Let’s talk about…

The new wave of cybersecurity regulation: What are the risks and how will they affect your examination

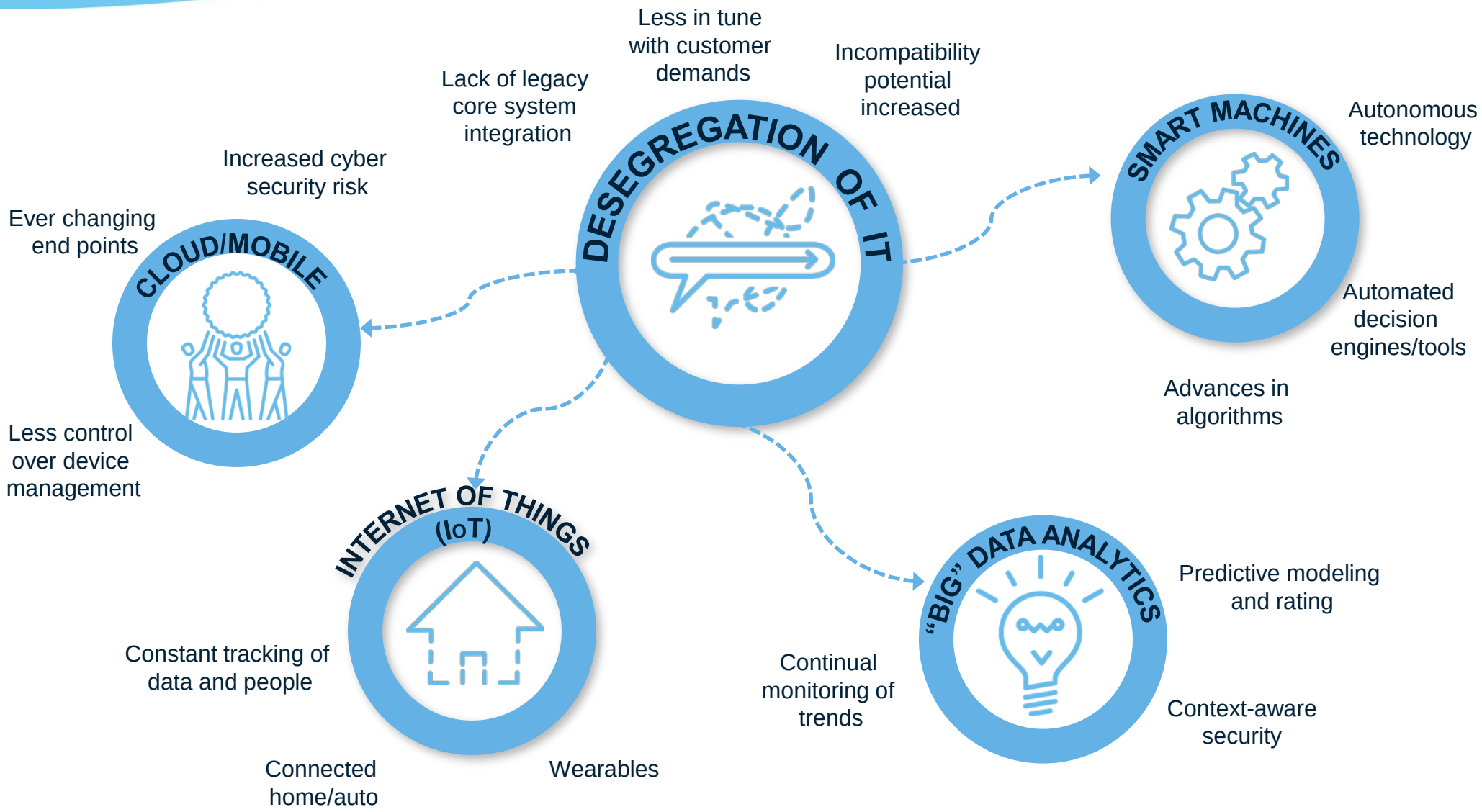
BAKER TILLY

Candor. Insight. Results.

Information technology (IT) trends

BAKER TILLY

Candor. Insight. Results.



Agenda

BAKER TILLY

Candor. Insight. Results.

1) Introduction to cybersecurity terminology

2) Emergence of cyber attacks in insurance
   - > Case Study

3) NAIC update and examination impacts

4) Cybersecurity program considerations

5) Questions and conclusion

Types of organizations

BAKER TILLY

Candor. Insight. Results.

