Cyber and Data Risk

Evaluating Program Effectiveness and Examination Readiness

Buckley Sandler LLP

Legal Counsel to the Financial Services Industry

Digital Commerce & Payments Series Webinar

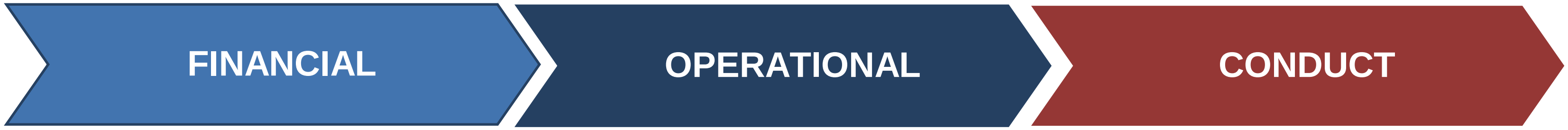
February 4, 2015

Introduction & Overview

- Today's discussion:
  - Defining program effectiveness
  - Privacy and security program development
  - Impact: regulation, cyber-threat landscape, conduct risk
  - Metrics: relevant, actionable, timely, impactful
  - Effective reporting to stakeholders

Data Risk: Nature & Timing

Definition of data risk is evolving and expanding:



FINANCIAL

OPERATIONAL

CONDUCT

Financial risk:

- Market risk
- Credit risk
- Liquidity risk
- Operational risk

Risk of a change in value caused by the fact that actual losses, incurred for inadequate or failed internal processes, people and systems, or from external events (including legal risk), differ from the expected losses. Basel II

Risk that firm does not operate with integrity and transparency with its customers or when it is a market participant.

Timeframe of risk analysis and response is evolving and expanding:

