WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Measuring Privacy

July 21, 2022

Office of Privacy and Data Protection

Today's outline

I. Why measure privacy

II. Challenges and obstacles

III. Potential privacy metrics

IV. Considerations for defining and implementing

OPDP

Why measure privacy?

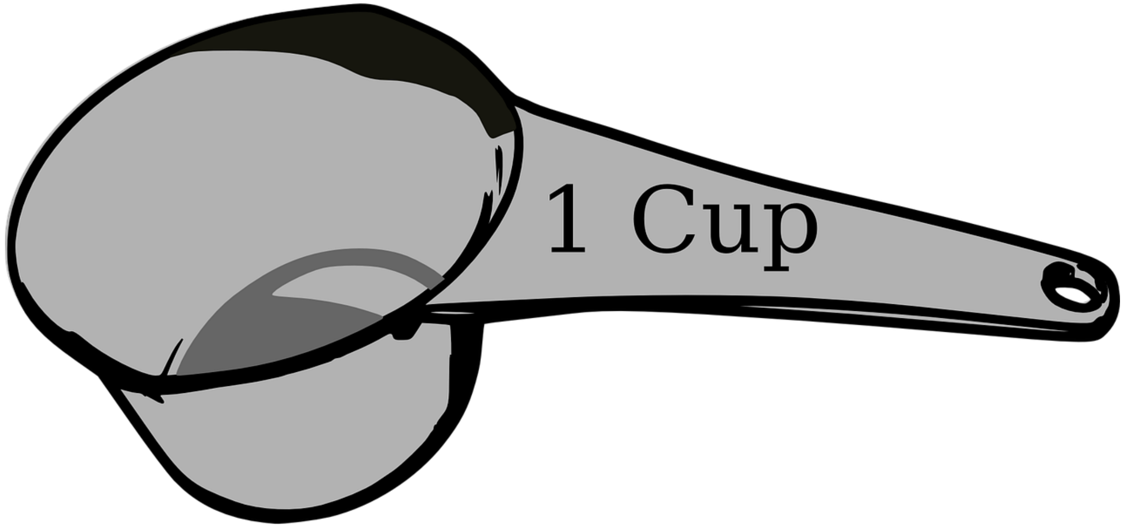
OPDP

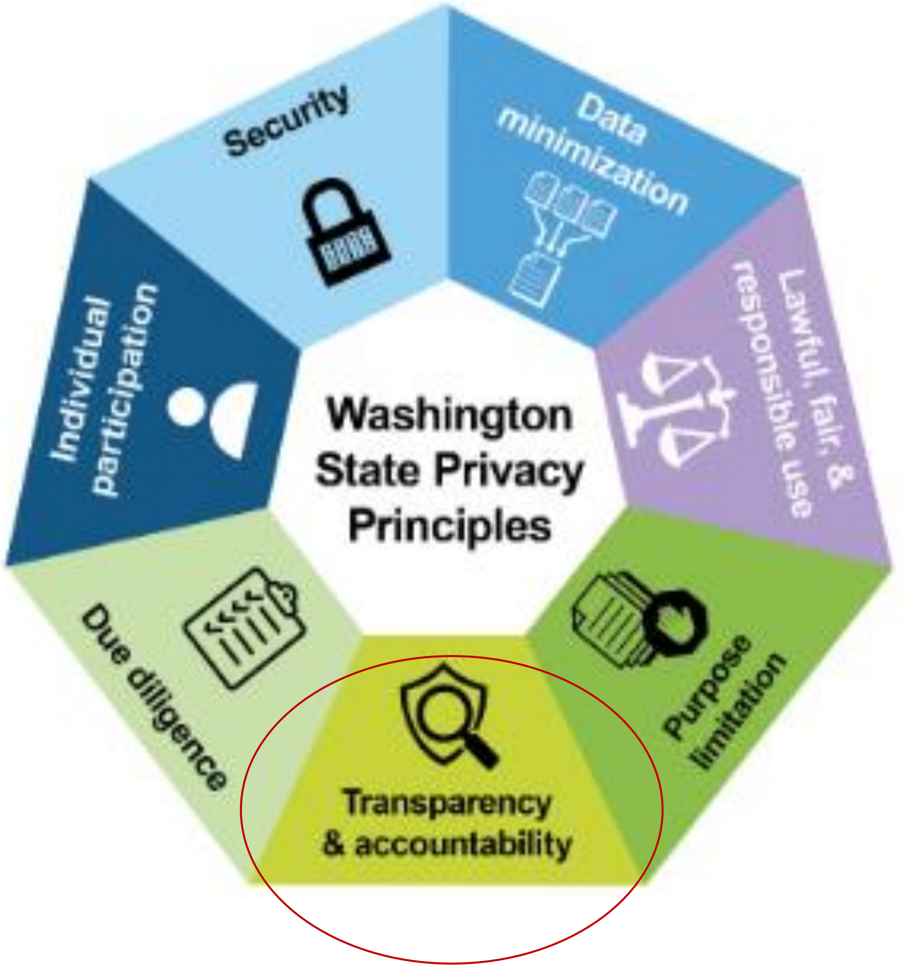
Metric – A quantifiable measurement of a business activity that allows you to measure the success or failure of that activity

KPI – A metric or combination of metrics that shows the success or failure of meeting a strategic goal or objective

KRI – A metric or combination of metrics that identifies when an acceptable level risk is exceeded

