Deloitte.

Data Security Leading Practices

4A's Information & Technology C.I. and Data Security Safeguards Task Force Meeting

February 2014

Introductions

Greg Banks, Director
Specializations: Advanced Advertising strategy, operations

Tim Davis, Principal
Specializations: Advanced Advertising strategy, operations, analytics, risk management

Sameer Ansari, Senior Manager
Specializations: IT risk, privacy, compliance, and security

Deloitte is again named a leader "with exceptional client feedback" in Information Security Consulting Services

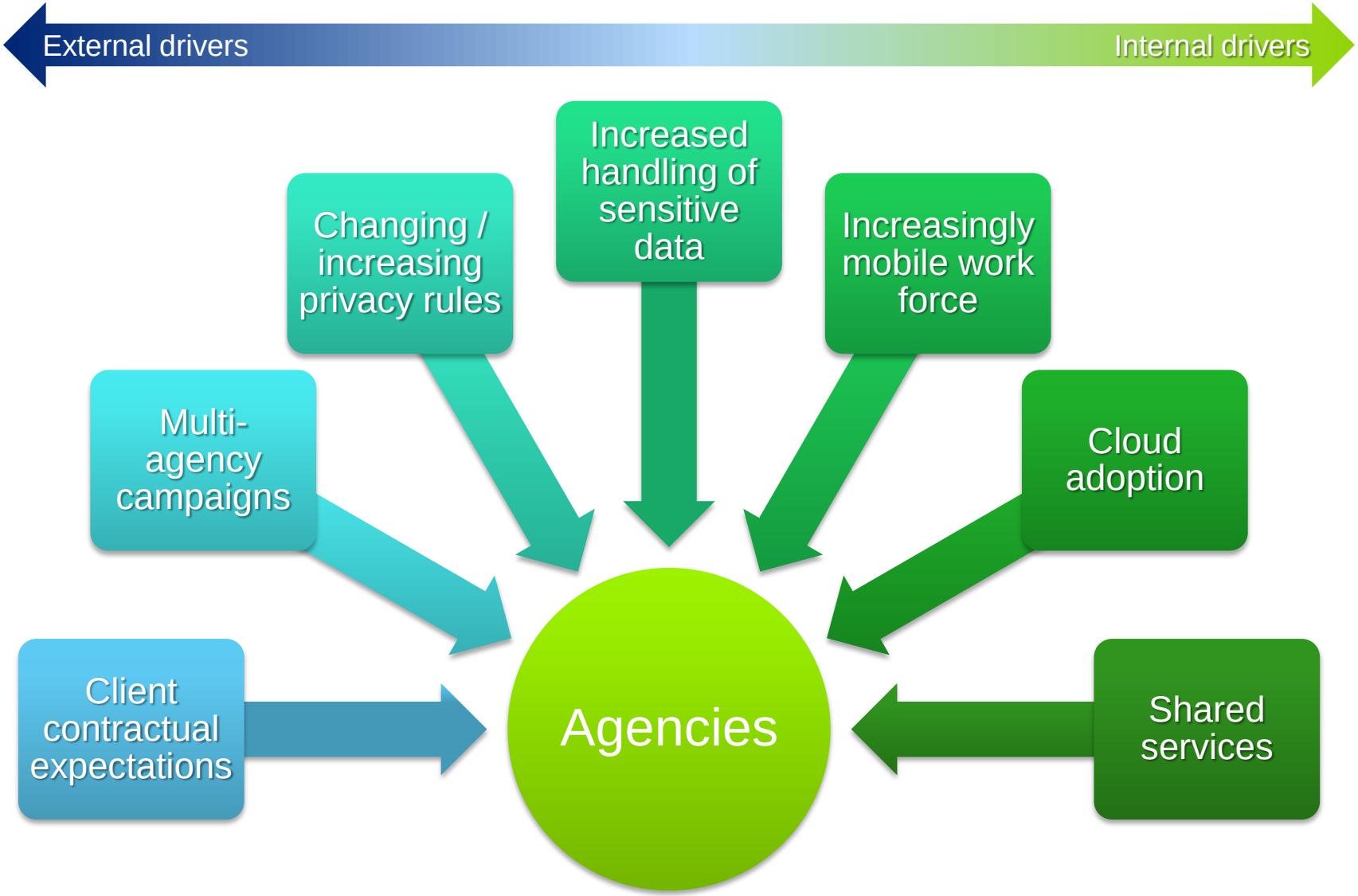
Forrester Research, Forrester Wave™: Information Security Consulting Services Q1 2013", Ed Ferrara and Andrew Rose, February 1, 2013

Gartner ranks Deloitte #1 for worldwide Security Consulting Services, based on market share in 2012

Gartner Market Share Analysis: Security Consulting, Worldwide, 2012

The forecast:
Dark clouds with severe weather likely

The situation in which we find ourselves



The security threat is underscored by recent headlines…

…breaches can and do occur in organizations of **all sizes** and **across a large number of industries**

The majority of breaches (62%) **take months (or even years!) to be discovered** and it's usually by someone outside the organization (nearly 70% of all breaches).

