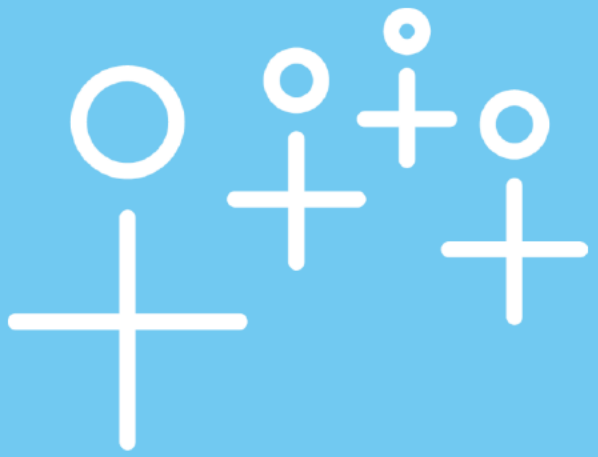
Decreasing risk across the four-legged stool: people, process, technology and insurance

Oct. 18, 2017



AHT INSURANCE

an independent member of BAKER TILLY INTERNATIONAL

BAKER TILLY

Candor. Insight. Results.

Agenda

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

- Enterprise risk management
- Cybersecurity
  - In the news
  - Main cybersecurity risks
  - Regulatory/Industry response
- Liability/Regulatory trends
- D&O and cyber liability insurance

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

Enterprise risk management

Enterprise risk management (ERM): six steps to managing risk effectively

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

Six steps to managing risk effectively

Enterprise risk management (ERM): six steps to managing risk effectively

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

> Establish an enterprise risk definition

- Improves risk management capabilities
- Increases awareness of risk tolerance as it relates to threats to financial condition and results
- Preserves and increases your financial institution's value

> Align business process risks

- Identifies risks inherent in your financial institution's critical business processes
- Encourages more effective execution of corrective actions to process deficiencies
- Improves allocation of resources to higher risk and value-oriented processes of your financial institution

Enterprise risk management (ERM): six steps to managing risk effectively

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

- Identify and evaluate key risk relationships
  - Eliminates risk management "silos"
  - Facilitates a more coordinated cost-effective approach to determining corrective and responsive actions
  - Enables long-term management of risk relationships for the benefit of your financial institution's value
- Develop a comprehensive risk assessment framework
  - Improves board and management ability to respond to key risk considerations timely and effectively
  - Helps board and management better manage operational and financial risks more timely
  - Improves understanding of historical experience and the relationship to the current risk environment

Enterprise risk management (ERM): six steps to managing risk effectively

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

> Evaluate financial account risk management

- Reduces inconsistencies and errors in financial account management
- Improves efficiency and results of the internal and external audit activities
- Enables consistent long-term financial management across all business activities
- Supports accuracy of financial reporting

> Evaluation of current and emerging threats

- Facilitates timely and effective responses to threats and opportunities
- Enhances ability to communicate timely the risk-responsive strategies and actions to critical business partners
- Fosters development of a culture that is consistently aware of economic, regulatory and other developments and how these impact your financial institution's value

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

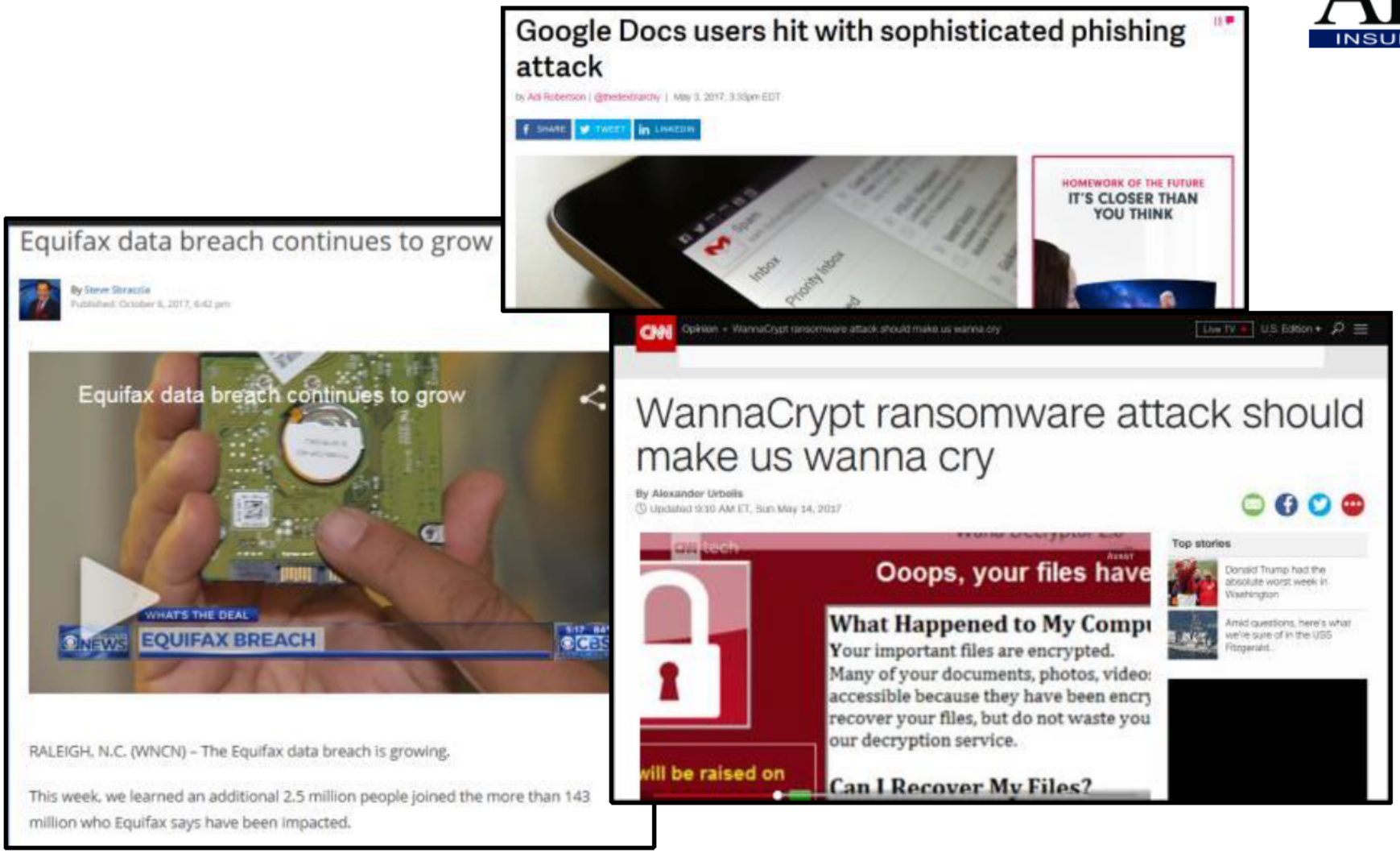
Cybersecurity

In the news

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE



Cybersecurity is a hot topic

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

83 percent

of organizations rated cyberattacks as a **top three threat.**

Three out of four

organizations have experienced at least one security incident in the past year – **60 percent were serious.**

CompTIA's 2016 International Trends in Cybersecurity

Many organizations are now wondering:

> Are we doing enough to mitigate cybersecurity risks?

