

Mapping the Journey to Effective Data Protection

SECURITY FOR A NEW ERA OF COMPUTING



Cindy Compert, CIPT/M

CTO Data Security & Privacy, IBM Security
cindycompert@us.ibm.com
@CCBigData

June 8, 2016

Notices and Disclaimers

Copyright © 2016 by International Business Machines Corporation (IBM). No part of this document may be reproduced or transmitted in any form without written permission from IBM.

U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IN NO EVENT SHALL IBM BE LIABLE FOR ANY DAMAGE ARISING FROM THE USE OF THIS INFORMATION, INCLUDING BUT NOT LIMITED TO, LOSS OF DATA, BUSINESS INTERRUPTION, LOSS OF PROFIT OR LOSS OF OPPORTUNITY. IBM products and services are warranted according to the terms and conditions of the agreements under which they are provided.

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law

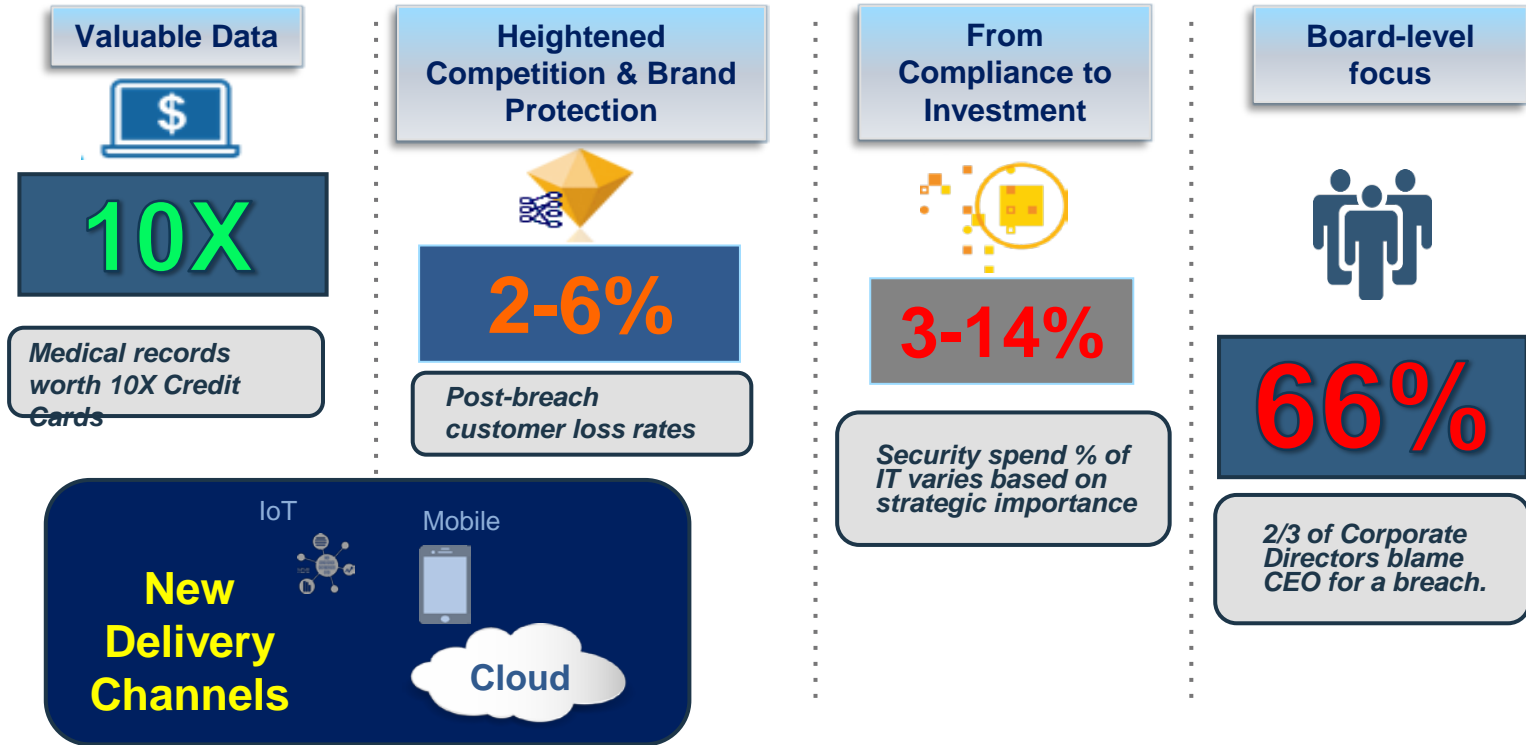
Agenda

- Introduction- Industry trends and challenges
- Best Practices
- What's Next?

Times have changed...



