A Retrospective

Presented by Jim Goldsmith
Houston ISACA
June 18th, 2015

- Multi-disciplinary approach looking at Anthem and breach details
- Includes federal and state regulation
- Demonstrate where control and framework gaps existed in the insurance ecosystem
- Document process improvements

- Event and its impact – discussion of the breach and its aftermath.
- Regulatory – Regulatory frameworks (NIST), penetration testing and National Association of Insurance Commissioners (NAIC)
- Compliance – Indiana and New York insurance departments, HIPAA
- There will be related data on the Primera and OMB breaches.

Primera cyber attack

- On May 5, 2014, Primera, a Blue Cross/Blue Shield company in Seattle, Washington became the victim of a cyber attack.
- The breach was not discovered until January 29th 2015.
- 11 million member records were compromised.
- The IT department was in a state of turmoil at the time of the breach and had been ordered to pay a $1.45 million judgement filed by current and former employees.
- The Chinese hackers compromised the system are thought to be the same ones who hacked Anthem.

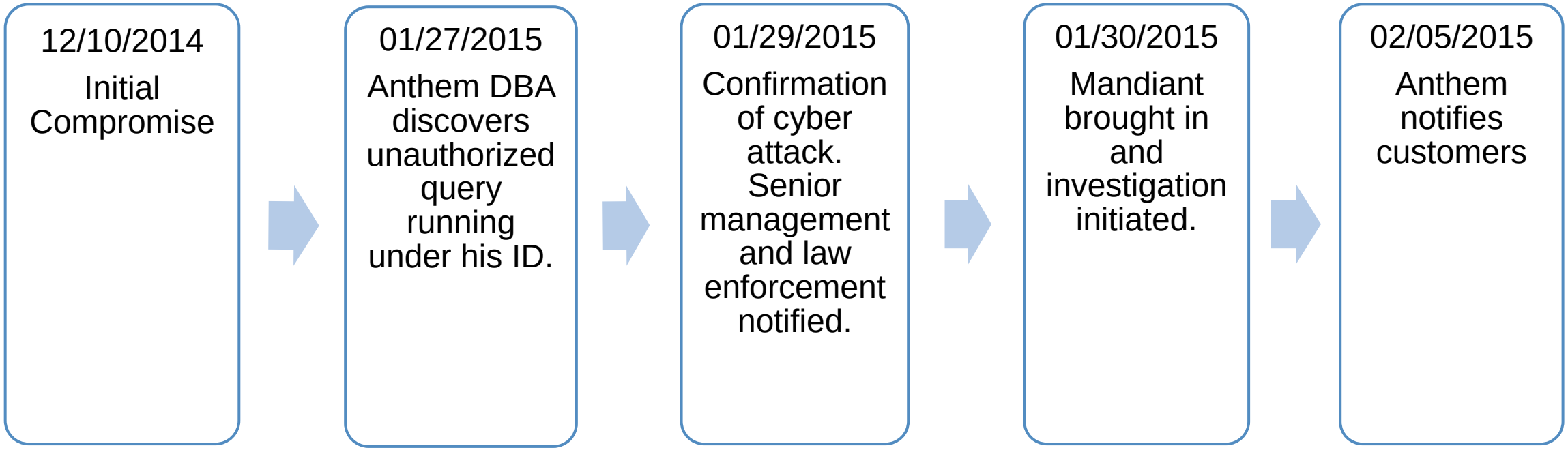
OMB Cyber Attack

- OMB had 4 million records for current and former employees were obtained.
- 11 of 47 servers lacked an authority to operate (ATO), which is a certification is required by the federal government.
- Two servers used for classified credentialing information (i.e. Top Secret) were so far from the ATO standards the Inspector General attempted to shut them down.
- Data related to background investigations for sensitive intelligence positions was obtained.
- The same Chinese hackers who were responsible for Anthem and Primera are thought to be responsible.

State-Sponsored cyber attacks

- State sponsored cyber attacks will require team work and co-ordination.
- Information sharing will be required.
- A disciplined approach will also be required.

