KNOWLEDGE ASSETS, THEIR DEFENSE AND REGULATION – MAKING THEM WORK FOR YOU

Jon Neiditz
Partner & Cybersecurity/Privacy Lead
Kilpatrick Townsend & Stockton LLP
Study Co-Author

Will Bracker
Senior Director, Privacy
Cox Communications
Study Co-Author

Dr. Chris Pierson
Chairman & Founder
Binary Sun Cyber Risk Advisors
Moderator
About this study

• The Second Annual Study on the Cybersecurity Risk to Knowledge Assets, produced by the Ponemon Institute and Kilpatrick Townsend, was done to see whether and in what ways organizations are beginning to focus on safeguarding “knowledge assets” (also often known as “crown jewels”) in a period of targeted attacks on those assets.

• “Knowledge assets” are defined as confidential information critical to the development, performance and marketing of a company’s core business, other than personal information that would trigger notice requirements under law. For example, they include:
  • trade secrets and corporate confidential information such as product design, development or pricing;
  • sensitive non-public information about the organization, its plans or relationships; and
  • competitively valuable or other important information of or about customers, including profiles.

• This presentation is about how the study provides practical guidance for successful advocacy and action toward securing knowledge assets.
### About our sample response

<table>
<thead>
<tr>
<th>Sample response</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sampling frame</td>
<td>17,991</td>
<td>17,540</td>
</tr>
<tr>
<td>Total returns</td>
<td>709</td>
<td>691</td>
</tr>
<tr>
<td>Rejected or screened surveys</td>
<td>75</td>
<td>88</td>
</tr>
<tr>
<td>Final sample</td>
<td>634</td>
<td>603</td>
</tr>
<tr>
<td>Response rate</td>
<td>3.5%</td>
<td>3.4%</td>
</tr>
</tbody>
</table>
Current position within the organization

- Senior Executive: 35%
- Vice President: 9%
- Director: 16%
- Manager: 21%
- Supervisor: 3%
- Technician: 2%
- Staff: 14%
The primary person reported to within the organization

- Chief Information Officer (CIO): 51%
- Chief Information Security Officer (CISO): 22%
- Chief Risk Officer (CRO): 9%
- Compliance Officer: 7%
- General Counsel: 4%
- Chief Security Officer (CSO): 3%
- Chief Financial Officer (CFO): 2%
- CEO/Executive Committee: 1%
- Human Resources VP: 1%
Primary industry classification

- Financial services: 18%
- Public sector: 12%
- Industrial & manufacturing: 11%
- Health & pharmaceutical: 10%
- Retail: 10%
- Services: 9%
- Technology & software: 7%
- Consumer products: 6%
- Energy & utilities: 5%
- Communications: 3%
- Hospitality & leisure: 3%
- Education & research: 3%
- Transportation: 2%
- Other: 2%
Worldwide headcount of the organization

- Less than 500: 7%
- 500 to 1,000: 12%
- 1,001 to 5,000: 19%
- 5,001 to 25,000: 8%
- 25,001 to 50,000: 27%
- 50,001 to 75,000: 9%
- More than 75,000: 18%
What are your crown jewels?
New study: Increased threats and awareness

- Likelihood that the company failed to detect a data breach: 74% (FY2016) vs. 82% (FY2017)
- Likelihood that one or more pieces of the company's knowledge assets are now in the hands of a competitor: 60% (FY2016) vs. 65% (FY2017)
Evidence of the growing awareness of threats to knowledge assets

- **Boards of directors requiring assurances**
- **Integration** into IT security strategy
- **Focus on employee carelessness and third party access**
- **Clear trends in technologies** to protect knowledge assets
Some more – but still few – consider their organizations good at this

1 = not effective to 10 = highly effective, 7 + responses reported

FY2016: 28%
FY2017: 35%
For the 65% who don’t think they’ve got this: What is holding your company back?

More than one response allowed

<table>
<thead>
<tr>
<th>Issue</th>
<th>FY2016</th>
<th>FY2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of in-house expertise</td>
<td>67%</td>
<td>73%</td>
</tr>
<tr>
<td>Lack of clear leadership</td>
<td>59%</td>
<td>55%</td>
</tr>
<tr>
<td>Lack of collaboration with other functions</td>
<td>56%</td>
<td>53%</td>
</tr>
<tr>
<td>Insufficient staffing</td>
<td>47%</td>
<td>42%</td>
</tr>
<tr>
<td>Insufficient budget (money)</td>
<td>43%</td>
<td>42%</td>
</tr>
<tr>
<td>No understanding how to protect against attacks</td>
<td>34%</td>
<td>30%</td>
</tr>
<tr>
<td>Not considered a priority</td>
<td>34%</td>
<td>15%</td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
<td>2%</td>
</tr>
</tbody>
</table>
For the 35% who think their company is effective: Why?