State sponsored cyber espionage groups

> We have enemies; they don't like our national policies and want to destabilize our economy; aka cyber terrorism; cyber warfare

Cyber criminals

> Organized and run like a business, focused on the profit motive

Hacktivists

> They mess up your stuff just because:
  - they don't like you
  - they don't like your mission
  - they can

Cybersecurity terminology

BAKER TILLY

Candor. Insight. Results.

- **Advanced Persistent Threat (APT):**
  An Internet-based attack typically organized by a group of individuals with significant resources, such as organized crime or a rogue nation-state.

- **Campaign:**
  A set of activity (or incidents) carried out by Threat Actors using similar specific techniques.

- **Malware:**
  Malicious software or code that typically damages or disables, takes control of, or steals information from a computer system. Broadly includes viruses, worms, Trojan horses, backdoors, spyware, and adware.

- **Threat actor:**
  An individual or group involved in malicious cyber activity.

- **Spear phishing:**
  Targeted phishing attempt that seems more credible to its victims and therefore has a higher probability of success. For example, an e-mail may spoof an organization or individual that the recipient actually knows.

- **Backdoor:**
  A backdoor is a tool installed after a compromise or network penetration to give an attacker easier access to the compromised system; bypassing any security mechanisms that are in place.

Changing cyber-risk landscape

BAKER TILLY

Candor. Insight. Results.

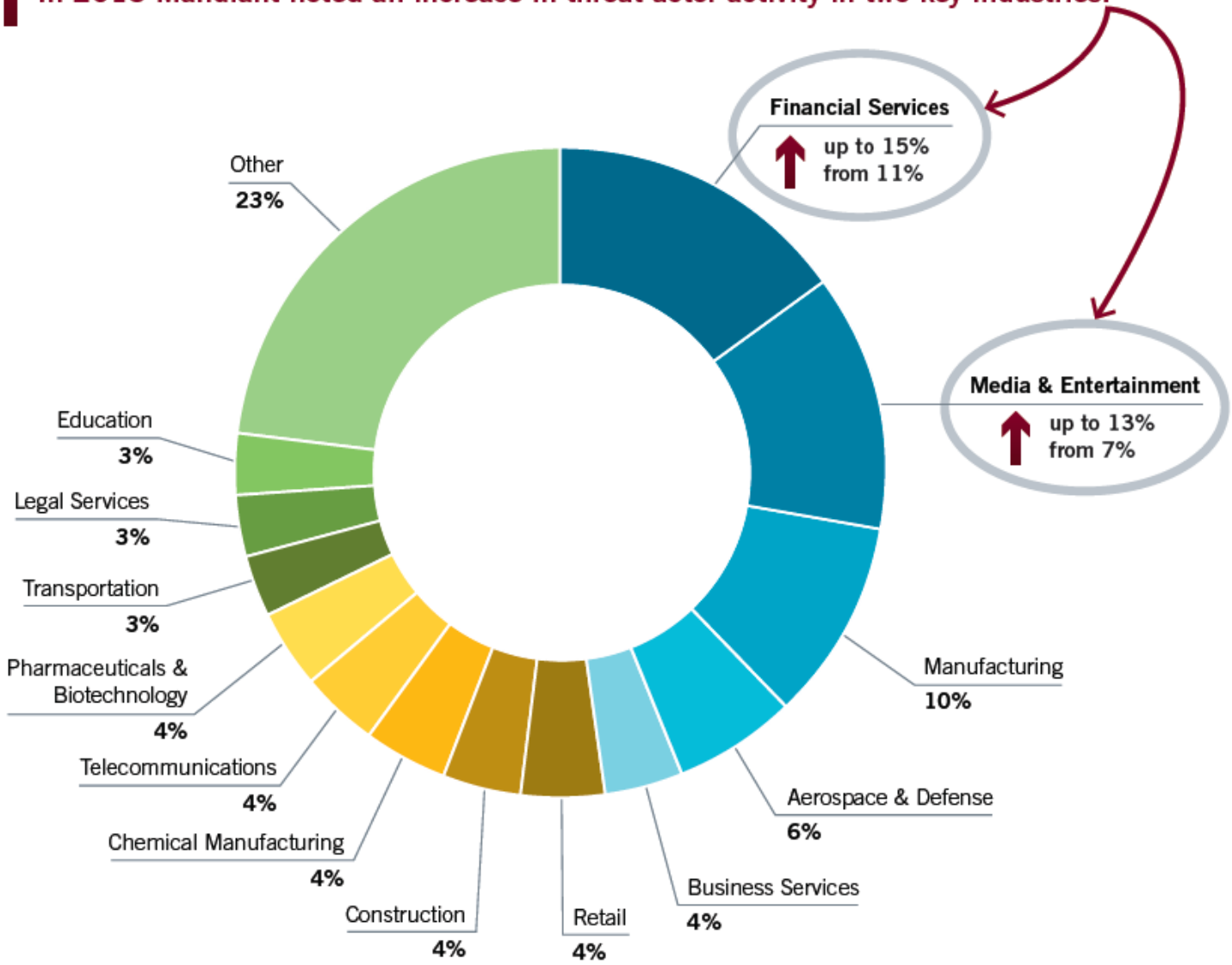
Past	Present	Implications
