card Skimmer</td>
<td>Financial Services, Retail</td>
</tr>
<tr>
<td>3. Crimeware</td>
<td>Public, Information, Retail</td>
</tr>
<tr>
<td>4. Web App Attacks</td>
<td>Information, financial services, public</td>
</tr>
<tr>
<td>5. Denial of Service Attacks</td>
<td>Public, retail, financial services</td>
</tr>
<tr>
<td>6. Physical Theft/Loss</td>
<td>Public, healthcare and financial services</td>
</tr>
<tr>
<td>7. Insider Misuse</td>
<td>Public, healthcare and financial services</td>
</tr>
<tr>
<td>8. Miscellaneous Errors</td>
<td>Public, information, healthcare</td>
</tr>
<tr>
<td>9. Cyber Espionage</td>
<td>Manufacturing, public, professional</td>
</tr>
</tbody>
</table>

Source: Verizon DBIR
## Classification Patterns with Confirmed Data Breaches 2014

<table>
<thead>
<tr>
<th>Classification</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>POS Intrusions</td>
<td>28.5%</td>
</tr>
<tr>
<td>Crimeware</td>
<td>18.8%</td>
</tr>
<tr>
<td>Cyber-espionage</td>
<td>18%</td>
</tr>
<tr>
<td>Insider misuse</td>
<td>10.6%</td>
</tr>
<tr>
<td>Web app attacks</td>
<td>9.4%</td>
</tr>
<tr>
<td>Miscellaneous errors</td>
<td>8.1%</td>
</tr>
<tr>
<td>Physical theft/loss</td>
<td>3.3%</td>
</tr>
<tr>
<td>Payment card skimmers</td>
<td>3.1%</td>
</tr>
<tr>
<td>Denial of service</td>
<td>0.1%</td>
</tr>
</tbody>
</table>

Source: Verizon DBIR
Classification Patterns Over Time

Source: Verizon DBIR
## By Incident Pattern and Victim Industry

### Table

<table>
<thead>
<tr>
<th>CRIMEWARE</th>
<th>CYBER-ESPIONAGE</th>
<th>DENIAL OF SERVICE</th>
<th>PHYSICAL THEFT/LOSS</th>
<th>MISCELLANEOUS ERRORS</th>
<th>PAYMENT CARD SKIMMERS</th>
<th>POINT OF SALE</th>
<th>INSIDER MISUSE</th>
<th>WEB APP ATTACKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1%</td>
<td>9%</td>
<td>1%</td>
<td>2%</td>
<td>91%</td>
<td>5%</td>
<td>1%</td>
<td>45%</td>
<td>18%</td>
</tr>
<tr>
<td>32%</td>
<td>15%</td>
<td>11%</td>
<td>26%</td>
<td>13%</td>
<td>73%</td>
<td>7%</td>
<td>9%</td>
<td>9%</td>
</tr>
<tr>
<td>36%</td>
<td></td>
<td>2%</td>
<td>7%</td>
<td>14%</td>
<td>11%</td>
<td>31%</td>
<td>9%</td>
<td>9%</td>
</tr>
<tr>
<td>1%</td>
<td>4%</td>
<td>16%</td>
<td>32%</td>
<td>12%</td>
<td>46%</td>
<td>9%</td>
<td>9%</td>
<td>9%</td>
</tr>
<tr>
<td>14%</td>
<td>37%</td>
<td>2%</td>
<td>5%</td>
<td>7%</td>
<td>35%</td>
<td>1%</td>
<td>4%</td>
<td>1%</td>
</tr>
<tr>
<td>34%</td>
<td>60%</td>
<td>2%</td>
<td>5%</td>
<td>4%</td>
<td>1%</td>
<td>9%</td>
<td>9%</td>
<td>9%</td>
</tr>
<tr>
<td>14%</td>
<td></td>
<td>2%</td>
<td>5%</td>
<td>7%</td>
<td>79%</td>
<td>9%</td>
<td>9%</td>
<td>9%</td>
</tr>
<tr>
<td>25%</td>
<td>52%</td>
<td>2%</td>
<td>10%</td>
<td>5%</td>
<td>4%</td>
<td>4%</td>
<td>4%</td>
<td>4%</td>
</tr>
<tr>
<td>51%</td>
<td>5%</td>
<td>3%</td>
<td>23%</td>
<td>11%</td>
<td>6%</td>
<td>5%</td>
<td>5%</td>
<td>5%</td>
</tr>
<tr>
<td>11%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Industry Categories

