Data Protection, Privacy and Cybersecurity

ISACA
North America CACS
Orlando, Florida
16-18 March, 2015
## Agenda

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warning signs</td>
<td>3</td>
</tr>
<tr>
<td>A matter of trust</td>
<td>5</td>
</tr>
<tr>
<td>How we got here</td>
<td>7</td>
</tr>
<tr>
<td>Security</td>
<td>11</td>
</tr>
<tr>
<td>Data protection</td>
<td>13</td>
</tr>
<tr>
<td>Privacy</td>
<td>18</td>
</tr>
<tr>
<td>A recipe for success</td>
<td>27</td>
</tr>
<tr>
<td>Make data protection, privacy, and cybersecurity an essential part of the mission</td>
<td>30</td>
</tr>
<tr>
<td>Employ experts for reliable advice</td>
<td>33</td>
</tr>
<tr>
<td>Adopt a nomenclature and frameworks for context and conditions</td>
<td>35</td>
</tr>
<tr>
<td>Adopt an appropriate risk management model</td>
<td>42</td>
</tr>
<tr>
<td>Build and maintain trust by design</td>
<td>47</td>
</tr>
<tr>
<td>Leverage balanced scorecards</td>
<td>49</td>
</tr>
</tbody>
</table>
Warning signs
Data protection, privacy, and cybersecurity warning signs...

- The Board is unaware or not involved
- Legitimacy of data handling is unknown
- Nobody knows where data is
- Data protection, privacy and cybersecurity compliance requirements are unknown
- Data protection, privacy and cybersecurity risks are not considered when setting business objectives
- Data protection, privacy and cybersecurity are not included in the development life cycle of business processes and systems
- DPO, CPO and CISO are asked to demonstrate ROI
- There are disconnects between policies and operations
- Operations leads risk management
- There are negative findings and penalties
- There are security incidents and privacy breaches
- Stakeholder trust in the organization is weakening
A matter of trust
Trust is the foundation for faceless transactions

**SPEED OF CHANGE**
Businesses are forced to embark on innovative change programs to exploit new technologies.

**MOBILE**
Smartphones offer new opportunities for businesses. Mobile payments will underpin the digital economy. Trust is essential for users to feel safe using it.

**SOCIAL MEDIA**
Businesses can understand and interact with patients in new ways and can leverage social media to build knowledge.

**HYPER-CONNECTIVITY**
Businesses operate in a dynamic environment that is increasingly interconnected and inter-dependent and built around a model of open collaboration and trust.

**DIGITAL IDENTITY**
Identity and security: The next wave of digital innovation relies on knowing who you are dealing with. Protecting systems and information is even more critical.

**CLOUD**
Cloud services break down the concept of a defined physical location and introduce an internet of applications. We will be trusting cloud providers with much more.

**ANALYTICS**
Big Data presents huge opportunity for new business insights – but organizations will need to trust the information that drives their decisions.

It takes years to build, a moment to break, forever to repair, and the need for it increases every day.

When business makes data protection, privacy, and cybersecurity afterthoughts, the entity can unknowingly assume risks to information and IT, face civil and criminal penalties, and lose the trust of customer, investors, and regulators.
How we got here
Technological Advances

Interconnectivity, open-network architectures, and an ever increasing reliance on innovative (and vulnerable) technologies, expose a growing pool of confidential information and personal and sensitive data to threats jeopardizing data subject privacy as well as economic and national security.