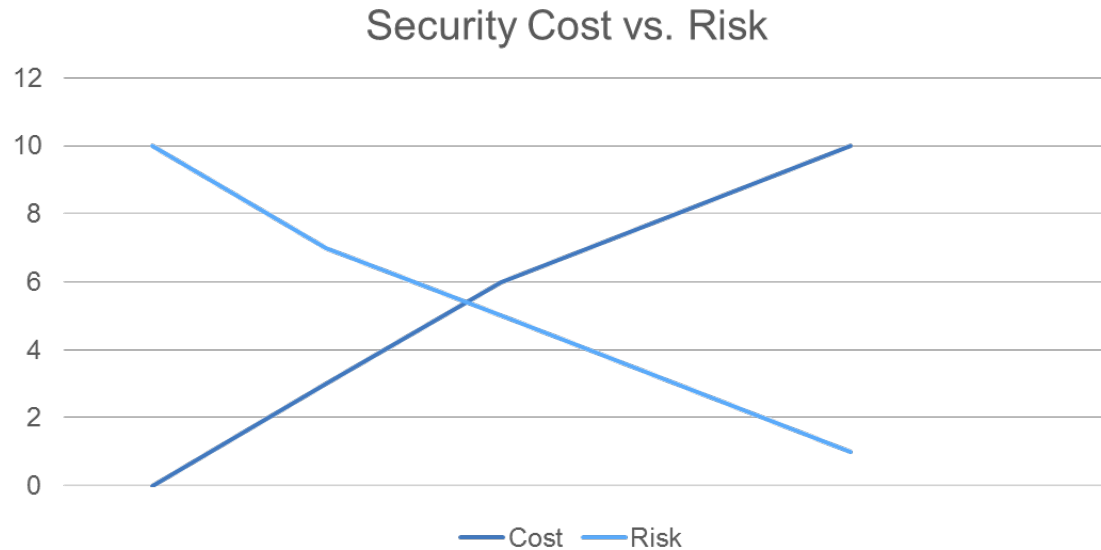
Security & Privacy: Strategic Imperative



It's all Big Data: IoT, Analytics, Cognitive, Cloud



Security Cost/Risk

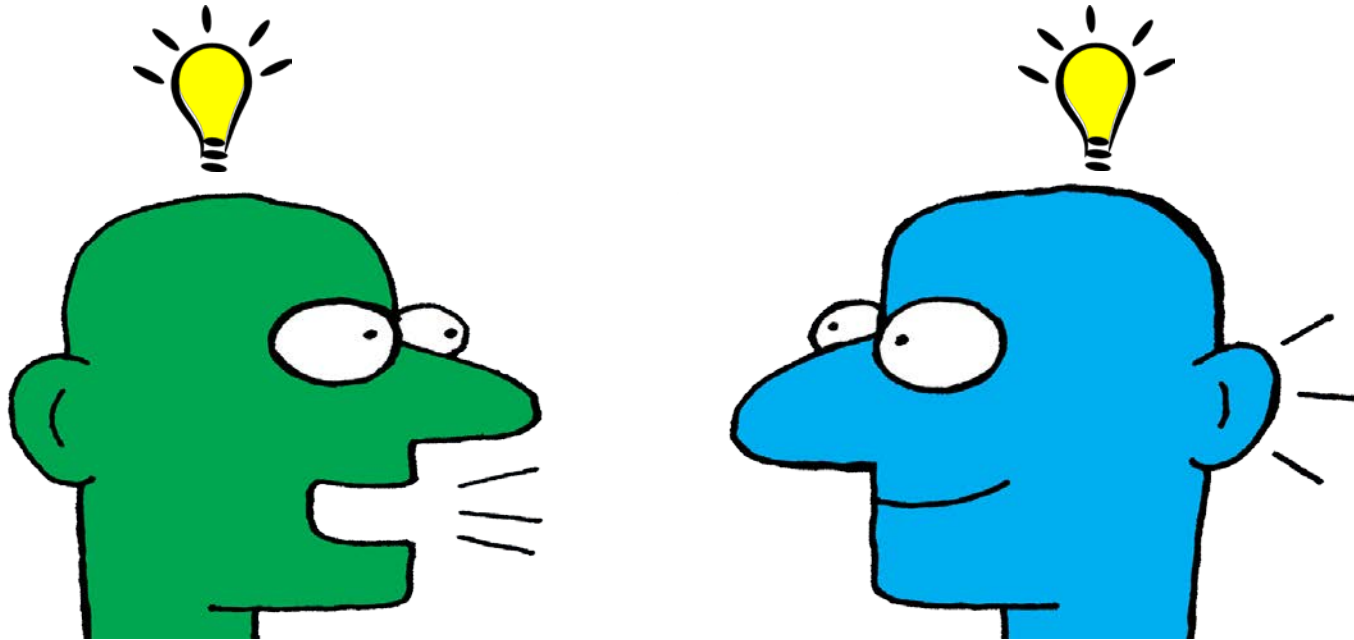




Best Practices



1. Learn the Language



International Association of Privacy Professionals (IAPP) Glossary → <https://iapp.org/resources/glossary>

Two Different Languages

4.7.2

The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

4.7.3

The methods of protection should include

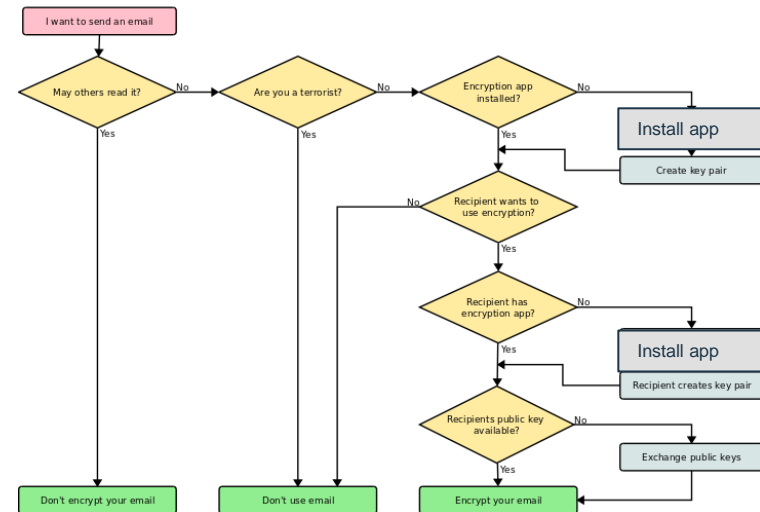
- (a) physical measures, for example, locked filing cabinets and restricted access to offices;
- (b) organizational measures, for example, security clearances and limiting access on a “need-to-know” basis; and
- (c) technological measures, for example, the use of passwords and **encryption**