- ACCOMMODATION
- ADMINISTRATIVE
- EDUCATIONAL
- ENTERTAINMENT
- FINANCIAL SERVICES
- HEALTHCARE
- INFORMATION
- MANUFACTURING
- MINING
- OTHER SERVICES
- PROFESSIONAL
- PUBLIC
- RETAIL

Source: Verizon DBIR
POS Compromised Payment Cards

Source: Verizon DBIR
Who gets stuck with the tab?

Sideswiped
Smaller banks pay more per card in reissue costs than their larger peers. Average reissue cost per card, by asset size of the bank

Bank asset size:
- Less than $1 billion
- $1B–$10B
- $10B–$50B
- $50B+

Note: Costs include mailing, card stock and estimated staff resources.
Source: American Bankers Association
THE WALL STREET JOURNAL.
Top 25 most common passwords used by Hackers with y/o/y changes

1. password (Unchanged)
2. 123456 (Unchanged)
3. 12345678 (Unchanged)
4. abc123 (Up 1)
5. qwerty (Down 1)
6. monkey (Unchanged)
7. letmein (Up 1)
8. dragon (Up 2)
9. 111111 (Up 3)
10. baseball (Up 1)
11. iloveyou (Up 2)
12. trustno1 (Down 3)
13. 1234567 (Down 6)
14. sunshine (Up 1)
15. master (Down 1)
16. 123123 (Up 4)
17. welcome (New)
18. shadow (Up 1)
19. ashley (Down 3)
20. football (Up 5)
21. jesus (New)
22. michael (Up 2)
23. ninja (New)
24. mustang (New)
25. password1 (New)

Source: Brian Krebs
Bad Guy Uses for Your PC

Source: Brian Krebs
Bad Guy Uses for Your Email

- Privacy
  - Your messages, calendar
  - Your Google/Skype Chats
  - Your photos
  - Call records (+mobile acct)
  - Your Location (+mobile/itunes)

- Spam
  - Commercial Email
  - Phishing, Malware
  - Stranded Abroad Scam
  - Facebook, Twitter Spam
  - Email Signature Spam

- Retail Resale
  - Facebook, Twitter, Tumbler
  - Macys, Amazon, Walmart
  - iTunes, Skype, Bestbuy
  - Spotify, Hulu+, Netflix
  - Origin, Steam, Crossfire

- Financial
  - Bank accounts
    - Email Acct. Ransom
    - Change of Billing
    - Cyberheist Lure

- Harvesting
  - Email, Chat contacts
    - File hosting accounts
    - Google Docs, MS Drive
    - Dropbox, Box.com
    - Software License Keys

- Employment
  - Forwarded Work Docs
    - Forwarded Work Email
    - Fedex, UPS, Pitney Bowes Acct
    - Salesforce, ADP Accounts

Source: Brian Krebs
2013 Identity Theft Complaints by Age Group

Source: Wikipedia Image Unknown
Victims v. Fraud in $ ‘05 to ‘12

Source: Verizon DBIR
12.7M Identity Fraud Victims, while Fraud Losses Decline in 2014

