Radar Actionable Insights

Real-time trend analysis and dashboards to inform and improve your privacy program metrics

RadarFirst

A strong culture of compliance depends on having information readily available at your fingertips. Data is a powerful tool in the hands of privacy professionals. It can inform improvement efforts, point out trends, and be a hub for real-time and data driven insights, allowing departments, executives, and board members to share, view, and measure the performance of a privacy program.

Despite all these known benefits of robust reporting and dashboards, many privacy teams find collection and timely access to this critical data to be both a challenge and an impediment to quantifying the strategic impact of their privacy programs.

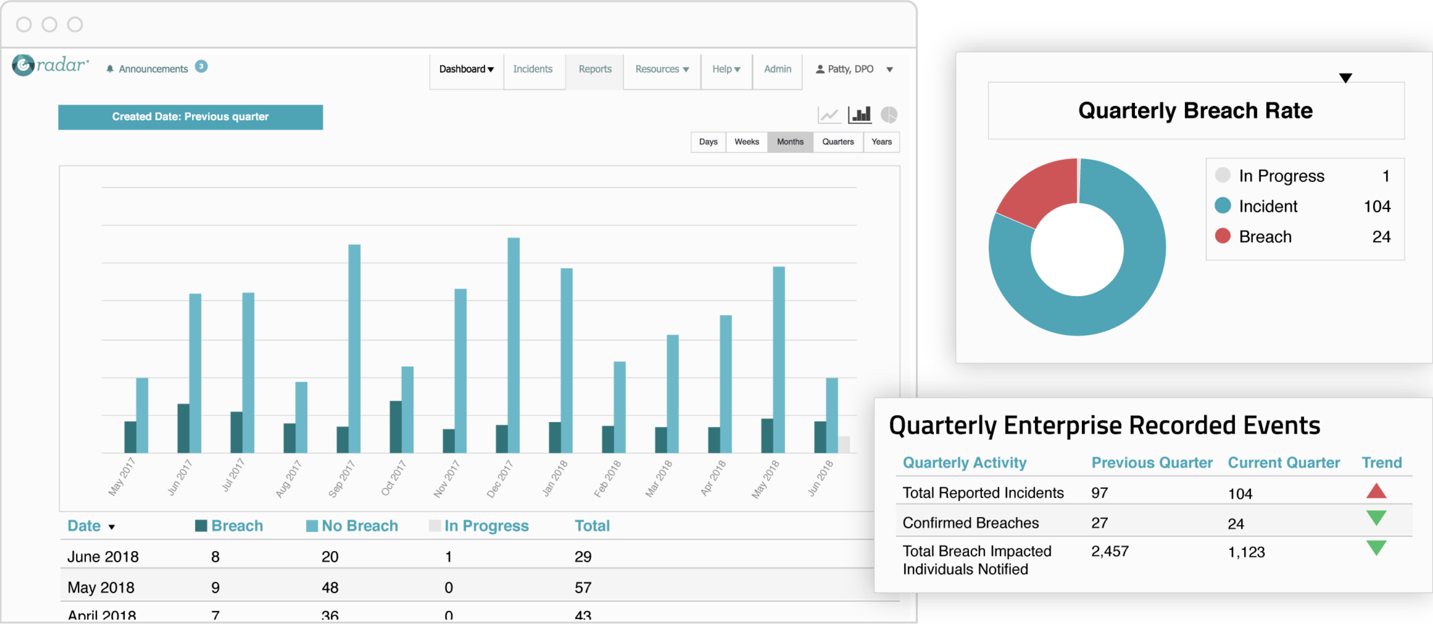
Executives struggle with a lack of visibility to real-time, actionable metrics and benchmarking data that is critical for internal stakeholders, regulators, and board members.

Radar's real-time reporting and dashboards provides data-driven and actionable insights into your organization's privacy program, making it easier to identify trends and uncover issues important for continuous improvement of your incident response process. Build, filter, sort, and export reports such as:

- Compliance metrics
- Trend analysis and charts
- Incident details and notification reports

Below, right: example 12-month breach/no breach report in Radar. Below, left: example board-level metrics.