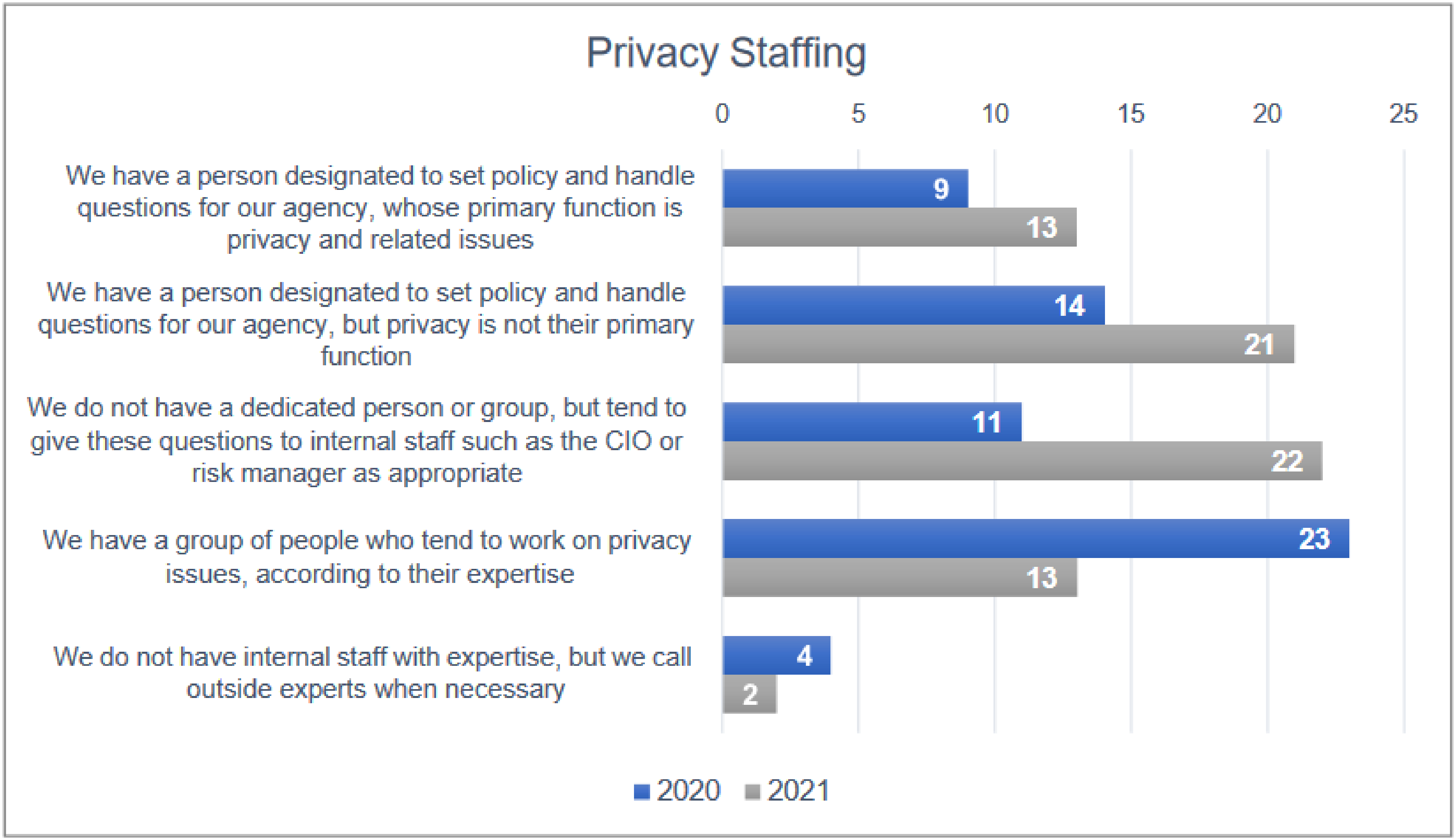
What gets measured gets managed. . . .




Security
Data minimization
Lawful, fair, & responsible use
Purpose limitation
Transparency & accountability
Due diligence
Individual participation
Washington State Privacy Principles

Ensure accountability for adherence to these principles, any applicable privacy laws, and the public's expectations for the appropriate use of personal information. Accountability includes creating and maintaining policies and other records to demonstrate compliance and appropriate information handling. It also includes processes for monitoring or auditing, receiving and responding to complaints, and redress for harmed individuals.

OPDP


Privacy Staffing
0
5
10
15
20
25
We have a person designated to set policy and handle questions for our agency, whose primary function is privacy and related issues
9
13
We have a person designated to set policy and handle questions for our agency, but privacy is not their primary function
14
21
We do not have a dedicated person or group, but tend to give these questions to internal staff such as the CIO or risk manager as appropriate
11
22
We have a group of people who tend to work on privacy issues, according to their expertise
23
13
We do not have internal staff with expertise, but we call outside experts when necessary
4
2
■ 2020
■ 2021

Challenges in measuring privacy

OPDP

What gets measured gets managed. . . . even when it's pointless to measure and manage it, and even if it harms the purpose of the organisation to do so.

- Simon Caulkin

Image by Steve Buissinne from Pixabay

OPDP

Measurement dangers

- Overfocus on things that can be reduced to numbers, without consideration of the unknown or unknowable
- Choosing the wrong measures (often by choosing things that are easier to measure)
- Managing exclusively to the measure, even when it’s the wrong measure

Case study

- UK health care competition efforts promoted reduced waiting times for emergency room admissions
- Result – Reduced waiting times. And increased mortality rates.
- Takeaway – “Hospitals in competitive markets reduced unmeasured and unobserved quality in order to improve measured and observed waiting times.”

What gets measured matters

How do you measure trust?

OPDP

- Limited scale and maturity at agency level

- Easier to measure negative outcomes (e.g., incidents) than successful avoidance (e.g., incidents prevented or avoided)

