“Identifying and Mitigating IT Security Risks “
in a Merger or Acquisition”

A Presentation To

The Geek Week 2015 Conference

Presented By

Dewey E. Ray and Donna Gallaher
About Dewey E. Ray

- 30 years of experience as a software developer, IT project manager, consultant, and CIO.
- Authored “The IT Professional’s Merger and Acquisition Handbook”.
- Offers M&A IT due diligence and integration consulting, an M&A IT Due Diligence Toolkit, and M&A IT training.
About Donna Gallaher

- Certified Information Systems Security Professional
- Bachelor of Science Electrical Engineering – Auburn University
- 20 years experience in engineering, sales, managed IT service delivery with Wipro and SunGard
- Global Infrastructure Operations & Security with ABB Software
- Expertise is post M & A integration in IT Operations
- Active Member of TAG Information Security Society, ISACA, ISSA and (ISC)²
Topics That Will be Covered in Today’s Talk

- An Overview of Mergers and Acquisitions (M&A)
- Why M&A IT Security Due Diligence is Important
- Key Factors and Scoping M&A IT Security Due Diligence
- The M&A IT Security Due Diligence Value Proposition
- Understanding the Business Value
- Some M&A IT Due Diligence Approaches
- Due Diligence Framework for
  - Identifying
  - Prioritizing
  - Quantifying
  - Recommending Mitigation Strategies IT Security Risks
- Summary
An Overview of Mergers and Acquisitions

- The 5 Phases of an M&A Transaction
- Some M&A Trends
- Some Common Reasons for M&A
- Some M&A Challenges
# The 5 Phases of an M&A Transaction

<table>
<thead>
<tr>
<th>Phase 1</th>
<th>Phase 2</th>
<th>Phase 3</th>
<th>Phase 4</th>
<th>Phase 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>M&amp;A Strategy</td>
<td>Target Screening</td>
<td>Due Diligence</td>
<td>Transaction Execution</td>
<td>Integration</td>
</tr>
<tr>
<td>Define M&amp;A Strategy and Goals</td>
<td>Organize Search Team and Plan Target Screening</td>
<td>Plan M&amp;A Due Diligence</td>
<td>Develop Target Valuation</td>
<td>Establish M&amp;A Integration Mgt. Office(s)</td>
</tr>
<tr>
<td>Create M&amp;A Executive Committee</td>
<td>Identify Potential M&amp;A Targets</td>
<td>Organize Due Diligence Teams</td>
<td>Develop M&amp;A Deal Structure</td>
<td>Communicate M&amp;A Integration Plan</td>
</tr>
<tr>
<td>Screen and Select Target Candidate(s)</td>
<td>Define Due Diligence Approach, Methods and Protocols,</td>
<td>Present M&amp;A Deal Offer</td>
<td>Integrate Customers, Markets, Products, IT Infrastructure, Data, and Systems</td>
<td></td>
</tr>
<tr>
<td>Contact Target(s)</td>
<td>Conduct M&amp;A Due Diligence</td>
<td>Negotiate M&amp;A Deal Terms</td>
<td>Integrate the Organization, Workforce, Functions, and Operations</td>
<td></td>
</tr>
<tr>
<td>Execute Confidentiality Agreement</td>
<td>Compile and Analyze Due Diligence Findings</td>
<td>Plan M&amp;A Integration</td>
<td>Integrate Locations and Facilities</td>
<td></td>
</tr>
<tr>
<td>Analyze Potential M&amp;A Synergies</td>
<td>Submit M&amp;A Letter of Intent</td>
<td>Conduct M&amp;A Deal Closing</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Cognitive Diligence, LLC
Some M&A Trends

- **Pre–Recession (2008) deal activity**
  - Record levels of M&A deals each year (2005–08).
  - Many deals done “on the fly”.
  - Numerous examples of value erosion resulting from M&A deals.

- **During the Recession (2008 – 2010)**
  - Deal counts dropped to less than 50% of the pre-recession level.
  - A more thoughtful, value-based approach to M&A began to emerge.