The Industrial Age

The Information Age

Data Protection, Privacy & Cybersecurity

PwC

HIPAA of 1996

March 2015

7

8
The world’s strongest military and largest economy are mutually dependent and increasingly reliant on cyber-based information systems. **Identify your assets and undertake to protect them.** *(President Bill Clinton, May 22, 1998)*

For illustrations capturing the largest data breaches, visit: [http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/](http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/)
Don’t become a statistic

- **97% of breaches were avoidable** if simple or intermediate controls were in place (2012 Verizon Data Breach Investigation Report)

- The average cost of a compromised record is **$145** (2014 Ponemon Cost of Data Breach Study)

- The average cost to an organization of a data breach is **$5.85M** (2014 Ponemon Cost of Data Breach Study)

- Average lost business cost following a breach is **$3.3M** (2014 Ponemon Cost of Data Breach Study)

- Financial motives are still the highest motivations, but espionage is rapidly increasing up 25% in 4 years (2014 Verizon Data Breach Investigation Report)

- Most CISOs report only receiving about **50%** of the resources they need (2014 Ponemon Cost of Data Breach Study)

- Abuse of privileges accounts for **88%** of insider misuse, while embezzlement accounts for **4%** (2014 Verizon Data Breach Investigation Report)

Variety of data-at-risk within Insider Misuse:

- **Personal data 34%**
- Payment data 29%
- Internal data 27%
- Secret data 18%
- Bank data 14%
- Credential data 9%
- Medical data 3%
- Other 3%
- Unknown 2%
- Classified 1%

Actor Motives:

- 72% Financial
- 18% Espionage
- 10% Grudge
- 4% Convenience
- 3% Fun
- 2% N/A

(2014 Verizon Data Breach Investigation Report)
Security
For all assets, security is a combination of administrative, operational, and technical safeguards that work together to help ensure:

- Confidentiality
- Integrity
- Availability
Data protection
Data has value

- Financial data
- Business strategy data
- R & D data
- Intellectual property
- Customer data
- Vendor data
- HR, payroll, benefits, healthcare and other employee data
- Shareholder data
To preserve value, data must be protected

Data protection is the safeguarding of data from unauthorized access (use), alteration or destruction
Does security equal data protection?

- Many believe that security is data protection, delegating responsibilities to a CISO. However, it is not that simple.
- Security satisfies many of the requirements essential to data protection, but not all.
- The distinction between security and data protection is most apparent when the data possessed or controlled include elements of personal and sensitive data.
Privacy includes the treatment of personal and sensitive data

**Personal data:** any information relating to an identified or identifiable *natural person*; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his identity

*(Article 2(a), Data Protection Directive)*

**Sensitive data:** personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life

*(Article 8, Data Protection Directive)*

Data concerning customers, shareholders, vendors, and employees include elements of personal and sensitive data
Privacy is the appropriate use of personal and sensitive data under the circumstances. What is appropriate will depend on the context, law, and the data subject’s expectations; also, the right of the data subject to control collection, use and disclosure of PII. (IAPP)

- **Information Privacy extends beyond information security** to consider the entire lifecycle of personal and sensitive data
- **There can be no (data protection) privacy without security**
- Security alone does not provide for the privacy of personal and sensitive data
Privacy

Generally Accepted Privacy Principles (GAPP)

The entity’s tolerance for risks for its infrastructure, confidential information, and personal and sensitive data drives the adoption of policy, architecture strategy, configuration management, acquisition, design, and the selection of safeguards.
**Security does not equal data protection**

### Security Addresses
- Inventory (IT)
- Identity & Access Management
- Authentication
- Configuration Management
- Device and Media Controls
- Integrity
- Logging and Monitoring
- Redundancy
- Incident Response
- Recovery

### Security Does Not Address
- Inventory of Personal Sensitive Data
- Legitimacy of Data Collection, Use, Disclosure, Retention, and Disposal
- Notice
- Consent/Authorization
- Data Subject Participation
- Quality of Data
- Onward Transfer
- Breach Response
Regional Perspectives

EU Member States: EU Directive requires
- Omnibus legislation
- Mandatory baselines

Member States are free to enact laws that are more stringent than the baseline

U.S.: A patchwork of national and state laws:
- Typically industry-focused or jurisdiction-specific
- Focus on limited data collectors uses and disclosures

Latin American Nations: Follow principles similar to EU Member States:
- Uruguay and Argentina most mature ("adequate")
- Other nations are developing frameworks

“Adequate” Nations: EU commission determination that a nation's laws provide laws “adequate” protection of personal data