4.7.4

Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

Sources: <http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf>
<http://dia-installer.de/shapes/Flowchart/index.html.en>

Should I encrypt my email?



2. Be Prepared- Security & Privacy by Design

Privacy Concerns Raised Over Kids' Apps And Websites



PRIVACY AND SECURITY FANATIC

By Ms. Smith | Follow

About

Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

8 in 10 Internet-connected baby monitors receive 'F' grade for security flaws



Credit: Morgan

Researchers revealed 10 new vulnerabilities in baby monitors.

Network World | Sep 2, 2015 3:28 PM PT

Report: Automakers Fail To Protect Connected Cars From Security, Privacy Hacks

By Ashlee Kieler | February 9, 2015



3. Know and Share the Rules



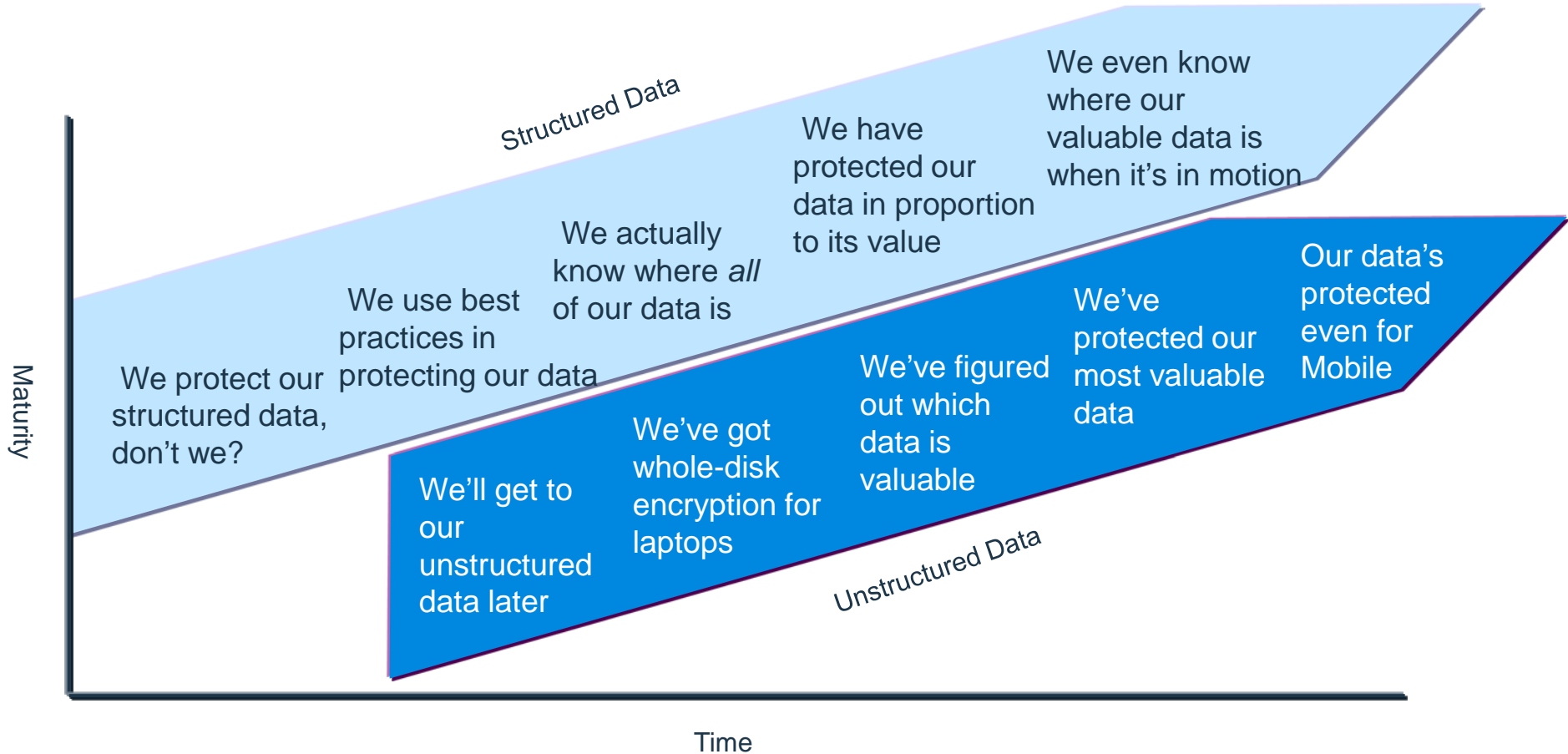
Magnum P. I. I.