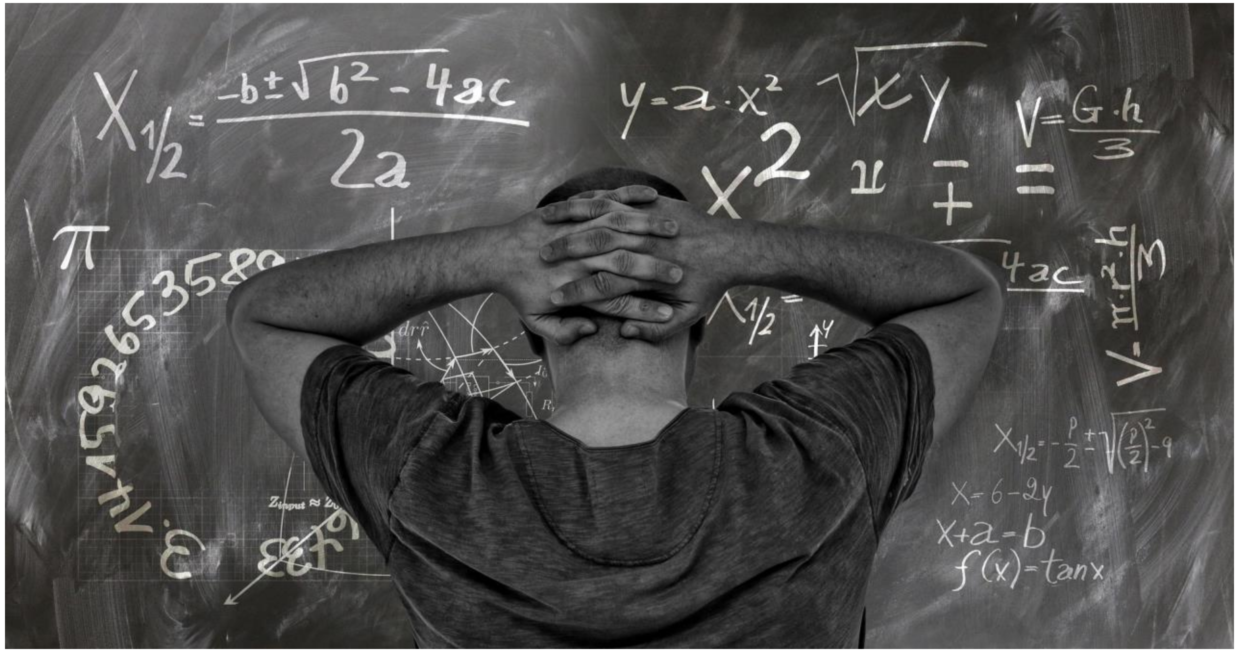
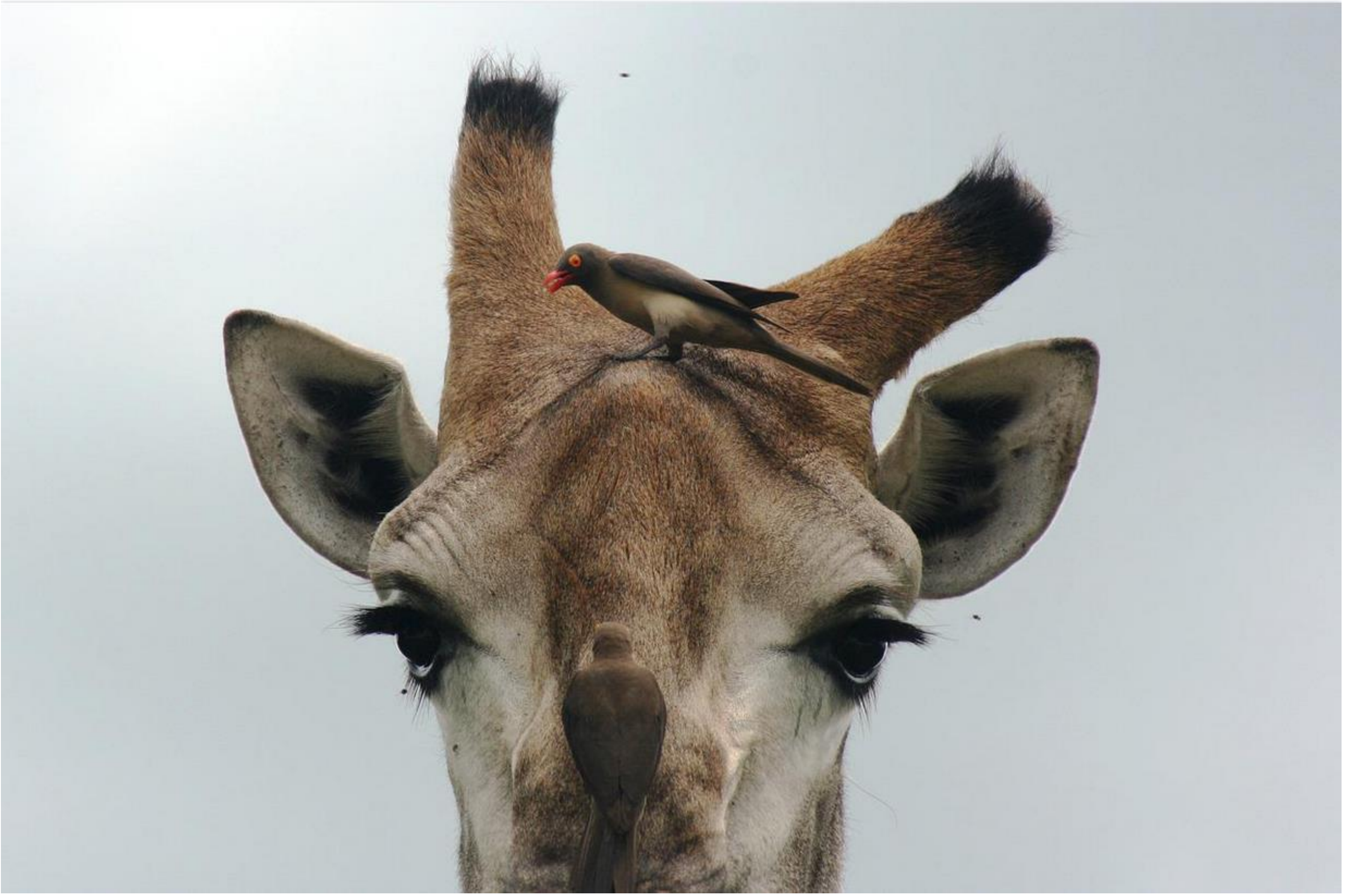

$X_{1/2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
$y = a \cdot x^2$
$\sqrt{xy}$
$V = \frac{G \cdot h}{3}$
x^2
π
$X_{1/2} = -\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q}$
$X = 6 - 2y$
$X + a = b$
$f(x) = \tan x$