> How do we protect ourselves from a data breach?

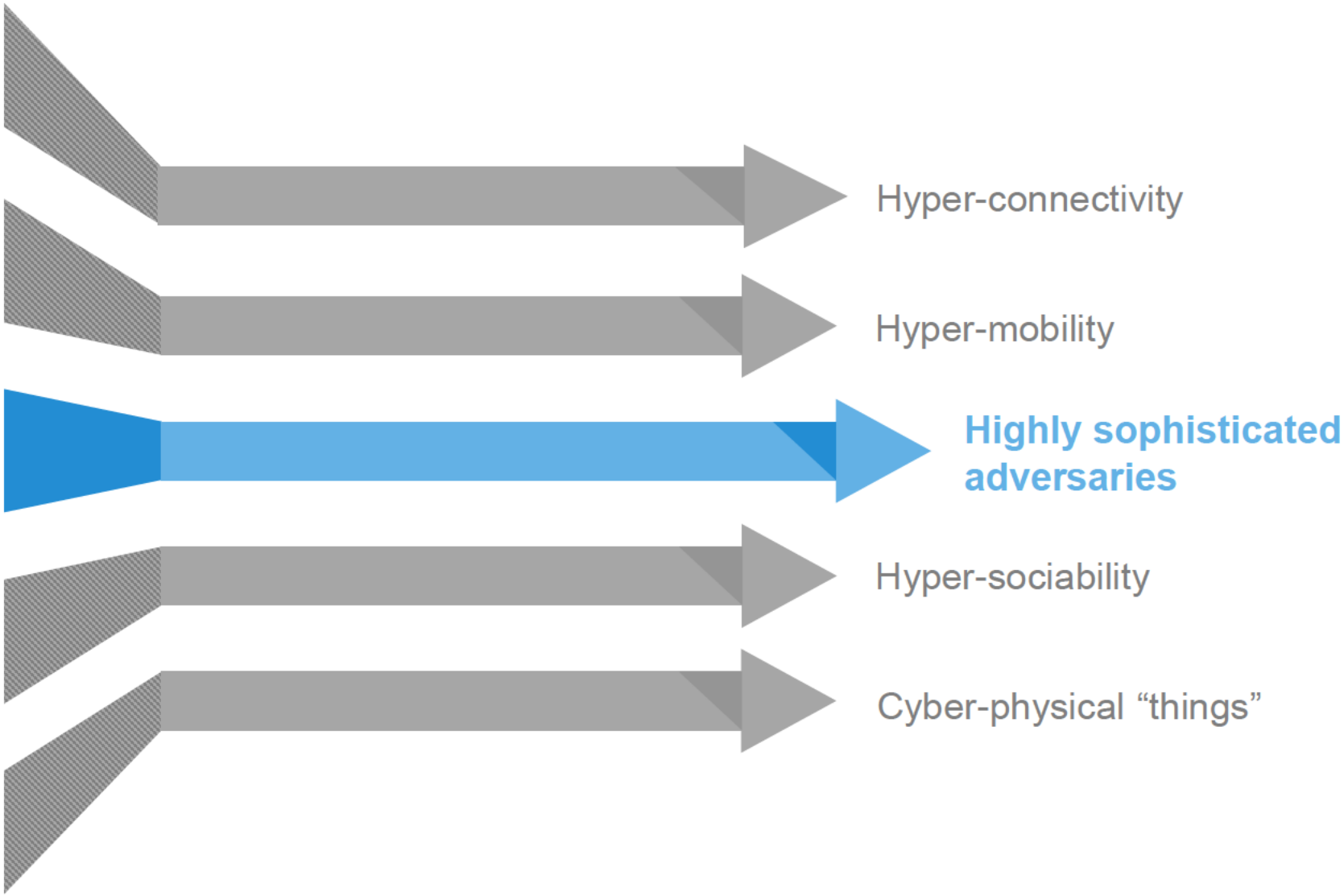
> Is our organization prepared to identify and respond to a data breach?