CryptoLocker ransomware leverages advanced file and data encryption techniques to **extract money from victims**. Over **250,000 effected** thus far

"'Shamoon' **virus most destructive ever to hit a business**," Leon Panetta warns. "**More than 30,000 computers** that it infected **were rendered useless**"

A series of distributed denial-of-service (DDoS) attacks—which…caused **disruptions at several institutions** — were waged by **hundreds of compromised servers**

The threats are evolving…

1	Data is money – criminal underground makes for easy monetization	Personally identifiable information (PII), intellectual property (IP)
2	Actors with differing motives and sophistication – often colluding with each other	Hactivists, cyber criminals, malicious insiders
3	Attacks are exploiting the weakest links / paths to critical information	Application software, people (including targeted attacks on senior executives), partnered systems with poor controls
4	Attacks are targeted with varying degrees of sophistication	System availability attacks, virus attacks, malicious programs
5	Speed of attack is increasing and response times are shrinking	Rapid exploits and immediate transfer of assets to overseas locations

…and have a much broader reach than in the past

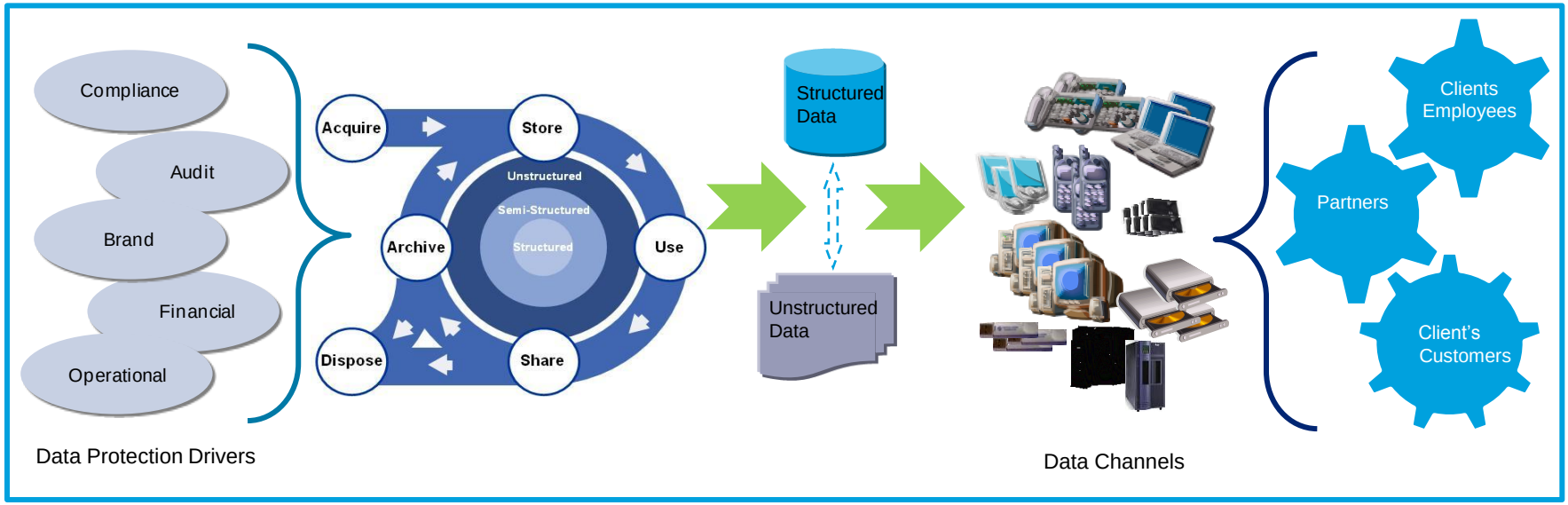
6 Attackers have no geographical boundaries – global theater	Attacks from global locations, often beyond U.S. law enforcement reach
7 Organizational boundaries have disappeared – anytime, anyhow, anywhere computing	Internet, mobile, social, cloud – driving need for a "data" centric security approach
8 Recent events continue to elevate the information security agenda with the Board and management	Financial, reputational, regulatory and operational risk implications
9 Privacy rules are complicated and getting tougher	Various privacy laws and regulators focus on customer notification
10 Regulators and government are key stakeholders with ever increasing focus	GLBA, Dodd-Frank, SEC guidelines, HIPAA Omnibus Rule, Senator Jay Rockefeller letter, pending cyber legislation, Leon Panetta speech

Putting the risks in perspective

Agencies are facing several issues

Agencies are collecting an increasing amount of customer and confidential data in order to serve their clients needs

- Clients are imposing data protection requirements via contracts and other mechanisms
- The more data an organization collects the more likely they are to be a target of cyber crime
- Many clients are in heavily regulated industry and those regulations and expectations of protection follow the data