Mostly physical assets (plants, equipment) - relatively few digitized assets.	Highly digitized asset base (IP, financial, PII), mobile and cloud technologies.	Strong **cybersecurity controls** and processes are **required** to protect these assets.
Simple, unsophisticated attacks (e.g., web site defacement intended to embarrass).	Advanced Persistent Threats (APTs) involve high degree of complexity and sophistication; hacker "gangs" steal IP and other assets for financial gain, sometimes using ransom to hold the data "hostage".	Company must have **adequate resources and capabilities** to protect the IT environment; may even require obtaining third-party assistance or even using Managed Security Services (MSS) provider. May require working closely with law enforcement.
IT budgeted HW/SW expenditures; managed deployment and use.	Ability of IT to manage alone may be insufficient; budgets increasing.	**Budget for cybersecurity** should be rolled up at an **enterprise level**, not necessarily tied to one dept.
Relatively insulated, self-contained IT environment with limited complexity. Application support provided in-house with limited use of 3rd parties for hosting and cloud services.	Cybersecurity needs to be managed in the context of extended "digital ecosystem" involving outside stakeholders and 3rd parties/vendors.	Cybersecurity must be managed as an **enterprise-wide risk**, not just an IT issue.
Limited use of mobile data access. IT provided a restricted list of mobile device choices which provided robust security support.	Mobile user access to applications containing personal/financial data and use of BYOD is nearly commonplace.	More challenging for IT to assure security of "**end point**" devices.