Society has become highly digital

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE



BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

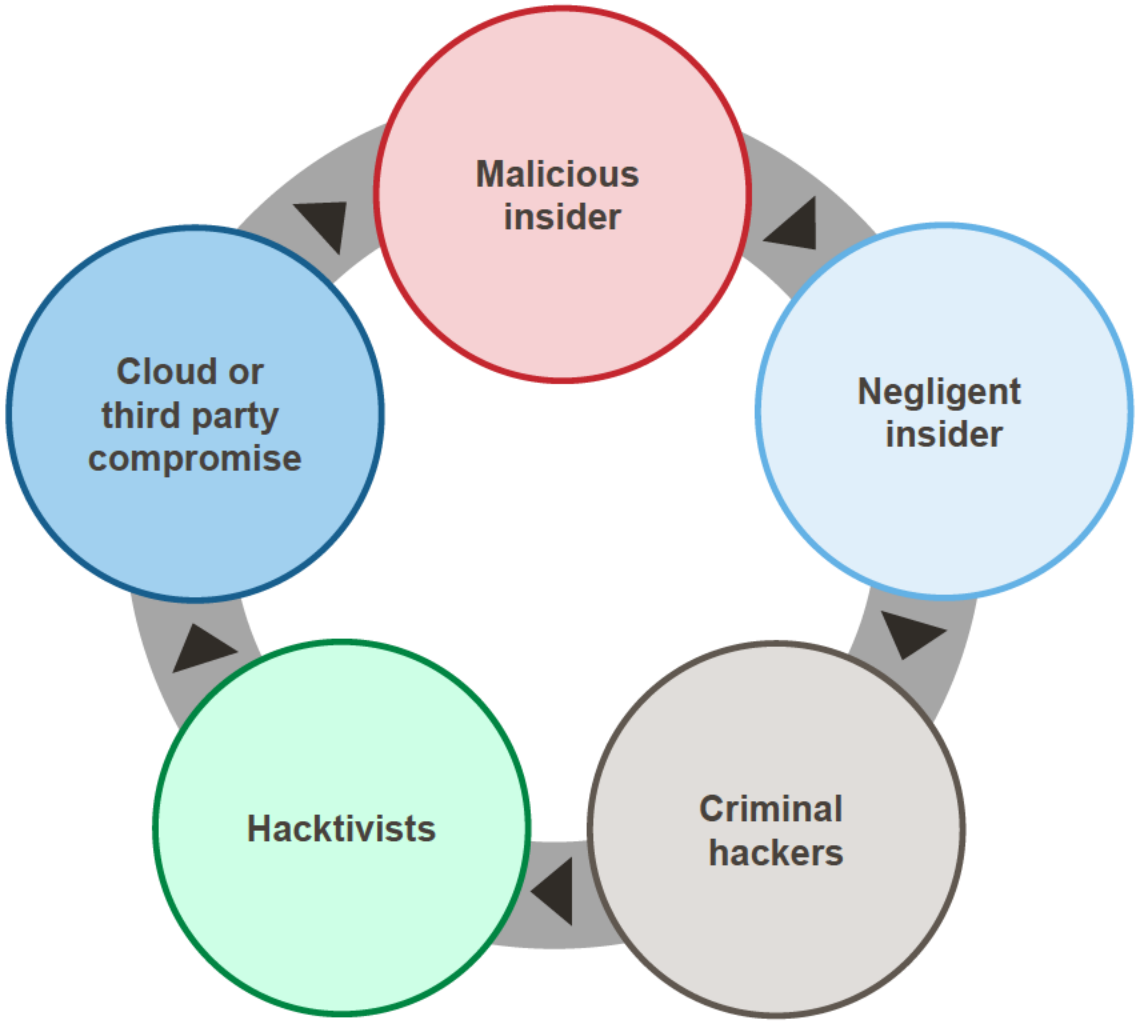
Main cybersecurity risks

The threat environment

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE



The top threats we face

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

- Socially engineered malware
- Password phishing attacks
- Unpatched software
- Social media threats
- Advanced persistent threats
- Vendor insecurity

"It is not a matter of if, but when …"

–Countless leaders and security professionals

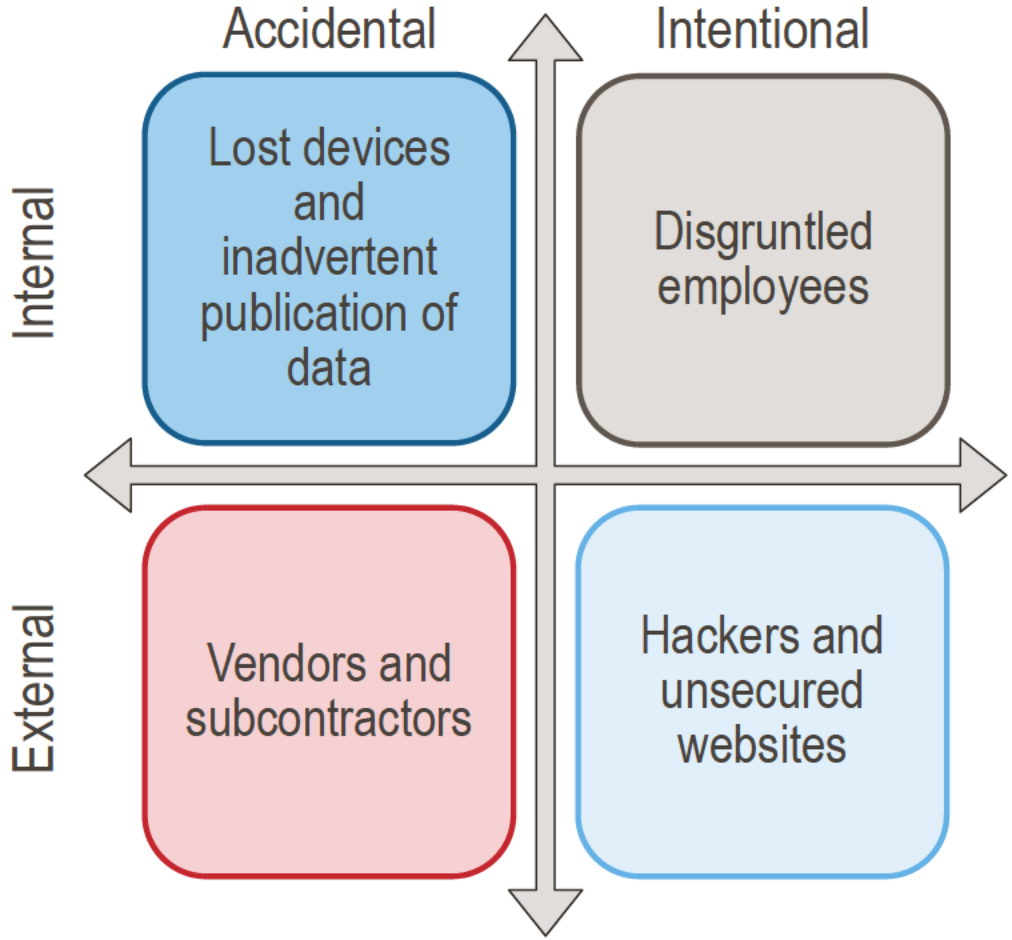
https://www.csoonline.com/article/2616316/data-protection/security-the-5-cyber-attacks-you-re-most-likely-to-face.html#tk.csoendnote

How do data breaches occur?