  - M&A activity has increased dramatically from 2011 – 2015.
  - M&A deal activity for the CYQ1 puts 2015 on track to be the most active year for M&A since 2008.
  - Companies are taking more time to close deals suggesting that more emphasis is being placed upon due diligence and value creation.
## Common Reasons for M&A

<table>
<thead>
<tr>
<th>Economy of Scale or Economy of Scope</th>
<th>Increased Revenue or Market Share</th>
<th>Synergy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cross Selling Opportunities</td>
<td>Geographical Diversification</td>
<td>Vertical Integration</td>
</tr>
</tbody>
</table>
Some M&A Challenges

- Much of the deal-making process may be obscured.
- The inherent risk in most M&A deals.
- Limited amount of time allowed for due diligence.
- Enormous pressure to deliver the promised benefits quickly.
Ponemon Costs Per Data Breach by Industry

![Bar chart showing costs per data breach by industry for 2014 and 2015. The x-axis represents the years 2014 and 2015, and the y-axis represents costs in dollars ranging from $0 to $450. Each bar is color-coded to represent a different industry category, including Healthcare, Transportation, Education, Energy, Financial Services, Communications, Pharmaceutical, Industrial, Consumer, Media, Technology, Public, Retail, Hospitality, and Research.]
2014 Key Factors Impact Cost of Breach

- Organization with Strong Security Posture: $21 savings
- Organization with Formal Incident Response Plan: $17 savings
- Organization with CISO: $10 savings

- Data Breach Caused by 3rd Party: $25 increase
- Loss or Theft of Data Bearing Devices: $18 increase
- Notified Customers Too Quickly: $15 increase

2015 Key Factors Impact in Cost of Breach

Figure 7. Impact of 11 factors on the per capita cost of data breach

- Incident response team: $23.8
- Extensive use of encryption: $19.0
- BCM involvement: $13.6
- CISO appointed: $12.2
- Employee training: $11.0
- Board-level involvement: $9.8
- Insurance protection: $7.9
- Consultants engaged: -$2.4
- Lost or stolen devices: -$12.0
- Rush to notify: -$12.7
- Third party involvement: -$29.0

Source: 2015 Ponemon Cost of Data Breach Study - US
The M&A IT Security Due Diligence Value Proposition

“To identify and mitigate M&A business risks while identifying potential business value.”
Due Diligence and Risk

Meet Jane

And Jane:
- Is the Application SME for a company using a highly customized legacy application for management of the replacement parts database for their customers
- SHE IS THE ONLY ONE WHO KNOWS THE SYSTEM WELL
- Legacy application is out of maintenance with the vendor
- Secured in DMZ
- Segmented Network with End-to-End Encryption
- Encrypted Laptop/Workstation
- Sign on to VPN with RSA Token and Complex Password which is changed frequently
Business Risk and Security Risk Convergence

Increasing Overlap

Business Risks

Security Risks
Why Can’t We Have More Time?

- Other bidders
- Executive Pay Structures/Incentives
- Fiscal Targets, Quarter End, Year End
- Interest Accruals
- Deadlines from Funding Sources
# Timelines for M&A