Cartoon courtesy of <http://adexchanger.com/>

4. Have a (good) Treasure Map



Data-Centric Maturity Model



Business Risk – Critical data are the “Crown Jewels”



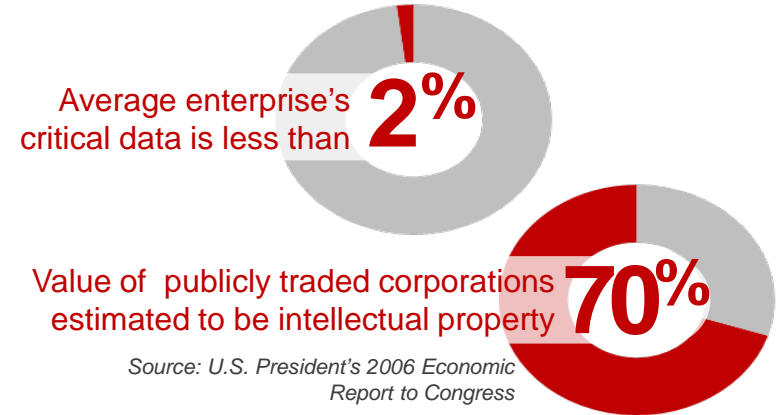
Crown Jewels

An organization’s most sensitive or business critical information.

Today, many organizations are not aware of what their Crown Jewel information is, where it resides, who has access to it, or how it is protected.

Possessing information about Crown Jewels is necessary in order to determine whether adequate controls are in place.

Crown Jewel protection is dependent upon having access to vital information in order to apply proper controls.



Crown Jewel Examples

Enterprise

- Intellectual property
- Top-secret plans and formulas

Executive

- Acquisition and divestiture plans
- Executive and board deliberations

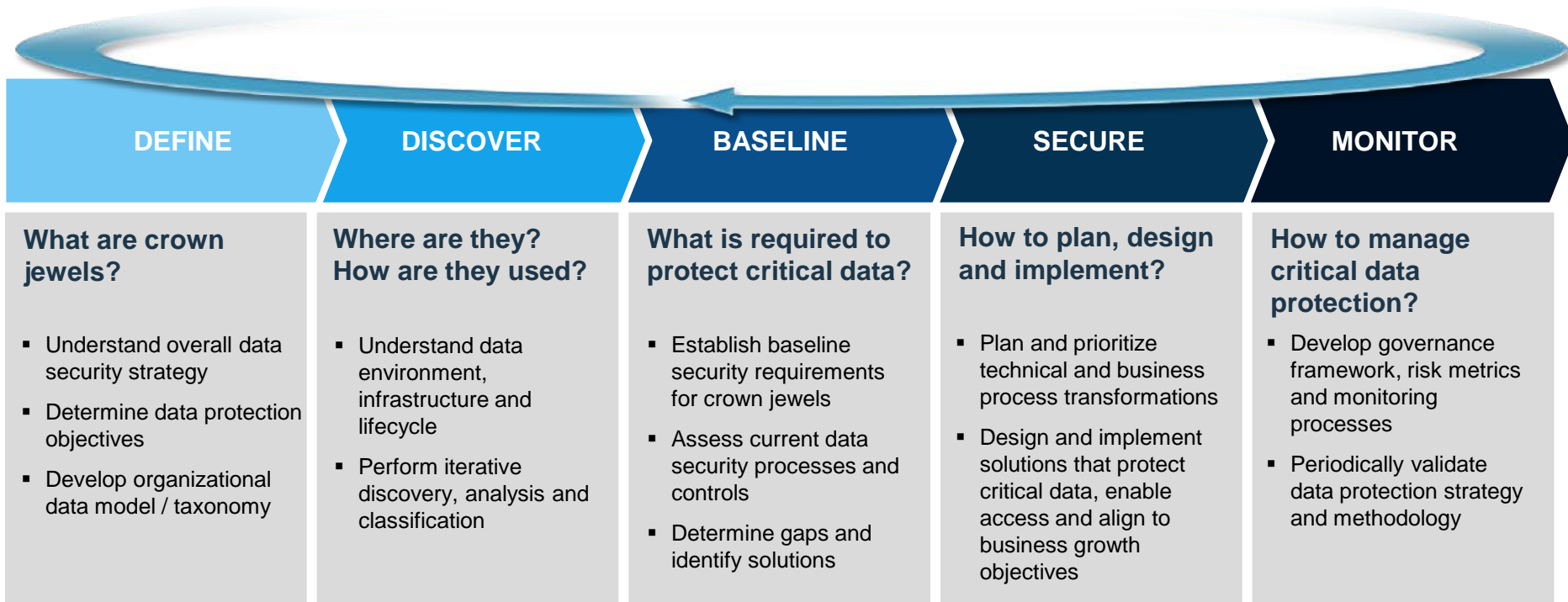
The level of security is determined by the value of data

Data Value	Data type	Security	% of Sensitive Data
	Enterprise Critical	Secure Communication, Separate Network, Backup Security, Physical Isolation, Real-time Response to 100% of Incidents, Insider Monitoring	0.01-0.1%
	Executive	Secure Communication, Separate Network, Backup Security, Physical Isolation, Real-time Response to 100% of Incidents	0.1-2%
	Regulated	Physical Isolation, Real-time Response to "Significant" Incidents, Insider Monitoring, Privacy	1-50%
	Business Strategic	Physical Isolation, Real-time Response to "Significant" Incidents, Insider Monitoring	1-5%
	Business Unit Critical	Near-Real-time Response to "Significant" Incidents, Insider Monitoring	10-20%
	Operational	Best Efforts Response to "Significant" Incidents	20-80%
	Near-Public	Event Response if Available Only	10-80%