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE



BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

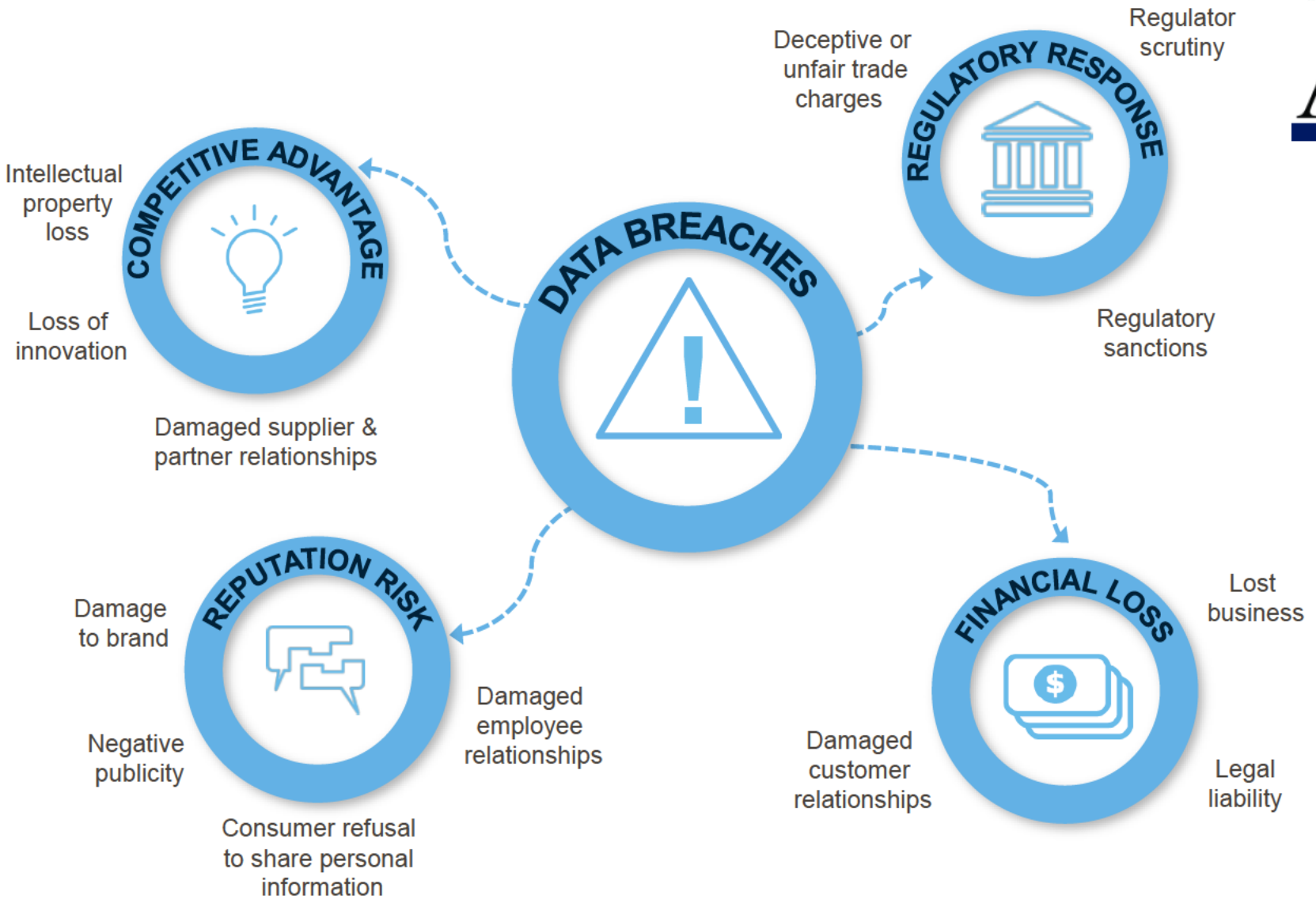
Regulatory/Industry response

Cybersecurity business risks

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

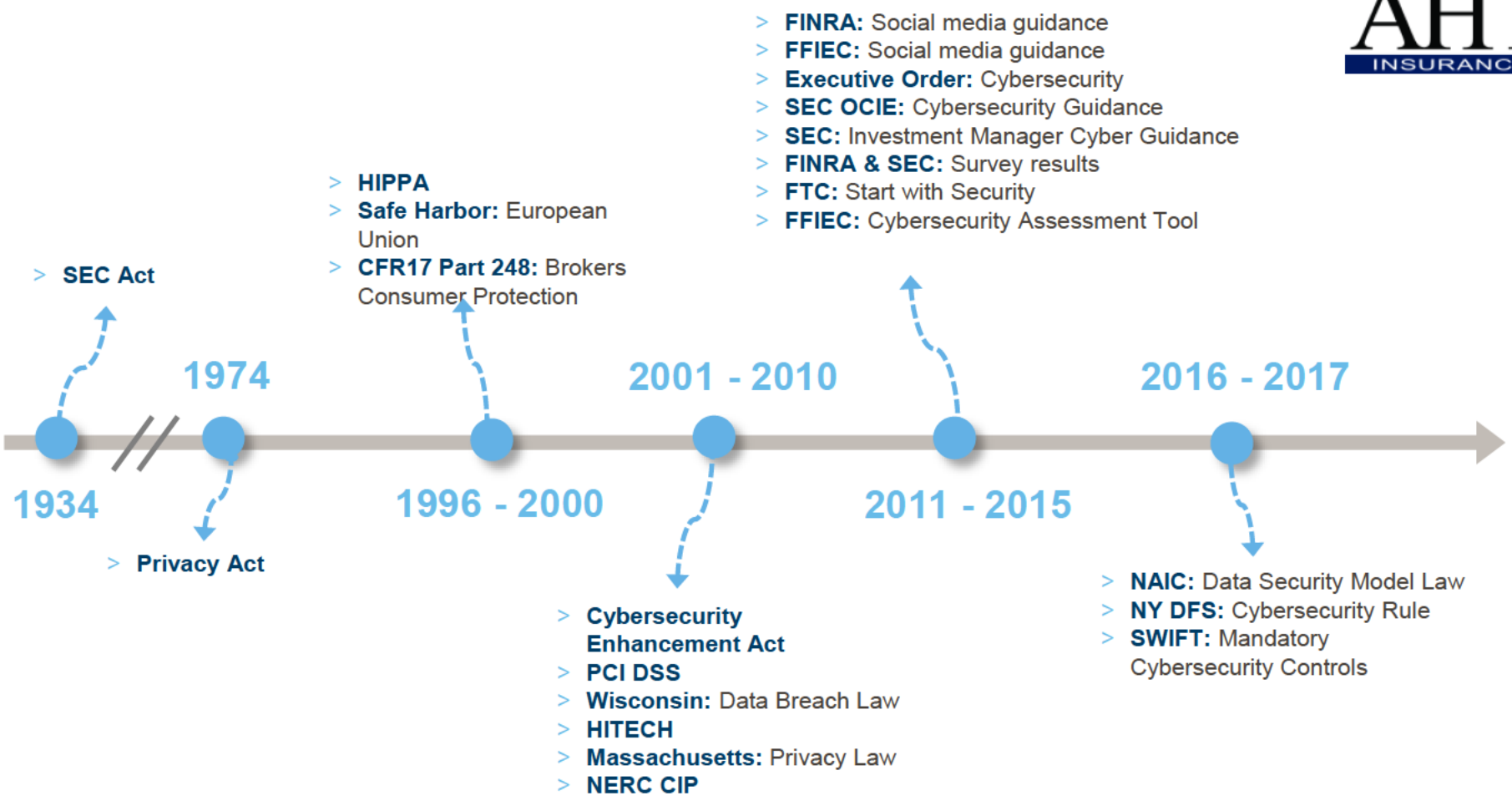


Regulatory response over time

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE



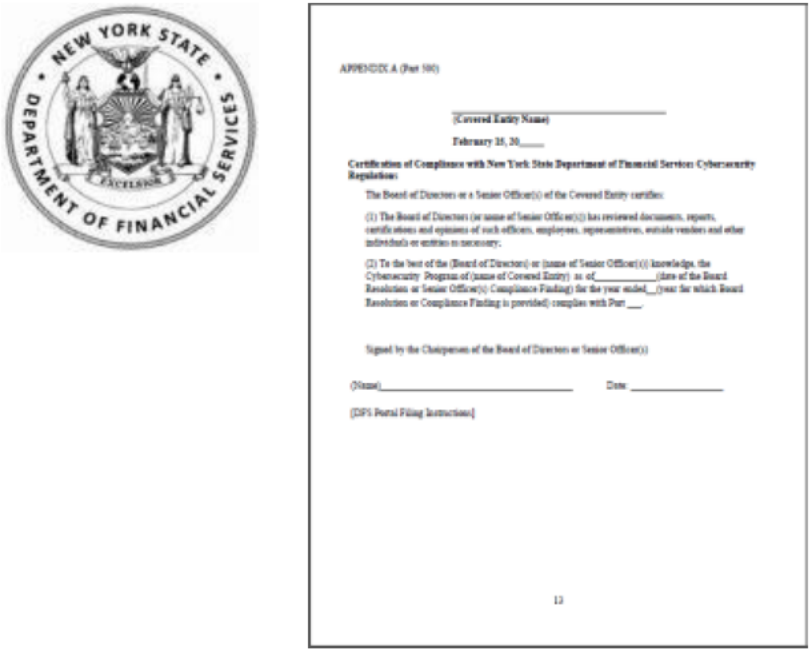
New York Department of Financial Services

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

[23 NYCRR Part 500 (Financial Services Law)]



APPENDIX A (Part 500)

_____
(Covered Entity Name)

February 18, 20___

Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulation

The Board of Directors or a Senior Officer(s) of the Covered Entity certifies:

(1) The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;

(2) To the best of the [Board of Directors] or [name of Senior Officer(s)] knowledge, the Cybersecurity Program of [name of Covered Entity] as of _____ [date of the Board Resolution or Senior Officer(s) Compliance Finding] for the year ended __ [year for which Board Resolution or Compliance Finding is provided] complies with Part ___.