Industries targeted by cyber threat

BAKER TILLY

Candor. Insight. Results.

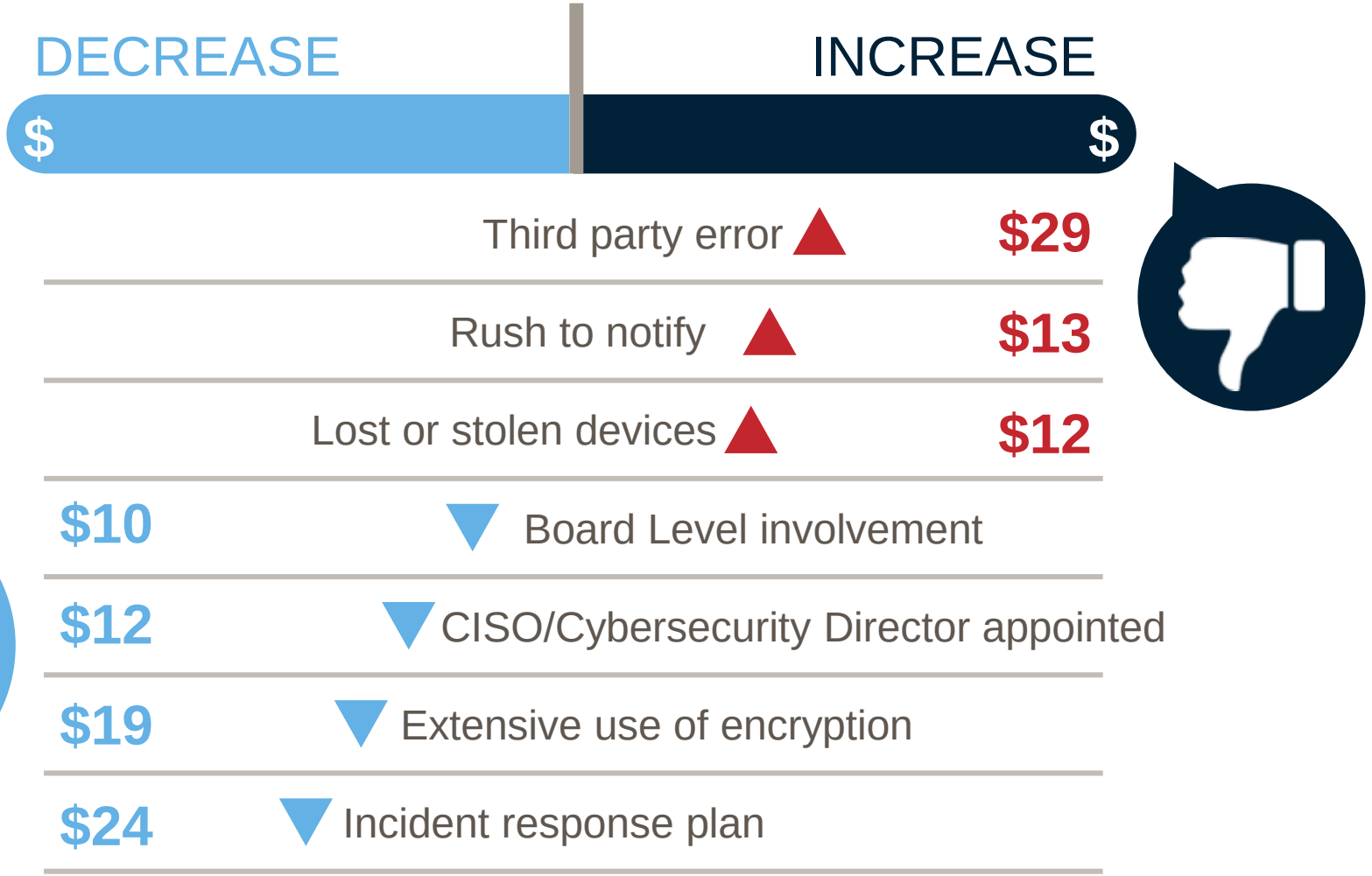
In 2013 Mandiant noted an increase in threat actor activity in two key industries.



What drives the cost of breaches?

BAKER TILLY

Candor. Insight. Results.



"2015 Cost of Data Breach Study," Ponemon Institute LLC

Recent breaches in the news

BAKER TILLY

Candor. Insight. Results.

Personal data; SSNs, DOBs affecting 25.7m accounts

SSNs, DOBs, claims data affecting 11m accounts

Personal data breach affecting 80m accounts

Breach of 700 customers' credit card information

Case study comparison

BAKER TILLY

Candor. Insight. Results.

	Anthem	Premera
Initial Breach:	April 22, 2014*	May 5, 2014
Identified Breach:	January 29, 2015	January 29, 2015
Days from Breach to Identification:	283 days	270 days
Type of Attack:	APT	APT
How accessed:	Phishing scam – *we11point.com*	Phishing scam – *prennera.com*
Records compromised (est):	80,000,000	11,000,000

*Date domain registered and distributed, Anthem cited December 2014.

Deeper dive: Anthem

BAKER TILLY

Candor. Insight. Results.

1) Thought to be generated by same espionage agency out of China – Deep Panda.

2) Was an advanced persistent threat (APT) with an internal Trojan horse – Derusbi.
   > Operated under the firewall by acquiring a normal ID & password and acting as a user.

3) At rest data was vulnerable, passwords compromised in non-multifactor authentication applications.

Source: http://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/ and NAIC CyberSecurity Taskforce meeting with Anthem CIO, 3/29/15.

Deeper dive: Anthem
How an APT works

BAKER TILLY

Candor. Insight. Results.

Source: http://resources.infosecinstitute.com/anatomy-of-an-apt-attack-step-by-step-approach/

Lessons learned from Anthem

BAKER TILLY

Candor. Insight. Results.