CRITICAL DATA
0.01-2.0%

Personally identifiable information (PII), or Sensitive Personal Information (SPI), Health Insurance Portability and Accountability Act (HIPAA); International Traffic in Arms Regulations (ITAR)

5 steps to a Critical Data Protection Program



Supported by:

Consulting Method | Industry-specific Data Models | Global Consulting Expertise | IBM Data Security Research
IBM Guardium, StoredIQ, DLP and other leading data protection technologies

Discover your Crown Jewels: Automate

Create New Discovery Scenario ? 📄

Name and description	✔️ Find PII	Edit 📄
What to discover	✔️ 2 Rules	Edit 📄
Where to search	✔️ 1 Datasource	Edit 📄
Run discovery	✔️ Last Run: 2015-09-08 21:01:10	Edit 📄
Review report	Review report of sensitive objects	Hide 📄

Generation Time: Sep 8, 2015 9:01:10 PM |
 Add to Group |
 Advanced Actions |
 Export |
 Process Log |
 Filter











<input type="checkbox"/>	Catalog	Schema	Table Name	Column Name	Rule Description	C
<input type="checkbox"/>		APEX_040000	WWV_FLOWS	DEFAULT_LABEL_TEMPL	//CREDIT_CARD credit_card_rule_1_09082015055912	
<input type="checkbox"/>		APEX_040000	WWV_FLOWS	GLOBAL_ID	//CREDIT_CARD credit_card_rule_1_09082015055912	
<input type="checkbox"/>		APEX_040000	WWV_FLOW_BUTTON_T	REFERENCE_ID	i://CREDIT_CARD credit_card_rule_1_09082015055912	

Audit	<i>Optional: Define auditors for reviewing and signing discovery results</i>
Schedule	<i>Optional: Define a schedule for the audit process</i>

Sensitive Data Discovery- Files- Example

- FAM Discovery

Start Date: 2015-08-28 00:00:00 | End Date: 2015-09-08 19:45:41 [More](#)

         Export ▾ Actions ▾ 

File ID	File Name	Source Directory Path	File Full Name	Category	Scan Time
3f181d85de179be41d41901a46	Cardiovascular Lab.doc	/GUARD/FAMGUARD	/GUARD/FAMGUARD/ HIPAA /Cardiovascular Lab.doc	PCI	2015-09-01 10:51:24
3f181d85de179be41d41901a46	Cardiovascular Lab.doc	/GUARD/FAMGUARD	/GUARD/FAMGUARD/ HIPAA /Cardiovascular Lab.doc	HIPAA	2015-09-01 10:51:24
f65a11043d16205083378a2c34	CreditRequest.doc	/GUARD/FAMGUARD	/GUARD/FAMGUARD/ HIPAA /CreditRequest.doc	PCI	2015-09-01 10:51:24
f65a11043d16205083378a2c34	CreditRequest.doc	/GUARD/FAMGUARD	/GUARD/FAMGUARD/ HIPAA /CreditRequest.doc	HIPAA	2015-09-01 10:51:24

5. Protect Your Treasure



Organizations Need a Comprehensive Enterprise-wide Approach to Data Security and Compliance

Understand and define sensitive data

Assess vulnerabilities

Monitor database activity

Help protect sensitive data

Manage access

Automate detection of sensitive data and enterprise data relationships

Capabilities:

- ✓ Discover database instances
- ✓ Automate detection of sensitive data in databases
- ✓ Automate responsive actions
- ✓ Discover sensitive data in documents
- ✓ Create a data taxonomy
- ✓ Classify sensitive data

Automate database vulnerability and configuration change detection

Capabilities:

- ✓ Automated vulnerability assessment and remediation suggestions
- ✓ Audit any configuration or security setting changes

Provide essential safeguards to protect high value databases across heterogeneous environments

Capabilities:

- ✓ Continuous, real-time database activity monitoring
- ✓ Comprehensive audit trail
- ✓ Policy-based controls to detect unauthorized or suspicious activity
- ✓ Review and update policies and procedures

Help protect data – in both production & non-production, both structured & unstructured - from unauthorized use

Capabilities:

- ✓ Mask information using realistic values
- ✓ Automate key management process
- ✓ Database encryption
- ✓ Redact data in documents and forms
- ✓ Endpoint and network data loss prevention
- ✓ End user device encryption