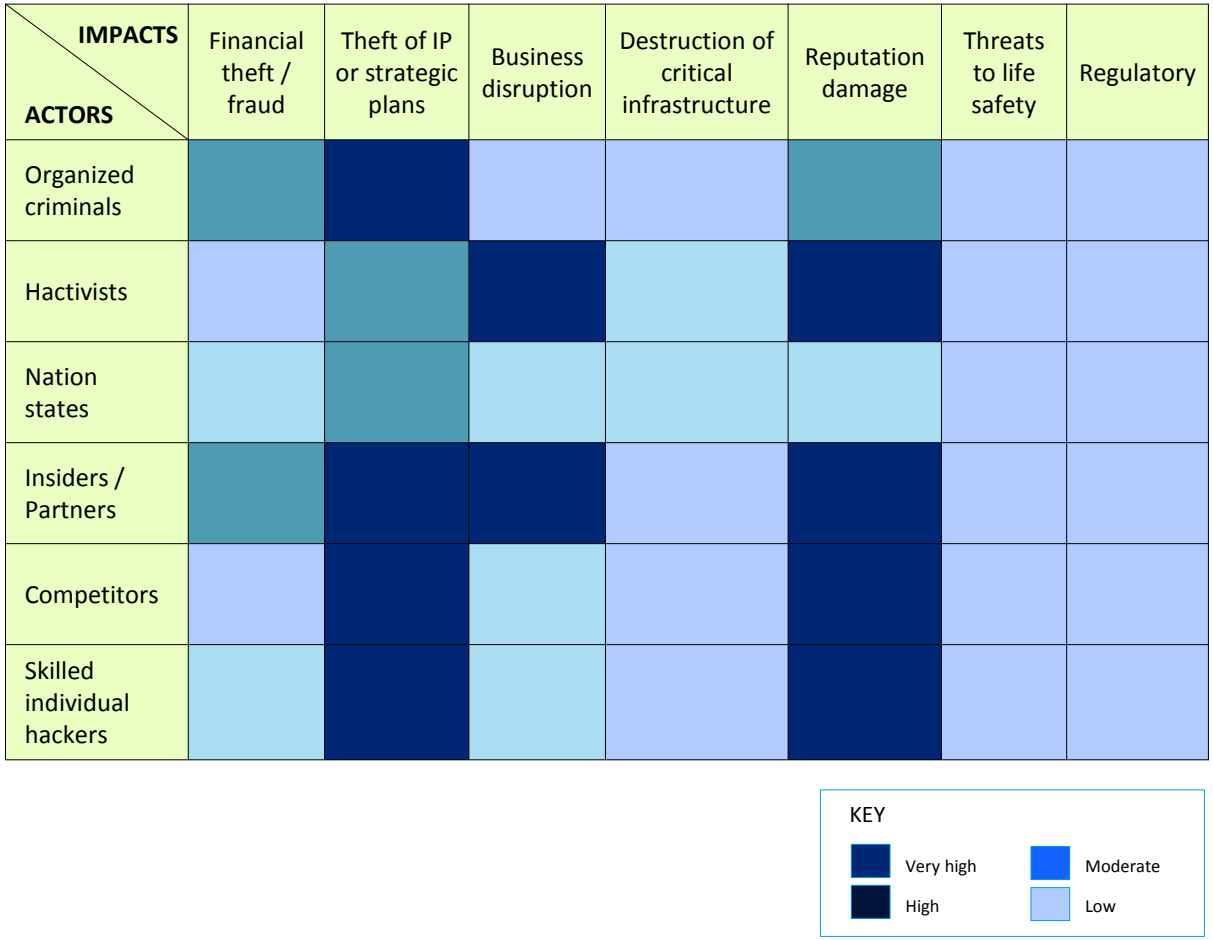
One of the biggest challenges for an agency is to remain in control without sacrificing flexibility, creativity and the entrepreneurial spirit. The following slides cover addressing data risks and developing a sustainable program

Threat actors and their motives vary by industry and organization

A typical cyber risk heat map for Agencies

Notable insights:

- Organized criminals are after direct financial assets, plus critical IP, customer and employee data (PII) – all of which have monetary value and are abundant within the Advertising industry
- Espionage from within is a major concern for the Advertising industry and is rooted in the competitive nature of the industry. Particular threat for reputational damage within Advertising sector.
- Particular to Advertising and Media industry, the strong use of temporary and project-specific talent and contractors, lends itself to heightened and unique cyber risks