Middle East: Inconsistent approaches
- Israel most mature ("adequate")
- Other nations are developing frameworks

APEC Nations: 21 member economies instituting the APEC Privacy Framework:
- Nine privacy principles in a
- Business code of conduct
- Third-party certification to demonstrate compliance
**EU Member States and the European Economic Area:** Consistently define personal and sensitive information and handling with limited variations across jurisdictions and industries

**Right to Be Forgotten:** A new framework allowing citizens the “right to be forgotten” and additional requirements for express consent, enhanced policies, and increased enforcement

**Snowden Disclosures:** Created a sense of uncertainty surrounding Safe Harbor with Germany threatening suspension of the framework

**EU Safe Harbor Reform:** With 11 of 13 recommendations having been agreed, discussions continue about US law enforcement access to personal data and the publishing of commercial contracts and policies. After the Snowden disclosures, agreement was reached on reforms dealing with transparency, redress, and enforcement

**Means of Transferring Data:** A push to use Model Clauses in light of the Article 29 Working Party document in 2014 on a cooperation procedure for DPAs to use for authorizing international data transfers.

- The 2010 changes added express language regarding sub-processors and the requirement for prior written consent of the controller before subcontracting any processing obligations
**Trends – Asia-Pacific**

- **APEC Nations:** Focuses on legitimacy of collection practices and a “do no harm” approach; however, whether by coincidence or by design, the region is in some ways **trending toward a EU-type of approach**

- **Hong Kong:** Perceived erosion of autonomy and interference from China created **poor optics for Hong Kong for international data transfer**

- **India:** A data handling law addresses security practices and procedures for personal and sensitive data and information, but India **wants to become an EU “adequate” jurisdiction**

- **Australia:** The Privacy Amendment Act of 2012 overhauled existing data privacy laws and **incorporates privacy principles which have increased burden on entities handling personal information**

- **Singapore:** The Personal Data Protection Act 2012 established a baseline privacy framework and is now **issuing sector-specific guidelines and promulgating regulations**
Trends – Latin America

• **Brazil:** The new *Internet Law places privacy restrictions on online companies* hosting user-generated content that do business in Brazil or collect information online from Brazilian consumers.

• **Chile:** A new *data protection authority might be created* to enhance enforcement and to develop a framework that is more consistent with the region and with the EU.

• **Costa Rica & Peru:** *Each has omnibus data privacy legislation in place similar to the EU* data protecting regime with trends to enhance regional alignment.

• **Mexico:** Surveillance concerns in Mexico are worrying privacy advocates who fear the *new telecom law might allow law enforcement to monitor calls and text messages without warrants*.
Trends – United States

- **No Constitutional Right:** No movement for a Constitutional right to privacy

- **No Omnibus Privacy Legislation:** No progress toward an omnibus privacy law

- **Personal and Sensitive Data Not Defined:** No movement to define personal and sensitive data in a consistent manner

- **The Patriot Act and Intelligence Agency Surveillance:** Surveillance laws were recently reauthorized and funded by Congress and there is no movement to restrict law enforcement or intelligence agencies from accessing business records of companies to obtain customer data. The FTC fined companies for failures of transparency for not revealing information sharing arrangements with law enforcement and intelligence agencies in privacy notices.

- **Non-Centralized Enforcement:** No move to consolidate enforcement agencies and mechanisms, depending on sector and industry – HHS, FTC, State Attorneys General, etc.
A recipe for success
**Improve privacy and security risk posture**

1. Set the tone at the top by *making data protection, privacy and cybersecurity an essential part of the mission statement*

2. Know your programs strengths and weaknesses as well as leading safeguards by *employing experts for reliable advice*

3. Provide essential context by *adopting a nomenclature and framework for context and conditions*

4. Assure informed, risk-based decision making by *adopting an appropriate risk management model*

5. Make sure that processes and systems do not exceed the entity’s tolerance for risk by *building and maintaining trust by design*

6. Make sure your policies, procedures, and safeguards are effective and efficient by *employing balanced scorecards*
Making data protection, privacy and cybersecurity an essential part of the mission statement
Data protection, privacy, and cybersecurity are board-level issues that impact...