Manage and enforce privileges enterprise-wide

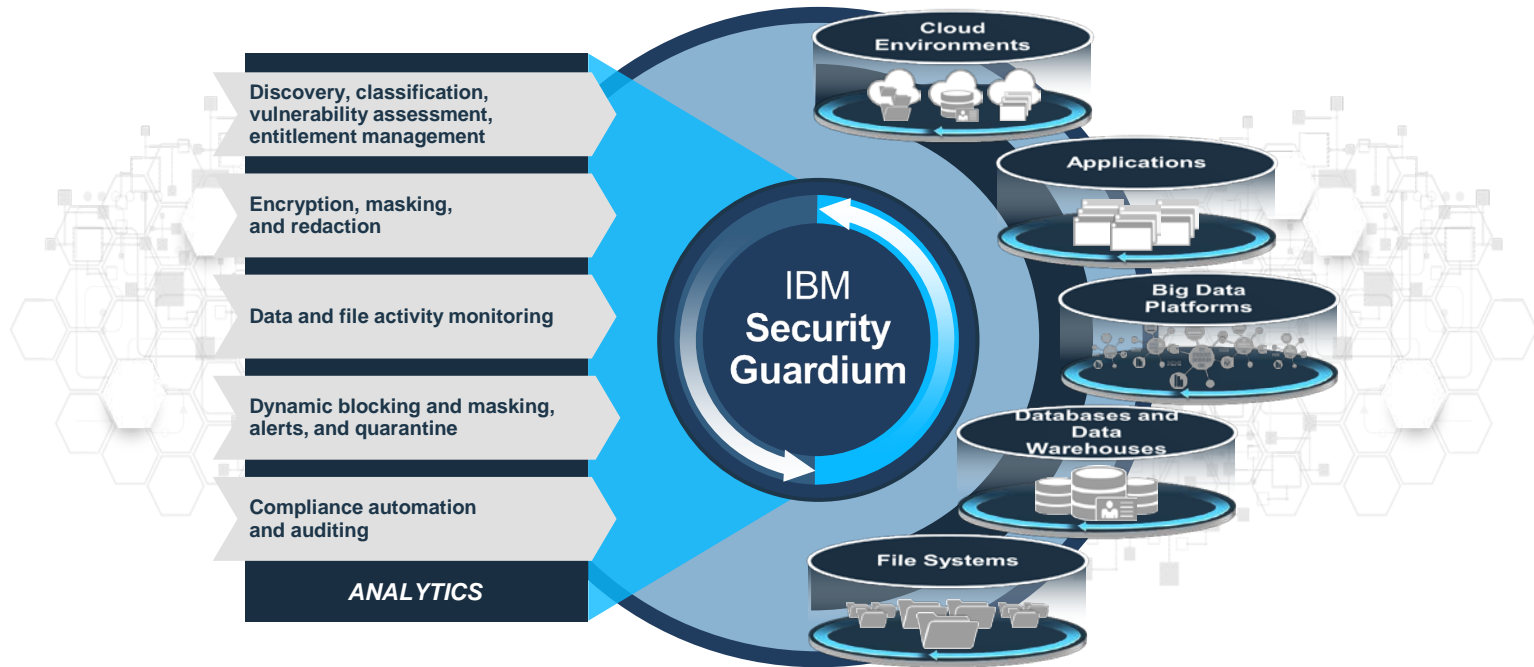
Capabilities:

- ✓ Centralize and automate collection of entitlement information
- ✓ Assess privileges granted directly and indirectly

Create a DBMS Security Reference Architecture and Governance Framework

ANALYZE. PROTECT. ADAPT.

Data Security Controls



6. Hide the **Critical** Parts With Invisible Ink



Data Obfuscation Terminology

Original Value

4536 6382 9896 5200

Masking

- The ability to desensitize sensitive information and make it unreadable from original form while preserving format and referential integrity
- it is a one way algorithm – ie. No unmasking data
- SDM – Static Data Masking
- DDM – Dynamic Data Masking

Masked Value

4212 5454 6565 7780

Redaction

- The process of obscuring part of a text for security purposes.
- The ability to replace real data with substitute characters like (*)

Redacted Value

4536 6382 **** **

Tokenization

- The process of substituting a “token” which can be mapped to the original value
 - Token is a non-sensitive equivalent which has no extrinsic value
 - Must maintain a mapping between the tokens and the original values

Token Value

ABCD GDIC JIJG VXYZ

Encryption

- The process of encoding data in such a way that only authorized individuals can read it by decrypting the encoded data with a key
 - Format Preserving Encryption (FPE) is a special form of encryption

Encrypted Value

1@#43\$%!xy1K2L4P

7. Ensure the Rulers are Informed



Build a Bridge..



Project Execution – Managing Steady State Data Risk (iDNA™)

