PROTECTING KNOWLEDGE ASSETS WITH CYBERSECURITY

Jon Neiditz and Larry Ponemon, With Special Guest Richard May
The survey was conducted to determine the extent of the risk and organizational effectiveness in safeguarding their knowledge assets.

Knowledge assets are confidential information critical to a company’s core business – other than personal information that would trigger notice requirements under law.

More than 600 individuals familiar with a company's approach to managing knowledge assets and involved in the management process were surveyed.
<table>
<thead>
<tr>
<th>Sample response</th>
<th>Freq</th>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sampling frame</td>
<td>17,540</td>
<td>100.0%</td>
</tr>
<tr>
<td>Total returns</td>
<td>691</td>
<td>3.9%</td>
</tr>
<tr>
<td>Rejected or screened surveys</td>
<td>88</td>
<td>0.5%</td>
</tr>
<tr>
<td>Final sample</td>
<td>603</td>
<td>3.4%</td>
</tr>
</tbody>
</table>
Understanding the risk to knowledge assets

- The risk to knowledge assets is increasing.
- Employee negligence and third parties threaten the security of knowledge assets.
- Nation state attacks are also a serious threat.
- IT security believes current approaches to protecting knowledge assets are ineffective.
74% of respondents say that their company likely failed to detect a data breach involving the loss or theft of knowledge assets.

60% state one or more pieces of their company's knowledge assets are likely now in the hands of a competitor.
31% of respondents say their company has a classification system that segments information assets based on value to the organization.

28% rate their companies’ ability to mitigate the loss or theft of knowledge assets by insiders and external attackers as effective.

Companies Don’t Know “What” or “How”
59% say a data breach involving knowledge assets impacts their company’s ability to \textit{operate as a going concern}.

53% replied that senior management is more concerned about \textit{a data breach involving credit card information or SSNs} than the leakage of knowledge assets.
Heads in the Sand

69% believe that senior management does not make the protection of knowledge assets a priority

37% state that the board requires assurances that knowledge assets are managed and safeguarded appropriately.
Costs of the Theft or Loss of the Assets

Nearly 7 out of 10 respondents

>$100 million

Almost 5 out of 10 respondents

>$250 million
Remediation Cost and Coverage

5.4 million
is the average cost to remediate attacks against knowledge assets in the past 12 months

35%
of losses resulting from knowledge asset theft are believed to be covered by a company’s current insurance.
### Allocation of total cost of attacks against knowledge assets

**Total of 100 points**

<table>
<thead>
<tr>
<th>Category</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reputation loss and brand damage</td>
<td>44</td>
</tr>
<tr>
<td>Disruption to normal operations</td>
<td>21</td>
</tr>
<tr>
<td>Remediation &amp; technical support activities</td>
<td>14</td>
</tr>
<tr>
<td>Users’ idle time and lost productivity because of downtime or system performance delays</td>
<td>12</td>
</tr>
<tr>
<td>Damage or theft of IT assets and infrastructure</td>
<td>9</td>
</tr>
</tbody>
</table>

*Total of 100 points*
Some Key Risks: Employees, Clouds

63% state that their company stores knowledge assets in the cloud.

33% say their companies carefully vet the cloud providers storing those assets.

50% of respondents replied that both privileged and ordinary users have open access to the company’s knowledge assets.
Do you believe your company’s knowledge assets are targeted by nation state attacks?

<table>
<thead>
<tr>
<th>Response</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, very likely</td>
<td>17%</td>
</tr>
<tr>
<td>Yes, somewhat likely</td>
<td>33%</td>
</tr>
<tr>
<td>No, not likely</td>
<td>42%</td>
</tr>
<tr>
<td>No chance</td>
<td>8%</td>
</tr>
</tbody>
</table>
The main motivations of attackers who steal a company’s knowledge assets

1 = most likely to 4 – least likely

- Economic espionage: 1.78
- Hacktivism: 2.73
- Cyber warfare: 3.26
- Sabotage: 3.62
How to protect knowledge assets

- Strong governance improves the protection of knowledge assets.
- Sharing knowledge assets with third parties should require strict safeguards.
- A formal approach aligned with the IT security strategy is needed.
- Most incident response plans and audits are informal.
- More centralized control over the protection of knowledge assets is needed.
- Training programs are not addressing employee negligence. Access to knowledge assets is not managed properly.
How to protect knowledge assets (cont’d)

• Preventing access to knowledge assets from remote locations and preventing the use of personally-owned mobile devices could reduce the risk.