Timeline of Anthem breach



- 80 million records dating back to 2004 compromised.
- Includes 9 to 19 million BCBS policyholders who did not have Anthem's insurance, but used the Anthem's BCBS network for out-of-area claims.
- 1/3 of the residents in Missouri (population 6 million) had PHI information compromised.

- The data at rest stored in the data warehouse was not encrypted. This was not a HIPAA requirement.
- Estimated costs are fluctuating wildly – from $100 million to a billion to 28 billion. Anthem made approximately $2.5 billion dollars profit in 2014.

Observations/Conclusions

- PII in a data warehouse. This was a lapse in their data management processes (should have been identified and the data scrambled/omitted).
- Too much data being stored. Data going as far back as ten years was stored on the database and should have been archived.
- There was no multi-factor authentication to the database (such as a key) to access the database for reading purposes.
- Consideration should have been given to encrypting data at rest.
- Network bandwidth monitoring appears to be inadequate as there should have been unusual spikes in network activity related to extraction of large amounts of data.

Regulatory

- National Association of Insurance Commissioners (NAIC) is a governing body that enables regulation of the insurance industry.
- The NAIC was using an outdated framework (Cobit 4.1) that had not changed since 2012.
- A cyber-security oversight working group in late 2014, but it had not issued any guidance prior to the breach.

Regulatory Environment

- Society Of Financial Examiners (SOFE) – Professional credentialing organization for the NAIC for financial examiners.
- Financial auditing (not operational) with emphasis based on knowledge of regulatory financial accounting and financial statement preparation.
- Supports a number of designations, including the Automated Examinations Specialist (AES).
- State insurance auditors (examiners) are effective performing statutory financial examinations
- Insurance department management is populated by individuals well versed in regulatory financial examinations.

Conclusions/observations:

- State insurance departments do not generally have the breadth or depth of understanding to adequately understand IT issues.
- The NAIC was not on top of IT environment changes indicating a blind spot in their risk management processes which was exposed as a result of this breach.

Federal/State compliance

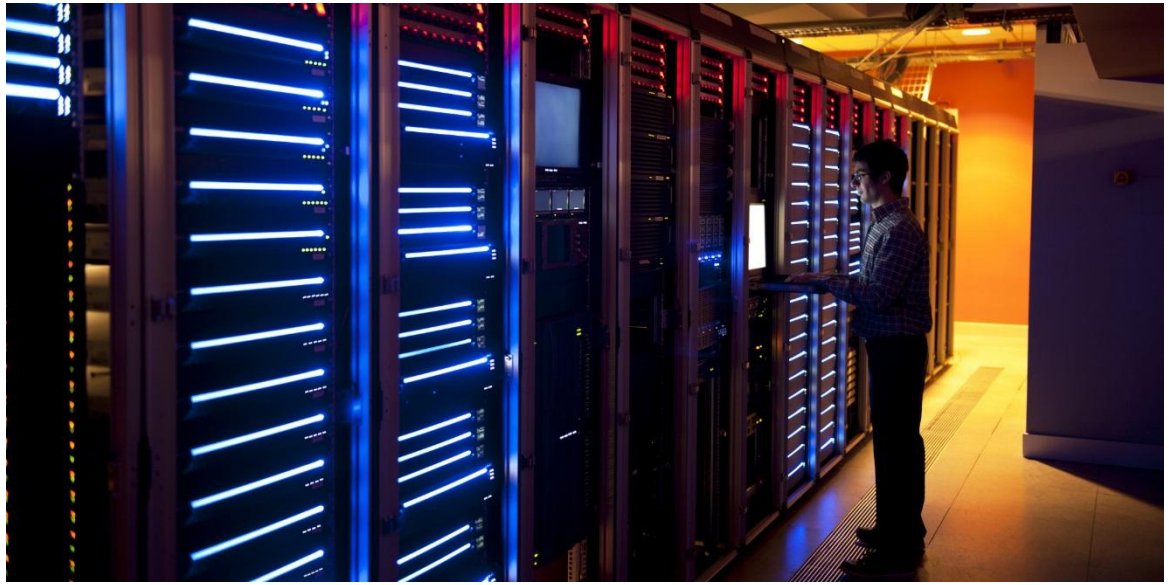
- The Office of Personnel Management Office of Inspector General performs annual scans on health insurers who are part of the Federal Health Employee Health Benefits Program.
- The OIG attempted to schedule a scan of Anthem's networks in January of 2013 and a limited-scope follow-up in 2015 and were refused.
- OIG is now seeking to amend Anthem's FEHPB contract to require such reviews in the future.
- There is no evidence that the examination team (from the state of Indiana) considered this a reportable issue.