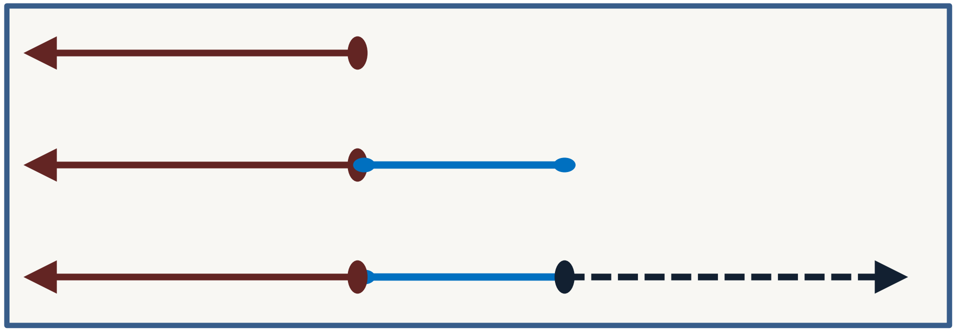
Assessment/Evidence of Past Performance

+

Real Time Analysis & Rapid Response

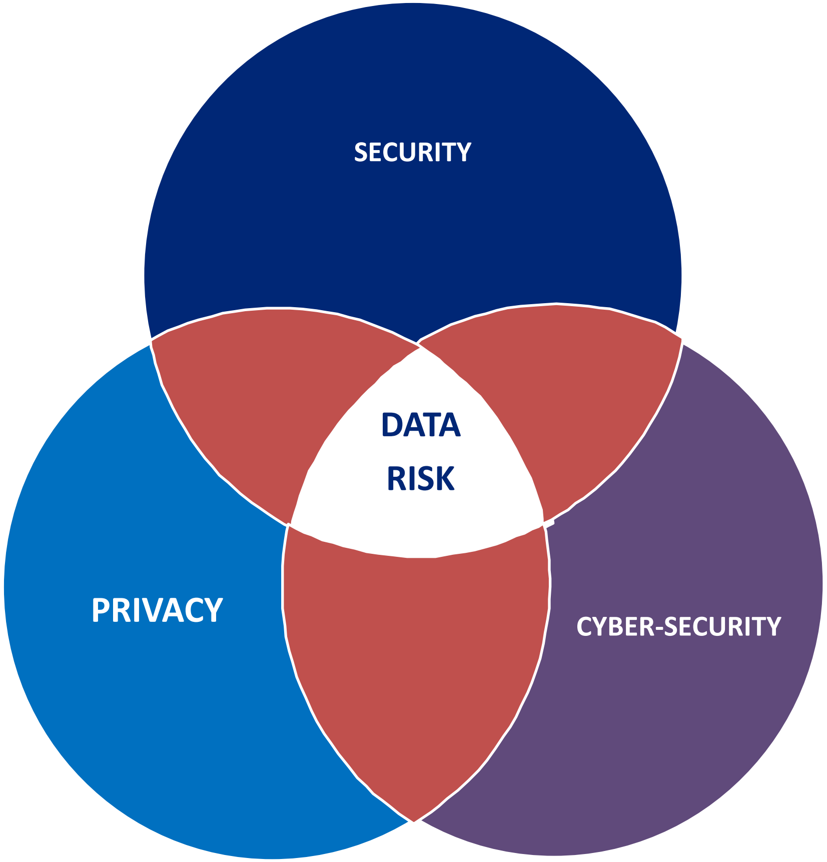
+

Predictive Analysis & Preventive Action



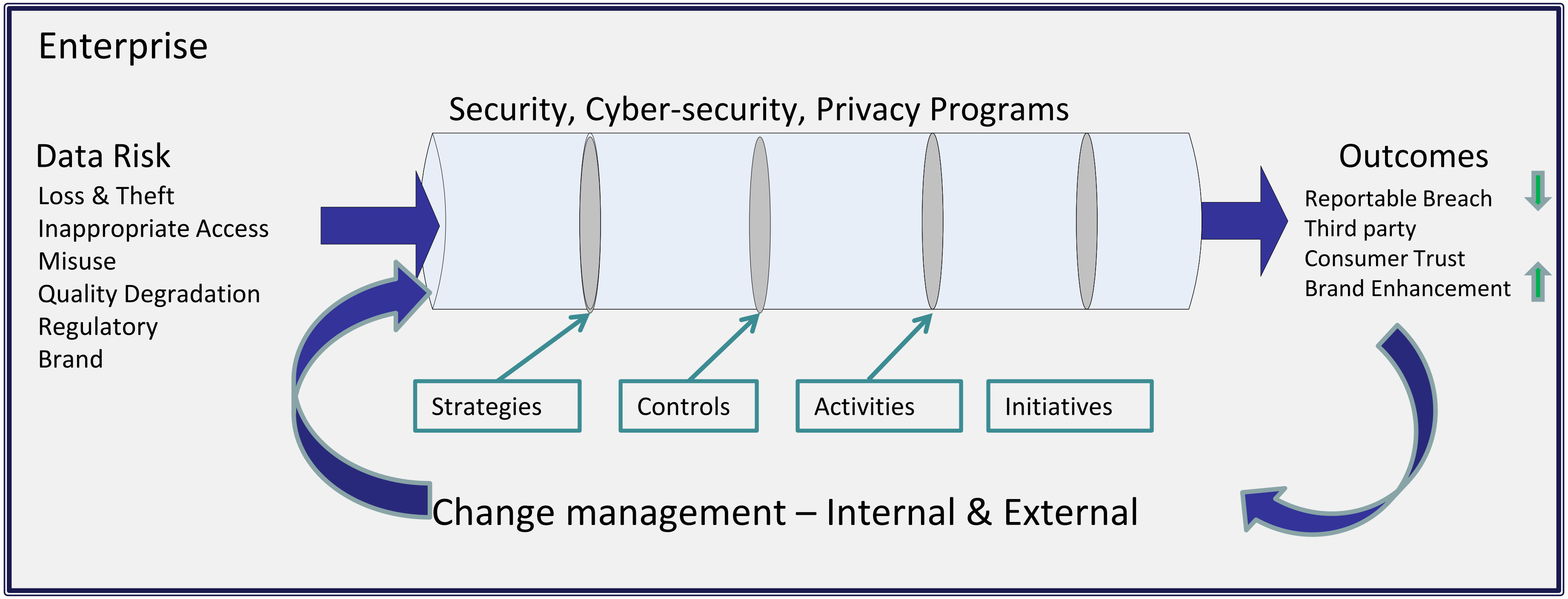
Data Risk Mitigation Programs

- Security, privacy and cybersecurity programs all focus on data risk mitigation
  - **Security**: Consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets
  - **Privacy**: focus on the rights and responsibilities associated with the collection, protection and dissemination of personal or private information about individuals or organizations.
  - **Cybersecurity**: The process of protecting, detecting, and responding to attacks