*More than one response allowed*

- Restricts access to only those who have a need to know: 64% (FY2016) - 69% (FY2017)
- Creates employee awareness about information risk: 56% (FY2016) - 63% (FY2017)
- Accomplishes mission within budgetary constraints: 40% (FY2016) - 35% (FY2017)
- Prevents attacks that seek to exfiltrate information: 37% (FY2016) - 35% (FY2017)
- Innovates in the use of enabling security technologies: 23% (FY2016) - 29% (FY2017)
- Detects and contains data breaches quickly: 19% (FY2016) - 21% (FY2017)
- Other: 3% (FY2016) - 4% (FY2017)
The “high performers,” the 14% who rate their firms 9 or 10, are instructive:

<table>
<thead>
<tr>
<th>Much greater attention by <strong>senior management</strong> and <strong>the board</strong></th>
<th>External, third-party <strong>audits</strong> and regular, customized, actionable <strong>training</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Much greater reliance on these 3 techs/processes:</strong> <strong>access governance,</strong> <strong>privileged user management</strong> and <strong>DLP</strong></td>
<td><strong>More convinced that their knowledge assets are very valuable to a nation state attacker</strong></td>
</tr>
</tbody>
</table>
Perceptions about senior management and boards of directors

Strongly agree and Agree responses combined

- **Board of directors requires assurances that knowledge assets are managed and safeguarded appropriately**: 52% (Hi Performer) 44% (Overall)
- **Senior management understands the risk caused by insecure knowledge assets**: 48% (Hi Performer) 35% (Overall)
- **Senior management is more concerned about a data breach involving credit card information or Social Security numbers (SSNs) than the leakage of knowledge assets**: 42% (Hi Performer) 50% (Overall)
Differences in security practices

Strongly agree and Agree responses combined

- Employee access is restricted to knowledge assets based on a need to know basis: 70% for Hi Performer, 61% for Overall.
- Our company is effective in protecting trade secrets: 61% for Hi Performer, 50% for Overall.
- The theft of knowledge assets is increasing in our company: 45% for Hi Performer, 58% for Overall.
- All information asset types are considered equal in terms of risk: 10% for Hi Performer, 19% for Overall.
More training/awareness, audits for the handling of insiders (vs. monitoring, evals, incentives)

- Regular training and awareness programs: 83% (Hi Performer), 71% (Overall)
- Monitoring of employees: 83% (Hi Performer), 71% (Overall)
- Audits and assessments of areas most vulnerable to employee negligence: 55% (Hi Performer), 47% (Overall)
- Part of performance evaluations: 38% (Hi Performer), 39% (Overall)
- Incentives to stop negligent behavior: 7% (Hi Performer), 7% (Overall)
- Other: 3% (Hi Performer), 3% (Overall)
High performers strongly favor independent 3rd-party audits

- **Independent audit by third parties**: 40% (Hi Performer) vs. 26% (Overall)
- **Combination of independent and internal audit**: 31% (Hi Performer) vs. 32% (Overall)
- **Internal audit by in-house experts**: 40% (Hi Performer) vs. 26% (Overall)
- **Other**: 3% (Hi Performer) vs. 2% (Overall)
Root Causes: Rise of Nation State Attackers

52% of High Performers think their Knowledge Assets are “very valuable” to nation states, vs. 45% of all participants.

All participants are increasingly seeing nation-state attacks as “very likely”.

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very likely</td>
<td>17%</td>
<td>25%</td>
</tr>
<tr>
<td>Somewhat likely</td>
<td>33%</td>
<td>36%</td>
</tr>
<tr>
<td>Not likely</td>
<td>42%</td>
<td>35%</td>
</tr>
<tr>
<td>No chance</td>
<td>8%</td>
<td>4%</td>
</tr>
</tbody>
</table>
Root Causes: Who is responsible?

Careless insider most likely

75% of both High Performers & all respondents rate “employee negligence” “most significant” in 2017

<table>
<thead>
<tr>
<th></th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Careless insider</td>
<td>1.67</td>
<td>1.52</td>
</tr>
<tr>
<td>Malicious or criminal insider</td>
<td>2.45</td>
<td>2.33</td>
</tr>
<tr>
<td>External attacker</td>
<td>2.89</td>
<td>3.01</td>
</tr>
<tr>
<td>Combined insider and external attacker</td>
<td>3.49</td>
<td>3.50</td>
</tr>
</tbody>
</table>
Economic espionage most likely, particularly when one considers such espionage by nation states.
The knowledge-asset-type security gap

Three responses allowed

- Private communications: 45%
- Product / Market information: 27%
- Presentations: 24%
- Source code: 32%
- Trade secrets: 33%
- Business correspondence: 15%
- Company confidential information: 26%
- Operational information: 32%
- Financial information: 19%
- Research results: 13%
- Consumer data: 10%
- Analytics: 16%
- Privileged information: 8%
The knowledge-asset-type security gap