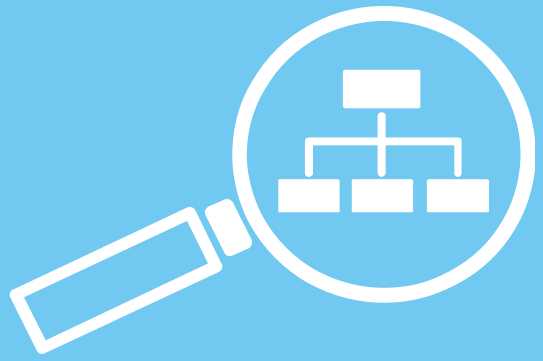
1) Better and more frequent employee security awareness training
2) Multi-factor authentication
3) Encrypted data at rest
4) Response speed and process
   - > Incident response plan and testing

Source: NAIC CyberSecurity Taskforce meeting with Anthem CIO, 3/29/15.

BAKER TILLY

Candor. Insight. Results.

REGULATOR RESPONSE AND IT EXAM ALTERATIONS



BAKER TILLY

Candor. Insight. Results.

NAIC Cybersecurity Task Force: Tasked to monitor development in cybersecurity

> Advise, report, and make recommendations to the NAIC's Executive Committee

> Coordinate activities with other NAIC committees, task forces, and working groups regarding cybersecurity

> Represent NAIC and communication with other entities/groups, including the sharing of information

Adopted cybersecurity principles document

> 12 Principles

IT Examination Working Group

NAIC releases 12 principles guidance: Company

BAKER TILLY

Candor. Insight. Results.

Principle 2

- **Confidential and/or personally identifiable consumer information** collected, stored or transferred should be **appropriately safeguarded**

- **Planning for incident response** by insurers and other regulated entities is an essential component to an effective cybersecurity program

Principle 7

Principle 8

- Insurers should take steps to ensure that **third parties and service providers have controls i**n place to protect data

- Cybersecurity risks should be **incorporated into ERM** processes
- Cybersecurity must include **all facets of an organization**

Principle 9

Principle 10

- **IT internal audit findings** should be **reported to the board** of directors (or a committee thereof)

- Insurers should engage in an **information-sharing and analysis organization (ISAO)** to stay informed of emerging threats

Principle 11

Principle 12

- Provide **periodic and timely training** (inclusive of an assessment) regarding security and cybersecurity threat awareness and protection

NAIC releases 12 principles guidance: Regulators

BAKER TILLY

Candor. Insight. Results.

Principle 1

- **Insurance regulators have responsibility** to ensure customer data is secure.
- Regulators should mandate insurers have **systems in place to alert consumers** in a timely manner of a breach.

Principle 3

- State insurance departments and the NAIC are also responsible for ensuring **consumer information sent to NAIC/Departments is secure**.

Principle 4

- Guidance must be **flexible, scalable, practical and consistent** with nationally recognized efforts (i.e. NIST)

Principle 5

- Guidance should include a **minimum set of standards, but be risk-based** and consider the resources of an individual insurer.

Principle 6

- State regulators should provide regulatory oversight, which would **include cybersecurity considerations into Financial and Market Conduct** exams.

BAKER TILLY

Candor. Insight. Results.

NAIC Risk-Focused Surveillance (E) Working Group: Created IT Examination Cybersecurity Task Force

- Charged with reviewing the NAIC IT exam guidance (Exhibit C) against NIST Cybersecurity framework for potential enhancements
- Task Force members included state regulators and private sector consultants

Resulted in alterations and updates to:

- Exhibit C
- Exhibit Y (interviews)
- General Examination Considerations section

NAIC Exhibit C – Examination Impact

BAKER TILLY

Candor. Insight. Results.

NAIC in process of adopting changes to exam approach

1. Incident Response Plan requirements added with an emphasis on plans to engage specialists as soon as breach is determined (or routinely).
2. Enhanced vendor management oversight with emphasis on access to systems and data.
3. Addition of security and cybersecurity awareness training requirements.
4. Threat and information received from information-sharing should be incorporated into IT risk assessment and profile
5. Board and CEO/President expected to be in tune with cybersecurity program

Key components of effective cybersecurity programs

BAKER TILLY

Candor. Insight. Results.

Summary and conclusion

BAKER TILLY

Candor. Insight. Results.

- Cybersecurity is a moving target.
- Effective cybersecurity management is a continuous process.
- Effective cybersecurity management programs need to start with solid data classification and a security-focused risk assessment.
- Examinations and Insurance Departments are being asked to expand their knowledge and expertise into “uncharted” waters.
- Guidance is just that, and needs to be tailored to the level of risk included at each individual organization.

Disclosure

BAKER TILLY

Candor. Insight. Results.

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.