Buckley Sandler LLP

Program as a System



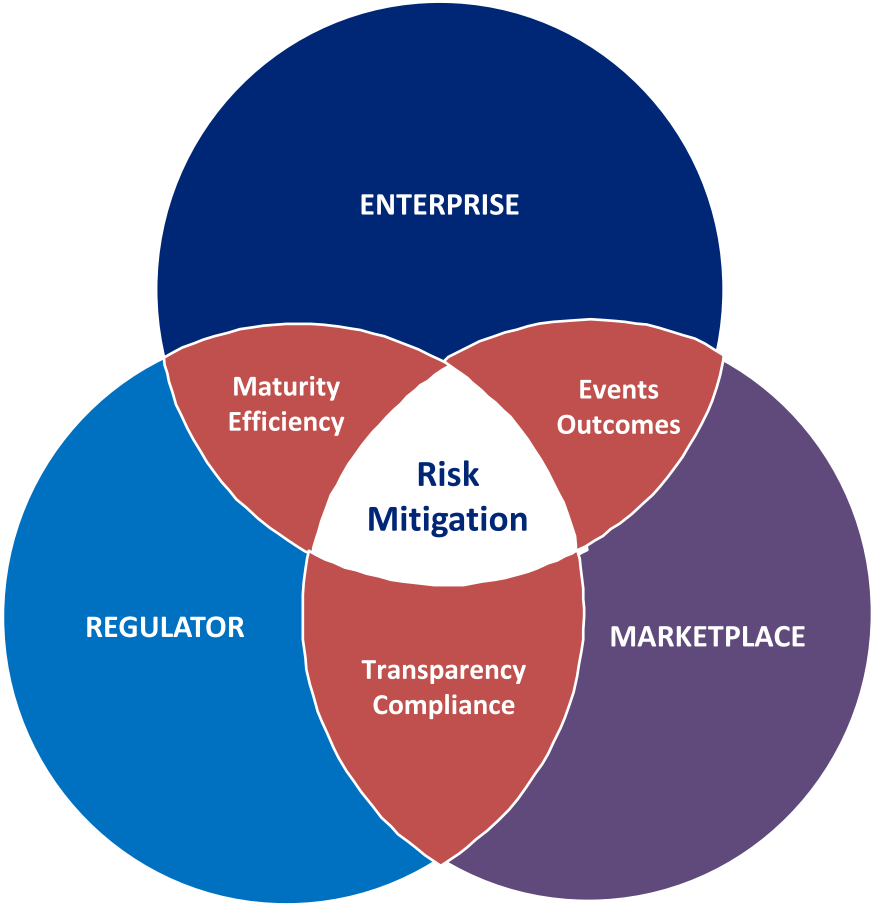
Whether “Security”, “Cyber-Security”, or “Privacy” – the program is a **system.** A **system is** an organized collection of parts (or subsystems) that are highly integrated to accomplish an overall goal. The system has various inputs, which go through certain processes to produce certain **outcomes,** which together, accomplish the overall desired goal for the system. *