NY Department of Financial Services report on Cyber Security

- The state of New York prepared a report on Cyber Security in the Insurance Sector, which was issued in February 2015.
- Cross-section of 43 companies, with reported assets ranging from $4 million to $403 billion and met regularly.
- Performed during 2013 and 2014.
- Statutorily required Enterprise Risk Management (ERM) reports were also analyzed.

Key Findings

- Pen Testing – 44% tested once a year, 19% quarterly and 30% tested monthly.
- Data breaches – 45% reported breaches within the past three years, including five percent who reported being breached 10 or more times.
- Only one entity provided in-depth ERM identification and analysis of cyber security risks
- 33% of organizations who experienced a data breach did not consider their data breaches significant enough to notify law enforcement.



Consequences

- Legal ramifications of the breach are still evolving.
  - As of early February, six state's Attorney's General have already filed suits as a result of alleged violations of data breach laws.
  - The NAIC announced on February 6, 2015, a multi-state examination targeting Anthem's Information Security risk management processes.

Conclusions and observations

- The lack of discussion or emphasis regards the refusal of pen testing appears to be a potential issue, not only because it was not mentioned during status meetings, but also because the NAIC has convened the targeted examination.
- Insurance companies risk management did not adequately incorporate data breach risk into their ERM programs.

Lessons learned and progress.

- NAIC creates cyber security committee (committee was actually initiated in 4th quarter of 2015) and issues regulatory principles on 4/17/2015. (http://www.naic.org/committees_ex_cybersecurity_tf.htm)
- NAIC adopts NIST Cyber security Framework on April 16, 2015 and adopts it into the Examiner's Handbook (http://www.insurerereport.com/2015/04/27/naic-adopts-cybersecurity-regulatory-guidance/) and creates an EX committee related to cyber security.

NIST Cyber Security Framework

- NIST Cyber Security framework (http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf)
- Created as a result of executive order 13636, issued February 12, 2013.
- A set of industry standards and best practices created through private/public collaboration to help organizations manage cyber security risk.

- Why NIST?
  - Non-regulatory federal agency
  - Unbiased source of scientific data and practices
  - Mission is to promote U.S. innovation and industrial competitiveness
  - Long history of successful partnerships with industry, other government agencies, and academia to address critical national issues
  - No cost framework
  - Designed to protect critical infrastructure and now used by bank regulators and now by the NAIC (insurance regulators) will have a major impact on the Financial Services sector.

Cyber Security Framework Goals

- Identify security standards and guidelines applicable across sectors of critical infrastructure
- Provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach
- Help owners and operators of critical infrastructure identify, assess, and manage cyber risk
- Enable technical innovation and account for organizational differences
- Provide guidance that is technology neutral and enables critical infrastructure sectors to benefit from a competitive market for products and services
- Include guidance for measuring the performance of implementing the Cyber security Framework
- Identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations

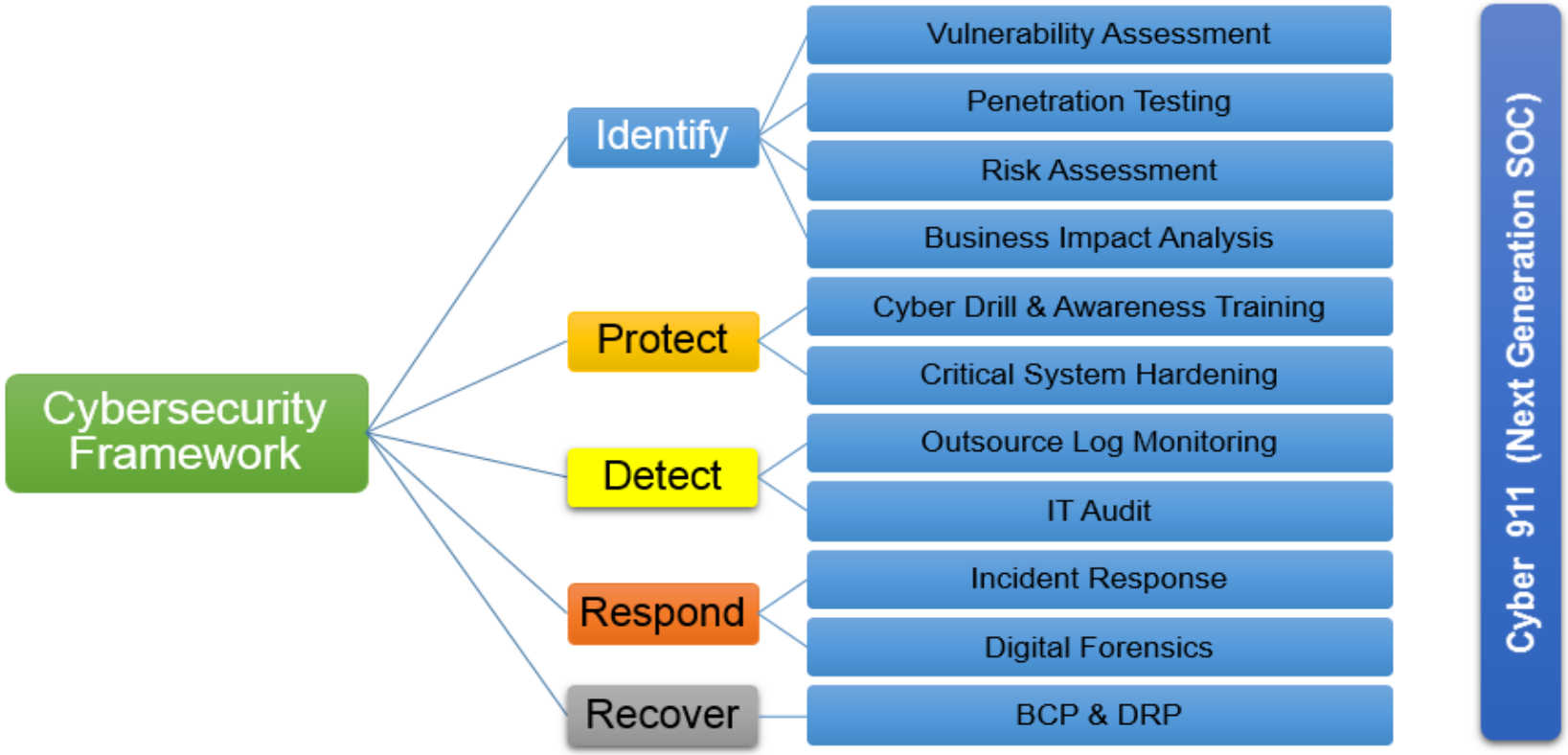
NIST Cyber Security Framework components

- Organized around a framework with three parts.
  - Framework Core consists of five concurrent and continuous functions organized by elements into a grid.
  - Maturity model with tiers to measure current capability
  - Framework profile that compares the current state to the desired state to measure gaps.

Cyber Security framework core mapping

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identity	ID:AM	Asset Management
		ID:BE	Business Environment
		ID:GV	Governance
		ID:RA	Risk Assessment
		ID:RM	Risk Management Strategy
PR	Protect	PR:AC	Access Control
		PR:AT	Awareness and Training
		PR:DS	Data Security
		PR:IP	Information Protection Processes and Procedures
		PR:MA	Maintenance
		PR:PT	Protective Technology
DE	Detect	DE:AE	Anomalies and Events
		DE:CM	Security Continuous Monitoring
		DE:DP	Detection Processes
RS	Respond	RS:RP	Response Planning
		RS:CO	Communications
		RS:AN	Analysis
		RS:MI	Mitigation
		RS:IM	Improvements
RC	Recover	RC:RP	Recovery Planning
		RC:IM	Improvements
		RC:CO	Communications