- Adoption of new technologies
- Setting of Business Objectives
- National & Economic Security
- Organizational Changes
- Risk and Reputation
- Regulatory Compliance
Characteristics mature organizations

Set the tone at the top!

- **Engage the board**
  - Brief on privacy, data protection, and cybersecurity risks
  - Timely respond to inquiries regarding risk posture
- **Include privacy, data protection, and cybersecurity in the mission statement**
- **Establish business objectives that can be achieved within an executive-defined risk tolerance**
Employ experts for data protection, privacy and cybersecurity
Expertise is essential

Privacy and security are nuanced and require educated experts to make sure they receive appropriate attention

- Privacy officials should be
  - **Certified Information Privacy Professionals** (CIPP)
  - Capable of understanding nuanced laws as well as how data and technology intersect in business processes
    - Certified in the Governance of Enterprise Information Technology (CGEIT)
  - Communicators, able to interface with executives, management, and operations

- Security officials should be
  - **Certified Information Systems Security Professional** (CISSP)
  - Capable of understanding nuanced laws as well as how data and technology intersect in business process
    - Certified in the Governance of Enterprise Information Technology (CGEIT)
  - Communicators, able to interface with executives, management, and operations
Adopt a nomenclature and framework for context and conditions
Enable Meaningful Communication

Employ a common nomenclature for data protection, privacy and cybersecurity

- Sector-neutral
- Industry-neutral
- Jurisdiction-neutral

Educate relevant stakeholders about defined terms and phrases

Rely on your defined terms when communicating about data protection, privacy and cybersecurity issues, such as

- Risk assessments
- Risk analyses
- Risk management
- Policies and procedures
- Audit observations and recommendations
- Contract terms and conditions
**Simplify Requirements**

*Leverage frameworks to provide context to data protection, privacy and cybersecurity requirements.* An ideal framework will:

- Leverage your common nomenclature
- Define the lowest level of “what” but does not specify “how”
- Provide awareness about data protection, privacy and cybersecurity concepts
- Facilitate a mapping of requirements

*Frameworks communicate “what” must be addressed. Published standards and controls specify “how”.*
Privacy Frameworks

AICPA
1. Management
2. Notice
3. Choice and Consent
4. Collection
5. Use, Retention, and Disposal
6. Access
7. Disclosures to Third Parties
8. Security for Privacy
9. Quality
10. Monitoring and Enforcement

OECD
1. Collection Limitation
2. Data Quality
3. Purpose Specification
4. Use Limitation
5. Security Safeguards
6. Openness
7. Individual Participation
8. Accountability

EU/Swiss Safe Harbor
1. Notice
2. Choice
3. Onward Transfer
4. Security
5. Data Integrity
6. Access
7. Enforcement

NIST SP 800-53 Appendix J
1. Authority and Purpose
2. Accountability, Audit, and Risk Management
3. Data Quality and Integrity
4. Data Minimization and Retention
5. Individual Participation and Redress
6. Security
7. Transparency
8. Use Limitation
Security Frameworks

Identify your assets and protect them
Assets are people, places, and things
• Your employees, vendors, facilities, information, IT
Assess, analyze, manage, mitigate, and monitor risk to your assets
• Limit access
  - Unique user identifiers, limiting access privileges, means of authenticating authorized users, encrypting data at rest
• Assure integrity
  - For example: Encrypting data at rest and in transmission
• Assure availability
  - Backup data, have alternative means of processing data
• Safeguard the environment
  - Fire, floods, hurricane, earthquake...

Safeguard hardware, software, and devices
Be prepared for failure

NIST SP 800-53
Appendix F

1. Access Control
2. Awareness & Training
3. Audit & Accountability
4. Security Assessment & Authorization
5. Configuration Management
6. Contingency Planning
7. Identification & Authentication
8. Incident Response
9. Maintenance
10. Media Protection
11. Physical & Environmental Protection
12. Planning
13. Personnel Security
14. Risk Assessment
15. System & Service Acquisition
16. System & Communication Protection
17. System & Information Integrity
Data protection, privacy and cybersecurity are part of information and IT governance.