Source: Verizon DBIR

© 2015 Javelin Strategy & Research
# Key Takeaways by Threat

<table>
<thead>
<tr>
<th>Classification</th>
<th>Takeaway</th>
</tr>
</thead>
<tbody>
<tr>
<td>POS Intrusion</td>
<td>Larger breaches tend to be multi-step</td>
</tr>
<tr>
<td>Payment Card Skimmer</td>
<td>Chip and pin mandate, but implementation?</td>
</tr>
<tr>
<td>Crimeware</td>
<td>Malware used to launch DOS #8 to #2, C&amp;C remains #1</td>
</tr>
<tr>
<td>Web App Attacks</td>
<td>95% involve harvesting credentials and logging into web apps</td>
</tr>
<tr>
<td>Denial of Service Attacks</td>
<td>Continued ideological + criminal = Patch often &amp; block access to known botnet servers</td>
</tr>
<tr>
<td>Physical Theft/Loss</td>
<td>15% of incidents take days to discover</td>
</tr>
<tr>
<td>Insider Misuse</td>
<td>55% was privilege abusing access</td>
</tr>
<tr>
<td>Miscellaneous Errors</td>
<td>60% errors by SYS Admins</td>
</tr>
<tr>
<td>Cyber Espionage</td>
<td>80% starts with email attachment or link w 15% a web drive-by</td>
</tr>
</tbody>
</table>

*Source: Verizon DBIR*
95% of these incidents involve harvesting credentials stolen from customer devices, then logging into web applications with them.

Source: Verizon DBIR
Websites are complex and uneven

Source: Hanzo Archives
So you wanna’ buy a card ‘dump’?

<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>Card Type</th>
<th>Exp Date</th>
<th>Valid</th>
<th>CVV</th>
<th>City</th>
<th>State</th>
<th>ZIP</th>
<th>Bank</th>
<th>BIN</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>41773</td>
<td>VISA</td>
<td>DEBIT</td>
<td>10/17</td>
<td>Yes</td>
<td>101</td>
<td>United States, NY, Rochester, 14623</td>
<td>BANK OF AMERICA N.A.</td>
<td>American Sanctions 1</td>
<td>52.8$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>422386</td>
<td>VISA</td>
<td>DEBIT</td>
<td>05/16</td>
<td>Yes</td>
<td>101</td>
<td>United States, IA, Bettendorf, 52722</td>
<td>WELLS FARGO BANK N.A.</td>
<td>American Sanctions 1</td>
<td>52.8$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>414548</td>
<td>VISA</td>
<td>DEBIT</td>
<td>05/16</td>
<td>Yes</td>
<td>101</td>
<td>United States, PA, Hanover, 17331</td>
<td>MEMBERS 1ST F.C.U</td>
<td>American Sanctions 1</td>
<td>52.5$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>486831</td>
<td>VISA</td>
<td>DEBIT</td>
<td>04/17</td>
<td>Yes</td>
<td>101</td>
<td>United States, CO, Littleton, 80120</td>
<td>WELLS FARGO BANK N.A.</td>
<td>American Sanctions 1</td>
<td>52.8$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>448555</td>
<td>VISA</td>
<td>DEBIT</td>
<td>01/16</td>
<td>Yes</td>
<td>101</td>
<td>United States, WI, Green Bay, 54303</td>
<td>ITS BANK</td>
<td>American Sanctions 1</td>
<td>22.5$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>414708</td>
<td>VISA</td>
<td>CREDIT</td>
<td>10/16</td>
<td>Yes</td>
<td>101</td>
<td>United States, CA, Mission Viejo, 92662</td>
<td>CAPITAL ONE BANK (USA) N.A.</td>
<td>Dump or cc of this particular bank (BIN)</td>
<td>42.01$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Stolen credit cards for sale on Rescator's site index each card by the city, state and ZIP of the retail store from which each card was stolen.

Source: Brian Krebs
Let’s Go Cyber Shopping?

**Even more USA Dumps updated!**

Base name: **American Sanctions 6, 7, 8, 9**
Valid rate of: 100%
Track 1, Track 2, State/Zip. No replacements!