Mapping NIST Cyber Security Framework

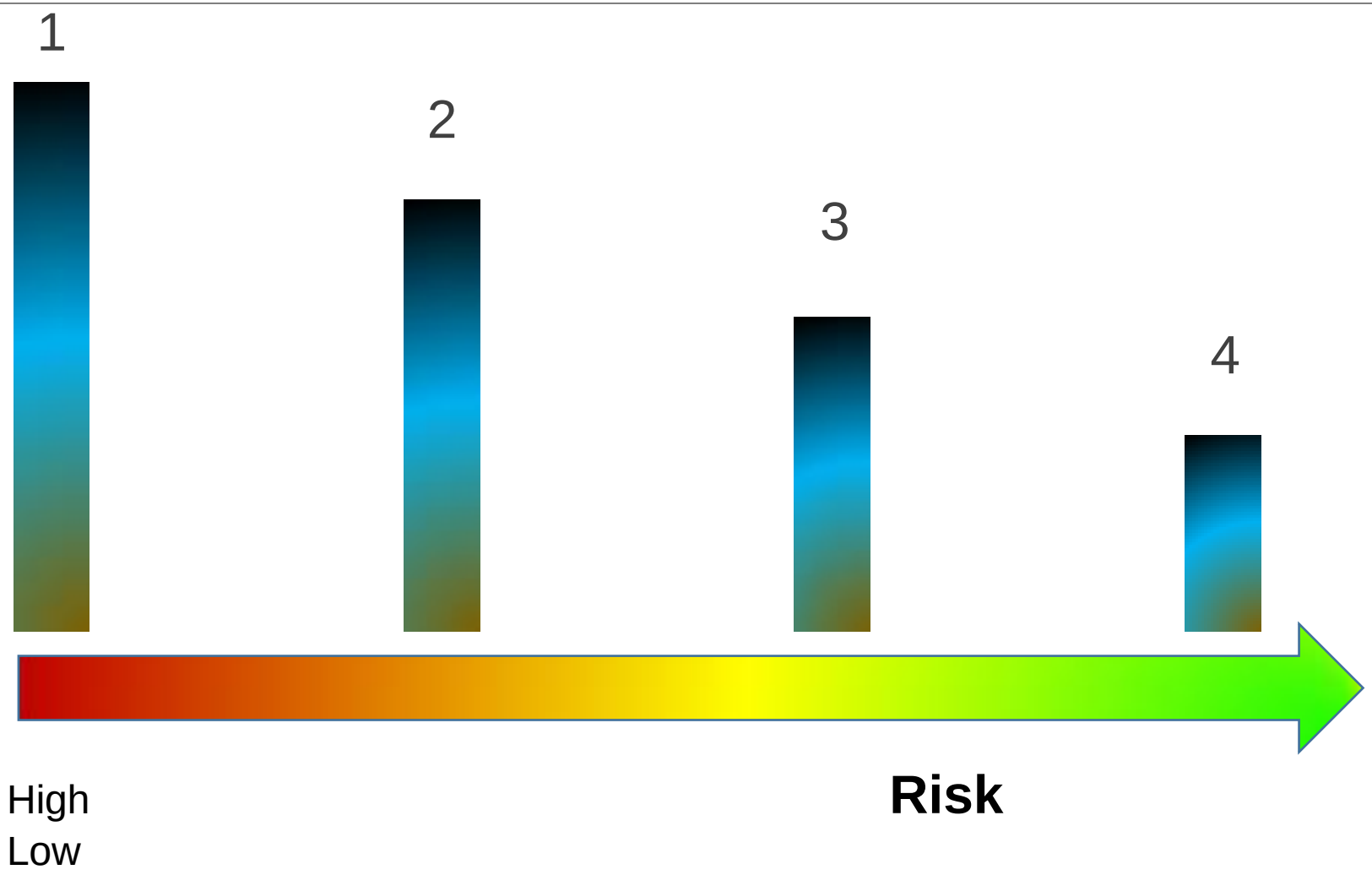


Maturity model tiers:

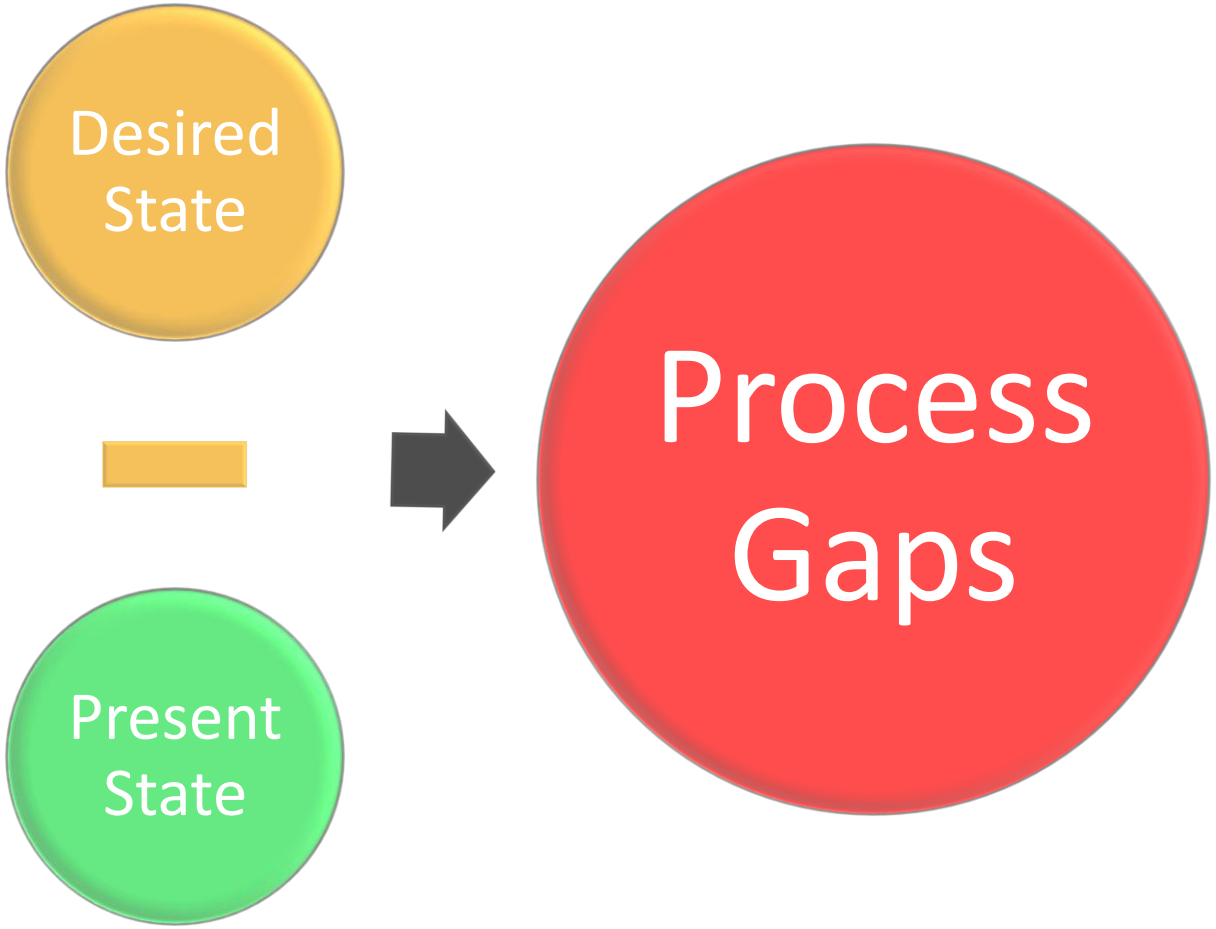
Tier 1 Low to none Tier 2 – Partial Tier 2 – Informed Tier 1 - Adaptive

Factors (bar chart colors):