Buckley Sandler LLP

**System Engineering Modeling and Design - Saurabh*

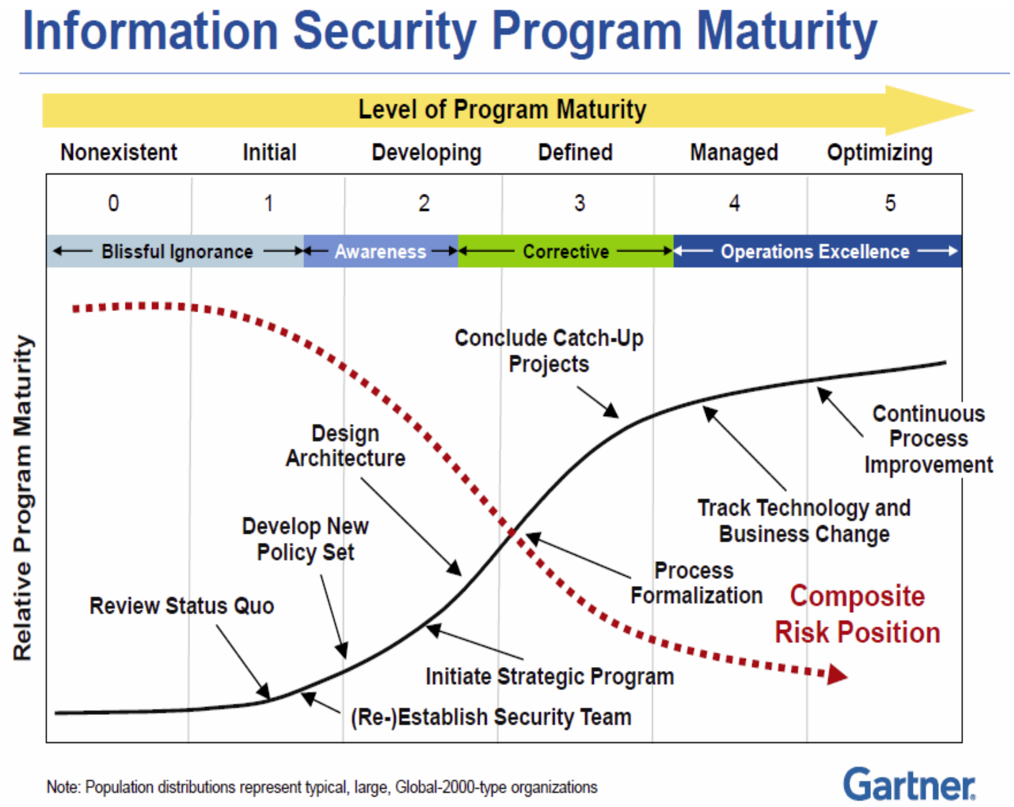
Effectiveness: Eye of the Beholder

- Enterprise:
  - Enterprise Risk Mitigation
  - Strategic Alignment
  - Function/Program Maturity
  - Efficiency – Resource Allocation
- Regulator:
  - Enterprise within the Ecosystem
  - Confidence in the markets
  - Consumer Protection
  - Compliance & Control
- Marketplace – Consumer, Business
  - Individual or Entity
  - Transparency
  - Competency
  - Trust
  - Willingness to do business



Buckley Sandler LLP

Enterprise – Effectiveness


Information Security Program Maturity
Level of Program Maturity
Nonexistent
Initial
Developing
Defined
Managed
Optimizing
0
1
2
3
4
5
Blissful Ignorance
Awareness
Corrective
Operations Excellence
Relative Program Maturity
Conclude Catch-Up Projects
Design Architecture
Develop New Policy Set
Review Status Quo
Continuous Process Improvement
Track Technology and Business Change
Process Formalization
Composite Risk Position
Initiate Strategic Program
(Re-)Establish Security Team
Note: Population distributions represent typical, large, Global-2000-type organizations
Gartner

Evolving approach to data risk:

- Board and Senior Management involvement
- Strategic alignment
- From compliance to risk-based
- From enterprise to ecosystem
- From "siloed" to integrated
- From 'look-back' to 'current' to 'predictive'
- Transition from primarily control assessment and compliance tasking to risk response and outcomes focused
- Evolving beyond **financial**, **operational, regulatory risk** to incorporate **control risk**

Impact on effectiveness metrics:

- Multiple stakeholders, variety of metrics and tailored reporting
- Increasing use of outcomes based metrics
- Asset management approach

Buckley Sandler LLP

Elements of an Effective Program*

- US DOJ and US SEC on compliance programs:
  1. Senior Management Commitment
  2. Code of Conduct and Compliance Policies and Procedures
  3. Oversight, Autonomy, and Resources
  4. Risk Assessment
  5. Training and Continuing Advice
  6. Disciplinary Measures and Incentives
  7. Third-party Due Diligence and Payments
  8. Confidential Reporting and Internal Investigation
  9. Continuous Improvement: Periodic Testing and Review

*US Dept of Justice and US SEC – *A Resource Guide to the U.S. Foreign Corrupt Practices Act* – *Nov 2012*

Regulator: NY DFS Cyber Sec Exam

Exam Focus

- Corporate governance
- Cybersecurity process integration
- Resources – info sec, risk management
- Shared infrastructure risk
- Intrusion detection
- Authentication – multi-factor
- Server and database configurations
- Testing, monitoring, pen-testing
- Incident detection and response
- Training – info sec and others
- Third party provider management
- Info sec integration with BC/DR
- Cybersecurity insurance

Additional Questions

- CISO or equivalent CV, skillset
- Security policy set
- Data classification integration
- Vulnerability and patch management
- Identity and access management
- Multi-factory authentication
- 3rd party service provider vetting, selecting, monitoring, and due diligence
- Application development standards including secure development life cycle
- Incident response program
- Info sec is incorporated into BCP/DR
- Significant changes to IT portfolio over previous 24 months

Marketplace: Trust & Competency

- Forbes: January 2014 – Five Lessons… from Target's Data Breach*
  - Communicate the problem, pronto
  - Be ready to respond to your customers
  - Push for updated security technology
  - Invest in prevention
  - Rebuild trust