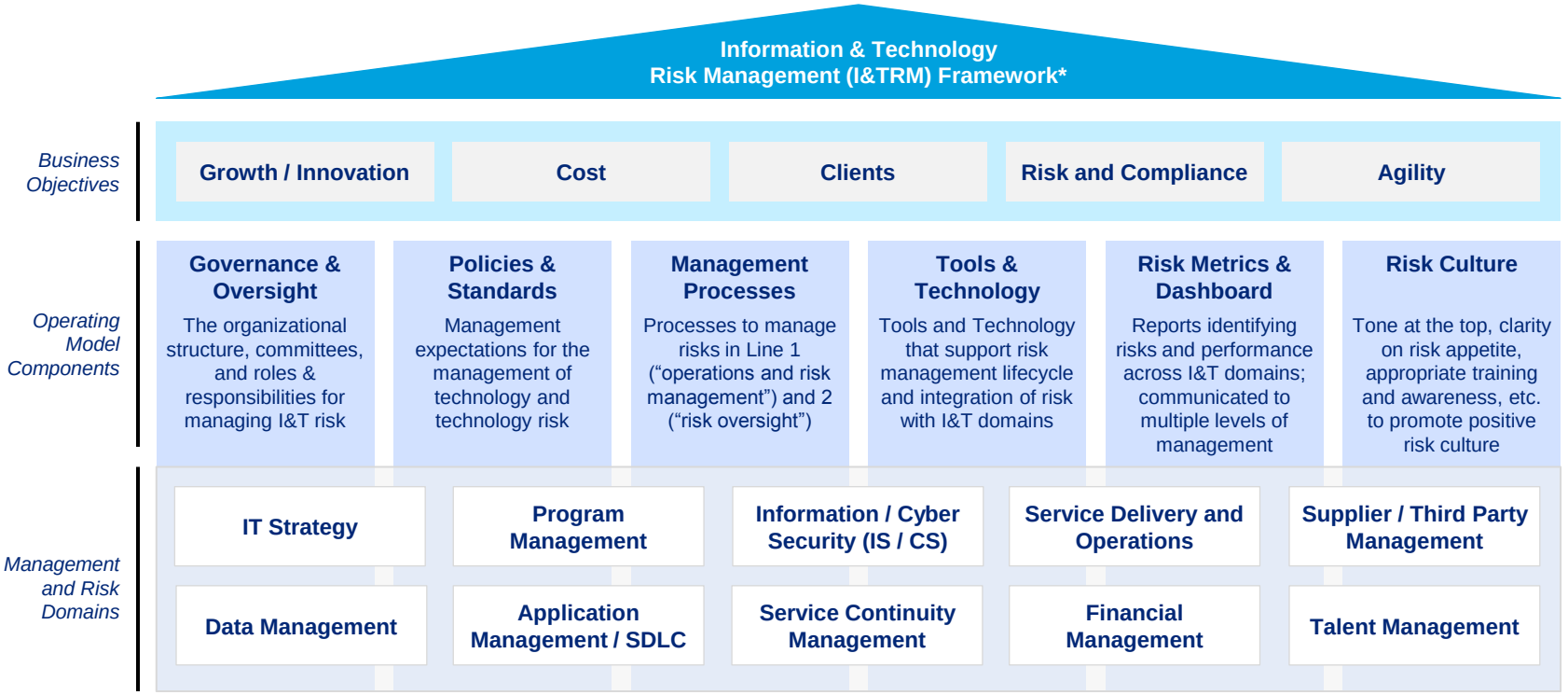
Leading Practices

Cornerstones

1. Don’t let clients define your security program, take the lead
2. Identify the standards you need to achieve then rationalize the requirements for operational simplicity
3. Develop a high risk data program including a data life cycle
4. Standardize approach across the organization; exec buy-in essential
5. Make security easy to consume, hard to avoid
6. Don’t underestimate the cyber threat; involve experts
7. Continuously evaluate

Having a common framework will allow for consistency

An IT risk management framework / strategy can help an organization to optimize both risks and costs while meeting contractual and regulatory requirements



Organizational actions should be risk prioritized to their industry and operating environment

The framework should be aligned to common industry standards…

Maintain an inventory across global regulation and IT risk domains that can assist in the build-out of your Cyber Risk Program

T Risk Management Framework Risk Domains	Information Security	I&T Risk Management	I&T Governance	IT Service Management	Data Mgmt. and Privacy
Leading practice and industry standard themes	Leading Practices and Industry Standards				
	ISO 27001 NIST 800-53* PCI DSS BS 25999	COSO ISO 27005 ISO 31000	COSO ISO 27005 ISO 31000	ISO 20000 ITIL	GAPP SOC2 Principles ISO 15489
IT Strategy	■	■	■	■	
Program Management	■	■	■	■	■
Information / Cyber Security	■		■	■	
Service Delivery and Operations	■		■	■	
Supplier / Third Party Management	■	■	■	■	■
Data Management	■	■			■
Systems Development Lifecycle	■		■		
Service Continuity Management	■		■	■	
Financial Management		■	■	■	
Talent Management	■		■	■	

Developing a common IT Risk Management Framework will limit an agencies need to be reactive to new regulatory and contractual requirements

Identify the types of data you have

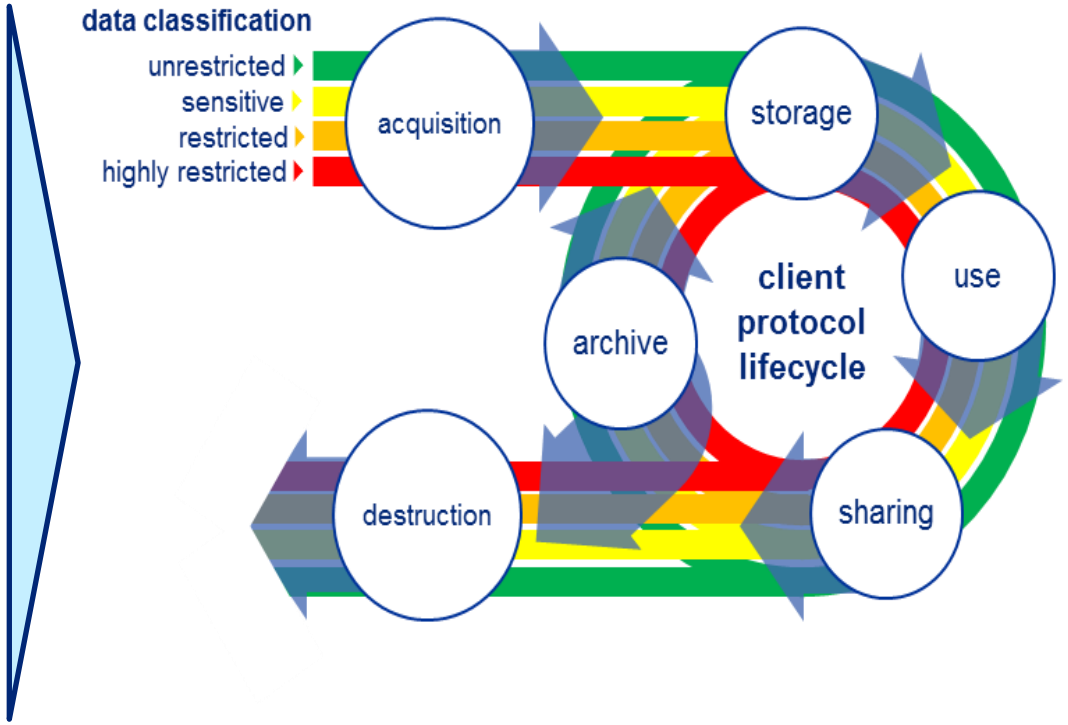
You need to know what you have, in order to protect it

Clients ask for protection of their data to protect their customers' private information; There are some common challenges, that agencies have based on the variety of data they receive from the clients

- **Unstructured information is stored in a variety of places**
  - E-mail messages
  - Word processing documents
  - Spreadsheets, electronic images
  - Presentations, images and so on.

