Are We Ready to Comply with Data Privacy requirements?

James Fong
RSA Archer Solution Leader
Asia Pacific & Japan
Who is affected?

Anyone processing personal data!

Personal data refers to data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access. Singapore Personal Data Protection Act 2012 (PDPA)
Current State of Security

70% Compromised in the last year¹
66% Growth in incidents YoY²
56% Unlikely to detect an attack³
90% Are unsatisfied with response speed⁴
80% CISOs re-thinking strategy in next 12-18 months⁵

¹ RSA Cybersecurity Poverty Index 2016
² PWC Global State of Information Security Survey 2015
³ EY Global Information Security Survey 2015
⁴ RSA Threat Detection Effectiveness Survey 2016
⁵ RSA Estimate
Breach Readiness

- Lack capability to gather data across their estate and provide centralized alerting (55%)
- Do not have an active vulnerability management program in place (40%)
- Do not have a formal incident response plan in place (30%)

RSA Threat Detection Effectiveness Survey
Prevention vs Detection And Response

By 2020, 60% of security budgets will be allocated to rapid detection and response. Up from less than 20% in 2015.

Source: Gartner “Shift Cybersecurity Investment to Detection” 2016

Less than 5% of organisations even knew the split of investment between prevention, detection and response.
Why Does this Gap Exist?

Multiple disconnected point solutions

Alert fatigue

Lack of context & ability to prioritize
Rapid Response is Everything

The longer they are in, the higher the risk
New Requirements

- Full Visibility
- Rapid Insight
- Business Context
- Efficient, Comprehensive Response
- Aligned to Business Priorities
We believe the velocity and magnitude of compliance obligations and associated efforts distracts companies from their core business objectives.

Does this apply to us?

How do these obligations need to be met?

When do we have to comply?

Don't we have these controls in place already?

Which part of the businesses is responsible?

What if these change again soon?
A New Compliance World

We must focus on business priority, the flow of incoming regulatory obligations and automation to stay on top of the pressing regulatory environment
GAP OF GRIEF

The **Technology** perspective...

- What is the important data?
- Where is the important data?
- What are the most critical applications?
- How important is this part of the infrastructure?
- What does this security event impact?
- Where are we vulnerable?
- Who are the 3rd parties the business rely on?
- What happens if IT services are disrupted?

The **Business** perspective...

- What part of the business strategy is the most critical?
- Where are our biggest risk areas?
- What is our risk appetite and tolerance?
- What are our regulatory obligations?
- What are the most valuable pieces of our business that needs to be protected?
- How bad could it be?
- Are we effectively managing our privacy risks to achieve our objectives?
The **Wedges** in the gap...

- Outdated reporting
- Manual processes
- Lack of ownership
- Information silos
- Inconsistent controls
- Limited risk visibility
...lead to **Risk** in the business

- Inaccurate insights & misinformation
- High costs & inefficiency
- Unresolved issues
- Disconnected data & lack of context
- Holes & gaps
- Poor business decisions & missed opportunities

**Resource Constraints**

**ROI**
WHAT’S NEEDED TO CLOSE THE GAP?
Where do you start?

- Understand what personal data you process
- Where is it and how is it used
- User should always be first
- Privacy at every level
- Mitigation plan
- Risk Management review
- Incident detection and response planning
Who is Responsible for Privacy?

- Privacy combines elements of Security, Compliance, and broader Data Risk Management considerations.
- Each respective area, function, and process has a role in ensuring that sensitive corporate information is appropriately protected.
Inspire everyone to own Risk
Components
Privacy Management Program

- Governance model,
- Audits & Review,
- Education,
- Process & practices,
- Policies

- Data Inventory
- Self-Assessments & Compliance Posture

- Response & Complaints Mgt Process
- Data Access Request Handling Process
- Communications Governance

- Information Security Practices
- Policies
- Legal – contracts, indemnities, agreements
WHAT WE NEED
BUSINESS DRIVEN MODEL FOR READINESS, RESPONSE & RESILIENCE

Visibility

Single UI
Incident Management & Reporting

Controls

- A/V
- IDS/IPS
- Firewall/VPN
- Proxy
- DLP
- Packets
- Host
- File

- SIEM Log Alerts
- DLP Alerts
- Signature less Alerts

Context

- Business Context
- Risk Context
- Threat Context

- Line of Business Owner Policy
- Assessments Criticality Vulnerability
- Subscriptions Community Open Source