- 2014: A Year of Mega Breaches released in January 2015** (Ponemon Survey of IT and IT Sec pros)
  - Data breach did not change fundamental behavior (90% still shop at location) but it did change payment method (40% decline to use debit cards, 18% cash only)
  - Reputation loss and tarnished brand value was seen as the biggest impact of data breach.
  - Lost customers, reduced revenues or regulatory fines were the lowest perceived impact
  - Increased senior management awareness led to expanded budget for info security tools
  - Root cause determination difficult – but forensics funding to support analysis not priority
  - Organizations not able to detect breaches in a timely manner – months, years or not at all
  - Malware was most prevalent root cause -- but one of lowest investment categories
  - Training is still leading response to a data incident

** Forbes, Five Lessons For Every Business From Target's Data Breach – 01/17/2014*

*** 2014 – Year of the Mega Breach - Ponemon Institute Research Report – Sponsored by Identify Finder*

Measuring What Matters or….
Measuring What We Can?

Metrics: Characteristics

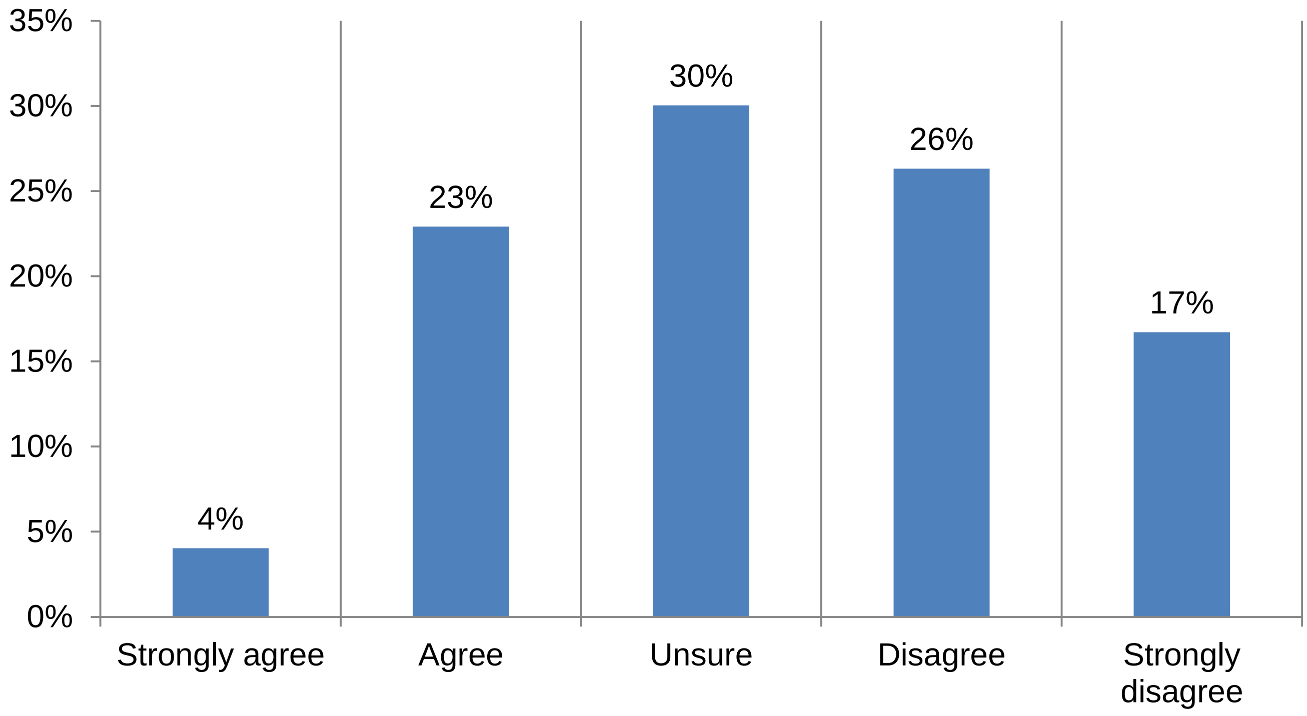
- Good metrics are:
  - Measurable
  - Meaningful
  - Defined
  - Usable
  - Measure progress against an organizational goal
- Characteristics
  - Accuracy
  - Precision
  - Validity
  - Correctness

- A development method:
  - Goals-Questions-Metrics: (GQM)*
  - Metrics should be tied to a goal of the organization.
  - Steps to create metrics:
    - Goal is defined first
    - Series of questions are created to determine progress against goal or sustainment of goal
    - Specific Metrics are defined, collected and analyzed to answer the questions