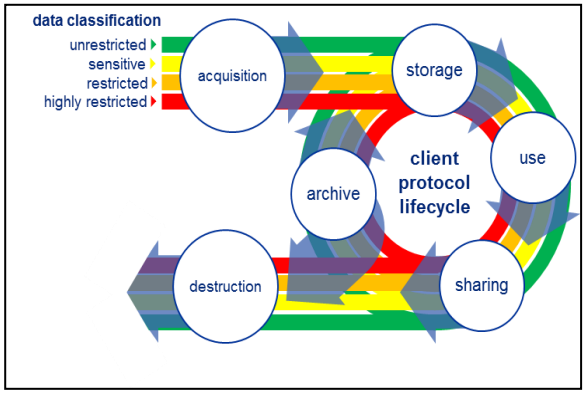
- **Sensitive & critical content not dealt with properly –**
  - All data is treated the same (An important e-mail message from one executive to another and an MP3 music file downloaded by a summer intern have the same safeguards)

- **Unknowns can cause a security risk -** Not knowing what is inside files can create security risks because an organization could inadvertently mishandle sensitive or confidential material.



Know where your data is, and the controls in place to protect it

Data Mapping is a comprehensive approach for documenting the flow of customer and employee data within a business process across the data lifecycle

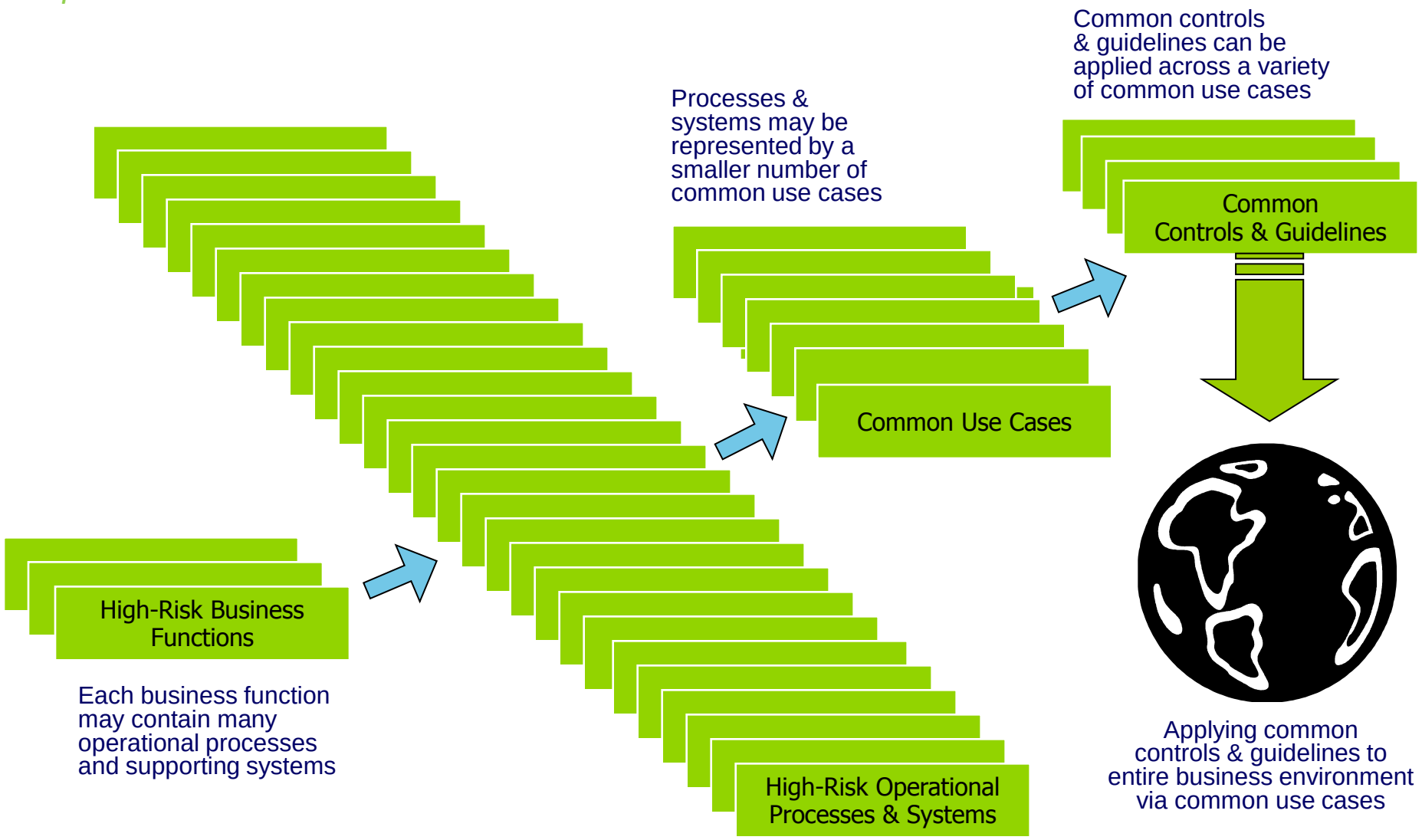


- Data Mapping presents a data centric view of data within a business process
- Data Mapping includes identification of:
  - Systems that support the business processes;
  - Users with access to personal data;
  - Data protection and privacy requirements;
  - Process specific risks; and
  - Controls and gaps
- Data mapping also includes the various channels used to share data

	Acquisition	Storage	Use	Sharing	Archival / Disposal
General Questions	Has the customer been provided a Privacy Notice?	Is data stored in a Centralized or Distributed form?	Is data usage fair and lawful?	Is data access allowed only for staff that need such access?	Is data retained longer than required?
	Has customer consent (opt-in/opt-out) been obtained ?	Is data storage distributed across network?	Is data used only for the purposes specified?	Is data only shared with third parties as necessary?	Is data disposed when its purpose is over?
	Is data acquired only for the purpose specified?	Is data-at-rest appropriately secured?	Is data limited to minimum necessary uses?	Are third-party controls appropriate?	Are data disposal mechanisms secure?