Signed by the Chairperson of the Board of Directors or Senior Officer(s)

[Name]_____ Date: _____

[DFS Portal Filing Instructions]

13

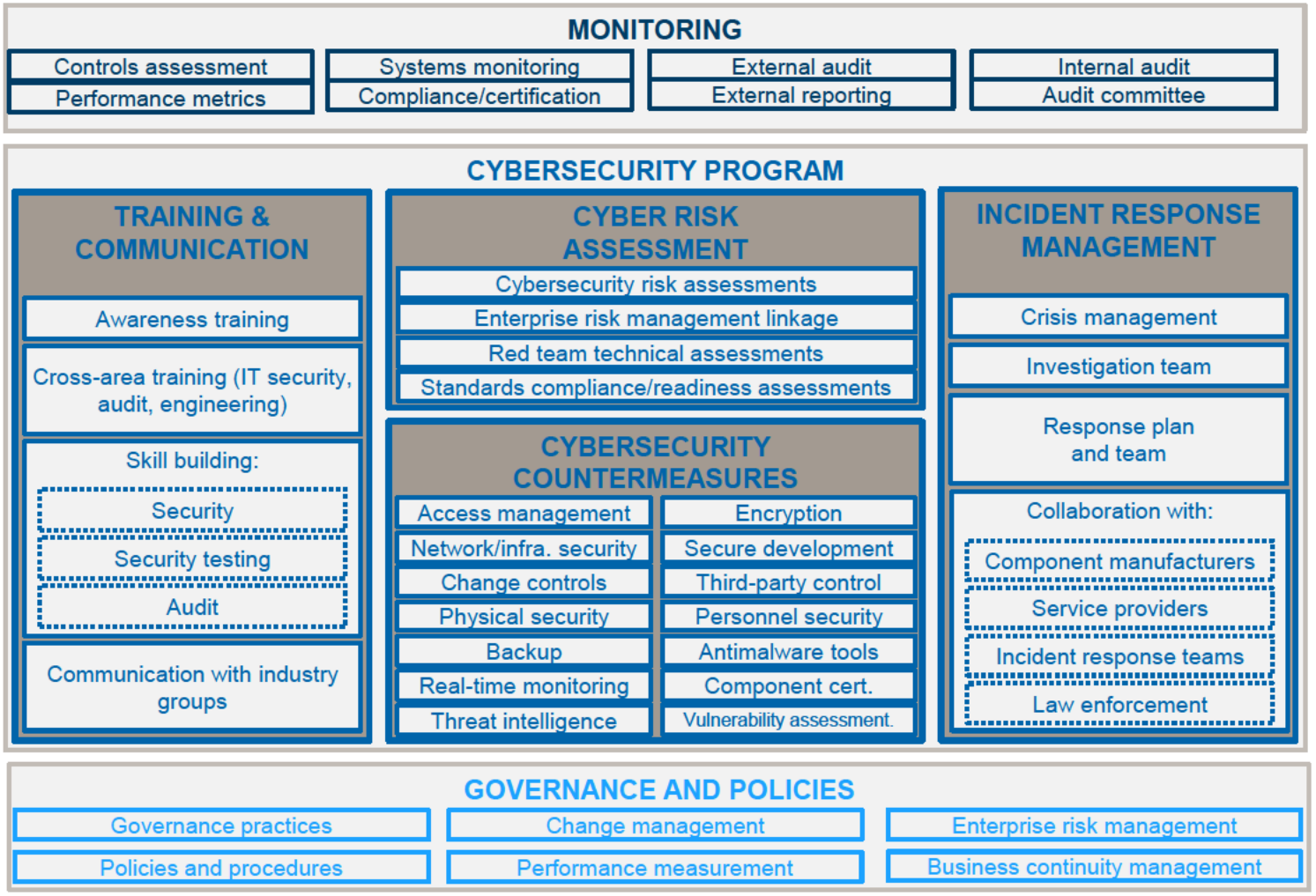
Section	Description
Section 500.01	Definitions
Section 500.02	Cybersecurity Program
Section 500.03	Cybersecurity Policy
Section 500.04	Chief Information Security Officer
Section 500.05	Penetration Testing and Vulnerability Assessments
Section 500.06	Audit Trail
Section 500.07	Access Privileges
Section 500.08	Application Security
Section 500.09	Risk Assessment
Section 500.10	Cybersecurity Personnel and Intelligence
Section 500.11	Third Party Information Security Policy
Section 500.12	Multi-Factor Authentication
Section 500.13	Limitations on Data Retention
Section 500.14	Training and Monitoring
Section 500.15	Encryption of Nonpublic Information
Section 500.16	Incident Response Plan
Section 500.17	Notices to Superintendent