Image by Gerd Altmann from Pixabay

- Known numerator but unknown denominator

Cross-disciplinary nature of privacy



Potential privacy metrics

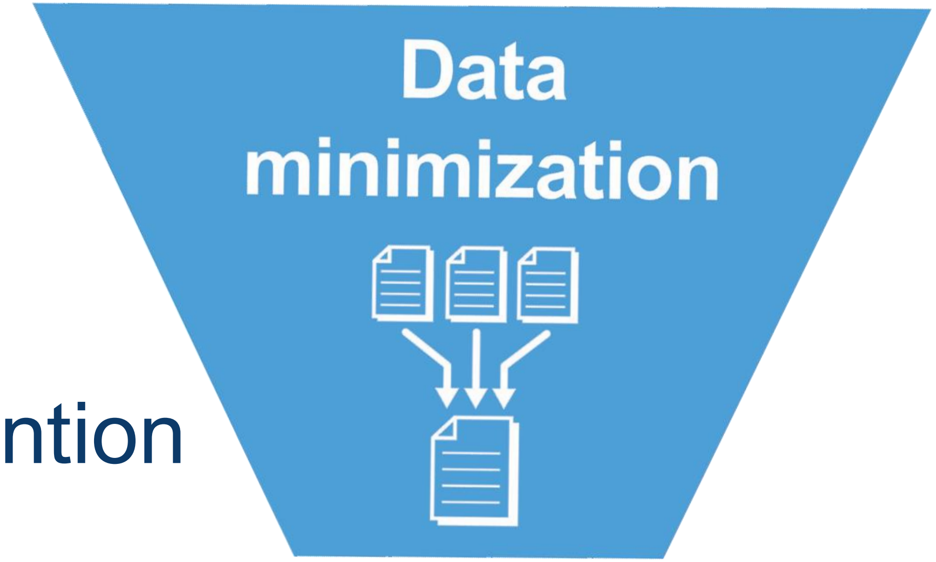
Data minimization

Collection and use

- Privacy impact assessments completed
- Personal information elements in data inventory
- Purged information; records retention compliance

Disclosure

- Data requests reviewed/modified/denied



Lawful, fair & responsible use

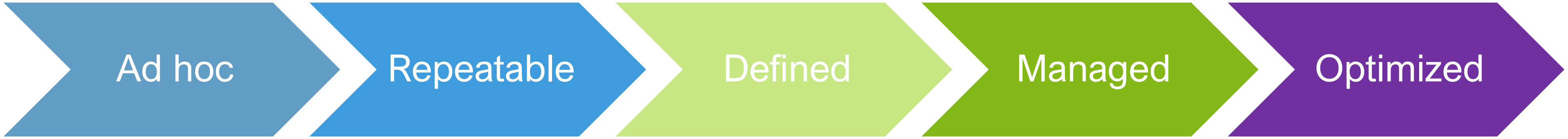
Lawful, fair, & responsible use

- Privacy impact assessments completed
- Number of assessment requiring significant remediation/mitigation
- Timeframe for completion
- Identified risks mitigated after prescribed time

OPDP

Lawful, fair & responsible use

- Documented standards and guidance
- Age of privacy documents
- Privacy framework or maturity model adoption


Ad hoc
Repeatable
Defined
Managed
Optimized

OPDP

Purpose limitation

Privacy impact assessments; periodic review

Data mapping, data catalogs or inventories

- # of applications catalogued

- # of applications that need to be catalogued

Transparency & accountability

Transparency & accountability

Notices provided

Accuracy of contact information

Age of notices

Transparency & accountability

Privacy spend

Transparency & accountability

Complaints from individuals
Inquiries from regulators
Response/success rate of each

Transparency & accountability

Incidents

- # of incidents by type/program
- # of breaches requiring notification
- # of individuals impacted by incidents/breaches
- Time from occurrence to discovery
- Time from discovery to escalation
- Time from discovery to determination/notification

O P D P

Transparency & accountability

# employees who complete training on time

Training scores

Time from onboarding to initial training completion

Privacy engagement

Due diligence

- Data requests reviewed
- Initial vendor assessments
- Permissible use audits
- Third party incidents – discovery and management
- Non-disclosure agreements
- Certificates of destruction
- DSA implementation/review

Individual participation

# of requests received, closed, in progress (to access PI, to send PI to third party, to modify PI, to restrict use or to delete)

Time to respond to each

Outcomes for each

Individual participation

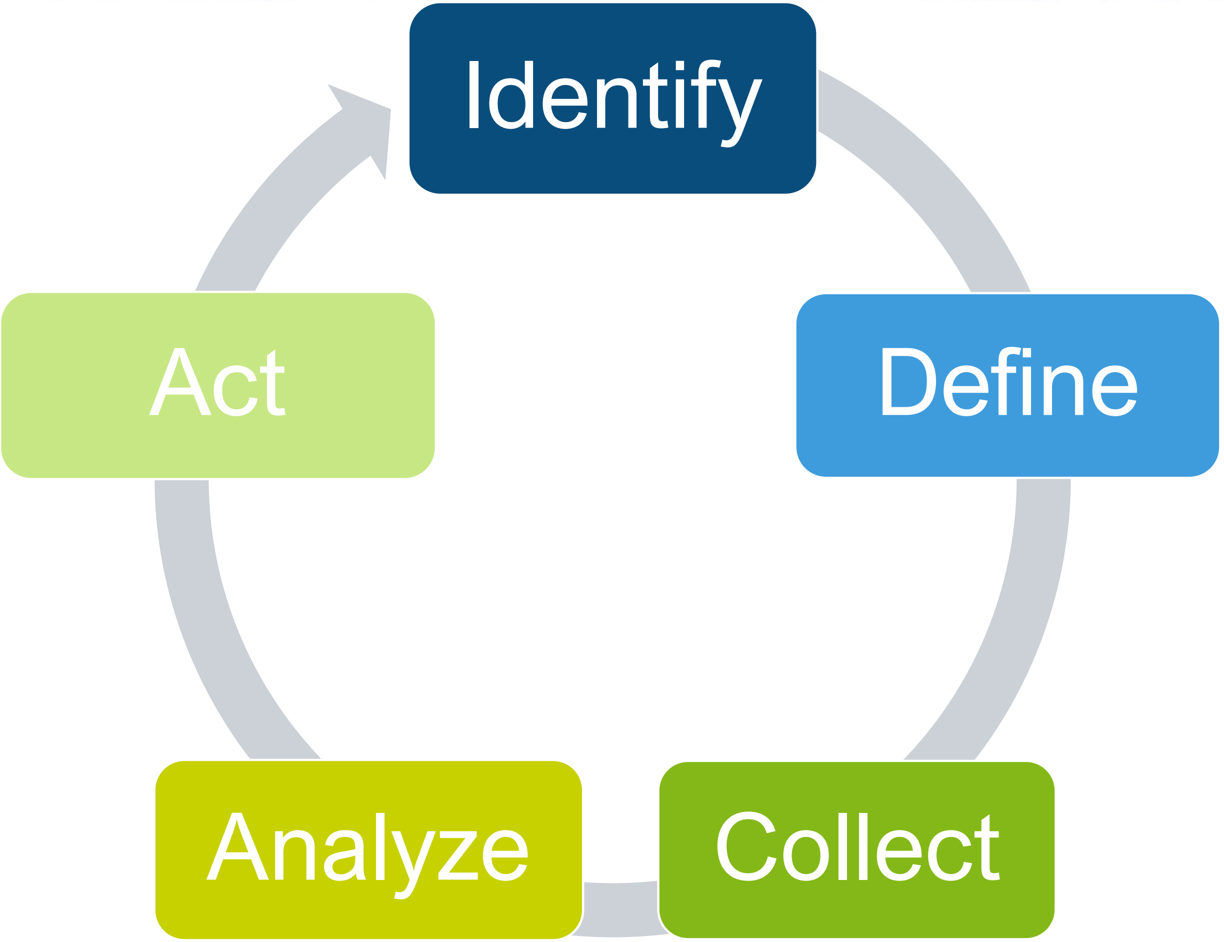
Consent received (data sharing, processing)