ISACA’s COBIT 5 is a body of knowledge furthering information and IT governance.

ISACA will publish a privacy framework and guidance that can be used with COBIT 5.
Adopt an appropriate risk management model
Understand who you are, what you do, and how you do it

Information Lifecycle

Does your organization:

✓ Inventory and classify your data?
✓ Know your high-risk business processes?
✓ Identify the threats and vulnerabilities inherent in the business processes, including the people and technology that perform the process?
✓ Ascertain whether the administrative, physical, and technical controls in place are those that are recommended by published perspectives?
✓ Document risks accepted, including the rationale?

Increasingly, compliance with law requires a governance and risk management process that considers data protection, privacy and cybersecurity.
**EXECUTIVE LEVEL**

- Sets the tone at the top
- Is transparent with stakeholders (and the Board)
- Manages stakeholder risks by establishing risk tolerance and setting strategy
- Demonstrates due diligence in decision making - that decisions are risk-based and informed
- Establishes business objectives that can be achieved within risk tolerance

**NOTE:** The illustration above is derived from the NIST Cybersecurity Strategy and CobIT 5.0, an internationally recognized body of knowledge promoting information & IT governance and risk management.
**Perspectives from NIST, ISO and ISACA**

**SENIOR MANAGER LEVEL**

- Analyzes risks and recommends mitigation
- Understands and communicates potential business impact
- Provides insight into specialized areas
- Translates executive-defined risk tolerance into policies
- Leverages policies to steer development of procedures, prioritize projects, and develop operational strategies for architecture, acquisition, and vendor oversight
- Works with operations to adopt appropriate standards and controls

*NOTE: The illustration above is derived from the NIST Cybersecurity Strategy and COBIT 5.0, an internationally recognized body of knowledge promoting information and IT governance and risk management.*

Data Protection, Privacy & Cybersecurity

PwC

March 2015
OPERATION LEVEL

✓ Includes innovation, implementation, and operations
✓ Are accountable for assessing risk to information and IT
✓ Helps to analyze risk by providing perspectives
✓ Assesses risk, identifying threats and vulnerabilities
✓ Has specialized knowledge, certifications and insight into specific areas
✓ Recommends mitigation techniques, implement safeguards, and monitor the efficiency and effectiveness of mitigation

NOTE: The illustration above is derived from the NIST Cybersecurity Strategy and CobIT 5.0, an internationally recognized body of knowledge promoting information and IT governance and risk management.
Build and maintain trust by design
**Trust by Design**

- **Privacy by Design** is an approach to the engineering of processes and systems that takes privacy into account throughout the entire engineering process
  - **There is no privacy without security**
- Data protection, privacy and cybersecurity are a key components of information and information technology governance
- Business objectives must be met within the executive-defined risk-tolerance for (data protection) privacy and cybersecurity
- The determination of risk tolerances and business objectives must not only include functionality, interoperability, and ease of use but also investments for privacy, confidentiality, integrity, and availability

- **Trust by Design**
  - Assuring mitigation in place and working as intended as part of testing before going live
  - Monitoring the efficiency and effective of mitigation over time
  - Repeating assessments periodically or upon occurrence of a significant event
Employ balanced scorecards
Monitor, measure, and improve

More than key performance measurements, balanced scorecards are a strategic tool that facilitate planning and management of information and IT assets.

Business Strategy
Business Objectives and Risk Tolerance

Perspectives

- Financial
- Customer
- Internal
- Innovation
- Brand

Measurements

- Effectiveness
- Efficiency

Informed Changes

Opportunities for Improvement
Questions
Cybersecurity & Privacy

Frank Cindrich
Director, Cybersecurity & Privacy
Washington Metro
Phone: 571.758.8436
Email: frank.j.cindrich@us.pwc.com