Without accurate and timely measurement of the state of the privacy program, management is asked to make investment decisions without the supporting information and return-on-investment. Often the process to pull



Date ▾	■ Breach	■ No Breach	■ In Progress	Total
June 2018	8	20	1	29
May 2018	9	48	0	57
April 2018	7	36	0	43

Quarterly Enterprise Recorded Events

Quarterly Activity	Previous Quarter	Current Quarter	Trend
Total Reported Incidents	97	104	▲
Confirmed Breaches	27	24	▼
Total Breach Impacted Individuals Notified	2,457	1,123	▼

together the required performance metrics and trends for monthly and quarterly program assessments can take days with painfully manual and error prone processes, resulting in questionable data integrity.

Privacy professionals – those who manage the day-to-day operations of an organization's privacy program – are challenged to track daily operational metrics without proper tools, automation, and access to playbooks for best practices in incident response. As a result, privacy teams are deprived of the insights embedded in the incident response data and cannot establish appropriate metrics and dashboards that are easily tracked for continuous operational visibility and excellence.

Despite these challenges, data analysis and reporting remains a necessity. Every privacy program is required to provide metrics and reports – to their board, to regulators, or internally for program wellness checks.

Real-time reporting at the click of a button

Radar is a patented SaaS solution that helps organizations comply with US federal, state, and international breach notification laws, guiding users through a consistent and intuitive process for profiling and scoring any data privacy or security incident to determine whether the incident is a data breach requiring notice to regulators, impacted individuals, or other external entities. Radar's purpose-built workflow automates and simplifies the aggregation of your incident management metadata necessary for accurate and timely analysis and reporting.

Real-time dashboards provide visibility into incident assessment status and notification deadlines for prioritization, as well as high-level views of pending action items and emerging trends. The Radar reporting functionality makes it easy to build custom reports in minutes, automating the board and executive level analysis that may otherwise take weeks to pull together manually. Reports can easily be customized, filtered, sorted, saved and exported.

Sample reports readily available in Radar:

- For regulators: HHS Summaries, including the annual report of data breaches impacting fewer than 500 individuals; and monthly and quarterly reports required to OCC, FDIC, FRB;
- For internal purposes: board and executive-level reporting, benchmarking and key performance indicators such as volume of reported incidents, number of affected records, root cause, incident source, etc.

The reporting capabilities within Radar help prove your privacy program is remaining compliant and running efficiently, increases visibility of critical privacy statistics to executives and board members, and brings efficiency in remaining compliant with requests from auditors and regulators.

This is just one aspect of what Radar does to help organizations operationalize incident response. Contact us to learn more about full Radar functionality.

> *Without Radar, we couldn't give our Board of Directors the privacy metrics they've requested.*
>
> — VP Privacy Operations
> at a Fortune 50 Enterprise