Opt-in or opt-outs for emails, cookies

Consent withdrawn

OPDP

Considerations for development and implementation



Identify

Define

Collect

Analyze

Act

Potential audience - leadership

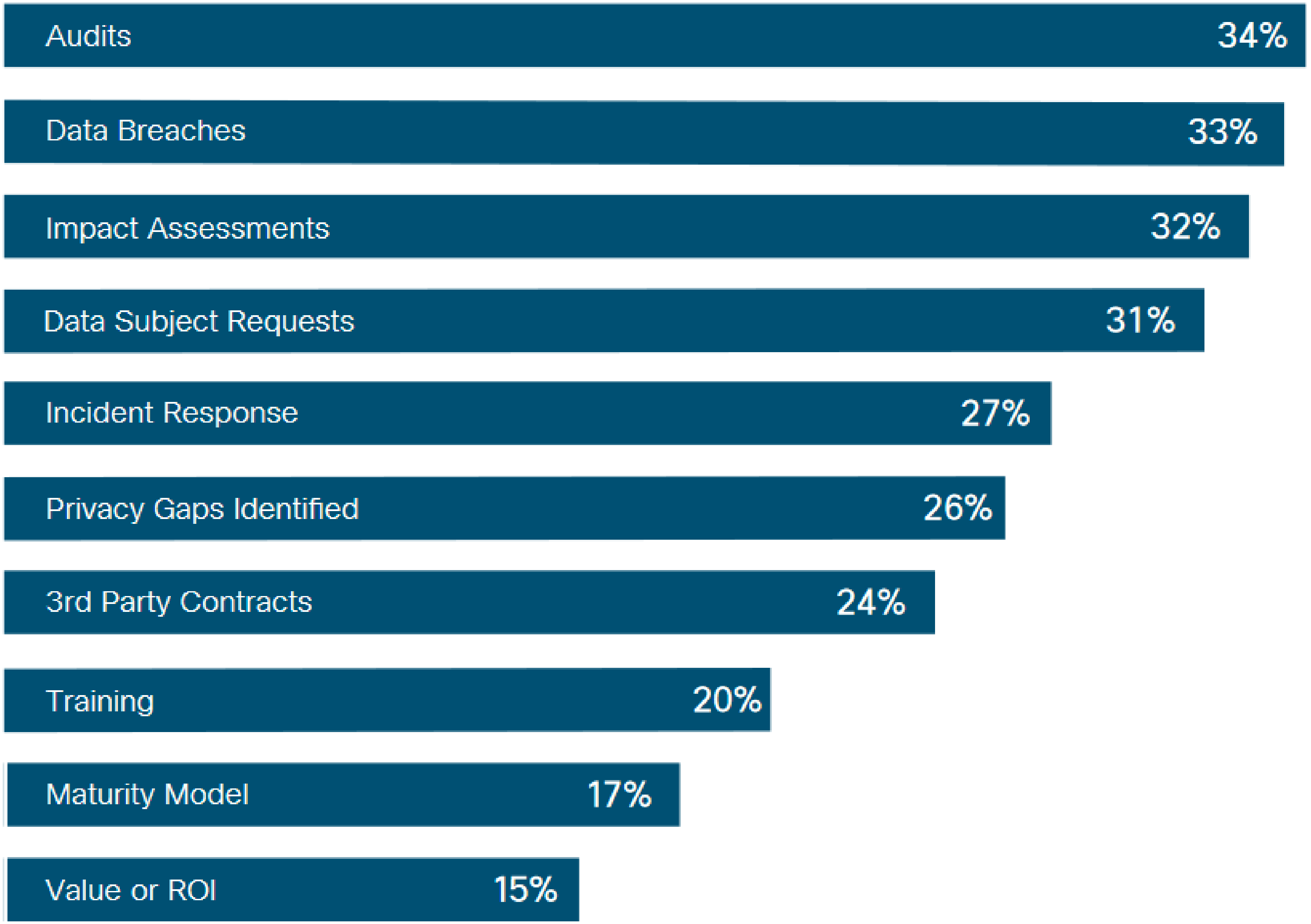
- Limited access and time
- Key performance indicators
- What matters to leadership?
- What matters to you?

Potential audience - leadership

- 94% report one or more metrics to board of directors
- Some report as many as 10 privacy metrics
- Most report between 1 and 3

Cisco 2022 Data Privacy Benchmark Study

Potential audience - leadership



Potential audience – management peers

- Broader audience than either leadership or your team
- Measurements that peers can influence
- Caution re: oversharing

Potential audience – privacy team

Photo by Marvin Meyer on Unsplash

- Operational focus
- Less important to limit number of metrics (but care still needed!)
- Dashboards

OPDP

Potential audience – other external parties

- Regulators
- Public records requests
- Authorizing environment
- Other agencies

OPDP

Key attribute - quantifiable

CIRCULAR REASONING WORKS BECAUSE

Metrics must measure things capable of being measured

Quantitative – objective, numeric values (counts, time)

Qualitative – subjective, quality and experience-based

OPDP

Call center performance

# of calls
Average call time
Average wait time
Abandonment rate

Surveys

- Satisfaction
- Promoter score
- Open-ended

Metric types

Activity – The level of activity

Trends – The level of an activity or occurrence over a period of time

Outcome – The measure of activity compared to some qualitative goal

SMART metrics

Specific – Does it clearly define objective and goals?

Measurable – Is success capable of being measured?

Achievable – Is success possible?

