



# The DLP Dilemma

**Duncan Hoopes**

**Product Manager, Security Management**

**IBM Tivoli**

**May 5, 2010**

**Rocky Mountain Information Security Conference**

# Abstract

- Is your DLP strategy rock solid and implemented, or is your internal team still arguing over what the acronym DLP stands for?
- We all know that data loss or leakage prevention shouldn't be a free ride to install a jumble of new hardware and software solutions, but it is easy to get caught up in the rhetoric.
- Let's discuss how your peers are setting a good data privacy foundation, and the merits of tackling the issue at the endpoint, the network or both.

## Why you should pay attention to this discussion

# I am smarter than Albert Einstein



### Proof:

- Albert Einstein said  
“**The definition of insanity is doing the same thing over and over again and expecting a different result**”.
- This statement is demonstrably false and I know it.
- Therefore, I am smarter than Albert Einstein.
- You would want to listen to Albert Einstein because he is smart.
- Therefore, you should listen to me.
  
- 'Course, if **you** know that it is false, too,  
then maybe you are at least as smart as I am.
  
- And, if you chose to attend this discussion,  
then you really ARE a genius.

Rita Mae Brown, *Sudden Death*, p.68

# Of course, your employees and foes are smart, too. And neither of them are insane...

## Employees

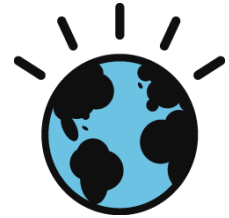
- They collect and create a lot of data
- They know that you care about it
  - So they do their jobs with it
  - So they trust you to have systems and processes that protect it
- They feel like you trust them with it
  - So they like to take it home
- They know that your friends and enemies care about it, too
  - So they try to share your data
  - And you haven't had a breach
  - Then, they keep doing the same thing over and over again, expecting the same result.

## Foes

- They like your data – a lot
- They know that you care about it
  - So they do stuff to collect it
  - So they watch what you do and track your progress
- They know you trust others with it
  - So they connect to your employees
- They know that your friends and enemies care about it
  - So, they try to get your data
  - And you haven't had a breach
  - Then, they keep doing the same thing over and over again, expecting a different result.



# The planet is smarter, too. But is it secure?



The planet is getting more  
**Instrumented, Interconnected, and Intelligent.**

**New possibilities.**  
**New risks...**

**15 petabytes** of new information are being generated every day. This is **8x** more than the information in all U.S. libraries

**508% increase** in the number of new malicious Web links discovered in the first half of 2009

Pervasive instrumentation creates vast amounts of data

New services built using that data, raises  
**Privacy** and **Security** concerns...



Critical physical and IT  
infrastructure



Sensitive information  
protection



New denial of  
service attacks



Increasing risks  
of fraud

# Smarter planet brings unrelenting change

**80%** Of enterprises consider security the **#1** inhibitor to cloud adoption

## Key drivers for security projects

### Increasing Complexity



Soon, there will be **1 trillion** connected devices in the world, constituting an “internet of things”

### Rising Costs



Spending by U.S. companies on governance, risk, and compliance will grow to **\$29.8 billion** in 2010

### Ensuring Compliance



The cost of a data breach increased to **\$204** per compromised customer record

# We encounter unprecedented complexity

## New Methods and Motives:

Adding to the complexity and sheer number of risks

**Compliance Spending:**  
Investing in more point products to solve more point problems

**The Global Economy:**  
Driving new security support requirements



**IT Innovation:**  
Requiring new ways to secure the new ways we collaborate

**Flexibility in Business Methods:**  
To improve operations and serve customers

***Complexity remains the biggest security challenge!\****

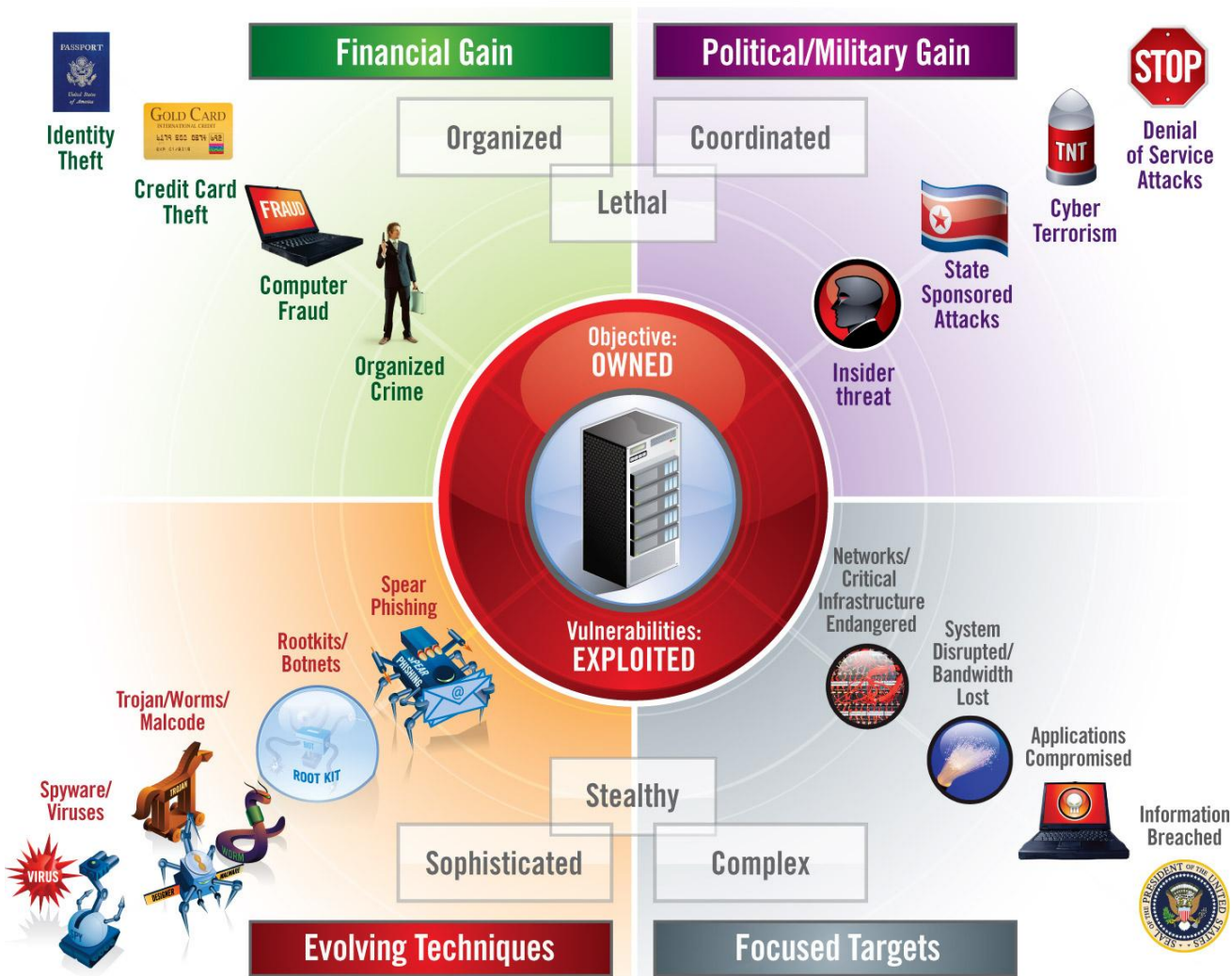
***Integration is key to managing the cost and complexity of the evolving landscape***

# Threats are evolving from increased cyber-terrorism to decreased employee loyalty

## “Trinity of Threat”

- **Prestige Nation**
  - Glory/Ego Motivated Vandals
- **Profit Nation**
  - Financially Motivated Cyber-Crime
- **Political Nation**
  - Politically motivated cyber-warfare/ terrorism
  - Insider risk and increases in holes

*As threats evolve, risk expands exponentially!*



New security technologies are often seen as “just another point product” to add to a teetering mass of security stuff



*“We have put so many security products into our systems that the complexity of the sum of those security products has become itself part of the problem.”*

– **Dan Geer**

Keynote Speaker  
Source Boston Conference  
March 2008

- New technologies require new forms of protection – and can be “disruptive”
- Security systems themselves carry data that amplifies risk

# Rising costs

People are becoming more and more reliant on security

IBM believes that security is progressively viewed as every individual's right

Today's CIOs spend 55% of their time on activities that spur innovation. The remaining 45% is spent primarily on cost reduction, managing risk, and automation.