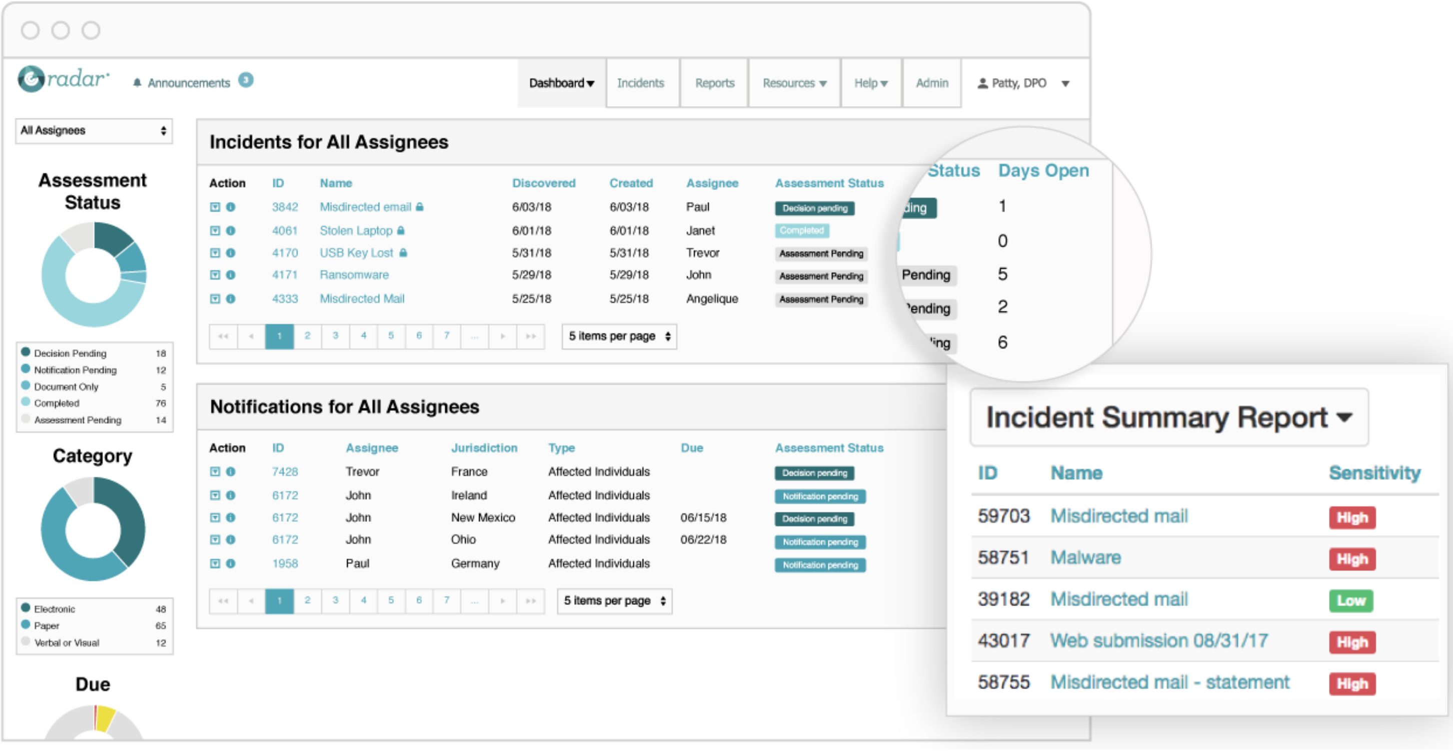
LEARN MORE AT RADARFIRST.COM

WINNER
The HPE-IAPP
Privacy Technology
Innovation Award
iapp

RadarFirst's award-winning incident response management software is trusted by organizations in heavily regulated industries to reduce risk and simplify compliance with US and international data breach laws, including the EU GDPR.

Learn more at radarfirst.com.

© Copyright RadarFirst, Inc. All Rights Reserved.   0718



Assessment Status

● Decision Pending	18
● Notification Pending	12
● Document Only	5
● Completed	76
● Assessment Pending	14

Category

● Electronic	48
● Paper	65
● Verbal or Visual	12

Due

Incidents for All Assignees

Action	ID	Name	Discovered	Created	Assignee	Assessment Status
	3842	Misdirected email	6/03/18	6/03/18	Paul	Decision pending
	4061	Stolen Laptop	6/01/18	6/01/18	Janet	Completed
	4170	USB Key Lost	5/31/18	5/31/18	Trevor	Assessment Pending
	4171	Ransomware	5/29/18	5/29/18	John	Assessment Pending
	4333	Misdirected Mail	5/25/18	5/25/18	Angelique	Assessment Pending