• Sixty-one percent of respondents say their organizations take steps to minimize the risk of employee carelessness.

• Companies are storing knowledge assets in the cloud without careful vetting of the provider.

• Encryption and identity management and authentication are most often deployed to safeguard knowledge assets.

• Companies need to have a process in place to understand what high-value information they must secure.

• The most difficult knowledge assets to secure are not appropriately safeguarded.
Why is your company effective in protecting knowledge assets?

More than one choice permitted

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>restricts access to only those who have a need-to-know</td>
<td>64%</td>
</tr>
<tr>
<td>creates employee awareness about information risk</td>
<td>56%</td>
</tr>
<tr>
<td>accomplishes mission within budgetary constraints</td>
<td>40%</td>
</tr>
<tr>
<td>prevents attacks that seek to exfiltrate information</td>
<td>37%</td>
</tr>
<tr>
<td>innovates in the use of enabling security technologies</td>
<td>23%</td>
</tr>
<tr>
<td>detects and contains data breaches quickly</td>
<td>19%</td>
</tr>
<tr>
<td>other</td>
<td>3%</td>
</tr>
</tbody>
</table>
Why is your company not effective in protecting knowledge assets?

More than one choice permitted

- Lack of in-house expertise: 67%
- Lack of clear leadership: 59%
- Lack of collaboration with other functions: 56%
- Insufficient budget (money): 43%
- Insufficient staffing: 38%
- No understanding of how to protect against…: 30%
- Not considered a priority: 15%
- Other: 2%
### 6 Key Components of Action Planning

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior Management/Board Involvement</td>
<td>Identify and Prioritize Knowledge Assets</td>
<td>Safeguards</td>
<td>Awareness and Education</td>
<td>Cloud Security</td>
<td>Cyber-Risk</td>
</tr>
<tr>
<td>Establishment of Responsibility</td>
<td></td>
<td>Detection</td>
<td>Contractor Access</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Response</td>
<td>Role-Based Access</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Departing Employees</td>
<td></td>
<td>Other Coverage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Risk Allocation</td>
<td></td>
</tr>
</tbody>
</table>
1. Governance

• Senior Management/Board Involvement
  – Would valuation be helpful?

• Establishment of Responsibility and Accountability
  – Policy determination and adaptation
  – Accountability for compliance
    • 23 percent of respondents said the chief information officer is primarily responsible
    • 15 percent of respondents said no one person or department is responsible
What best describes your company’s plan or approach for protecting knowledge assets?

<table>
<thead>
<tr>
<th>Plan or Approach</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>An informal or “ad hoc” plan or approach</td>
<td>28%</td>
</tr>
<tr>
<td>A formal plan or approach that depends on the types of knowledge assets</td>
<td>26%</td>
</tr>
<tr>
<td>A formal plan or approach that varies across business units or lines of business</td>
<td>19%</td>
</tr>
<tr>
<td>A formal plan or approach that is applied consistently across the enterprise</td>
<td>17%</td>
</tr>
<tr>
<td>No plan or approach</td>
<td>10%</td>
</tr>
</tbody>
</table>
Who determines how knowledge assets are protected and who is most responsible?

More than one choice permitted

- Chief Information Officer
- General Counsel
- Chief Information Security Officer
- Head of Human Resources
- Chief Operating Officer
- Chief Executive Officer
- Chief Privacy Officer
- Other

Who determines how knowledge assets are protected? Who is most responsible?

* Not a choice for this question
2. Data Classification: Examples of Restricted Knowledge Assets/Trade Secrets
The top five knowledge asset document types most difficult to secure and appropriately secured

More than one choice permitted

<table>
<thead>
<tr>
<th>Document Type</th>
<th>Most difficult to secure</th>
<th>Appropriately secured</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private communications</td>
<td>67%</td>
<td>16%</td>
</tr>
<tr>
<td>Product/market information</td>
<td>60%</td>
<td>19%</td>
</tr>
<tr>
<td>Business correspondence</td>
<td>52%</td>
<td>18%</td>
</tr>
<tr>
<td>Source code</td>
<td>51%</td>
<td>39%</td>
</tr>
<tr>
<td>Presentations</td>
<td>45%</td>
<td>19%</td>
</tr>
</tbody>
</table>

0% 10% 20% 30% 40% 50% 60% 70% 80%

#PSR16

1. Data classification based on risk

2. Build data classification into levels of security safeguards
   A. Encryption and/or tokenization
   B. “Least Privilege” principle and role-based access