Skills to deploy new technologies like Virtualization and Cloud computing are costly



IT departments have:

- Increasing responsibilities
- Time pressures
- Do more with less



Bulk of security budget is spent firefighting rather than innovating



Administrators and help desk resources are strained to support increasing base of users



# What's at stake?

## REPUTATION AND BRAND DETERIORATION

- Negative public attention
- Loss of future business

## INTELLECTUAL PROPERTY

- Exposure of company secrets

## EMPLOYEE MORALE AND CULTURE

- Mismanaged trust and accountability
- Unclear security expectations and approaches

## FINANCIAL VIABILITY

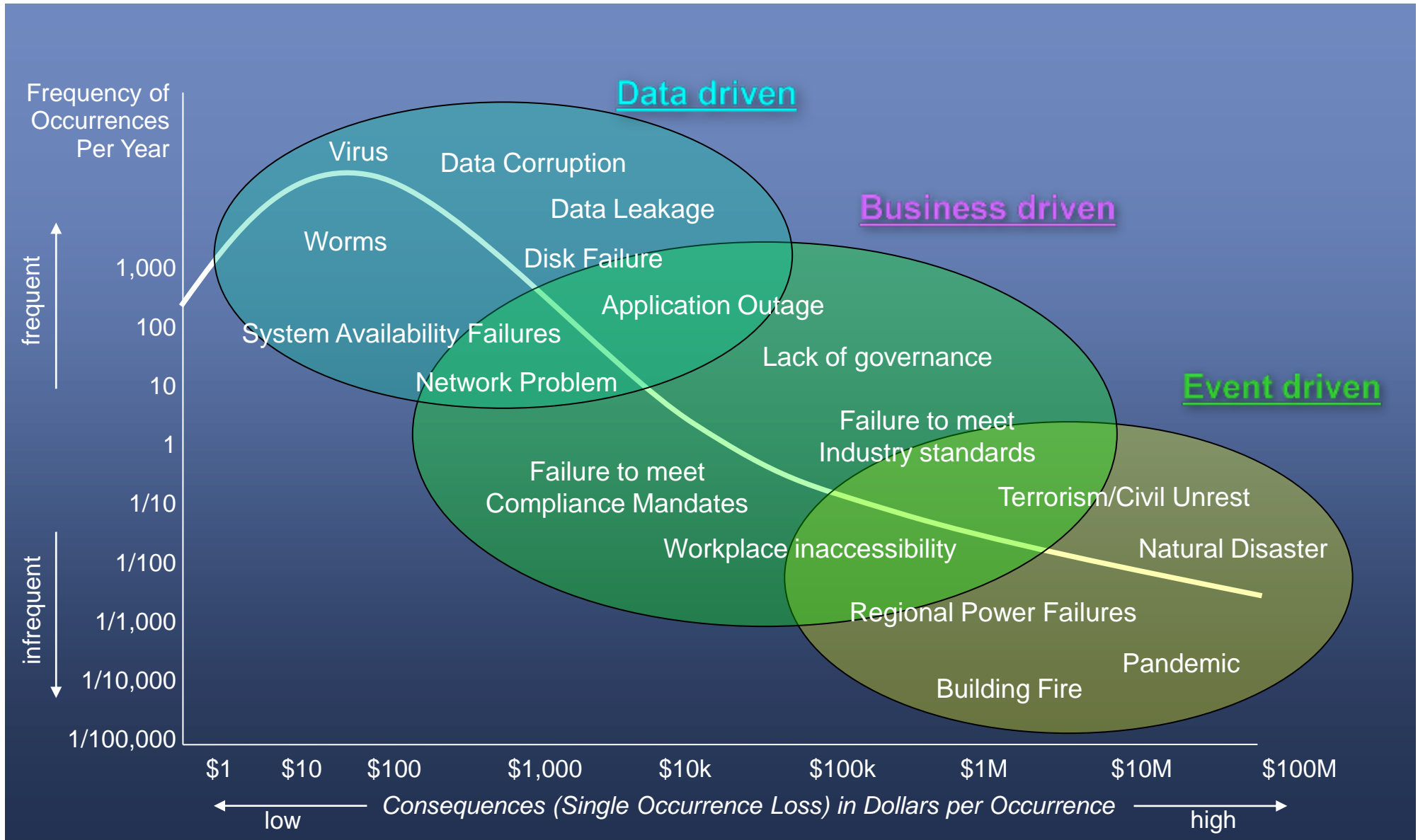
- Internal investigation and crisis management costs
- Penalties for noncompliance
- Loss of productivity
- Costs associated with data disclosure laws
- Decrease in stock value

## CUSTOMERS' AND PARTNERS' PRIVACY (AND TRUST)

- Class action lawsuits
- Loss of customer and partner confidence

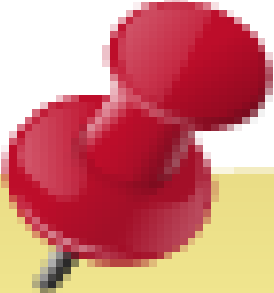
**AND MORE...**

# Not all risks are created equal



# Simple mistakes can cost a lot of money

## Causes of Data Breaches

- 
- 40%** Negligence, where people make mistakes, such as lost laptops
  - 36%** System glitches, such as sending out statements that should not have been sent
  - 24%** Malicious and criminal attacks
  - 42%** 3<sup>rd</sup> party mistakes