Status	Days Open
ding	1
	0
Pending	5
ending	2
ing	6

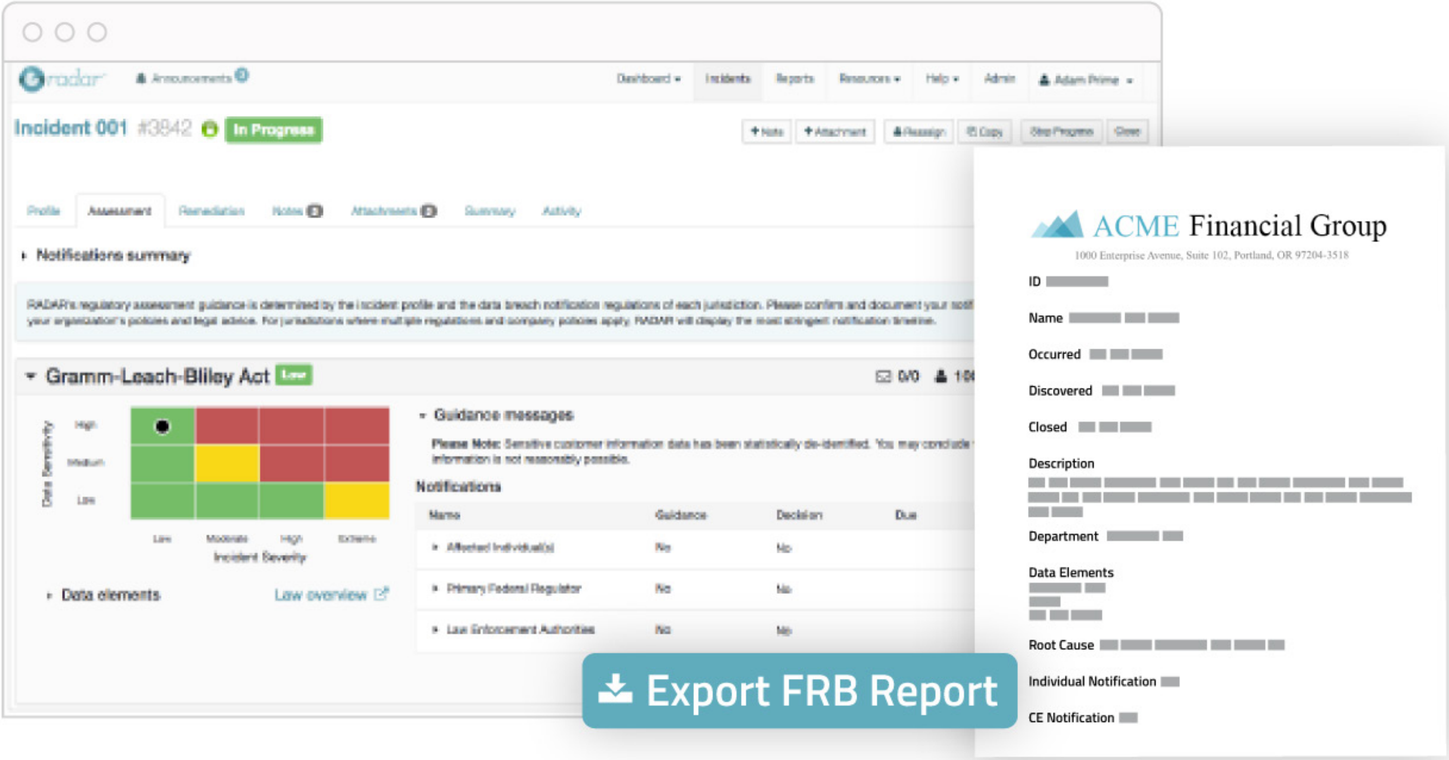
Notifications for All Assignees

Action	ID	Assignee	Jurisdiction	Type	Due	Assessment Status
	7428	Trevor	France	Affected Individuals		Decision pending
	6172	John	Ireland	Affected Individuals		Notification pending
	6172	John	New Mexico	Affected Individuals	06/15/18	Decision pending
	6172	John	Ohio	Affected Individuals	06/22/18	Notification pending
	1958	Paul	Germany	Affected Individuals		Notification pending

Incident Summary Report

ID	Name	Sensitivity
59703	Misdirected mail	High
58751	Malware	High
39182	Misdirected mail	Low
43017	Web submission 08/31/17	High
58755	Misdirected mail - statement	High

The Radar Dashboard allows you at-a-glance views into your organization's privacy practice, making it easier to prioritize urgent tasks.



Incident 001 #3842 In Progress

Notifications summary

RADAR's regulatory assessment guidance is determined by the incident profile and the data breach notification regulations of each jurisdiction. Please confirm and document your noti your organization's policies and legal advice. For jurisdictions where multiple regulations and company policies apply, RADAR will display the most stringent notification timeline.

Gramm-Leach-Bliley Act Low

Guidance messages

Please Note: Sensitive customer information data has been statistically de-identified. You may conclude information is not reasonably possible.

Notifications

Name	Guidance	Decision	Due
Affected Individual(s)	No	No	
Primary Federal Regulator	No	No	
Law Enforcement Authorities	No	No	