3. Assure detection systems are focused on most important knowledge assets
   A. Intrusion
   B. Data loss prevention, preventing exfiltrations
   C. Copy protection and embedded codes to trace copies
   D. Restrict downloading of sensitive company information

4. Assure incident response programs fully incorporate knowledge assets

5. Regulate visitor facility and premises access
Is the plan or approach for protecting knowledge assets aligned with the company’s IT security strategy?
Steps taken to respond to data loss and determine risks

- Incident response plan for dealing with the loss
- Assessments conducted to determine the risks

Yes, formal plan/assessment: 21% Yes, informal plan/assessment: 40% 39% No: 33% 30% Unsure: 6% 5%
The most important security technologies for protecting knowledge assets

- Encryption for data at rest: 54%
- Identity management & authentication: 52%
- Encryption for data in motion: 49%
- Data loss prevention (DLP): 48%
- Security information and event management (SIEM): 47%
- Endpoint management systems: 46%
- Access governance: 43%
- Tokenization technology: 42%
4. Employees

1. Role-based restricted employee access
2. “Need-to-know” distribution of knowledge assets
3. Ongoing security awareness and training for all employees
4. “Confidential” designations for all confidential information
5. Confidentiality agreements, NDAs and/or employee handbook provisions
6. Enforce employee compliance with confidentiality obligations from prior employments
7. Amend Company Mobile Device and BYOD Policies to address knowledge assets
Who has access to your company’s knowledge assets?

- 17% Only privileged users
- 33% Privileged users plus a small number of ordinary users
- 50% Both privileged and ordinary users
Are employees allowed to access knowledge assets from remote locations and their mobile devices?

- Yes: 66%
- No: 40%
- Unsure: 7%

Remote locations: 53%
Mobile devices: 40%
What steps are taken to address the risk of employee carelessness?

More than one choice permitted

- Regular training and awareness programs: 70%
- Monitoring of employees: 65%
- Audits and assessments of areas most vulnerable to employee negligence: 43%
- Part of performance evaluations: 36%
- Incentives to stop negligent behavior: 8%
- Other: 2%
4. Departing Employees

1. Remind employee of confidentiality agreements previously signed; explain that obligations continue
2. Demand return of all company information
3. Use a checklist!
4. Sign Separation Agreement acknowledging obligations in writing
5. If no Separation Agreement, consider requesting employee to sign affidavit or certification of return of corporate information
6. Must have ability to inspect or wipe mobile devices before employee separates!
5. Vendor Selection & Contracts

1. Most importantly, choose an appropriately secure platform
2. Clearly address vendor rights to retain and use data, particularly critical knowledge assets
3. Make sure the security breach notification provisions address breaches of knowledge assets as well as of information that is notice-triggering by law
4. Company-specific, independent security standards are preferable to “industry standards”
5. Require that security practices be regularly updated and audited/certified with comprehensive standards (e.g., SOC 2, Type II; ISO 27001)
6. Require notice of all requests for data (e.g., subpoenas, government inquiries) and opportunity to resist (being aware of the 3rd-party doctrine in the U.S.)
5. Vendor Risk Allocation

1. Liability for security breaches will typically be limited to vendor’s breach of its security obligations or a breach solely caused by vendor.

2. Customer instead should push to have vendor liable for all security breaches unless the customer has caused the breach.

3. If possible, ask for unlimited liability for the following:
   - Indemnification
   - Breaches of confidentiality and/or security
   - Violation of law
   - Gross negligence, willful/intentional misconduct and/or fraud

4. If the vendor won’t agree to unlimited liability, propose tiered caps (lower cap of the greater of $X or 12 to 24 months of fees for most claims, higher cap of $5X for confidentiality/security breaches).
### Steps taken to protect knowledge assets shared with third parties

More than one choice permitted

<table>
<thead>
<tr>
<th>Step</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contract with indemnification by the third party</td>
<td>50%</td>
</tr>
<tr>
<td>Encryption of data in motion</td>
<td>44%</td>
</tr>
<tr>
<td>Encryption or tokenization of data at rest</td>
<td>40%</td>
</tr>
<tr>
<td>Careful vetting of the third party</td>
<td>33%</td>
</tr>
<tr>
<td>Proof that the third party meets generally</td>
<td>31%</td>
</tr>
<tr>
<td>Proof that the third party adheres to compliance</td>
<td>25%</td>
</tr>
<tr>
<td>Site visit and assessment of the third party</td>
<td>22%</td>
</tr>
<tr>
<td>None of the above</td>
<td>39%</td>
</tr>
</tbody>
</table>
What steps are taken to secure knowledge assets in the cloud?