** Complete Guide to Security and Privacy Metrics – Debra S Herrmann*

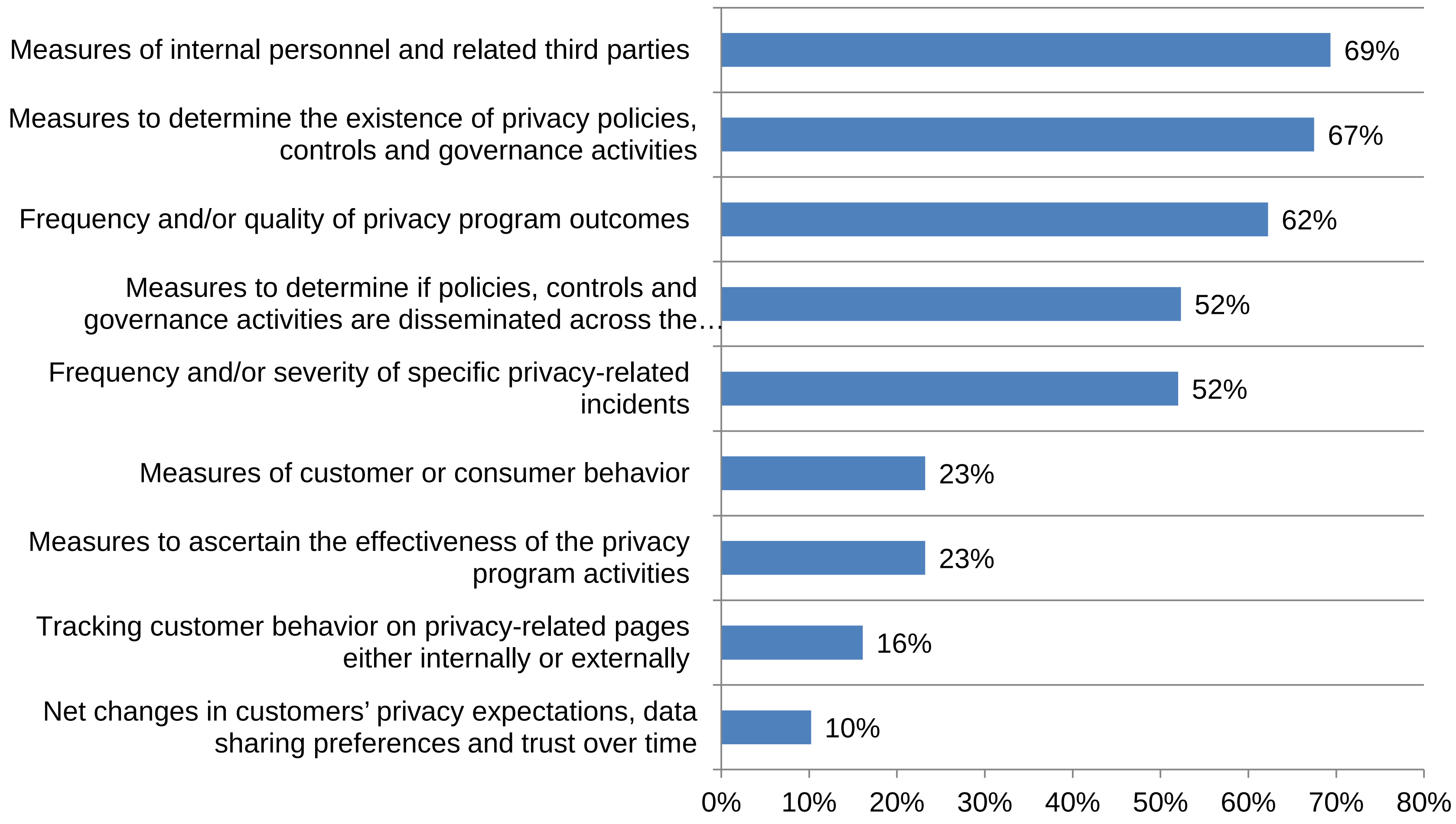
Actionable Metrics?

- Metrics currently tracked and available to the privacy program provides management with information that is actionable:



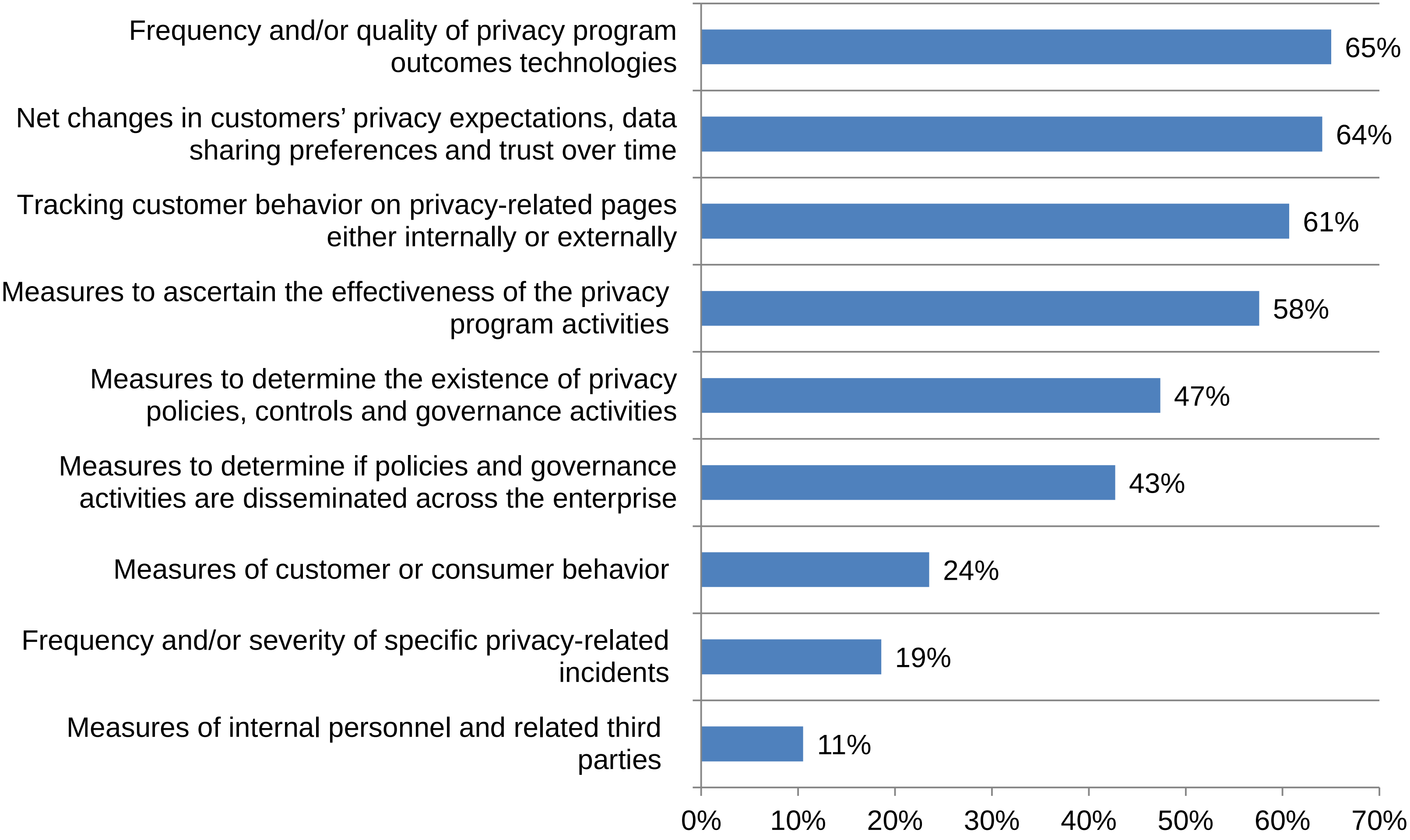
2013 - Ponemon Institute/RMCS LLP Metrics Study