Data elements

ACME Financial Group
1000 Enterprise Avenue, Suite 102, Portland, OR 97204-3518

ID

Name

Occurred

Discovered

Closed

Description

Department

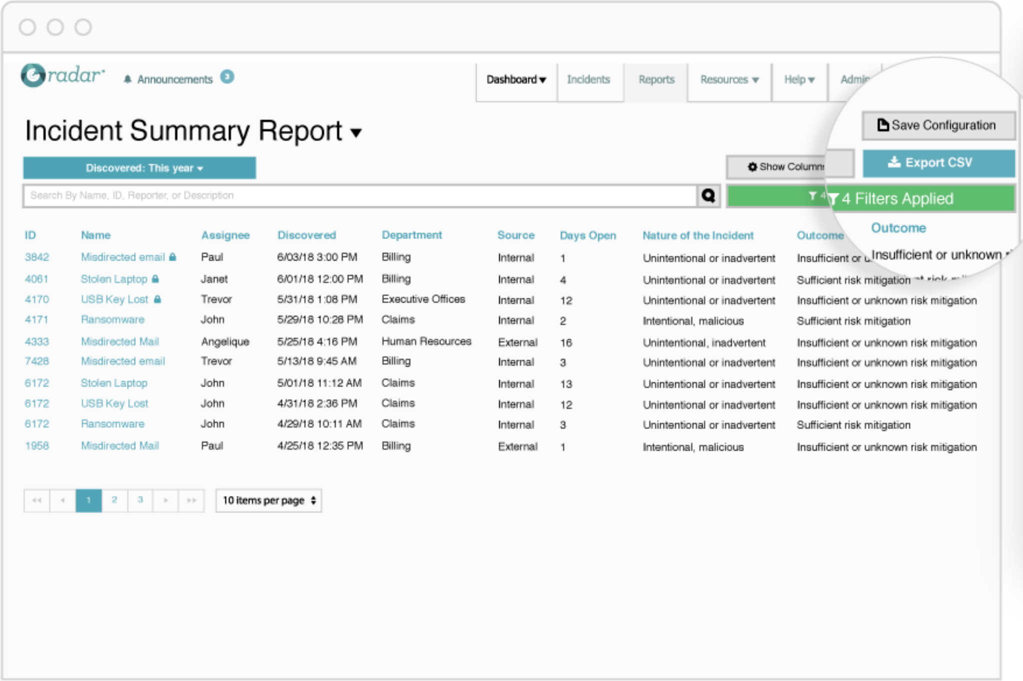
Data Elements

Root Cause

Individual Notification

CE Notification

Generate all the information needed to provide regulatory reports.

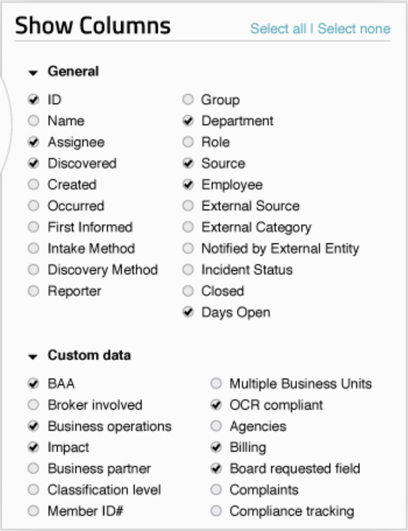


Incident Summary Report ▾

Discovered: This year ▾

Search By Name, ID, Reporter, or Description

ID	Name	Assignee	Discovered	Department	Source	Days Open	Nature of the Incident	Outcome
3842	Misdirected email	Paul	6/03/18 3:00 PM	Billing	Internal	1	Unintentional or inadvertent	Insufficient or unknown
4061	Stolen Laptop	Janet	6/01/18 12:00 PM	Billing	Internal	4	Unintentional or inadvertent	Sufficient risk mitigation
4170	USB Key Lost	Trevor	5/31/18 1:08 PM	Executive Offices	Internal	12	Unintentional or inadvertent	Insufficient or unknown risk mitigation
4171	Ransomware	John	5/29/18 10:28 PM	Claims	Internal	2	Intentional, malicious	Sufficient risk mitigation
4333	Misdirected Mail	Angelique	5/25/18 4:16 PM	Human Resources	External	16	Unintentional, inadvertent	Insufficient or unknown risk mitigation
7428	Misdirected email	Trevor	5/13/18 9:45 AM	Billing	Internal	3	Unintentional or inadvertent	Insufficient or unknown risk mitigation
6172	Stolen Laptop	John	5/01/18 11:12 AM	Claims	Internal	13	Unintentional or inadvertent	Insufficient or unknown risk mitigation
6172	USB Key Lost	John	4/31/18 2:36 PM	Claims	Internal	12	Unintentional or inadvertent	Insufficient or unknown risk mitigation
6172	Ransomware	John	4/29/18 10:11 AM	Claims	Internal	3	Unintentional or inadvertent	Sufficient risk mitigation
1958	Misdirected Mail	Paul	4/25/18 12:35 PM	Billing	External	1	Intentional, malicious	Insufficient or unknown risk mitigation