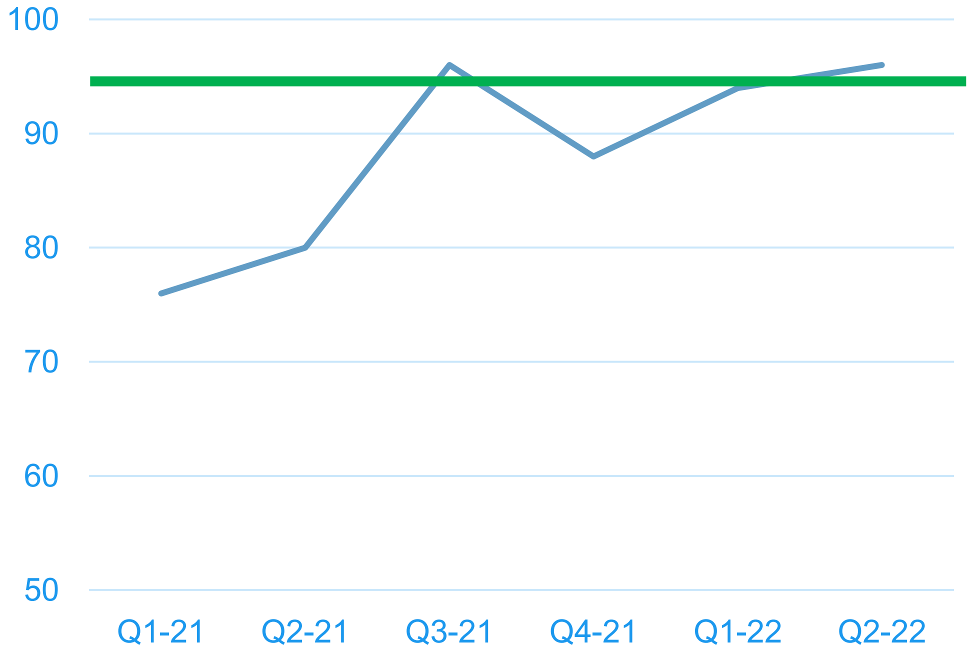
Relevant – Does measurement fit within overall goals?

Time-bound – Is there a relevant timeline for measurement?