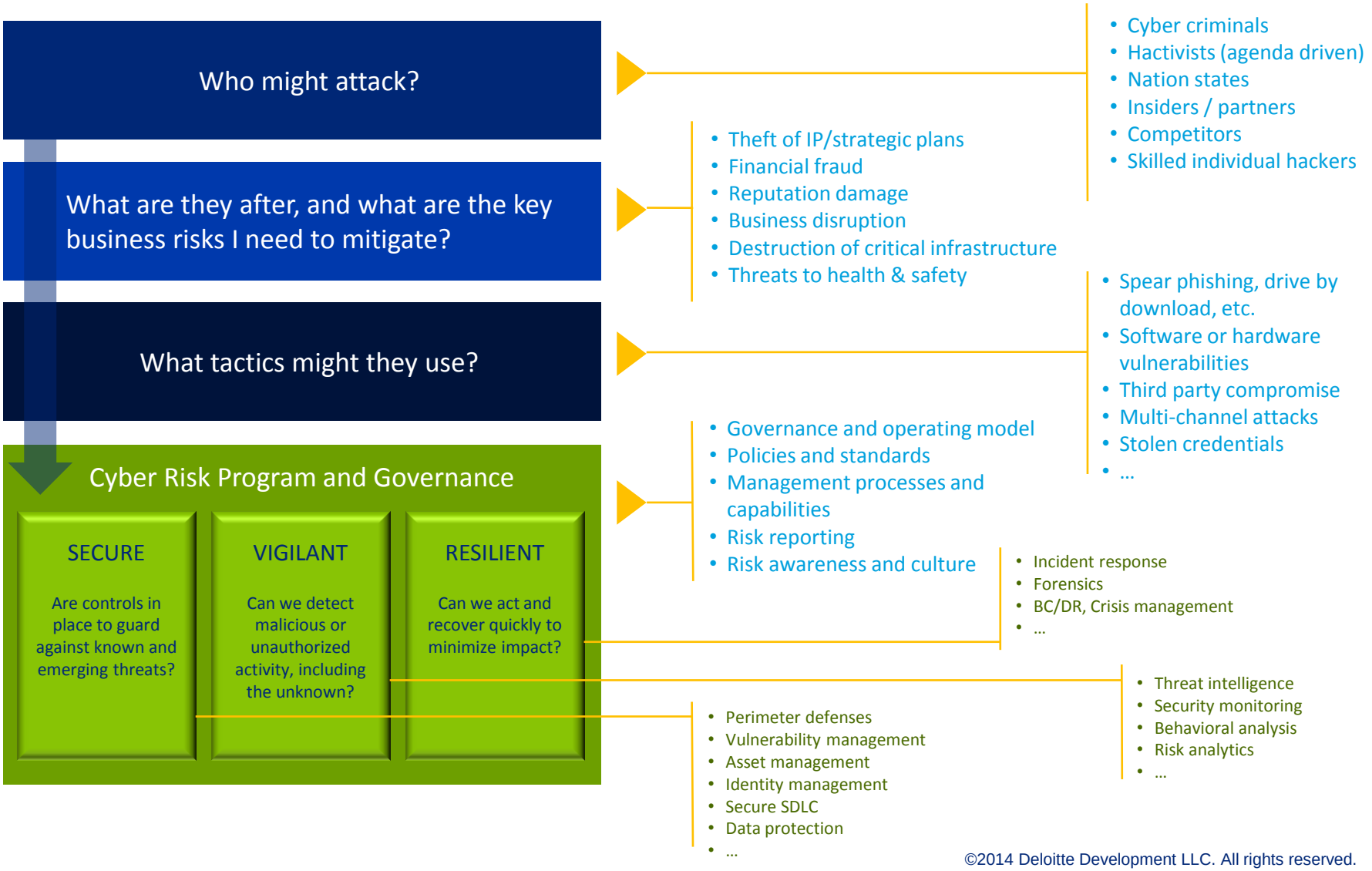
Develop Use Cases for the variety of data and processes

Identify common controls that can be used through out the organization rather than repetitive individual controls in siloed businesses