## Magnitude of Data Breaches



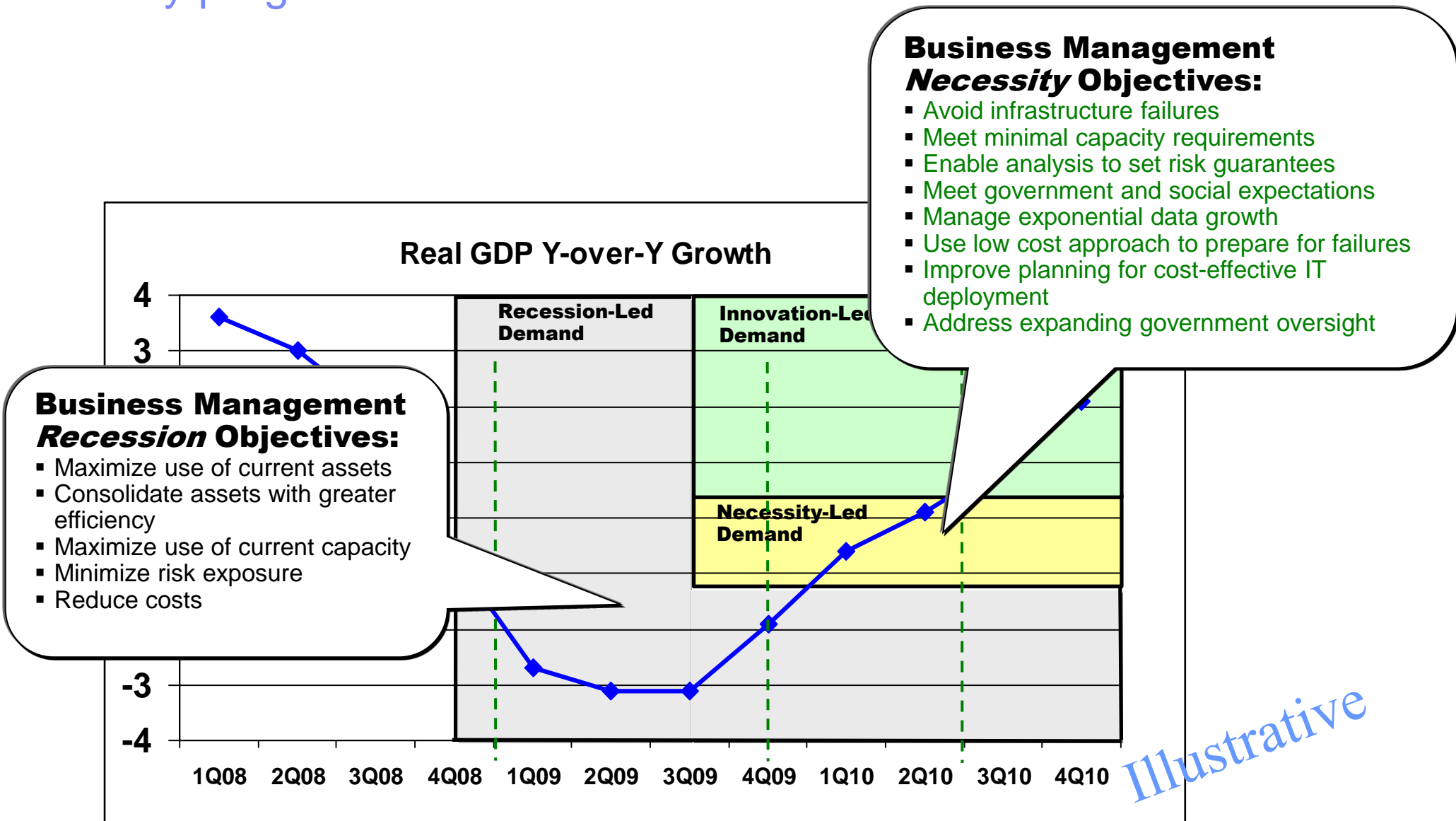
5,000 to 101,000 lost or stolen customer records

Most expensive breach cost nearly \$31 million to resolve

Least expensive breach cost \$750,000

More than 82% of organizations in the study had more than one data breach in 2009 involving the loss or theft of more than 1,000 records containing personal information

During the recovery, priorities and IT spending drivers can be expected to shift from cost reduction to meeting capacity requirements as the recovery progresses



Illustrative

# It's time to start thinking differently about security



## Products and services that are Secure by Design



Safely and Securely  
adopt  
new forms of technology  
and  
new business models

Less than 3% of a typical organization's  
overall assets are considered adequately  
classified for access purposes

# How is data lost?

- **Stolen laptops or USB storage**
- **Lost laptops and devices**
- **Incorrectly disposed storage media**
- **Cybercrime**
- **Exposure via the internet or via Email**
- **Malicious insider**



**\$204 cost per compromised record for a data breach**  
**Average total cost per data breach \$6.75 million**

# Cannot progress without Data Loss Prevention (DLP)

## • **Solves urgent pain**

- Prevent inadvertent or accidental loss or exposure of sensitive enterprise information
- Provides policy compliance monitoring and enforcement regarding the movement of information assets: across the corporate boundary, on the internal network, and on the desktop

## • **A set of technology components that:**

- Identify critical data, based on specified rules and policies using content inspection and contextual analysis techniques
- Apply remediation actions ranging from simple event logging to full blocking depending on the type of sensitive information and specified enforcement policy

## • **DLP is relevant for:**

- Unstructured documents, email
- Structured data (databases, spreadsheets)
- Personally Identifiable Information (PII)
- Non-Public Personal Information (NPII)
- Credit Card Data
- Health records, information
- Intellectual Property (IP)

## • **Complementary capability to current Identity and Access Management portfolio.**

- Focus is on content that users frequently have already been given access to, but what are they doing with it?
- Where is it located outside of structured applications and systems?

## • **Requires BUSINESS prioritization and information policies:**

- **IT & Security cannot do alone**

## But, “DLP” is not “smart” enough and cannot do it all

- **Most DLP solutions – as implemented – are not:**
  - Instrumented, Interconnected, and Intelligent.
  - cf. Centralized Policy Management
- **Even if a DLP implementation was pretty smart, it is not “wicked smart”:**
  - it likely does not cover your business partners, nor all of the following:

### Identity and Access Assurance

Provide efficient and compliant access for the right people to the right resources at the right time

### Data and Application Security

Protect integrity and confidentiality of business data and transactions from the browser to the disk

### Threat and Risk Management

Optimize service availability by mitigating risks while optimizing expertise, technology and process

### Information Management

Protect the lifecycle of information via classification, records management and content management repositories