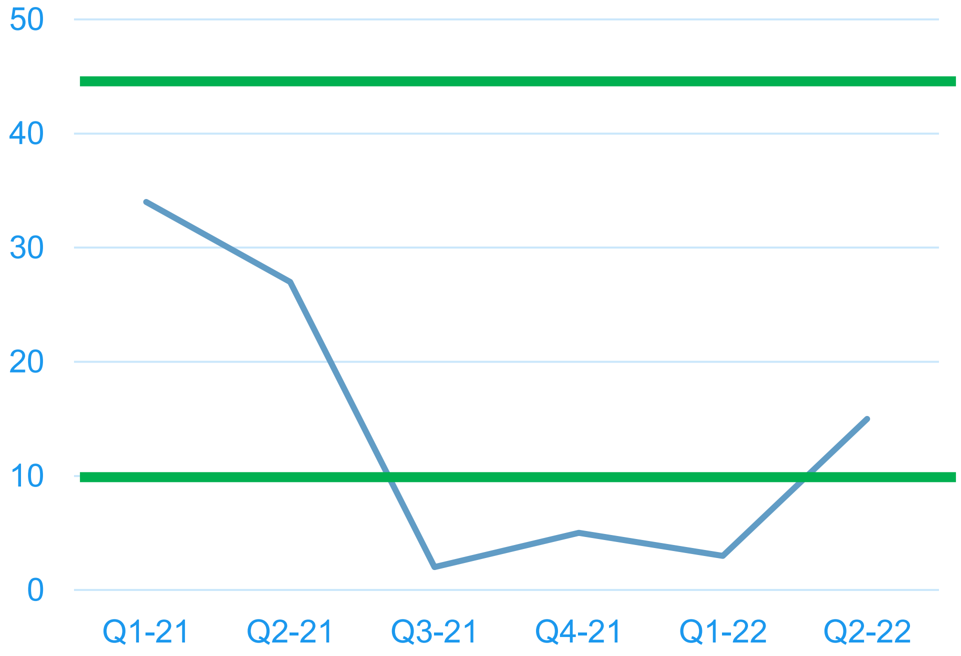
Thresholds for success

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

A count without a goal or risk level is likely of little value



Goal



Range

OPDP

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

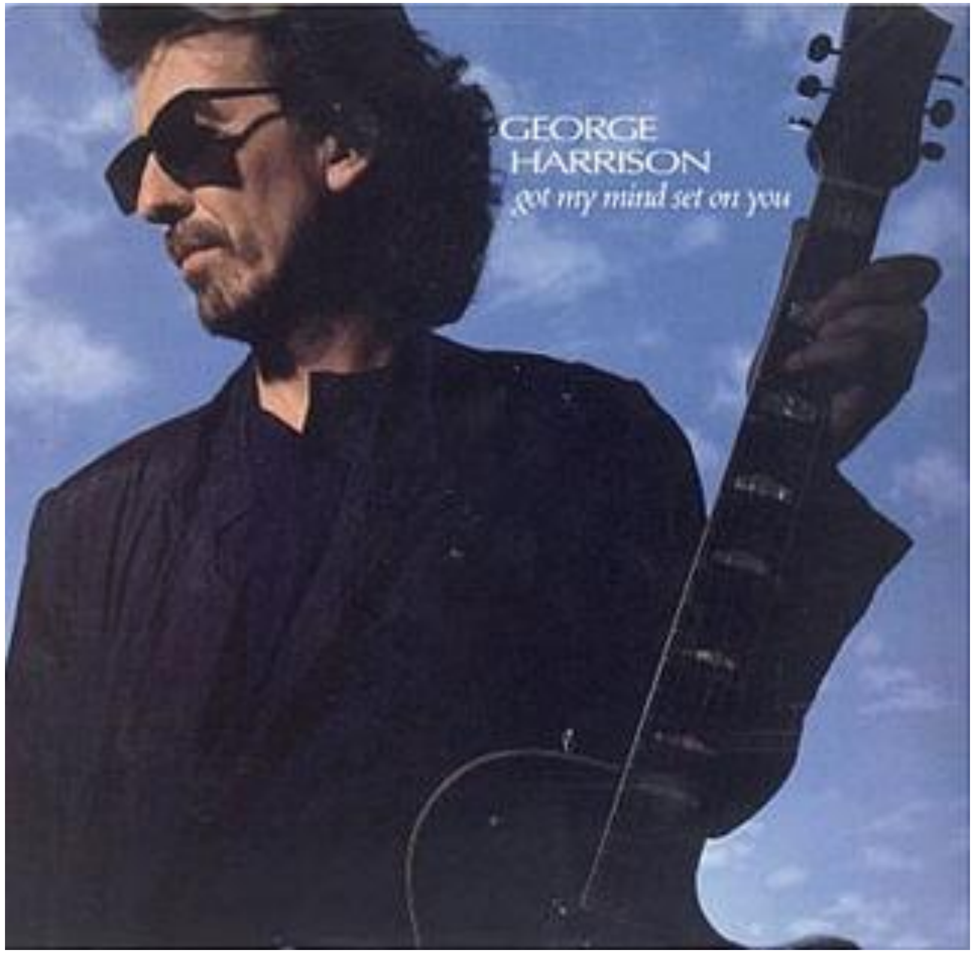
Thresholds for success

- Industry benchmarks
- Other agencies
- Other metrics in your own agency
- Applicable regulations
- Your own commitments, frameworks or maturity models
- Your own experience over time

OPDP

It's worth spending the time to fully define before putting into use.

- Consistency helps you evaluate over time
- Avoid analysis delays
- Doesn't mean you can't revisit (especially goals)



OPDP

Collection considerations

Repeatable and consistent

Embed early

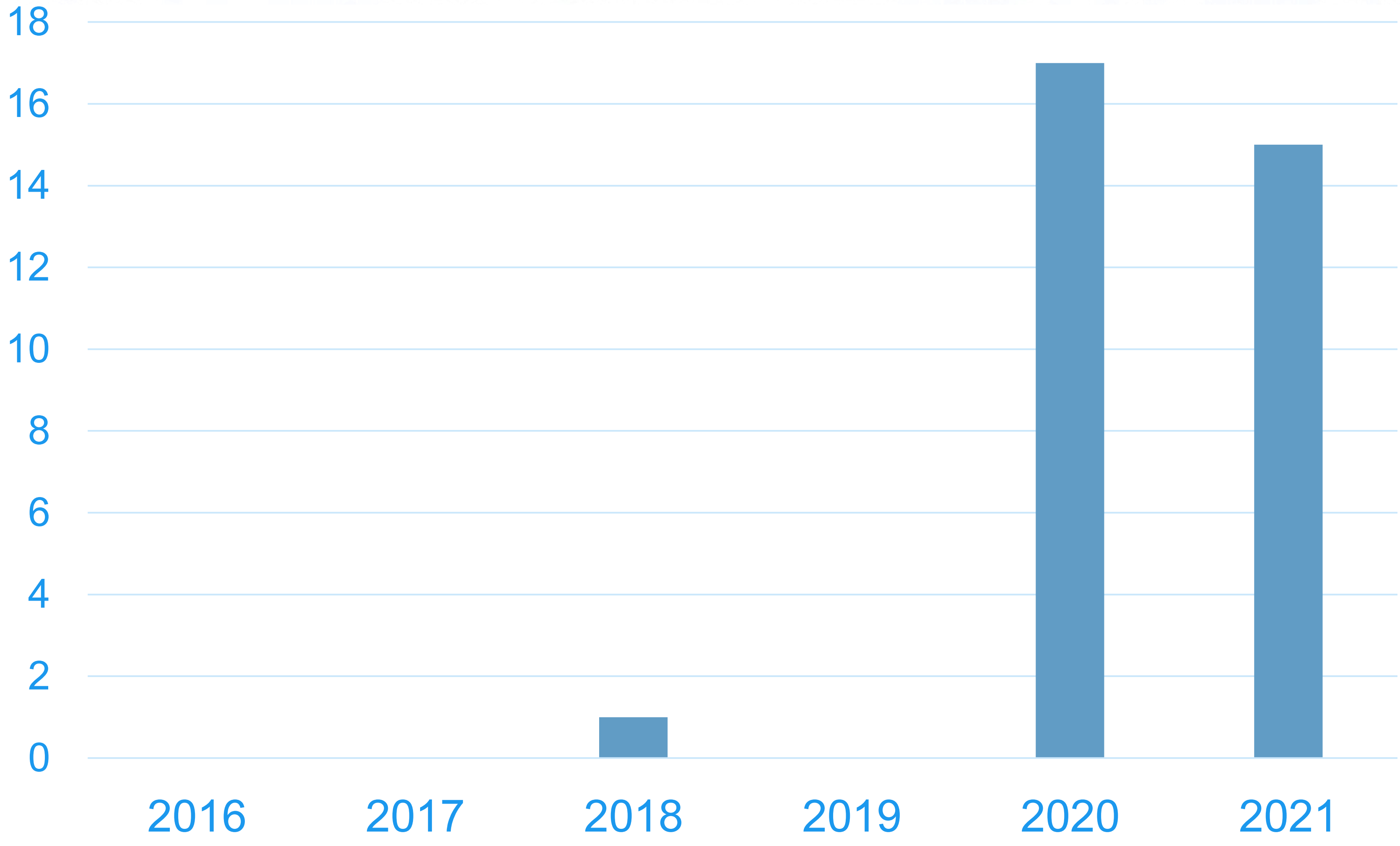
Leverage other processes

Cost shouldn’t exceed value

- Carefully consider overall story – don’t jump to conclusions
- Even when carefully defined, the measurements are the start