Base name: **American Sanctions 10, 11, 12**
Valid rate of: 100%
Track 1, Track 2, State/Zip. No replacements!

**USA Dumps update you asked for!**

Base name: **American Sanctions 5**
Valid rate of: 100%
Track 1, Track 2, State/Zip. No replacements!

Base name: **American Sanctions 4**
Valid rate of: 100%
Track 1, Track 2, State/Zip. No replacements!

Base name: **American Sanctions 3**
Valid rate of: 100%
Track 1, Track 2, State/Zip. No replacements!

Source: Brian Krebs
Card Checkers For Sale

Source: Brian Krebs
Where does stolen information go?

Many threat actors sell stolen information online using untraceable currencies in hard to track communities.

Source: Alvarez and Marsal
OUT TO THE DARK WEB
Question: *How Much Do Data Breaches Cost Big Companies?*

- Benjamin Dean Columbia University looked at 10-K filings breach related expenses for TGT, HD and SNE.
- Results were counterintuitive:
  - After insurance and write-offs, actual expenses were, on average, less than .01% of quarterly revenues.
New Scale? New Era?

Hacked by the #GOP... Warning we’ve already warned you, and this is just the beginning... We have obtained all your internal data including secrets and top secrets... if you don’t obey us, we’ll release data shown below to the world. Determine what will you do till November the 24th, 11:00 PM (GMT)

Source: Forbes
More than a Hack?

• Unreleased movies, embarrassing internal emails, personal data—including SS#s of 47,000 employees and celebrities and destroyed data... **WIPERWARE**
• $15M in investigation and remediation
• $35M in restoring financial and IT systems
Good idea: let’s name our most sensitive filename ‘SONY Clearance Lists’

Figure 3 - List of stolen data from Sony Picture servers

Source: Brian Krebs
SNE December 4, 2014

Source: MarketWatch
In spring of 2007, Sony's executive director, Jason Spaltro, discussed how protecting private data had become "a risk-based business decision."

...said that he "will not invest $10 million to avoid a possible $1 million loss."
Home Depot

50M CC#s + email addresses

From their Q3 2014 earnings report:

...recorded $43 million of pretax expenses related to the Data Breach, partially offset by a $15 million receivable for costs the Company believes are reimbursable and probable of recovery under its insurance coverage, for pretax net expenses of $28 million.”
Sept 8, 2014

Source: MarketWatch
And Target?

- 40M credit cards + phone #s
- CEO’s resignation

From their 2014 Q4 filing:

“full-year net expense of $145 million, which reflects $191 million of gross expense partially offset the recognition of a $46 million insurance receivable.”
Gone “Phishin”

Anatomy of the Target Retailer Breach

1. Attacker phishes a 3rd party contractor
2. Attacker uses stolen credentials to access contractor portal
3a. Attacker finds & infects internal Windows file server
3b. Malware scrapes RAM for clear text CC stripe data
4. Malware sends CC data to internal server; sends custom ping to notify
5. Malware sends CC data to internal server; sends custom ping to notify
6. Stolen data is exfiltrated to FTP servers

Has your Target shopping behavior changed in light of its security breach over the holidays?

- 65% still shop the same amount at Target
- 22% now shop at Target less
- 13% no longer shop at Target

Source: Bizrate Insights Target Study
Q: Has your Target shopping behavior changed in light of its security breach over the holidays?
Segment = Those who have shopped at Target (n=5,536)
Only the lowest spenders?

