Employees are Taking Data when They Quit

Rob Juncker
SVP | Research & Development
Odds are you’re suffering a data loss, leak or theft... and you don’t even know it.
Detection & response is lacking because

90% of insider data loss, leak, and theft goes undetected internally.
Employees are “looking”

The grass is always greener

GALLUP

50% of the labor force is looking for a new job

Half

Of job seekers have been at an employer for less than 1 year
More employees are quitting

Employee quits have risen every year for the past decade – totaling **40M** in 2018.

Source: U.S. Bureau of Labor statistics
Data portability is accelerating

There will never be enough security people, policies or products to prevent data loss from happening.

There are just too many vectors
Quitters are taking

The brutal truth

- 60% of departing employees admit to taking company data.
- 70% of IP theft happens in the 30 days before an employee announces their resignation.
- 66% of departing employees said they did it to help them get their next job.

Trend

Another Apple employee charged with stealing autonomous car...

Jan 30, 2019 - A second Apple employee was charged with stealing self-driving car project...
charged an Apple employee for trying to steal intellectual property related to the project in the last seven months. The news was first reported by NBC's Bay Area affiliate... Zhong Chen, a Chinese national, was charged with theft of trade secrets...

The ‘Why’ behind Intellectual Property Theft Cases - Loss Prevention...
https://lo spospreventi onmedia.com - Data Protection
Nov 14, 2018 - These are defined as crimes in which current or former employees, contractors...
Preventing Internal Intellectual Property Theft Cases from Happening.

Ex-Eastman employee charged with trade-secret theft - C&EN
https://cen.acs.org/policy/intellectual-property/Ex-Eastman-employee-charged.../8
Feb 15, 2016 - “Eastman took steps to protect its intellectual property seriously and we have controls in place to help prevent and to detect theft of confidential information.”

Lanxess is victim of Industrial secrets theft
“Departing employees are your single biggest insider threat to data loss.”
24 million people took data from their previous employer in 2018.
Why? Because...

- Data is more portable than ever
- Data loss detection is lacking
- Employee loyalty is declining
- Employee quits are growing
- Quitters are taking data
Yet most companies say...

"We don’t have a departing employee workflow."
In fact, less than 20% of large enterprise companies have a well defined incident response scenarios for insider threat.
The damage is already done

Companies have no idea quitters took data until the damage is already done

~60% of data breaches take months to detect, and even then, more than 20% take several more days to begin actioning
“prevention will fail. You’re missing a critical layer of protection.”
You don’t know...

<table>
<thead>
<tr>
<th>What</th>
<th>data you have where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who</td>
<td>has or had what data</td>
</tr>
<tr>
<td>When</td>
<td>data is leaving</td>
</tr>
<tr>
<td>What</td>
<td>data is leaving</td>
</tr>
</tbody>
</table>
When Employees Steal, You're Trending
DLP does not work

The culprits (not technically savvy):
Finance and Sales Ops

The timing (not super secretive):
Their last day of employment

The tools (not super sophisticated):
A thumb drive and email

The haul (not blocked, nor detected):
Pricing information, marketing plans, customer lists, deal flow, negotiating methods, personnel and other confidential and proprietary sales information on tens of millions of dollars in business.
Employee Offboarding
Typical Employee Offboarding Process

1. Employee gives notice
2. HR submits separation ticket
3. IT & Security remove access to systems
4. Employee turns in badge & laptop
What about the data?
What if the Offboarding Process Looked Like This?

- Employee gives notice
- HR submits separation ticket
- IT & Security remove access to systems & add to departing employee workflow
- Employee turns in badge & laptop
A Different Approach to Data Protection

**COLLECT**
- all endpoint & cloud data
  - Departing Employees
  - Organizational Change
  - High Risk Users

**MONITOR**

**DETECT**
- abnormal data activity
  - What data is at risk?
  - Who has/had what data?
  - Where is the data located?
  - How & When did it move?

**INVESTIGATE**

**RETRIEVE**
- files for content analysis
  - Take Legal / HR action
  - Investigate further
  - Close case

**RESPOND**

Investigate
- further
- Close case
Alex accepts a new sales job with a competitor.

When he gives his notice, security adds him to an alert profile.
Security reviews what Alex did before he quit

A 90-day look at his file activity shows nothing unusual happened.
3 days later, security receives an email alert

Alex added files to DropBox only minutes ago.
Security looks into what Alex put in DropBox

Most of the uploaded files look harmless, like his W-9 and resume, but one appears to be a customer list.
Security opens the customer list .xlsx file

A quick glance shows it contains information on active clients that Alex shouldn’t keep.

1-6 of 6 Results

<table>
<thead>
<tr>
<th>Date Observed (UTC)</th>
<th>Event Type</th>
<th>Filename</th>
<th>File Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-02-22 15:39:30 (UTC)</td>
<td>Modified</td>
<td>SalesProposalTemplate.pptx</td>
<td>Presentation</td>
</tr>
<tr>
<td>2019-02-22 15:39:45 (UTC)</td>
<td>Modified</td>
<td>EastCoast_Customers.xlsx</td>
<td>Spreadsheet</td>
</tr>
<tr>
<td>2019-02-22 15:40:02 (UTC)</td>
<td>Modified</td>
<td>2019_AlexResume.docx</td>
<td>Document</td>
</tr>
<tr>
<td>2019-02-22 15:40:30 (UTC)</td>
<td>Modified</td>
<td>Family-Vacation.jpg</td>
<td>Image</td>
</tr>
<tr>
<td>2019-02-22 15:40:45 (UTC)</td>
<td>Modified</td>
<td>Alex Johnson W-9.xlsx</td>
<td>Spreadsheet</td>
</tr>
<tr>
<td>2019-02-22 15:41:15 (UTC)</td>
<td>Modified</td>
<td>Project Summary.docx</td>
<td>Document</td>
</tr>
</tbody>
</table>
Alex must permanently delete the file from DropBox

Security tells Alex’s manager about the customer list. His manager watches while he permanently deletes the file from his DropBox account.

<table>
<thead>
<tr>
<th>Company Name</th>
<th>Client Name</th>
<th>Email Address</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reception Hub</td>
<td>Catherine Pierce</td>
<td><a href="mailto:c.pierce@receptionhub.com">c.pierce@receptionhub.com</a></td>
<td>+1 (212) 555-9450</td>
</tr>
<tr>
<td>Cloud Coder</td>
<td>Joel Fox</td>
<td><a href="mailto:joel.fox@cloudcoder.com">joel.fox@cloudcoder.com</a></td>
<td>+1 (803) 555-1219</td>
</tr>
<tr>
<td>NestEasy</td>
<td>Patrick Poole</td>
<td><a href="mailto:patrick.poole@nesteasy.com">patrick.poole@nesteasy.com</a></td>
<td>+1 (215) 555-3415</td>
</tr>
<tr>
<td>Ivy Ladder</td>
<td>Annie Ross</td>
<td><a href="mailto:annie.ross@ivyladder.com">annie.ross@ivyladder.com</a></td>
<td>+1 (212) 555-8589</td>
</tr>
<tr>
<td>Nuvillo</td>
<td>Beulah Reeves</td>
<td><a href="mailto:beulahreeves@nuvillo.com">beulahreeves@nuvillo.com</a></td>
<td>+1 (407) 555-9813</td>
</tr>
</tbody>
</table>
Questions?