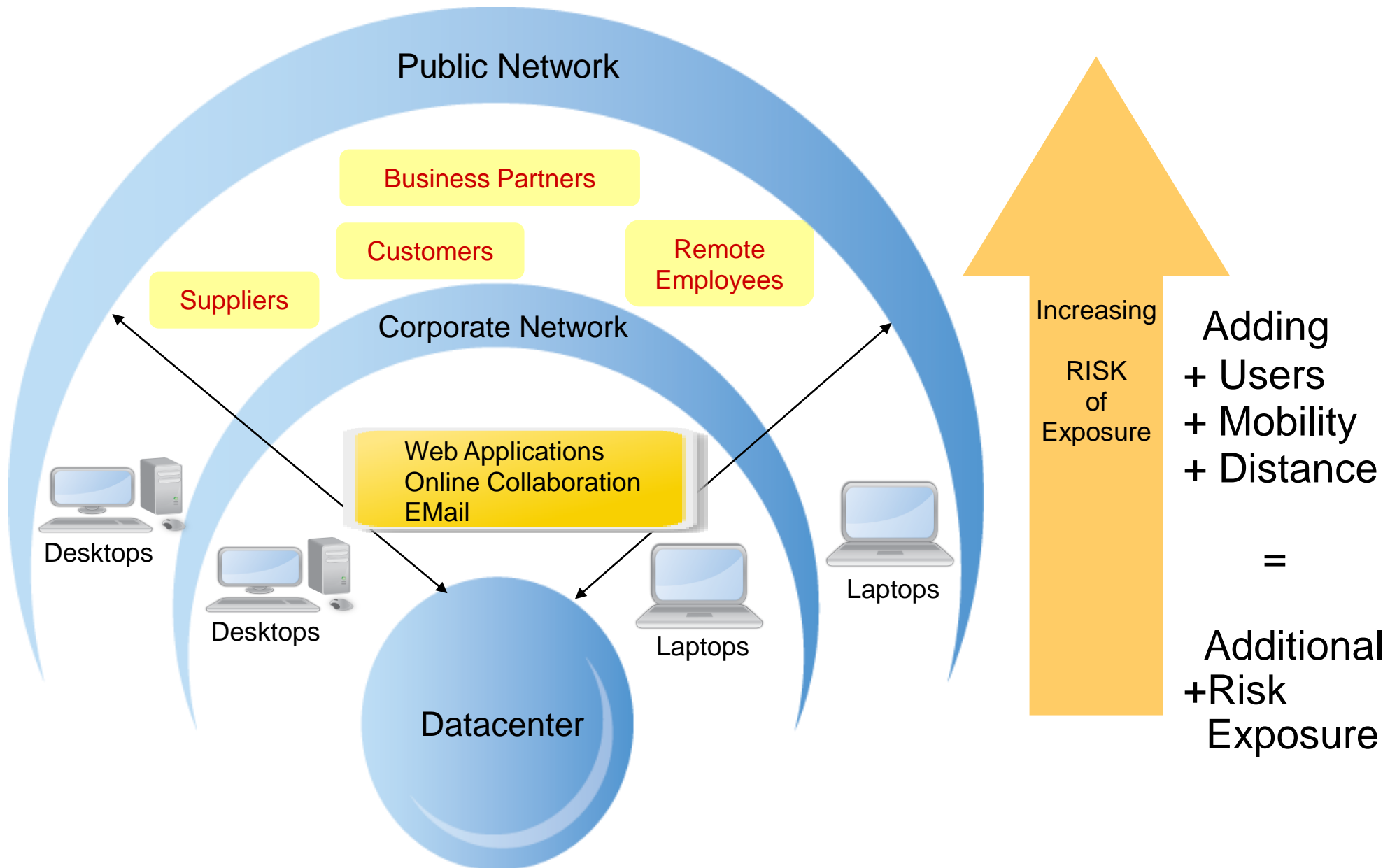
### Databases

Protect and control access to structured data and myriads of spreadsheets

### Collaboration and Email

Protect information exchange over email and collaboration systems

# Managing risks with sensitive data



# Perimeter defense is essential for blocking external threats...but it doesn't guard data against the human factor

<b>Lost or stolen devices</b>	<ul style="list-style-type: none"><li>• Intellectual property exposed to competitors</li><li>• Sensitive customer data compromised</li><li>• Competitive information leaked to the media</li></ul>
<b>Exposed business processes</b>	<ul style="list-style-type: none"><li>• Extracts pulled for processing and reporting</li><li>• Circulating data across organizations</li><li>• Workarounds during system outages</li></ul>
<b>Malicious insiders</b>	<ul style="list-style-type: none"><li>• Malware deployed within the network</li><li>• Intentional misuse of company information</li><li>• Identity theft and Industrial espionage</li></ul>
<b>Careless use of the corporate network</b>	<ul style="list-style-type: none"><li>• Viruses unwittingly downloaded at home</li><li>• Unsecured archives or copies of data</li><li>• Uncontrolled circulation of classified documents or personal e-mail messages</li></ul>

# Multiple forces are driving enterprise information solutions needs – cannot afford a simplistic approach

*Hard*

**Cost**

**Complexity**

**Compliance**

**Information Explosion**

- 57% CAGR thru 2010\*
  - 80% unstructured\*
- Unpredictable workloads



*Soft*

**Collaboration**

**Value Creation**

**Culture**

**Change**

**Risk and Cost Management**

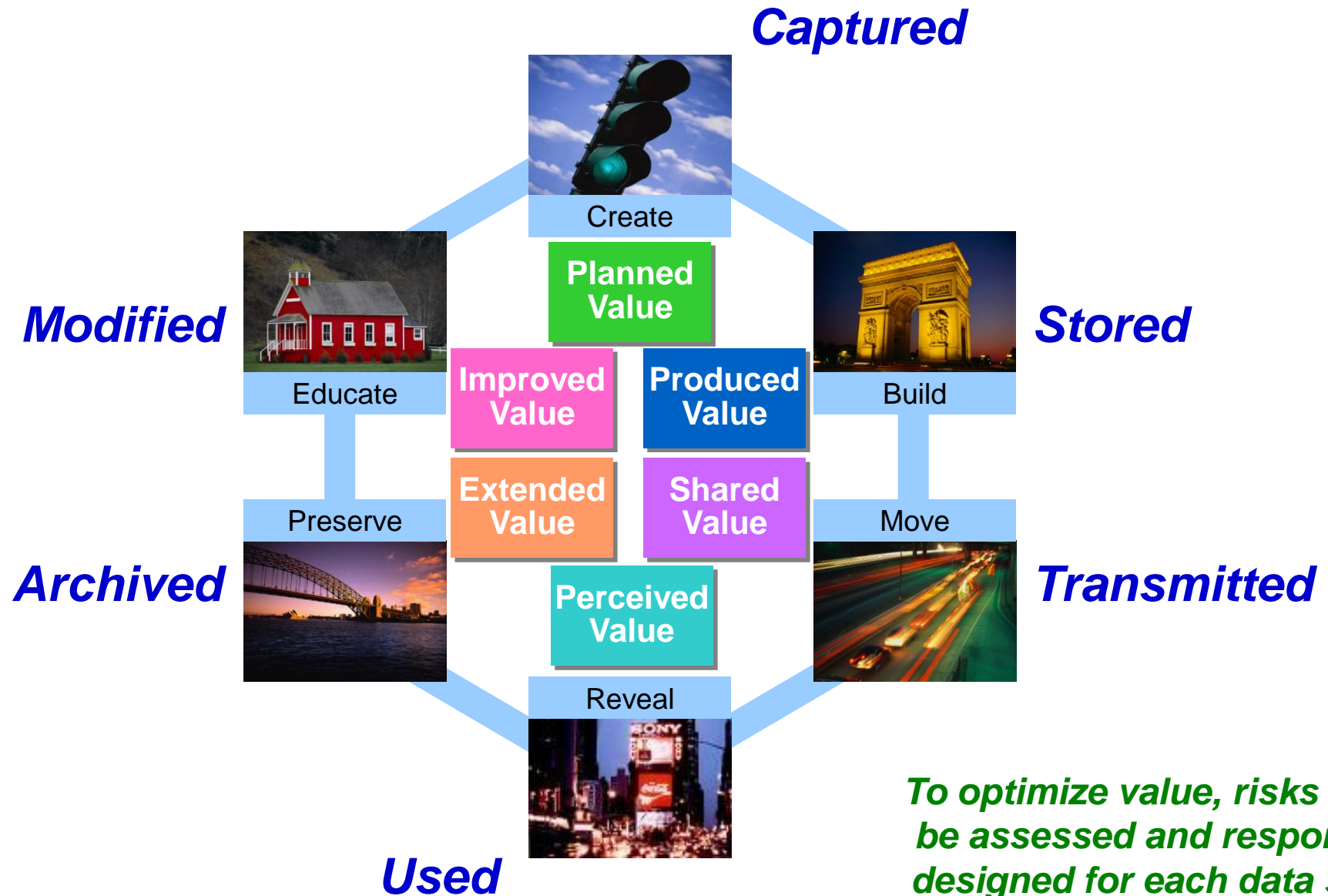
- Compliance / legal
- Security / privacy
- CapEx & OpEx control

**Business Opportunity**

- Improved analytics
- Holistic customer views
- Market / competitive insight

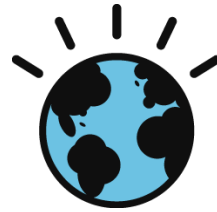
***Risk Mgmt: seven key components of a Balanced Risk Portfolio***

# The purpose of Data Security is to reinforce the value contribution for each stage of the information lifecycle



*To optimize value, risks must be assessed and responses designed for each data state*