Changes in Shopping Behavior after Target Data Breach
(Base: Credit card accounts with any purchase at Target, September to December 2013)

- Stopped Purchasing: 6%
- Fewer Purchases: 18%
- More Purchases: 20%
- No Change: 16%
- Infrequent Shoppers: 40%

<table>
<thead>
<tr>
<th></th>
<th>Avg # Trips / 4-month period</th>
<th>Avg Spend / Trip</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stopped Purchasing</td>
<td>0</td>
<td>$0</td>
</tr>
<tr>
<td>Fewer Purchases</td>
<td>4</td>
<td>$43</td>
</tr>
<tr>
<td>More Purchases</td>
<td>5</td>
<td>$46</td>
</tr>
<tr>
<td>No Change</td>
<td>3</td>
<td>$57</td>
</tr>
</tbody>
</table>

Source: Lightspeed Financial Services Group
How do you currently pay when purchasing from Target, in light of its security breach over the holidays?

- I still use a credit or debit card: 83%
- I now only pay in cash: 44%
- I paid only in cash before the breach and will continue to do so: 6%

Source: Bizrate Insights Target Study
Q: How do you currently pay when purchasing from Target, in light of its security breach over the holidays? (n=4,437)
December 2013

Source: MarketWatch
Internal Revenue Service Joins Cybercrime Hunt With New Investigation Team

– IRS sets up unit to probe identity-theft cases
– 3,000 Agents trained for 1.63M events
Federal Cybersecurity Spending and Total Federal Information Security Incidents

Breach at IRS Exposes Tax Returns

*Thieves used agency’s online services to get information for about 100,000 households...*

- Penetration was the result of an organized crime, not “one-off”

- Top leaders sought to emphasize that the breach didn’t involve the IRS’s core accounts

- Said wasn’t technically a data breach but instead represented a successful exploitation of an IRS application.

Source: WSJ
Asymmetrical Warfare?

They make millions, we spend billions, so where is the money being made?
What Happened to the Security Perimeter?

Cloud Services

Corporate Perimeter

Remote Workers

Mobile Devices

Advanced Malware

Source: Alvarez and Marsal
The Basics: Securing the Enterprise
Cyber Readiness Assessment to Identify Risk

- ID existing sec profile
- Vulnerabilities, threats & Risks
- Determine effectiveness of cyber framework/strategy:
  - C/S Policies
  - Network Topology
  - Incident Response
  - Acquisition Due Diligence
  - Data Classification
  - Remote Worker
  - Vulnerability Management
  - Log Analysis
- Calibrate your spend and effectiveness of budget (KPIs)

Source: Alvarez and Marsal
## Securing the Corporation

### 7 Questions for the Board and Executives

<table>
<thead>
<tr>
<th></th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Who is ultimately responsible for cyber risk in the corporation?</td>
</tr>
<tr>
<td>2</td>
<td>What and where are the most critical assets that could be attacked? What is their value?</td>
</tr>
<tr>
<td>3</td>
<td>Has a cyber attack simulation been performed in the corporation to test the incident response plan?</td>
</tr>
<tr>
<td>4</td>
<td>Has a cyber readiness assessment been conducted to identify gaps in information security defenses?</td>
</tr>
<tr>
<td>5</td>
<td>How many times has the corporation suffered a cyber breach in the last year? How do you know? Is there monitoring and reporting of cyber risk incidents (24/7?)</td>
</tr>
<tr>
<td>6</td>
<td>Is cyber risk covered in contracts with third parties vendors, etc.? How is compliance verified?</td>
</tr>
<tr>
<td>7</td>
<td>Is the Board aware of the risk exposure of the corporation?</td>
</tr>
</tbody>
</table>

Source: Alvarez and Marsal
Tangible & Intangible Costs

• Insurance premiums
• Damage to third parties
• Customer goodwill & Trust
• Reputational Risk
• Regulators
• Litigation

It’s inevitable, legal gets involved...
Information Governance Reference Model (IGRM)

Linking duty + value to information asset = efficient, effective management

- **Duty**: Legal obligation for specific information
- **Value**: Utility or business purpose of specific information
- **Asset**: Specific container of information
Challenges of Information Governance

• Era where vast amounts of electronically stored information (ESI) created daily.
• Enterprises must ensure all details relevant to litigation are correctly stored and easily recalled.
• Volumes, types and locations of ESI that must be preserved, collected and analyzed during e-discovery continues to escalate.
• Makes it extremely challenging to remain compliant.
• Need a repeatable process and technology in place to manage.
Content is the Target

Structured vs. Unstructured Content

What is the difference?