*Three responses allowed*

- **Private communications**
  - Most valuable asset: 45%
  - Asset appropriately secured: 16%
  - Most difficult to secure: 15%

- **Product / Market Information**
  - Most valuable asset: 27%
  - Asset appropriately secured: 15%
  - Most difficult to secure: 24%

- **Presentations**
  - Most valuable asset: 24%
  - Asset appropriately secured: 16%
  - Most difficult to secure: 32%

- **Source code**
  - Most valuable asset: 33%
  - Asset appropriately secured: 36%
  - Most difficult to secure: 19%

- **Trade secrets**
  - Most valuable asset: 51%
  - Asset appropriately secured: 15%
  - Most difficult to secure: 15%

- **Business correspondence**
  - Most valuable asset: 15%
  - Asset appropriately secured: 15%
  - Most difficult to secure: 23%

- **Company-confidential information**
  - Most valuable asset: 26%
  - Asset appropriately secured: 23%
  - Most difficult to secure: 19%

- **Operational information**
  - Most valuable asset: 45%
  - Asset appropriately secured: 19%
  - Most difficult to secure: 19%

- **Financial information**
  - Most valuable asset: 35%
  - Asset appropriately secured: 13%
  - Most difficult to secure: 10%

- **Research results**
  - Most valuable asset: 32%
  - Asset appropriately secured: 16%
  - Most difficult to secure: 20%

- **Consumer data**
  - Most valuable asset: 16%
  - Asset appropriately secured: 8%
  - Most difficult to secure: 52%
The knowledge-asset-type security gap

Three responses allowed

- Private communications: 72%
- Product/Market Information: 65%
- Presentations: 52%
- Source code: 50%
- Trade secrets: 51%
- Business correspondence: 48%
- Company confidential information: 46%
- Operational information: 41%
- Financial information: 45%
- Research results: 34%
- Consumer data: 35%
- Analytics: 32%
- Privileged information: 52%

Most valuable asset
Asset appropriately secured
Most difficult to secure
Note that the high performers are making strides here as well, even for private communications.
Trends in overall security technologies for protecting knowledge assets

Eight responses allowed

- Identity management & authentication
- Security information and event management (SIEM)
- Endpoint management systems
- Tokenization technology
- Web application firewalls (WAF)
- Mobile device management (MDM)
- Anti-virus & anti-malware
- Penetration testing
- Big data analytics

FY2016 vs FY2017
What technologies are used to secure access to knowledge assets?

Three responses allowed

- Identity & Access Management (IAM): 67%
- Access Monitoring & Tracking: 59%
- Access Governance: 53%
- Governance, Risk & Compliance (GRC): 53%
- Privileged User Management: 47%
- User Behavior Analytics (UBA): 45%
- Data Loss Prevention (DLP): 44%
- Digital Rights Management: 29%
- Other: 5%
High performers rely more on 4 technologies

- Identity & Access Management: 73% high performer, 67% overall
- Privileged User Management: 64% high performer, 47% overall
- Access Governance: 62% high performer, 53% overall
- Data Loss Prevention: 56% high performer, 44% overall
The mean time to identify (MTTI) a data breach involving knowledge assets caused by a careless insider or malicious outsider (in DAYS)

Mean time to identify (MTTI) a data breach involving a knowledge asset caused by a careless insider:
- Hi Performer: 144.6 days
- Overall: 202.6 days

Mean time to identify (MTTI) a data breach involving a knowledge asset caused by a malicious outsider:
- Hi Performer: 233.0 days
- Overall: 323.3 days
The mean time to contain (MTTC) a data breach involving knowledge assets caused by a careless insider or malicious outsider (in DAYS)

- Mean time to contain (MTTC) a data breach involving a knowledge asset caused by a careless insider: 76.3 days
- Mean time to contain (MTTC) a data breach involving a knowledge asset caused by a malicious outsider: 152.7 days

Hi Performer: 43.76 days
Overall: 118.00 days
Building for success

- Read the study
- Benchmark against the High Performers
- Understand where you have unbalanced security vs. value
- Benchmark technology use
- Benchmark MTTI & MTTC
- Raise awareness of gaps
Questions?

Ponemon Institute
Toll Free: 800.887.3118
Michigan HQ: 2308 US 31 N.
Traverse City, MI 49686 USA
research@ponemon.org

Jon Neiditz
jneiditz@kilpatricktownsend.com
https://www.linkedin.com/in/informationmanagementlaw
@jonneiditz
404.815.6004
Caveats

- This study utilizes a confidential and proprietary benchmark method that has been successfully deployed in earlier Ponemon Institute research. However, there are inherent limitations to benchmark research that need to be carefully considered before drawing conclusions from findings.

- 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 accurate responses.