<table>
<thead>
<tr>
<th>Type</th>
<th>Size of the Observed Organization</th>
<th>Minimum Number of Days*</th>
<th>Maximum Number of Days*</th>
<th>Onsite Staff/Days (up to)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Up to 150 employees, one major location, and up to three other locations</td>
<td>13</td>
<td>17</td>
<td>5</td>
</tr>
<tr>
<td>B</td>
<td>Between 150 and 350 employees, one major location, and up to five other locations</td>
<td>18</td>
<td>22</td>
<td>7</td>
</tr>
<tr>
<td>C</td>
<td>Between 350 and 750 employees, two to four major locations, and five to 15 other locations</td>
<td>25</td>
<td>29</td>
<td>9</td>
</tr>
<tr>
<td>D</td>
<td>Between 750 and 2,000 employees, three to five major locations, and 15-30 other locations</td>
<td>30</td>
<td>35</td>
<td>11</td>
</tr>
<tr>
<td>E</td>
<td>Between 2,000 and 3,500 employees, five to seven major locations, and 30-50 other locations</td>
<td>36</td>
<td>44</td>
<td>15</td>
</tr>
<tr>
<td>F</td>
<td>Between 3,500 and 6,000 employees, seven to 10 major locations, and 50-75 other locations</td>
<td>49</td>
<td>61</td>
<td>21</td>
</tr>
<tr>
<td>G</td>
<td>Between 6,000 and 10,000 employees, 10 to 15 major locations, and 75-100 other locations</td>
<td>69</td>
<td>85</td>
<td>29</td>
</tr>
<tr>
<td>H</td>
<td>More than 10,000 employees, more than 15 major locations and more than 100 other locations</td>
<td>88</td>
<td>112</td>
<td>36</td>
</tr>
</tbody>
</table>

* Indicates gross time. If more than one IS specialist is involved in delivery of IS due diligence, the period is shorter. For example, if three IS specialists work on due diligence, the activity will take between 30 and 38 days in total for the largest observed organization, with an onsite review of a maximum of 12 days; whereas, in the smallest observed organization, the total time required ranges from around six to seven days, with onsite review a maximum of two-and-a-half days.

Source: Conducting Due Diligence in a Structured Model Within a Short Period of Time, Delak & Bajec, ISACA Journal Vol 4, 2014
## Data Obtained in M&A

<table>
<thead>
<tr>
<th>If This Data is Important:</th>
<th>The Value/Motivation May Be:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong># of Customers</strong></td>
<td>• Synergy, Market Share, Cross Selling Opportunities, Geography</td>
</tr>
<tr>
<td><strong>Intellectual Property Value</strong></td>
<td>• Intellectual Property Transfer</td>
</tr>
<tr>
<td><strong>Supply Chain</strong></td>
<td>• Absorption, Vertical Integration</td>
</tr>
<tr>
<td><strong># of Units Produced</strong></td>
<td>• Economy of Scale, Economy of Scope, Resource Transfer</td>
</tr>
</tbody>
</table>
NIST SP 800–161 – Supply Chain Risk Mgmt

- Published April 2015, 282 Pages
- Information and Communication Technology Supply Chain Risk Management; ICT SCRM
- Thorough, Ongoing Assessment of 3rd parties. Key recommendations are right to audit, termination clauses, etc.
- Cannot be applied to Due Diligence due to time constraints
Frameworks – ITADD

“A Framework for Conducting IT Due Diligence in Mergers and Acquisitions”

by Sundberg, Tan, Baublits, Lee, and Stanis
## ITADD Dashboard

### Figure 2—ITADD Dashboard

<table>
<thead>
<tr>
<th>ITADD Domain</th>
<th>Question Category</th>
<th>Assessment Criteria</th>
<th>Raw Score (1-5)</th>
<th>Weighted Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategy Support</td>
<td>Organizational Integrity</td>
<td>Is IT adequately funded?</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Organizational Integrity</td>
<td>Is the IS department, including e-commerce, adequately meeting business needs?</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Business Continuity</td>
<td>Business Continuity Practices</td>
<td>Are operational practices adequate to ensure business continuity?</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Data Integrity</td>
<td>Are information capture, processing, storage and reporting controls adequate to ensure reliable financial reporting?</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>PPE/Data Center Security</td>
<td>Are data center business continuity controls adequate to ensure continuity of operations?</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Human Capital</td>
<td>Human Capital</td>
<td>Are key IT staff members competent to support the business after acquisition?</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Human Capital</td>
<td>Would the departure of key personnel create significant business continuity issues?</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Operations</td>
<td>Systems Administration</td>
<td>Are key operational responsibilities being discharged?</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Systems Administration</td>
<td>Are capacity and performance adequate to business needs?</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Network Security</td>
<td>Has the network architecture been designed and deployed such that it provides adequate security?</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>IT Assets</td>
<td>Hardware</td>
<td>Is hardware infrastructure sufficiently capable and up to date to support the business?</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Application Software</td>
<td>Are the primary and dependent business applications functioning adequately?</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Application Software</td>
<td>Are corporate and end-user software licensed and adequately maintained?</td>
<td>2</td>
<td>4</td>
</tr>
</tbody>
</table>