Enterprise Applications
- Student Information systems
- Financial systems
- HR systems
- CRM

20% Structured Application Content

Enterprise Content Management
- Marketing
  - Outreach
  - Recruiting
  - Collateral
- Admissions & Enrollment
  - Transcripts
  - Letters of recommendation
  - Applicant essays
  - Forms
- Financial Aid
  - FAFSA
  - Verification statements
  - W2s
  - Tax returns
  - Scholarship tracking
  - Correspondence
- Finance
  - Requisitions
  - Purchase orders
  - Invoices
  - Routing & approval
  - A/P & A/R supporting documentation
- Records Management
  - Governance
  - Compliance
  - Retention
  - Disposition
- Digital Asset Management
  - Rich media files such as images and videos
- HR
  - Staff & faculty onboarding
  - Employee records
  - Contracts

80% Unstructured content

Growth of Unstructured Data

Common Denominator: ESI

Digital Evidence

• Where is it and who has possession of it?
  – Identification, collection, preservation
  – Jurisdiction, international?

• Digital evidence is different
  – IP address = fingerprint
  – Hash (MD5)
  – ESI authenticity admissibility
    • Spoliation.

• Is it what it purports to be.
Four Categories of Digital Forensics

1. **STATIC MEDIA** such as hard drive.

2. **VOLATILE INFORMATION** such as RAM and CPU.

3. **NETWORK FORENSICS** is a top-down traffic analysis network or Internet.

4. **BINARY and MALWARE** analysis to deconstruct and determine when written and by who?

Source: http://idt911.com/education/blog/how-we-fight-cyber-bad-guys-so-you-dont-have-to
Mission Statement

USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.
What happens when a single character changes

• The hash value change resulting from the alteration of merely one single character in this sentence results in a change as dramatic as if “War and Peace” had been edited to become “The Cat in the Hat.” The MD-5 Hash value for the commonplace phrase: (“The quick brown fox jumps over the lazy dog”) = 9e107d9d372bb6826bd81d3542a419d6

• Even a small change in the message will result in a completely different hash. For example, changing d to e: (“The quick brown fox jumps over the lazy eog”) = ffd93f16876049265fbaef4da268dd0e

• Another hash value algorithm is called SHA-1. Instead of 32 characters, it has 40. Here is what it looks like on the same phrase: (“The quick brown fox jumps over the lazy dog”) = 2fd4e1c67a2d28fc ed849ee1 bb76e739 1b93eb12

• As with the MD-5, even a small change in the message will result in a completely different hash. For example, changing dog to cog: (“The quick brown fox jumps over the lazy cog”) = de9f2c7f d25e1b3a fad3e85a

Source: Assorted eDiscovery conference materials
Case Study: Big Data in Motion
When Third Party Vendors are involved

• Cross Border M&A – Large Global Drug Cos.
  – Identify, carve out IP assets and move
  – Review and confirm assets on a global basis
  – Harden supply chain to prevent leakage

• Bankruptcy – Lehman Brothers
  – Locate all information assets while in distress
  – Identify, cull and produce assets
  – Harden supply chain to prevent leakage
Sources

- Wall Street Journal (Assorted)
- Verizon 2015 DBIR
- Fortune Magazine, MAR 27 2015 (Hackett)
- Brian Krebs on Security Blogs (Assorted + website)
- SEC Filings TGT, HD, SNE
- Wikipedia (assorted images)
- Javelin Strategy & Research
- Ponemon Institute
- NYT (http://www.nytimes.com/2014/09/03/technology/home-depot-data-breach.html?_r=0)
- Alvarez and Marsal