What is a cybersecurity program

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE



BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

Litigation/Regulatory Trends

Litigation trends

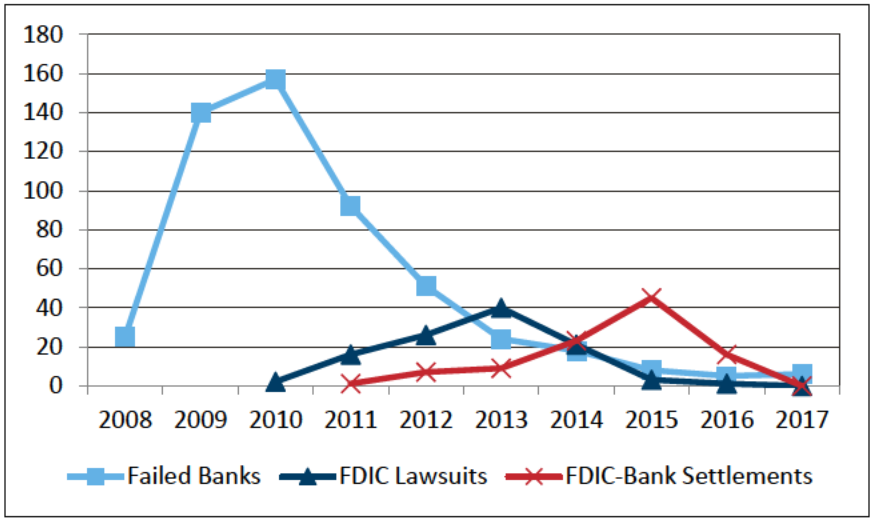
BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

- FDIC lawsuits against failed banks:
  - 2016: five failed banks totaling $277M in assets.
  - 2017: six failed banks totaling $6.3B in assets – exposure to oil and gas and rising interest rates.
- U.S. District Court for the Northern District of Georgia (October 2016) rejected FDIC's assertion that bank directors and officers (D&O) were personally liability for the approval of the majority of loans (mostly CRE loans made 2005 – 2008). Jury awarded FDIC $5M, although FDIC was originally seeking $25M.
  - The defendants took the case to trial because they have always maintained they did nothing wrong.
  - The FDIC was unable to point to any specific rule or law violated by the directors and officers in their loan approval process.

	Failed banks	FDIC lawsuits	FDIC-bank settlements
2008	25		
2009	140		
2010	157	2	
2011	92	16	1
2012	51	26	7
2013	24	40	9
2014	18	21	23
2015	8	3	45
2016	5	1	14
2017	6	0	2
Total	**526**	**109**	**101**



Regulatory trends

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

- The Consumer Financial Protection Bureau's (CFPB) recent ruling which would bar financial firms from forcing customers to agree to settle disputes only through arbitration (in lieu of lawsuit). This rule could lead to an increase in class action litigation.
  - House vetoes ruling 7/26/17 – currently in Senate (requires majority vote)

Regulatory trends

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

- The New York Department of Financial Services' (NY DFS) cybersecurity regulation applies to all financial institutions subject to the authorization of the NY DFS, regardless if the company is headquartered in New York. Exemptions include national banks, federal branches of foreign banks and some smaller insurance entities.
  - Documentation of cybersecurity program and incident response policy. Risk assessments of such policies are due by March 1, 2018.
  - CISO or equivalent is required. Also continuously trained cybersecurity personal (or third party) required.
  - Limit access privileges and periodically review those privileges.
  - Notify NY DFS superintendent within 72 hours after it determines an act/attempt was made to gain unauthorized access.

Insurance implications of NYDFS & GDPR; (***Notification costs, Forensics, Regulatory fines & penalties & Punitive Damages Wrap***)

Regulatory trends

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

- General Data Protection Regulation (GDPR)
  - Penalties up to €20M or 4 percent of global annual turnover (i.e. revenue)
  - Create a data protection plan
  - Hire or appoint a data protection officer (DPO)
  - Incidence response plan within 72 hours of breach

Insurance implications of NYDFS & GDPR; (***Notification costs, Forensics, Regulatory fines & penalties & Punitive Damages Wrap***)

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

D&O and cyber liability insurance

Basic insuring clauses of a D&O policy: insuring clause A

BAKER TILLY

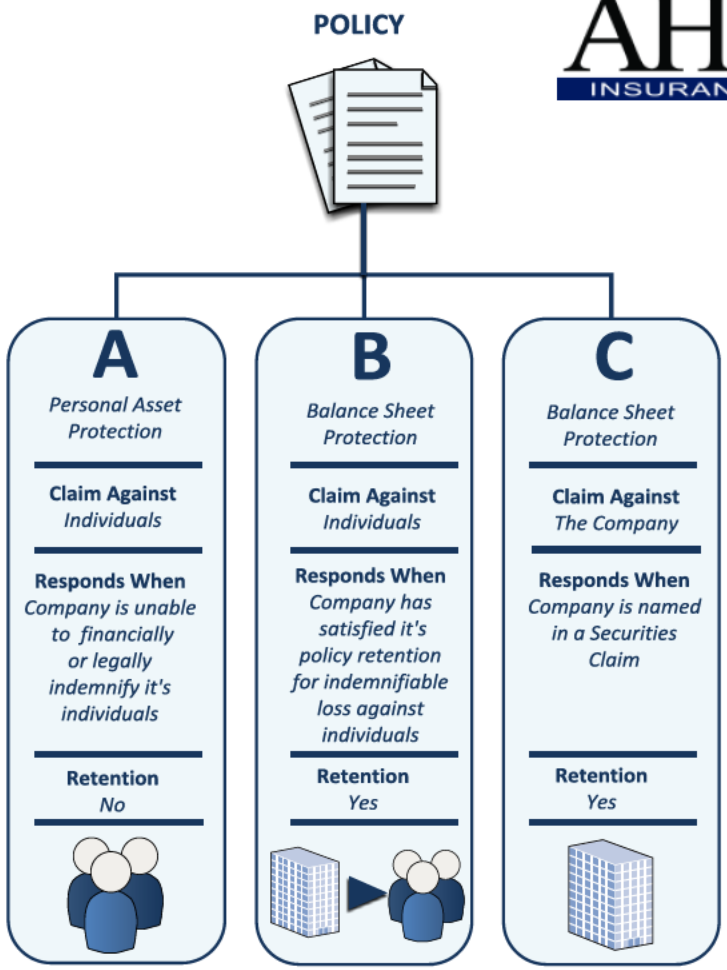
Candor. Insight. Results.