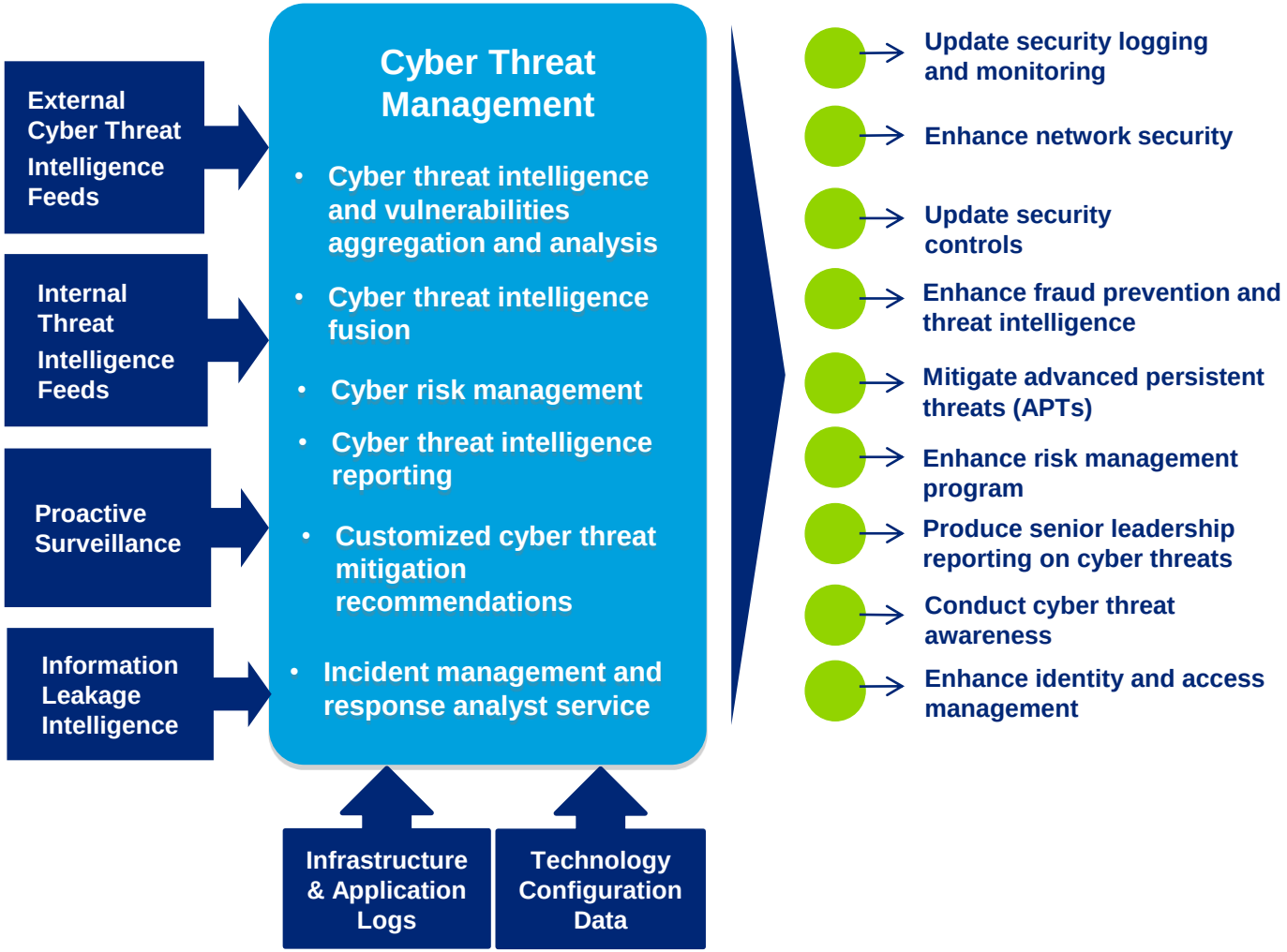
Executives must set risk appetite, and drive focus on what matters

It starts by understanding who might attack, why, and how



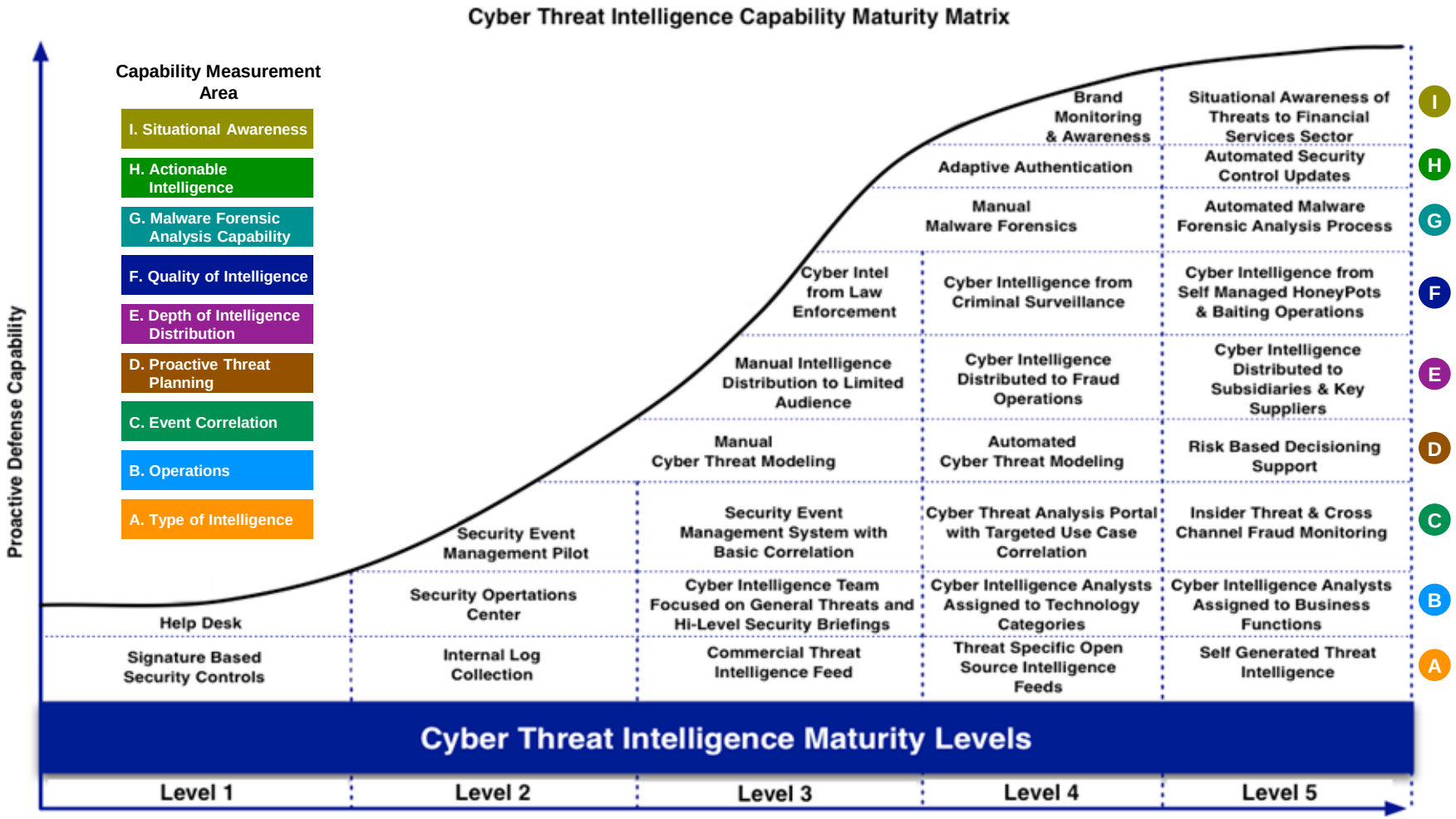
Key components of a cyber threat management program