# Assure the solidity of your security foundation

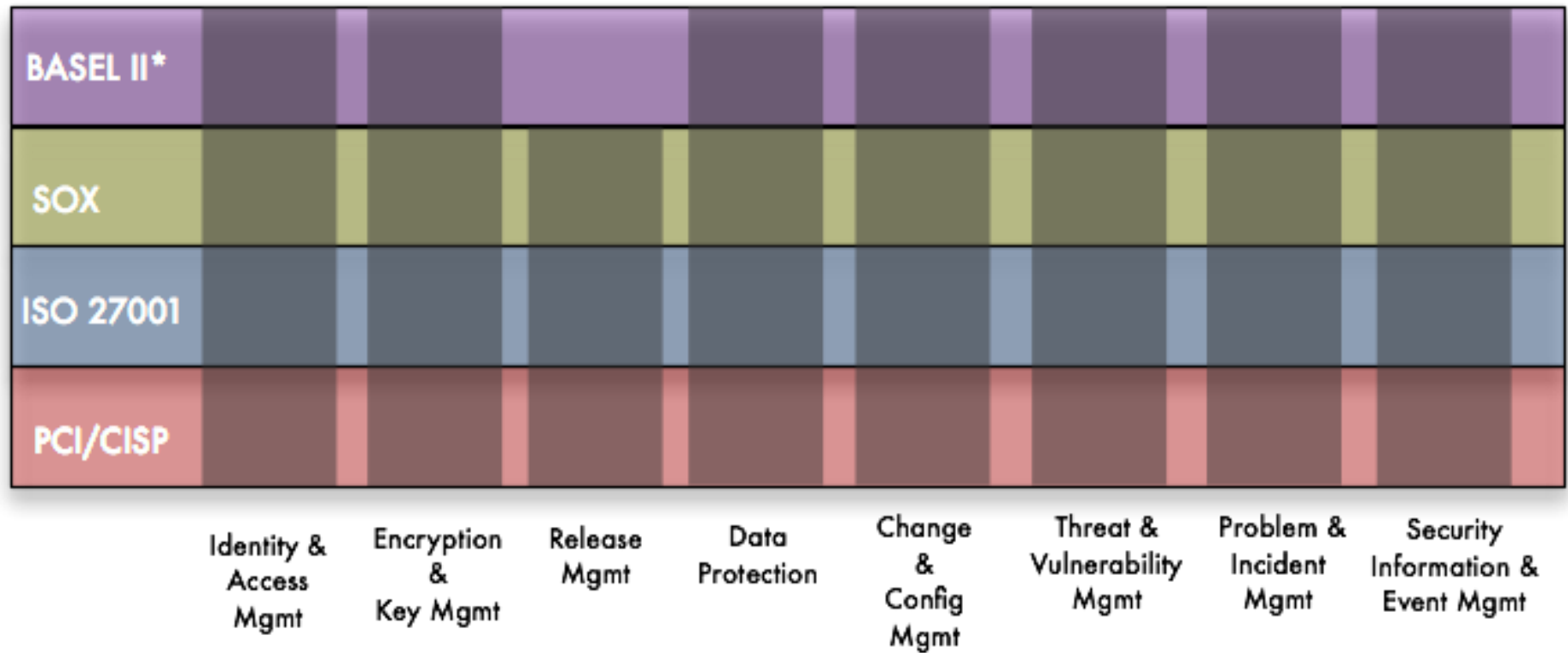


## Critical Controls

<b>Identity &amp; Access Management</b>	Process for assuring access to enterprise resources has been given to the right people, at the right time
<b>Encryption &amp; Key Management</b>	Capability enabling use of pre-existing investments by providing central management of encryption keys
<b>Database Protection</b>	Capability that allows for granular protection of data in test and production databases
<b>Release Management</b>	Process for assuring efficiency and integrity of the software development lifecycle
<b>Change &amp; Configuration Management</b>	Process for assuring routine, emergency and out-of-band changes are made efficiently, and in such a manner as to prevent operational outages.
<b>Threat &amp; Vulnerability Management</b>	Process and capabilities designed to protect the enterprise infrastructure from new and emerging threats
<b>Problem &amp; Ticket Management</b>	Automated workflow and Service Desk designed to assure incidents are escalated and addressed in a timely manner
<b>Security Information &amp; Event Management</b>	Automated log management, monitor and report security and compliance posture

The very nature of foundational improvements brings value across the information lifecycle

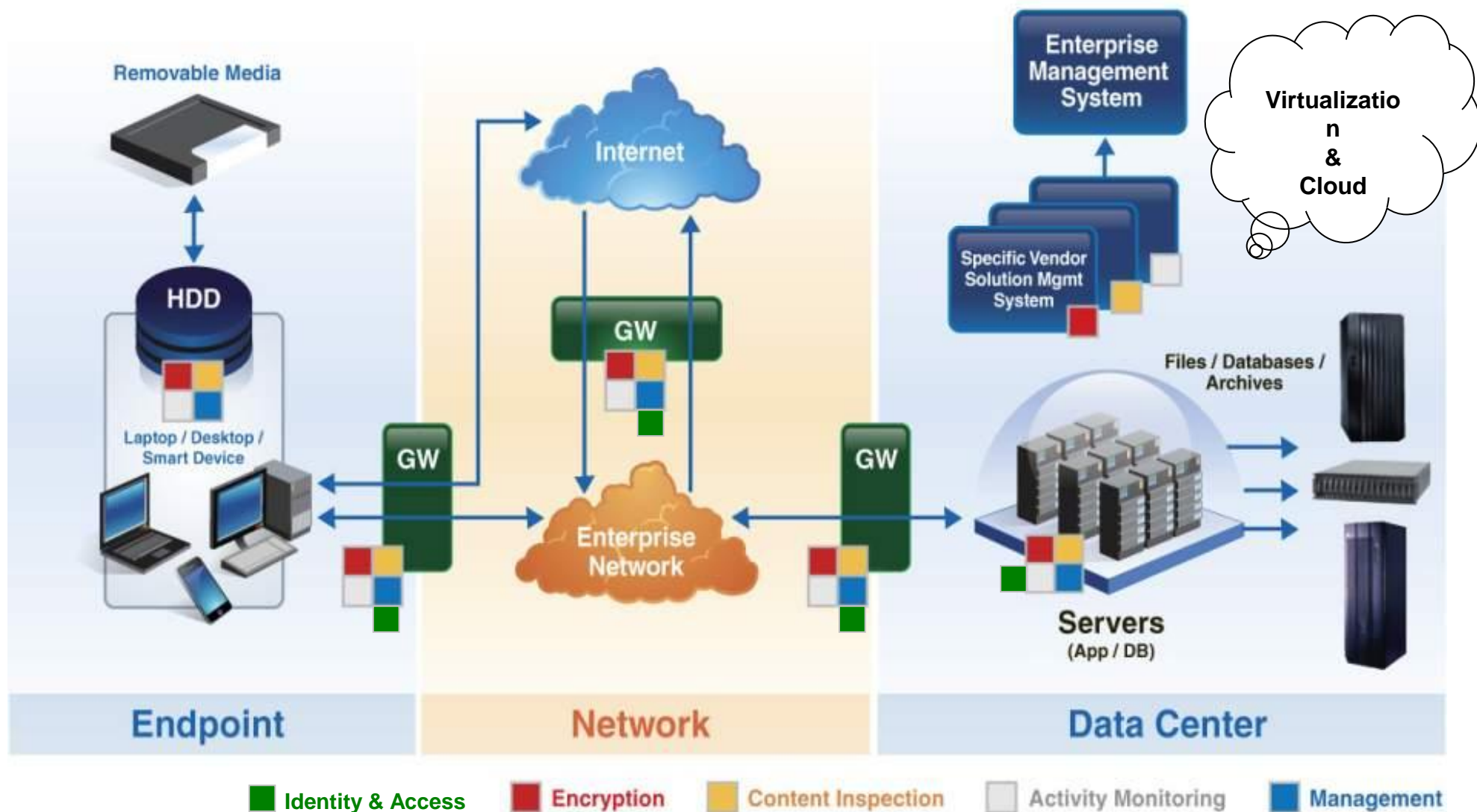
# Critical Controls support multiple compliance initiatives