AHT INSURANCE

The directors and officers (D&O) liability policy is broken down into three basic coverage sections:

> Insuring clause A

- This section of the policy is for claims made against individual directors, officers and employees of the company.
- It offers personal asset protection for the individuals.
- This coverage provision is for non-indemnifiable loss only.
- These are claims where the company cannot legally or financially indemnify its individuals.
- This could occur during bankruptcy (financially unable) or for a derivative suit (legally unable).
- New coverage enhancements are also now advancing defense costs to individuals when the company wrongfully or rightfully refuses to indemnify.



Basic insuring clauses of a D&O policy: insuring clause B

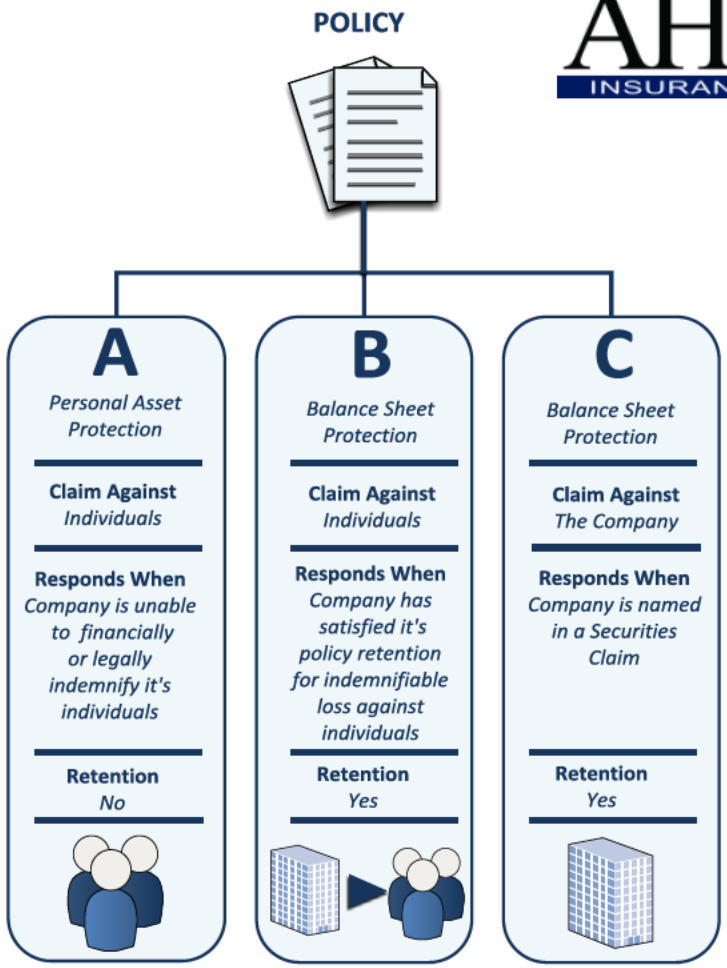
BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

The D&O liability policy is broken down into three basic coverage sections:

- Insuring clause B
  - This section of the policy is for claims made against individual directors, officers and employees of the company, where the company can and will indemnify.
  - It offers balance sheet protection to the entity.
  - This coverage provision is for indemnifiable loss only and is first subject to the applicable retention.



Basic insuring clauses of a D&O policy: insuring clause C

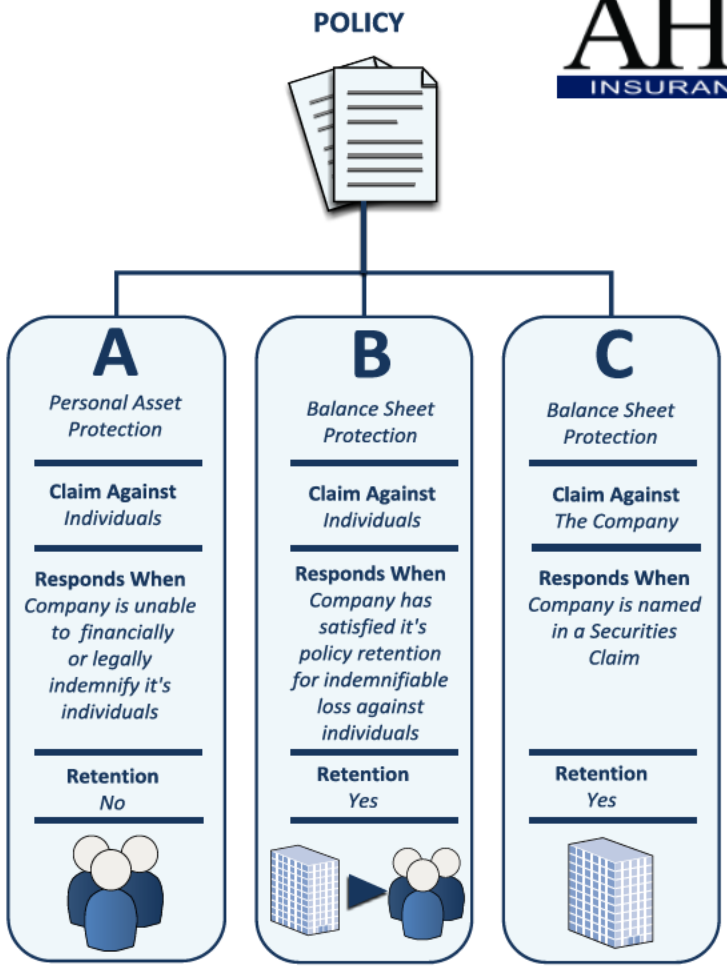
BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

The D&O liability policy is broken down into three basic coverage sections:

- Insuring clause C
  - This section of the policy is for claims made against the company directly.
  - It offers balance sheet protection to the entity.
  - The coverage provision is commonly for securities claims only, and is subject the applicable policy retention.