- Conduct emerging threat research
- Establish teaming to share intelligence
- Assign threat focus areas
- Establish live, dynamic intelligence feeds
- Implement a holistic approach to cyber threat identification
- Actively track the cyber criminal element
- Implement a holistic approach to cyber threat identification
- Actively track the cyber criminal element
- Perform daily emerging threat reviews
- Maintain awareness of the changing technology and business environment
- Patch operating system, network, process and application vulnerabilities
- Deploy and maintain signature and behavioral based controls
- Produce metrics and trending data for multiple key threat indicators
- Continuously improve automation capabilities



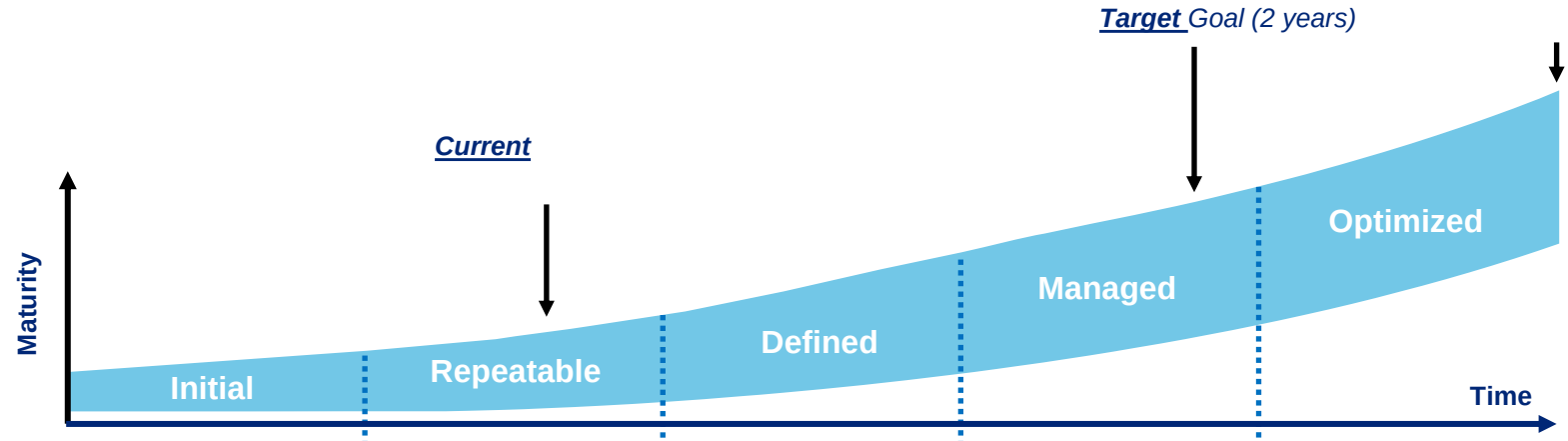
What leading class programs are doing

Where do you fit in the maturity curve?



Continuously Evaluate - Identify where you on the maturity curve and where you need to end up

Target goals and focus areas will vary by industry and company. A typical program takes 3-6 months to build/enhance and 12-24 months to fully operationalize. Investment is required to move to target maturity levels – organizations will need to make decisions based on expected benefits.



Project Types

Strategy / Program
- Align with business goals and enterprise risk objectives
- Identify key capability gaps (people, process, technology). Understand regulatory / compliance expectations
- Develop IT risk management strategy and roadmap

Governance & Operating Model
- Define operating model
- Establish business unit, IT, corporate center RACI – across multiple lines of defense

I&T Risk Management Capability Enhancement
- Implement policies and standards
- Implement processes, tools and technologies
- Establish risk monitoring, root cause and correlation processes – learning organization

Risk Reporting and Culture
- Develop IT, business and board risk reporting
- Formal training and awareness programs