Data
Warehouse & IT Ticketing

IT Team

Security
Architecture Team

Device
Administration

Workflow & Automation,
Rules, Alerts & Reports

Level 1 Triage

Level 2 Triage

Level 3 Triage

Threat Triage

Threat Intelligence

Expertise

Content Intelligence

Analytic Intelligence
A Strategy to manage Data Privacy

- Manage your Policy on the processes needed internally to comply
- Provide business and IT context to those processes
- Provide a central repository for Privacy regulations and remediation activities
- Automate the process of PIA and DPIA assessments and data breach reporting to regulators
A Strategy to manage Data Privacy

Define & enforce risk ownership through Accountability

Cross business lines & organizational boundaries for Collaboration

Consolidate data and enable risk Analytics & Visibility

Automate processes for Efficiencies
THE PROVEN PATH TO TAKE COMMAND OF RISK
A GRC Strategy to manage Data Privacy

3 Lines of Defence Model
A GRC Strategy to manage Data Privacy

- Compliance
  - Policy Management
  - Controls Assurance

- Risk Management
  - Catalog of Sensitive Information Assets and related devices
  - Business Hierarchy
  - Risk Assessments and Reporting

- Organization Specific tailoring
  - Data Breach process
  - Handling of Data Subject Rights processes

- Third Party Governance
  - Risk Based vendor Management
  - 3rd Party Compliance monitoring

- Issues Management
  - Handling of Findings and Exceptions
  - Remediation planning
  - Escalation Workflow

- Audit
  - Audit Program

- Risk Based Risk Management
- Third Party Compliance monitoring
- Escalation Workflow
CyberRisk Noise...

Is this an issue affecting a high risk business function?

Do we have a compliance issue?

How does this new vulnerability affect us?

What are the executive concerns?

Is this a coordinated advanced attack?

Is this an inappropriate attempt to access top secret information?
Third Party Noise...

Who are all of the third parties that support our business?

Which of our 3rd party relationships pose the most risk?

Should we be doing business with this new third party?

Are all of our third parties performing up to the levels we expect?

Do we have the needed contingency plans in place around third party risks?

Are the third parties we do business with compliant with laws and regulations?
The Journey to Advantaged GRC

As organizations mature their approach to GRC, they transition from a structure of siloed departments and units to a fully engaged business operation where everyone has a part in managing risk, ensuring compliance and contributing to performance outcomes. This leads to greater confidence, agility and resilience - advantages that ensure success.

**Siloed GRC**
- Focus on compliance
- Reporting is disconnected
- Processes are isolated

**Managed GRC**
- Focus is on risk
- Reporting is coordinated
- Processes are defined

**Advantaged GRC**
- Focus is on business opportunity
- Reporting is enterprise-wide
- Processes are optimized

---

**Compliance**

- We need to set up a comprehensive policy and training framework to address this risk.
- This compliance report says our incident data is not being reported properly.

**Risk**

- We've added key managers to focus on the top risks, but they don't report on common threads.
- At least everyone is using the same risk assessment methodology now.

**Operations**

- We've highlighted the top risks and incidents for IoT.
- These reports set us up to be alert for operational risks.

**Audit**

- It's easier to complete our audits with the new standardized testing methods.
- It helps that all the units are using the same methodology now.

**Business Benefits**

- Regulatory Change
  - Identified Opportunities
- Operational Change
  - Identified Opportunities
- Business Benefits

---

**Transitional**

- Focusing on repeatable processes

**Transforming**

- Focusing on business operations

---

**Developed by**: OCEG

**With contributions from**: RSA
Take **Command** of your journey

**Siloed**
Streamline compliance, build business context & reporting

**Managed**
Expand risk focus, Improve analysis & metrics

**Advantaged**
Connect risk and the business with cross functional processes

---

**Meet**
compliance obligations

**Manage**
known & unknown risks

**Make**
risk-based decisions

---

**Compliance**

**Risk**

**Opportunity**
Thank You

James Fong
Solution Leader | RSA Archer | Governance, Risk & Compliance
Asia Pacific & Japan

james.fong@rsa.com
M (65) 8533 1395

www.rsa.com
Questions?