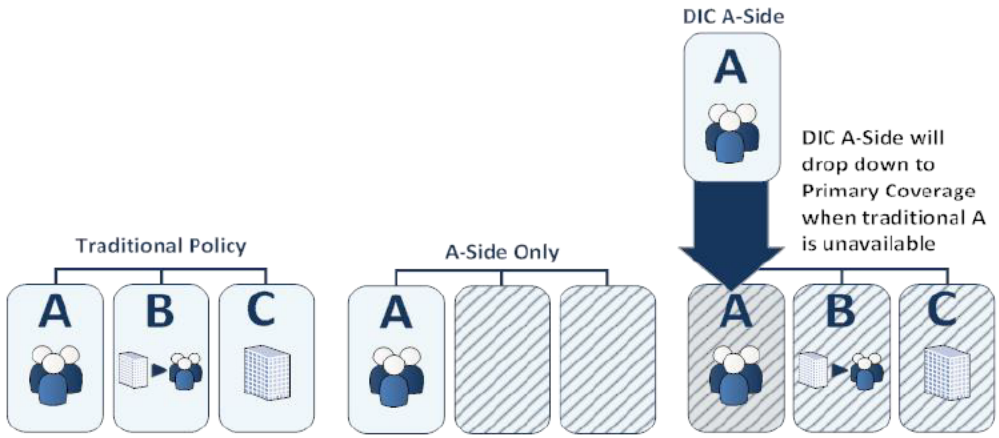
Advantages of a separate DIC A-side policy

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

- About 15 years ago, companies began purchasing a separate policy and separate limits only for the protection of the individual directors and officers of the company. This shift in purchasing coincided with the rise of shareholder derivative demands being settled in a stand-alone manner without being consolidated with the class.
- The fear was that a class action could be settled first and potentially use the entire tower of insurance; leaving the individuals without the proper protection to settle a derivative demand action. Due to the nature of a derivative action, in most cases the company cannot indemnify a settlement, so without insurance the individuals would be personally liable.



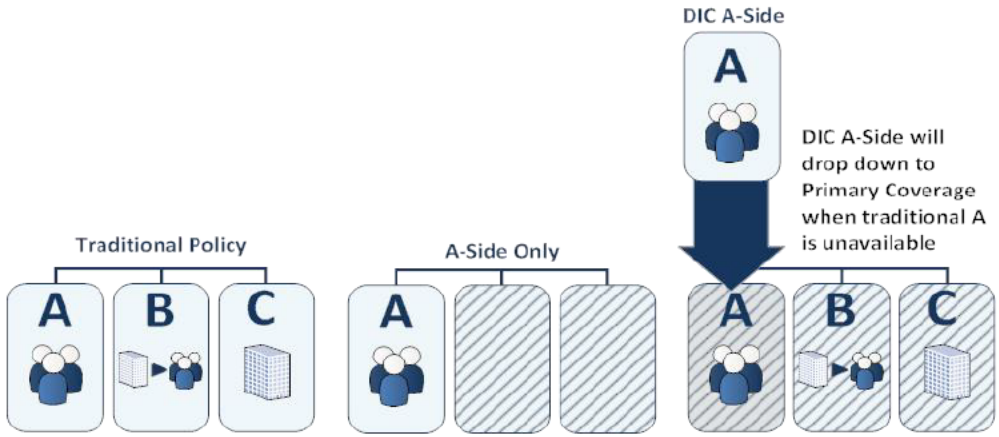
Advantages of a separate DIC A-side policy

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

- This policy provides excess ("follow form") A-side coverage on exhaustion of underlying insurance, but also drops down as primary in many scenarios:
  - Insolvency of underlying carrier(s)
  - Rescission of underlying policy(ies)
  - Wrongful refusal to indemnify (improper denial of coverage)
  - Denial of coverage where DIC A-side policy provides broader coverage
  - Company refuses to answer indemnification requests
  - Broader coverage with limited exclusions



Sample renewal process: 2017 recommended timeline

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

Date	Action
September 2017	**Renewal strategy meeting:** Review current program, limits benchmarking, carrier quality and renewal recommendations.
October 2017	**Information gathering and initial submission to D&O markets:** > Send blank applications along with copies of last years completed application (as reference). > Send conglomeration of publicly available information (submission) to 15-25 insurance carriers (A.M. Best rated A- or better).
Mid-November 2017	**Coordinate/Host carrier meetings/call:** You would provide a similar presentation as you would for an analyst. The call begins with a general overview of the company operations, recent results and any changes in the past 12 months. At the end the underwriters would ask any questions they feel they need more details. The benefits of this meeting include, but are not limited to: > Generate a personal connection with the underwriting community so they are underwriting not just on what they read in the filings. This would also be good in the event of a claim. > Limit the underwriters ability to ask for additional information in their quotes thus streamlining the binding process. > Take advantage of the competitive influences in the marketplace as the underwriter will see their competitors across the proverbial table.
Early-December 2017	**Follow-up communication to carriers:** Obtain primary premium indications and resolve any open questions/issues. Coordinate excess options.
Mid-December 2017	**Final renewal presentation meeting and binding orders:** Ensure expectations have or will be met. Discuss the need, if any, of premium financing.
Dec. 31, 2017	**EXPIRATION DATE – Confirm binder obtained from all carriers.**
+1 – 2 days	Confirmation of insurance, include invoice and confirmation letter.
+14 – 20	Confirm payment received or down payment, if financed.
+60	Policy issuance.
+90, +180, +270	Quarterly contact meeting. Discuss: > Possibility of mid year strategy meeting or underwriter visit. > Claims management. > Litigation activity or claims trends in the industry sector.

D&O liability: top 10 enhancements

BAKER TILLY

Candor. Insight. Results.

AHT INSURANCE

- Definition of claim should be as broad as possible
- Update the definition of loss to include pre-judgment and post-judgment interest, regulatory costs (Sarbanes-Oxley and Dodd-Frank) and most favorable venue
- Notice provision – ASAP with limited people who can provide notice
- Investigative costs coverage sublimit
- Limit definition of application to past 12 months filings
- Order of payments
- Add non-rescindable language and limit the imputation of knowledge (severability)
- Insured versus insured carve-backs for:
  - Creditors committee and bankruptcy trustee
  - FDIC
  - Whistleblowers, prior board member and foreign equivalents
- Limit when insurance carrier can cancel policy
- Limit the threshold of the conduct exclusions (fraud and personal profit)

Disclosure

The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.

Tax information, if any, contained in this communication was not intended or written to be used by any person for the purpose of avoiding penalties, nor should such information be construed as an opinion upon which any person may rely. The intended recipients of this communication and any attachments are not subject to any limitation on the disclosure of the tax treatment or tax structure of any transaction or matter that is the subject of this communication and any attachments.