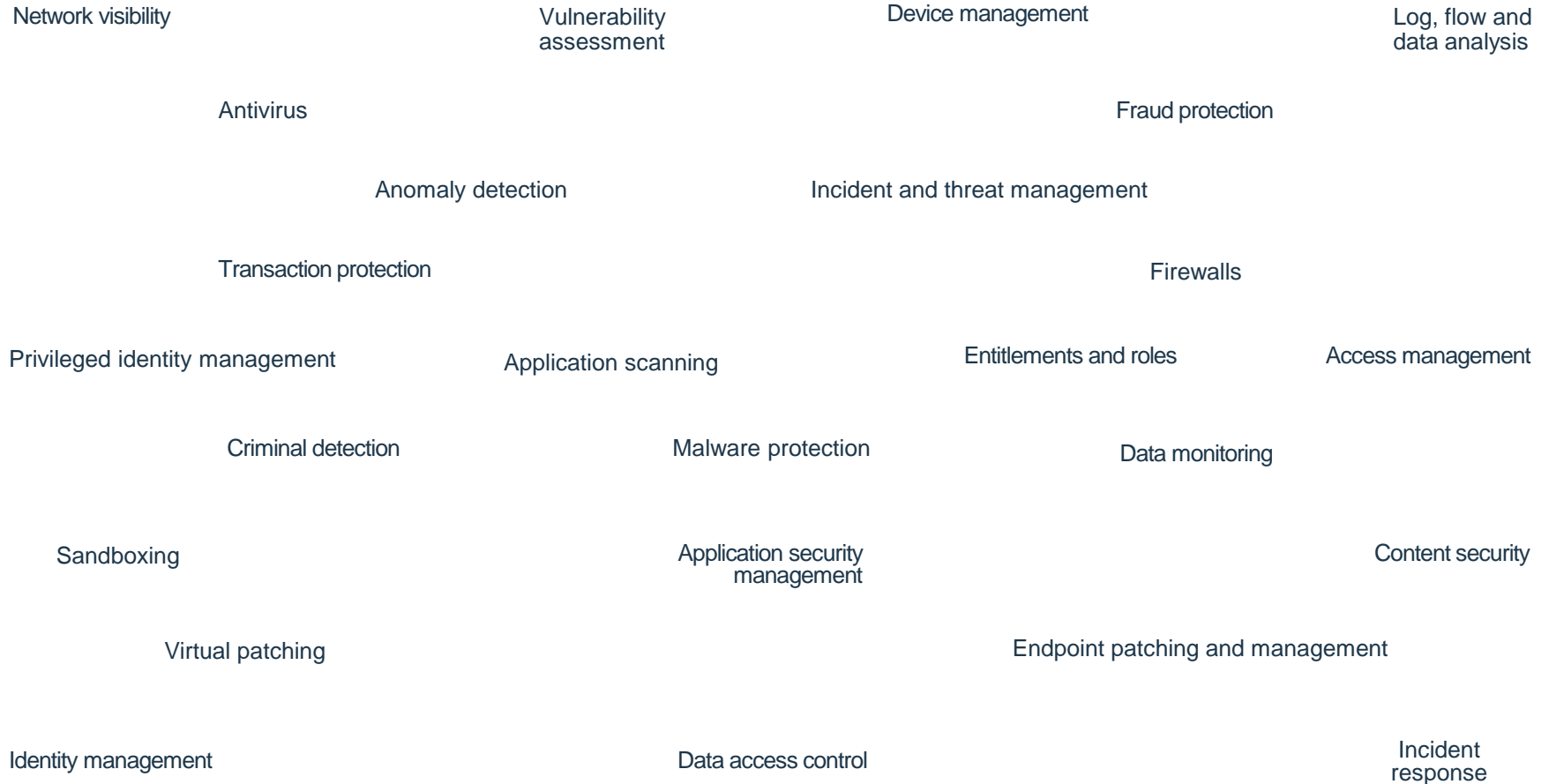
The image shows a screenshot of the iDNA™ dashboard interface, which is used for managing data risk. The dashboard is divided into several sections:

- Top Navigation:** IDNA > LOBs > Corp HQ
- Left Sidebar:** Domains, Lines of Business, IT/CIO, CFO, and a Stakeholder wheel.
- Main Content Area:** A grid of data points categorized by Lines of Business (Organizational, Functional, Client, Informational) and various processes (Program Portfolio, Process Management, Vendor/Partner Management, Patterns & Practices, Budgeting, Accounting, PO processing, Internal/External Communications, Content Policy).
- Right Panel:** Infrastructure overview showing Database (DB2, IBM Connections, Oracle) and Compute resources with associated issues and risk levels.
- Bottom Panel:** Stakeholder & Owner information, Process Asset Inventory, Risk Business, and a Message Board with Alerts and Notes.

Five callout boxes pose the following questions:

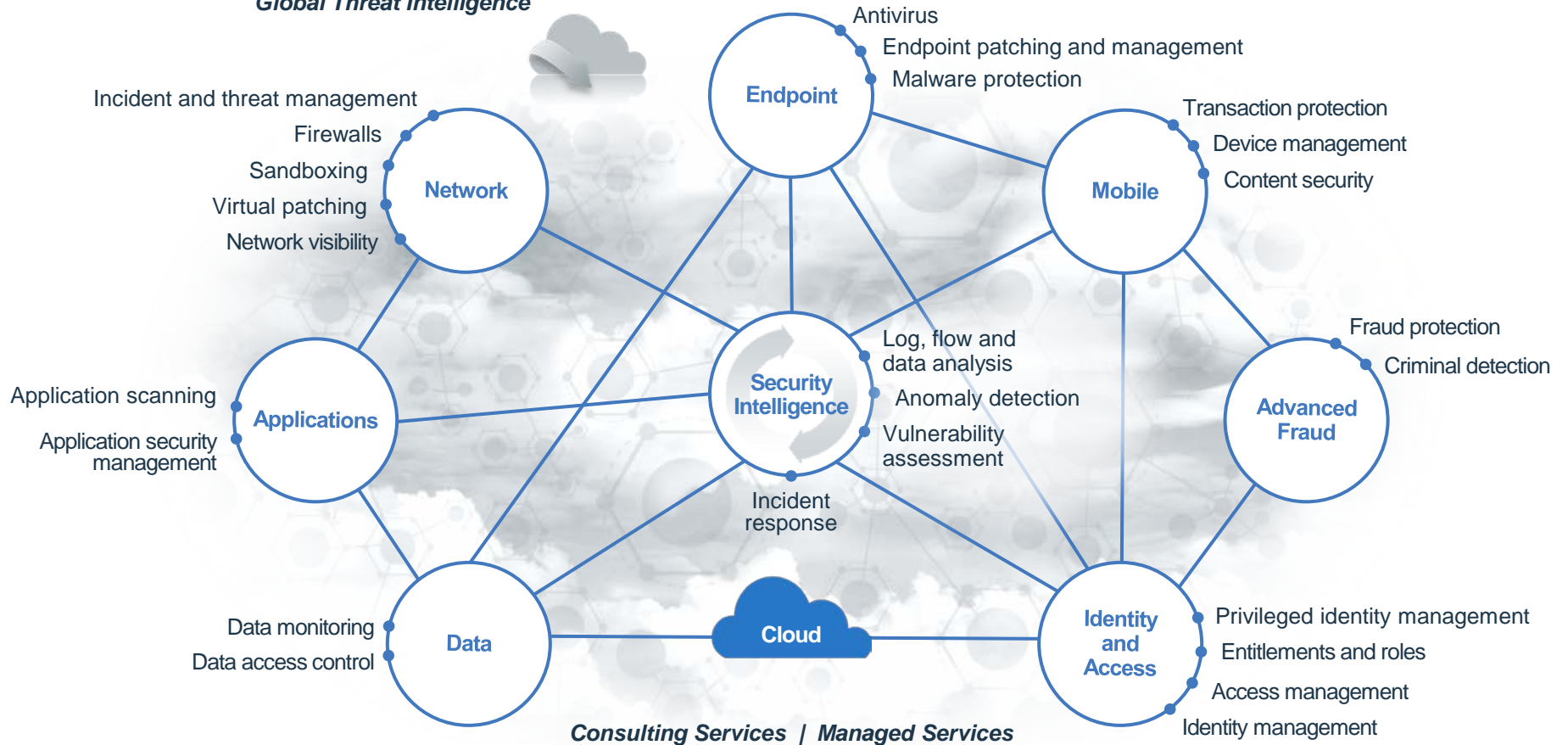
- Which lines of business have the highest risk?** (Points to the Lines of Business section)
- What are our most Sensitive data or "Crown Jewels" and are they safe and protected?** (Points to the Program Portfolio and Process Management tiles)
- Where are our "Crown Jewels"?** (Points to the Infrastructure section)
- What vulnerabilities or compliance issues do we have?** (Points to the Alerts and Notes in the Message Board)
- Who are the data owners?** (Points to the Stakeholder & Owner section)

Establish security as an immune system



Security as an Immune System

Global Threat Intelligence

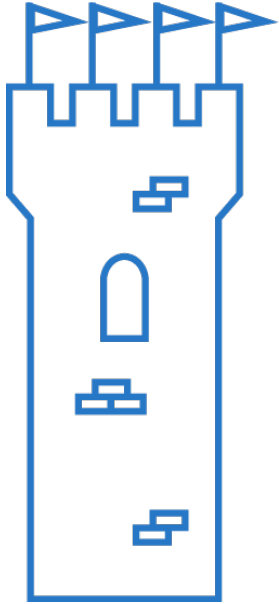




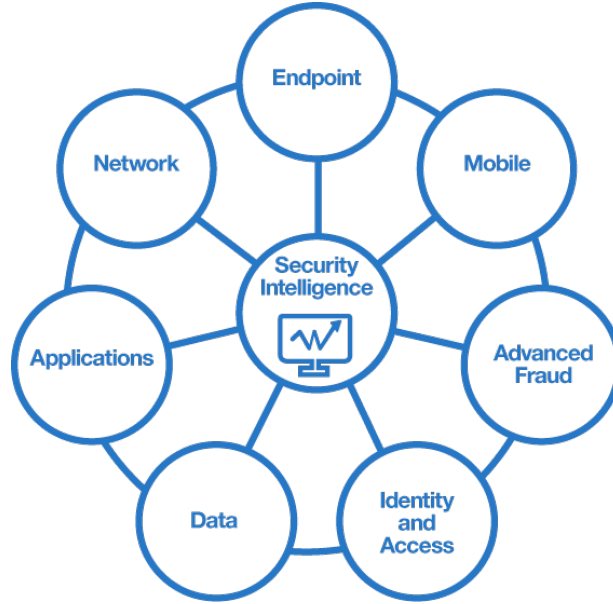
Where Next?



The next era of security



**Moats,
Castles**



**Intelligence,
Integration**



**Cloud, Collaboration,
Cognitive**

Questions to ask yourself






- 1. Where am I most concerned regarding the gap between where my privacy and data security program is today and where it needs to be?**
- 2. How do I want to close the gap, be compliant and stay off the evening news?**
- 3. Where do I need help?**
- 4. What do we do next?**





THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

Start the Conversation..

Start an executive discussion: Forbes “8 Privacy Steps To Keep ‘Pirates’ Away From Your Firm's "Crown Jewels“: <https://ibm.biz/BdXV7m>

Start a technical discussion: *“Find the Map, Locate the Treasure and Keep the Pirates Away: 10 Data Security & Privacy Best Practices (Part I)”*: <https://ibm.biz/BdXY3p>
and Part II: <http://ibm.biz/BdH5rQ>