<table>
<thead>
<tr>
<th>Step</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity and access governance</td>
<td>56%</td>
</tr>
<tr>
<td>Contract with indemnification by the cloud provider</td>
<td>49%</td>
</tr>
<tr>
<td>Encryption of data in motion</td>
<td>45%</td>
</tr>
<tr>
<td>Encryption or tokenization of data at rest</td>
<td>40%</td>
</tr>
<tr>
<td>Multi-factor authentication</td>
<td>37%</td>
</tr>
<tr>
<td>Careful vetting of the cloud provider</td>
<td>33%</td>
</tr>
<tr>
<td>Proof that the cloud provider meets generally accepted</td>
<td>30%</td>
</tr>
<tr>
<td>security requirements</td>
<td></td>
</tr>
<tr>
<td>Proof that the cloud provider adheres to compliance</td>
<td>23%</td>
</tr>
<tr>
<td>mandates</td>
<td></td>
</tr>
</tbody>
</table>
6. Insurance

1. Consider the extent to which current insurance covers losses arising from a knowledge asset breach – e.g. the Sony Pictures breach:
   - First Party Losses
   - Third Party Liability
   - Secondary Liability (e.g. D&O, errors & omissions, defamation, regulatory)

2. Seek to delete or limit exclusions for “acts of foreign enemies” and “acts of employees”

3. Seek broad definitions for triggering language, e.g. the definition of “privacy or security act”

4. Seek to limit trade secret and IP exclusions

5. Seek to broaden cyber business interruption, beyond network interruption, to reputational and other causes of revenue loss arising from a knowledge asset breach

6. Seek broad data asset recovery and cyber-extortion coverage
How much of the loss resulting from the theft of knowledge assets is covered?

Extrapolated value = 35 percent
Does your company have cyber insurance?

- Yes: 49%
- No, but plan to within the next 12 months: 37% (CRO), 31% (All Others)
- No: 15% (CRO), 42% (All Others)
Allocation of total cost of attacks against knowledge assets

Total of 100 points

- Reputation loss and brand damage: 44 points
- Disruption to normal operations: 21 points
- Remediation & technical support activities: 14 points
- Users’ idle time and lost productivity because of downtime or system performance delays: 12 points
- Damage or theft of IT assets and infrastructure: 9 points
Methods
Position level within the organization

- Senior Executive: 17%
- Vice President: 20%
- Director: 33%
- Manager: 15%
- Supervisor: 2%
- Technician: 3%
- Staff: 2%
- Contractor: 8%
The primary person reported to within the organization

- 53% Chief Information Officer (CIO)
- 20% CEO/COO
- 10% Chief Information Security Officer (CISO)
- 8% Chief Compliance Officer (CCO)
- 5% Chief Risk Officer (CRO)
- 4% General Counsel (GC)
- 3% Chief Financial Officer (CFO)
- 2% Chief Security Officer (CSO)
Primary industry classification

- Financial services: 19%
- Public sector: 12%
- Health & pharmaceutical: 11%
- Industrial & manufacturing: 10%
- Retail: 9%
- Services: 9%
- Energy & utilities: 6%
- Consumer products: 5%
- Technology & software: 5%
- Hospitality: 4%
- Communications: 3%
- Education & research: 2%
- Entertainment & media: 2%
- Transportation: 2%
- Agriculture & food services: 1%

#PSR16
Worldwide headcount of the organization

- Less than 500: 10%
- 500 to 1,000: 12%
- 1,001 to 5,000: 21%
- 5,001 to 25,000: 29%
- 25,001 to 75,000: 8%
- More than 75,000: 10%
## Global location of employees

<table>
<thead>
<tr>
<th>Region</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>100%</td>
</tr>
<tr>
<td>Canada</td>
<td>70%</td>
</tr>
<tr>
<td>Europe</td>
<td>68%</td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td>61%</td>
</tr>
<tr>
<td>Latin America (including Mexico)</td>
<td>58%</td>
</tr>
<tr>
<td>Middle East &amp; Africa</td>
<td>44%</td>
</tr>
</tbody>
</table>
CAVEATS

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

• Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

• Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are familiar with their companies’ approach to managing knowledge assets and involved in the process and are located in the United States. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.

• Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.
Thank You!