**\*Basel II is NOT prescriptive, instead it required adoption of an integrated control framework**

# Data security requires a holistic framework across the key control points

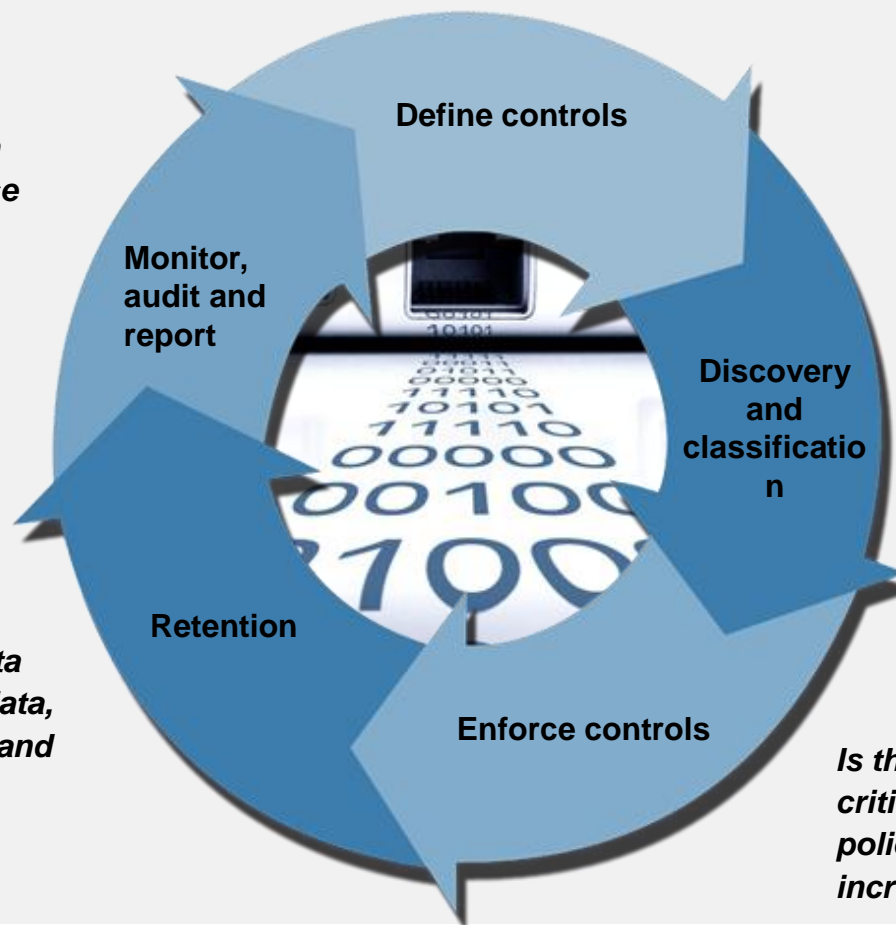
Captured > Stored > Transmitted > Used > Archived > Modified



# ... And a repeatable process for safeguarding information: the Information Security Lifecycle

Over 80% of enterprise information is unstructured – requiring classification, protection and monitoring

*Is there a way to streamline reporting and tracking information so I can easily sift through the false positives to target the real violations?*



*Do I have intellectual property, confidential records or personally identifiable information that violates policy or government regulations and/or is on the verge of being comprised?*

*Are there sophisticated ways to categorize my data, standardize my policies and manage my data protection issues?*

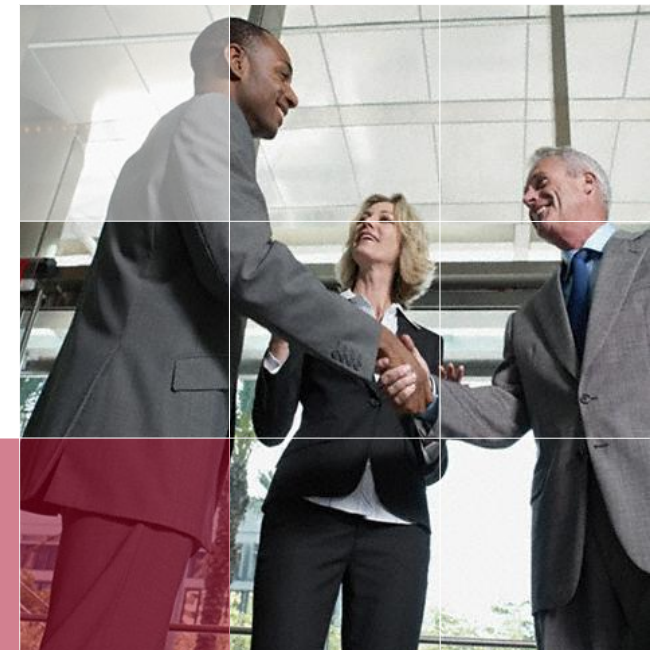
*How can I keep track of which data retention policy applies to what data, what data needs to be encrypted and how long I need to retain it?*

*Is there a way to share and guard critical data with manageable policies to mitigate against increasing internal threats?*

**Your information security strategy needs to address these key phases**

## Balancing to your risk tolerance delivers targeted ROI

- Improve organizational effectiveness through increased **collaboration** & sharing
- Lower the **cost** of operating a security-rich, resilient business
- Reduce operational **complexity** in your security disciplines
- Ensure consistent enforcement of corporate security policies and regulatory **compliance**
- Managing the impact on employee **culture**
- Deliver **value creation** and ROI from security investments
- Enhance ability to manage **change** – in business processes and business units – including establishing better information and tools to help prioritize and integrate future security investments



# Responding to the dynamic landscape demands proven expertise, up-to-date knowledge, and ongoing optimization

Requirements and planning

Discovery assessment

Policy design

Implementation

Support desk

Ongoing monitoring, response & reporting

Ongoing remediation & analysis

## ***Eight key activities***

...in response to:

- **Insider risk and the “human factor”**
  - Intentional misuse / Theft
  - Careless activity /  
Lost data & equipment
  - Incomplete business processes /  
Intentional workarounds
- **Compliance and audit requirements**
  - PCI and similar regulations
  - Proof of repeatable process

with solutions across the enterprise:

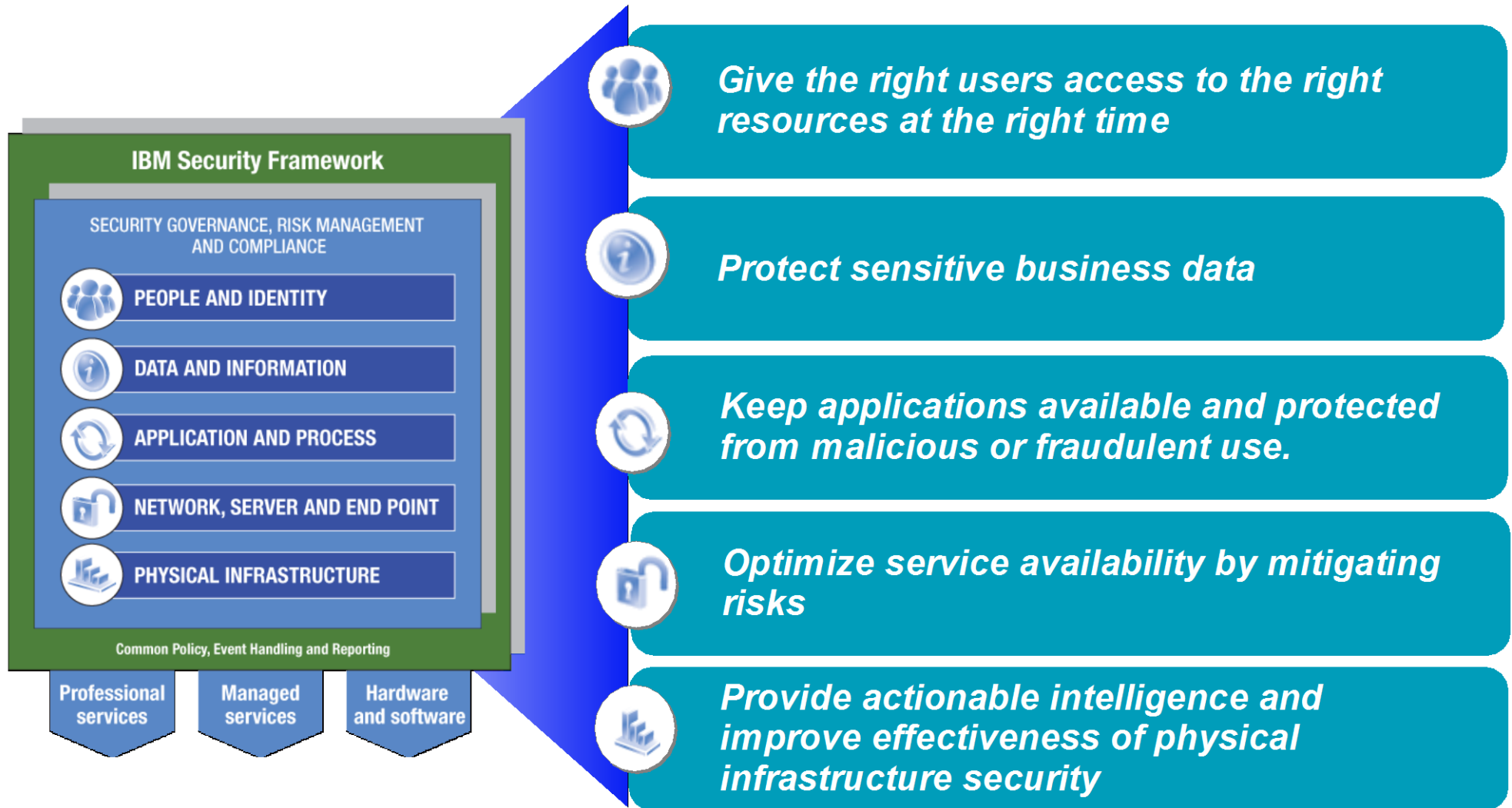
- Identity & Access Management
- Encryption & Key Management
- Database Protection
- Release Management
- Change & Configuration Management
- Threat & Vulnerability Management
- Problem & Incident Management
- Content Inspection
- Security Management
- Security Event & Information Mgmt
- DLP

# The not so obvious, but obvious smart points

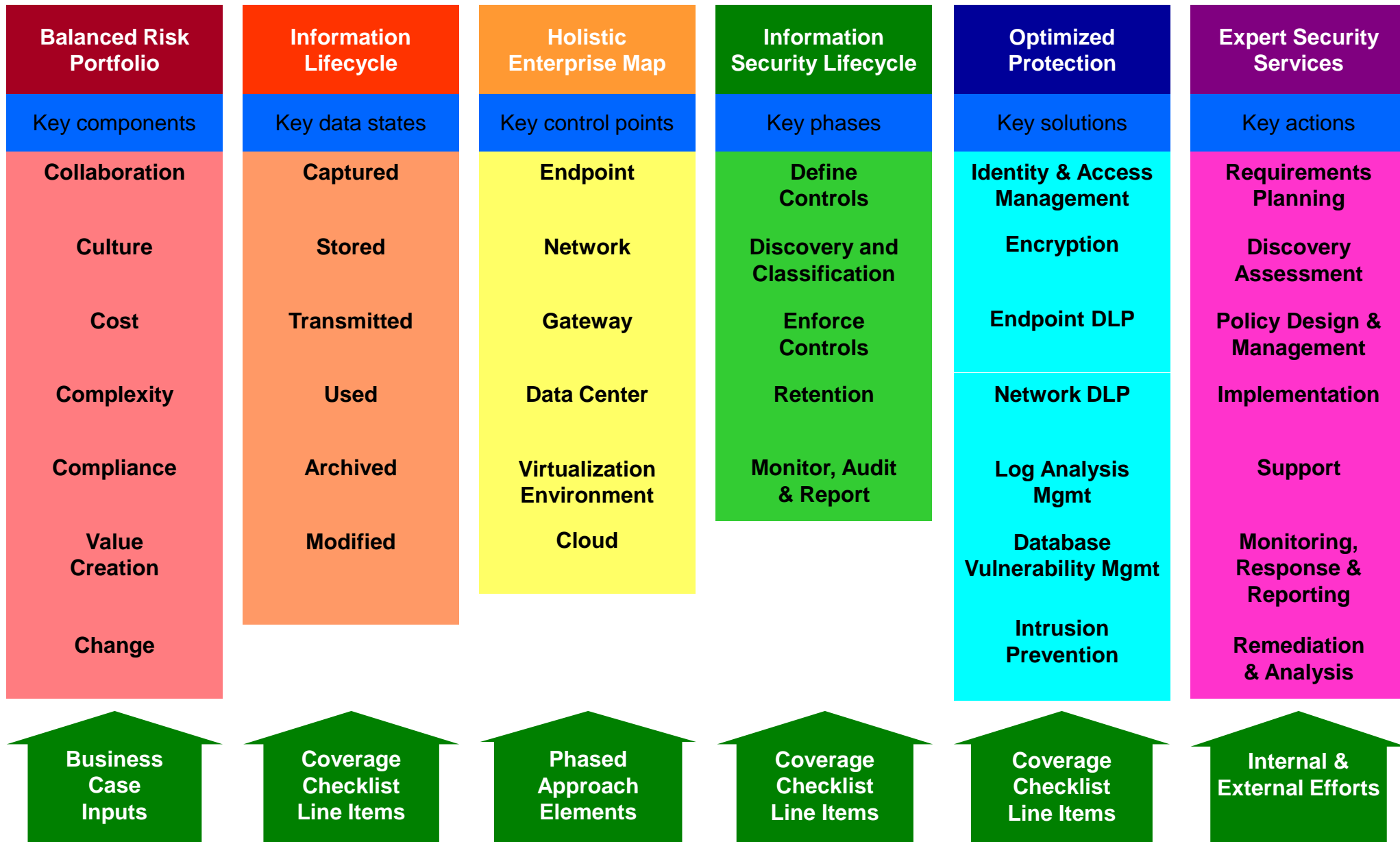


- DLP needs to tie to Identity & Access Management implementations, evolving to content and context awareness
  - Implication: **IAM is a prior priority**
- DLP should be approached by protecting key information at its sources
  - Implication: **Servers (physical, virtual, database) need core protection**
  - Implication: **Integrated Security Management controls & alerts for data stores**
- Content management, archive management, service management, and collaboration tools are the foundation of information sharing and protection
  - Implication: **Integrated, foundational controls are fundamental**
  - Implication: **Network inspection is critical to reveal where to target investments**
- Protect information throughout its lifecycle, ensuring access is controlled based on policy
  - Implication: **Policy Management is critical and must link to IAM**