Show Columns

Select all | Select none

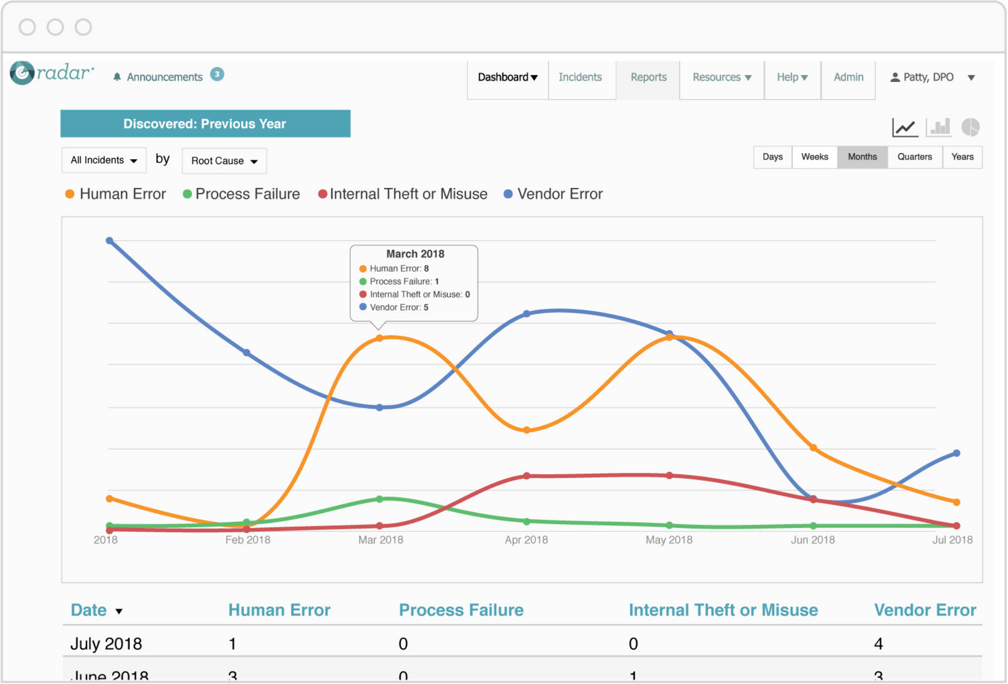
General

- ☑ ID
- ○ Name
- ☑ Assignee
- ☑ Discovered
- ○ Created
- ○ Occurred
- ○ First Informed
- ○ Intake Method
- ○ Discovery Method
- ○ Reporter
- ○ Group
- ☑ Department
- ○ Role
- ☑ Source
- ☑ Employee
- ○ External Source
- ○ External Category
- ○ Notified by External Entity
- ○ Incident Status
- ○ Closed
- ☑ Days Open

Custom data

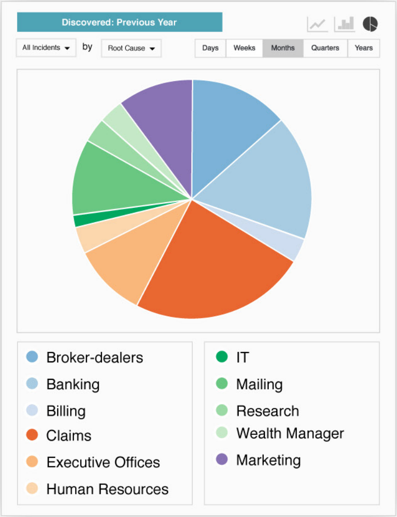
- ☑ BAA
- ○ Broker involved
- ☑ Business operations
- ☑ Impact
- ○ Business partner
- ○ Classification level
- ○ Member ID#
- ○ Multiple Business Units
- ☑ OCR compliant
- ○ Agencies
- ☑ Billing
- ☑ Board requested field
- ○ Complaints
- ○ Compliance tracking

Sort, filter, and save custom reports.



March 2018
- Human Error: 8
- Process Failure: 1
- Internal Theft or Misuse: 0
- Vendor Error: 5

Date ▾	Human Error	Process Failure	Internal Theft or Misuse	Vendor Error
July 2018	1	0	0	4
June 2018	3	0	1	3



Example reports showing root cause and departmental origins for privacy incidents.