Environmental **Legal and Regulatory** Institutional

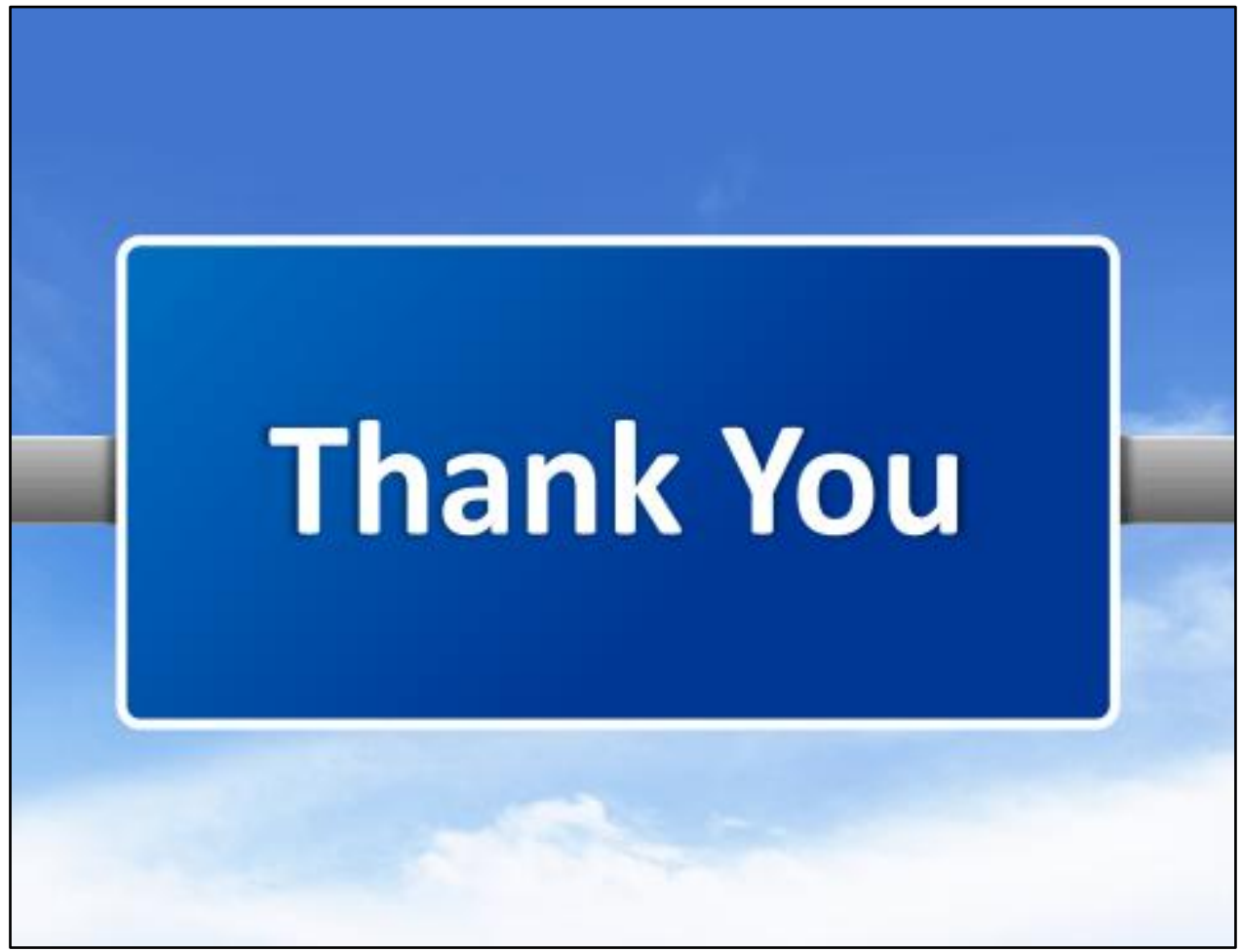


Framework Profile



Desired State – outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories.

- Conclusions:
  - The bad news:
    - Companies did not:
      - Assess the risk of a data breach and did not incorporate it into their ERM.
      - Maintain adequate borderline defenses to detect the breach
      - Appropriately classify or archive their data
    - Regulatory bodies did not:
      - Provide a framework to enable an adequate assessment of cyber security risks
      - Have adequate insight into their internal risk management processes
  - The good news:
    - Companies are:
      - Redoubling their efforts to share data breach information
      - Spending more money and increasing visibility with regards to data security and protection
    - Regulators are:
      - Redoubling efforts on training employees
      - Fostering more open communication and giving their IT Audit staff an increased role
      - Adopting a framework that will serve as a blueprint for industry to improve process performance and results.


Thank You