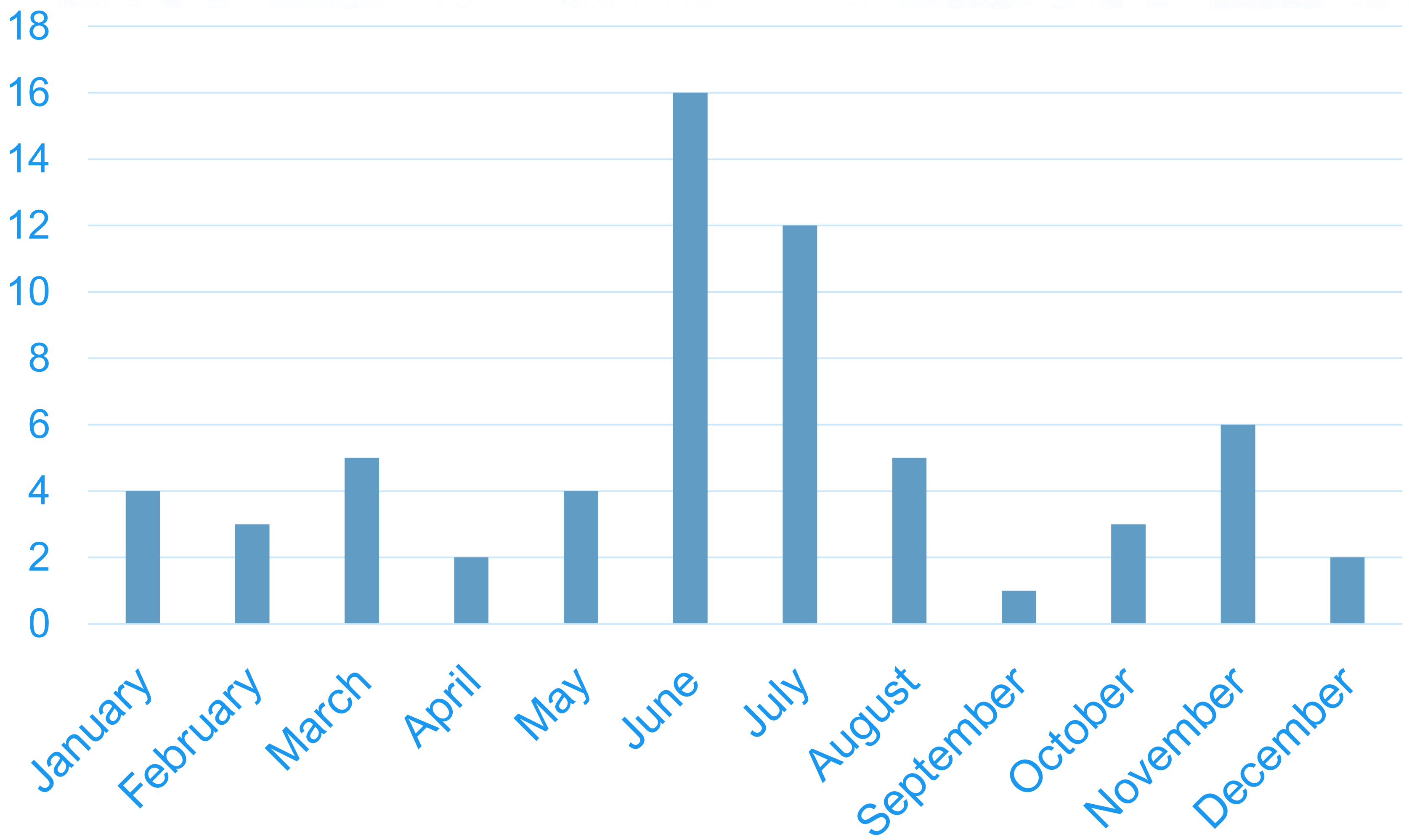
O
P
D
P

Incidents by Year



OPDP

Incidents by Month



OPDP

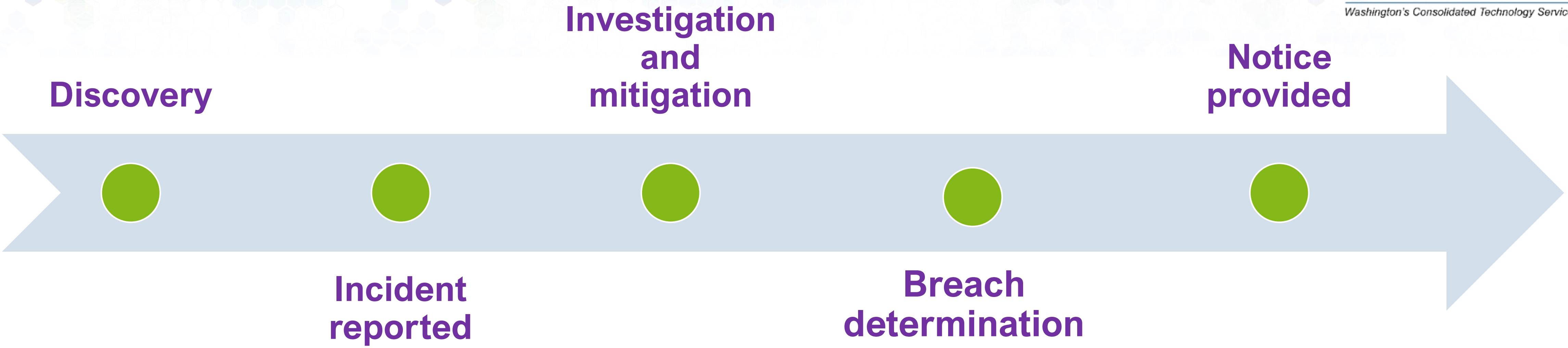
Good metrics drive change.

Requirement – Agencies must provide notice of breach to affected individuals within 30 days of discovery

Measure – Average time from discovery to notification

Goal – 25 days

Results – Missed target 9 out of last 12 months



Discovery

Incident reported

Investigation and mitigation

Breach determination

Notice provided

Lag in reporting – insufficient training and awareness

Lag in investigation – possibly insufficient privacy resources or lack of cooperation from business units

Lag in determination – possibly insufficient privacy resources or poor relationship with attorneys or leadership

Lag in providing notification – possibly insufficient privacy resources, lack of cooperation or other challenges like translation

How will it be communicated?

- Reporting mechanisms and communication channels
  - Existing processes?
  - Required formats?
  - New relationships needed?
- Dashboards, slides, narrative reports

OPDP

Wrap-up

- Metrics should be quantifiable, relevant and actionable
- Consider intended audiences and how they will be used
- Think outside the box (and early) about data collection opportunities
- Take the time to understand and tell the story behind the data

Other resources

RadarFirst – How to Use Privacy Metrics for Program Improvement and to Prove ROI

Cisco 2022 Data Privacy Benchmark Study

FPF Privacy Metrics Report

Aaron Weller Importance of Metrics

NIST Privacy Framework

AICPA Privacy Management Framework

Questions?

privacy@watech.wa.gov

watech.wa.gov/privacy