Nine Metrics – Ranked in Order of Use



2013 - Ponemon Institute/RMCS LLP Metrics Study

Nine Metrics – Order of Importance

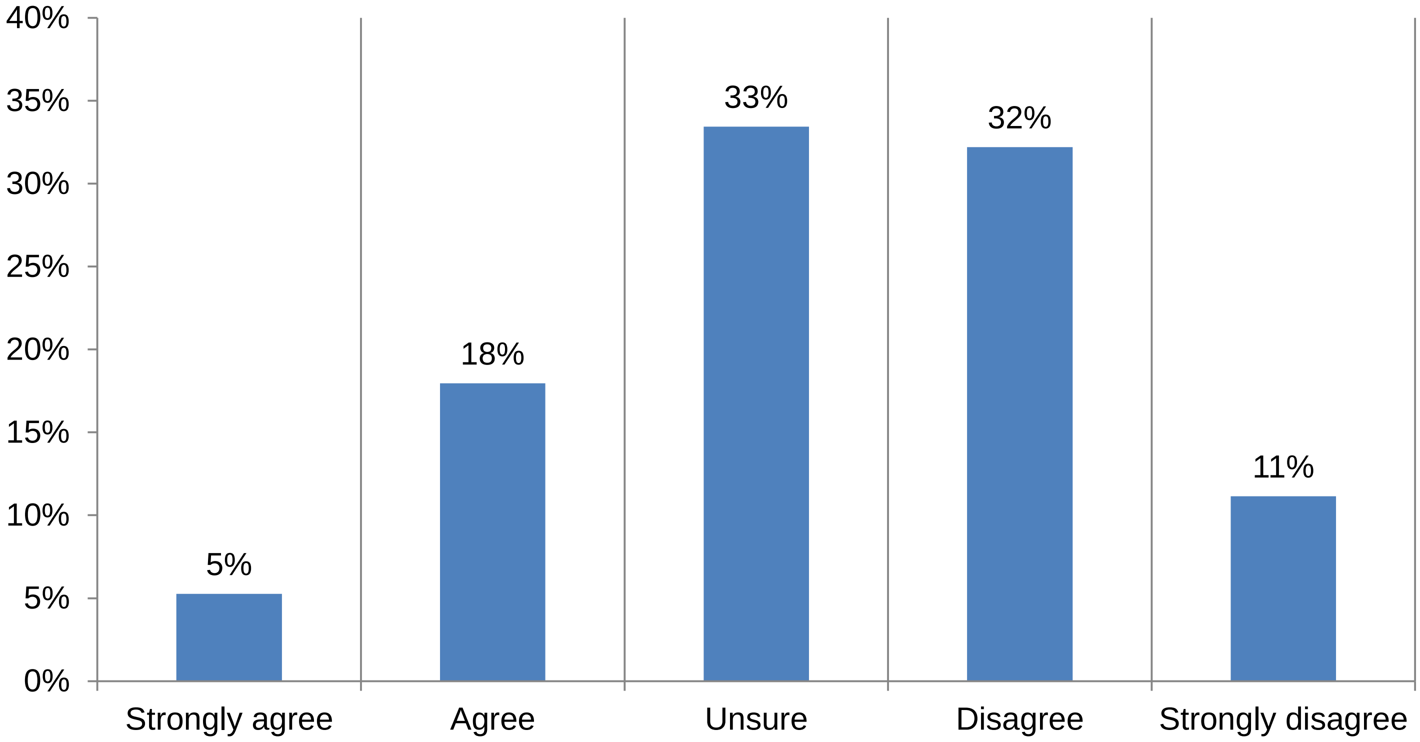


Buckley Sandler LLP

2013 - Ponemon Institute/RMCS LLP Metrics Study

Metrics – Conduct Risk

- Privacy preference/sensitivity is evaluated in ways similar to those of other customer and consumer behavior attributes and is used for marketing and product management:



2013 - Ponemon Institute/RMCS LLP Metrics Study

To Summarize

- The definition of data risk is evolving and will continue to evolve
- A data risk management program must establish goals within the context of the enterprise, the market and the legal and regulatory environment in which it operates
- Metrics should measure the impact of risk mitigation program strategies, controls, activities, and initiatives on achieving the goals and objectives of the program
- The determination of “effectiveness” varies by stakeholder and may affect the number and types of metrics used to determine the state of the program
- Measures and metrics should provide useful and actionable information and form the basis of the “change management” process in the risk program system

Practical Steps

- Create Cybersecurity/Privacy program goals that align and support corporate strategies and goals
- Create metrics that answer questions such as: “Do we have a culture of privacy?” “Are we compliant with ________?”
- Design measurements with identified thresholds, baselines, POA, PODs, benchmarks to provide context for evaluating results
- Track the impact of investments, actions, initiatives on established metrics. (*e.g.*, trend analysis)
- Evaluate data risk mitigation programs using a maturity model – merely “fixing defects” does not move program forward.
- Start with something – no matter how ad hoc – track from ad hoc to formal to validated. Build on demonstrated success.
- Provide metrics relevant to the view of effectiveness held by stakeholder
- Create vision, goal, objectives and a plan to achieve it – your customers, leaders and regulators expect it.

Speakers

Margo H.K. Tank
Partner
BuckleySandler LLP
1250 24th Street NW, Suite 700
Washington, DC 20037
202.349.8050
mtank@buckleysandler.com

Rena Mears
Managing Director
Privacy, Cyber Risk &
Data Security Group
BuckleySandler LLP
1250 24th Street NW, Suite 700
Washington, DC 20037
202.349.7977
rmears@buckleysandler.com

Al Silipigni
Senior Vice President,
Head of Conduct Risk &
Chief Privacy Officer
HSBC Bank USA
10 East 40th Street
New York, NY 10016
212.525.4595
al.r.silipigni@us.hsbc.com