**ITADD INDEX:** 56
Framework #2 – FISDD

- Cited this source earlier when we discussed the timelines for M&A by company size

- Framework includes several RACI matrices for each phase:
  1. Preparation
  2. Realization/Onsite Review
  3. Analysis
  4. Decision

- Focus seemed to be division of labor rather than what to actually focus on

“Framework for IS Due Diligence”, ISACA Journal Vol 4, 2014
So to Reduce M&A IT Security Risks

Understand What the M&A deal drivers are and develop an IT security due diligence plan that addresses these business goals.

Conduct IT security due diligence and identify where the security risks lie within the target firm.

Communicate IT security due diligence findings to senior management and develop a mitigation plan.
A New M&A IT Security Due Diligence Framework

Org Chart
- CISO, CRO, Security Governance Council

Security Policy, Process & Documentation
- (Including Audits, Analytics and Other Reports)

Security Systems Design
- (Network, Software Tools, Encryption Technologies)

Security Back Office Support
- (Awareness Training, HR Termination Processes, 3rd Party Audit, Supply Chain Single Points of Failure)
Code Spaces hosted source code for developers in the Amazon Cloud

DDoS / Ransomware wiped out all customer data and backups

Out of Business

Code hosting Code Spaces destroyed by extortion hack attack

Cloud code hosting service Code Spaces is forced to shut down, as a DDoS attack coupled with an unsuccessful extortion attempt was followed by the attacker deleting most of its code repositories and backups.

According to the notice on the service's website, the DDoS attack started on Tuesday. The company then noticed that a number of messages were left by the attacker on their Amazon EC2 control panel, meaning that he or she had access to it.

The identity of the attacker is still unknown, as well as how he or she was able to access the control panel. The service says that they have "no reason to think its anyone who is or was employed with Code Spaces."

The initial internal investigation revealed that no machine access had been achieved by the attacker. Not wanting to pay the large fee requested by the attacker to stop the DDoS attack, they attempted to regain control of the panel by changing passwords.

Unfortunately for them, the intruder was prepared for that attempt, and had already created a number of backup logins. He retaliated by proceeding to randomly delete artifacts from the panel.

"We finally managed to get our panel access back but not before he had removed all EBS snapshots, S3 buckets, all AMI's, some EBS instances and several machine instances," they shared. "In summary, most of our data, backups, machine configurations and offline backups were either partially or completely deleted."

"Code Spaces will not be able to operate beyond this point, the cost of resolving this issue to date and the expected cost of refunding customers who have been left without the service they paid for will put Code Spaces in a irreversible position both financially and in terms of on going credibility," they explained. "As such at this point in time we have no alternative but to cease trading and concentrate on supporting our affected customers in exporting any remaining data they have left with us."

"All that we can say at this point is how sorry we are to both our
Summary

- M&A is a popular growth strategy with significant challenges.

- Information Security Risks and Business Risks are Converging

- Information Security Needs to Adapt to the Business Drivers. In M&A that means
  - Understanding the value of the business and working within reduced timeframes
  - Identifying and Prioritizing risks appropriately for M&A
  - Quantifying results

- Take a methodological approach to M&A IT security due diligence using best practices.
Questions?

Dewey Ray

404–861–9293 Cell
deweyeray@gmail.com
https://www.linkedin.com/in/deweyeray

Donna Gallaher, CISSP

678–520–3838 Cell
dcappuccio@mindspring.com
www.linkedin.com/in/donnagallaher

Dewey Ray

Donna Gallaher, CISSP