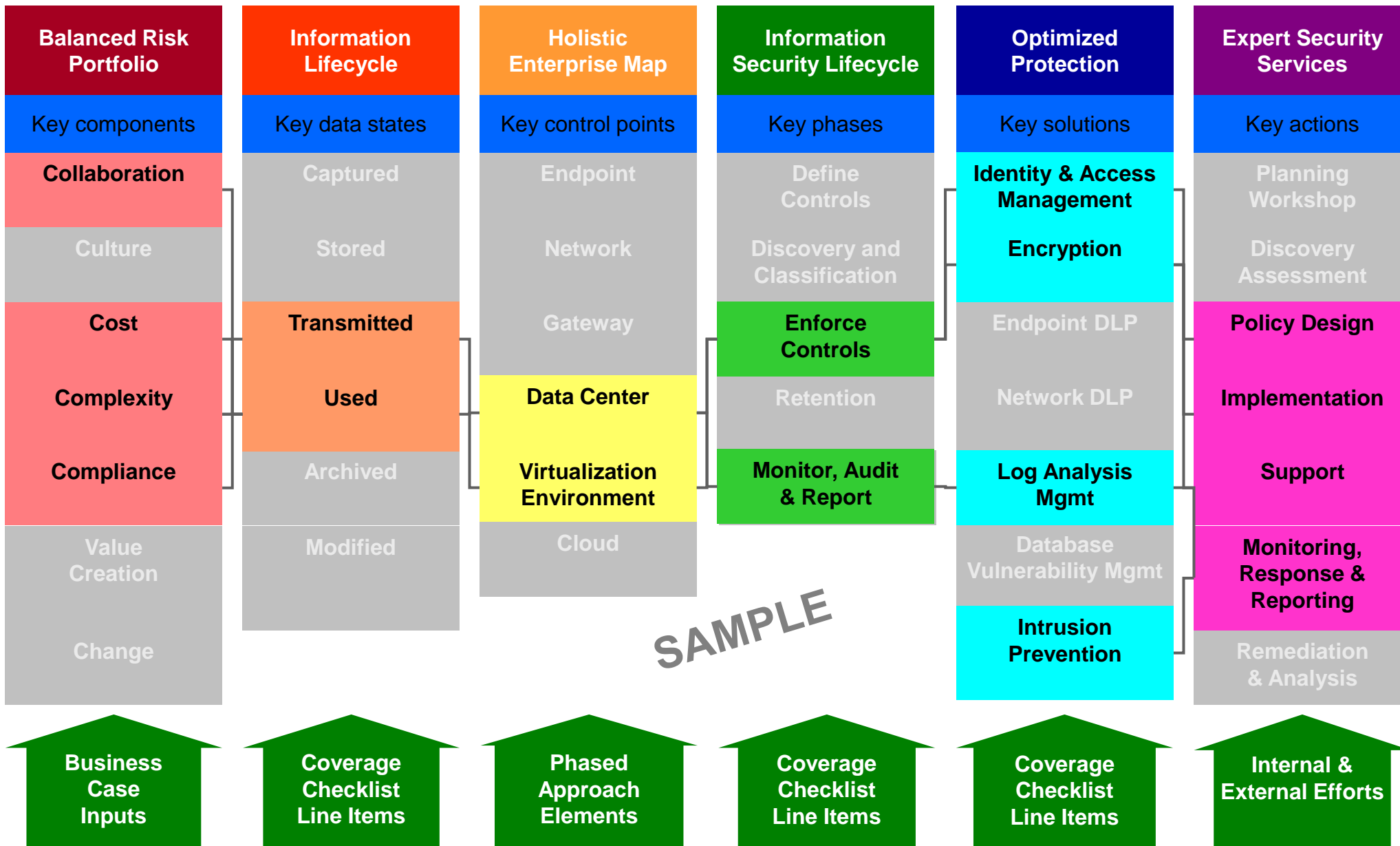
# IBM Security framework



# Summary: key inputs for managing to your risk tolerance

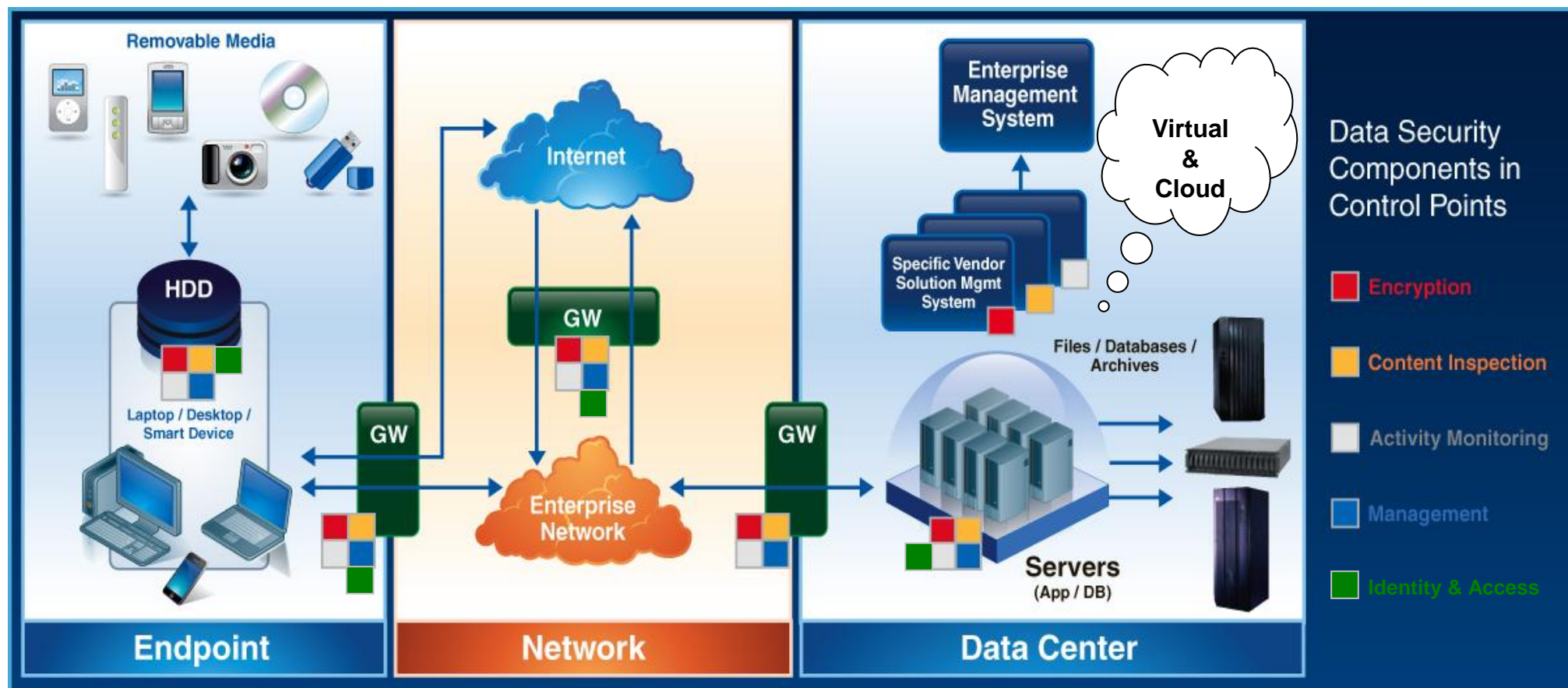


# Action: Align with your risk tolerance, set the priorities, and go!



“as simple as possible, but not simpler” – Albert Einstein

Reducing operational cost and complexity  
by managing and optimizing at the enterprise’s **foundation**



THANK YOU!



Duncan Hoopes  
[Duncan.R.Hoopes@us.ibm.com](mailto:Duncan.R.Hoopes@us.ibm.com)  
813-322-3534