KPMG

cutting through complexity

Cyber Security Insurance

How IT Audit & Security can make a strong business case for organization protection

March 17, 2016

Agenda

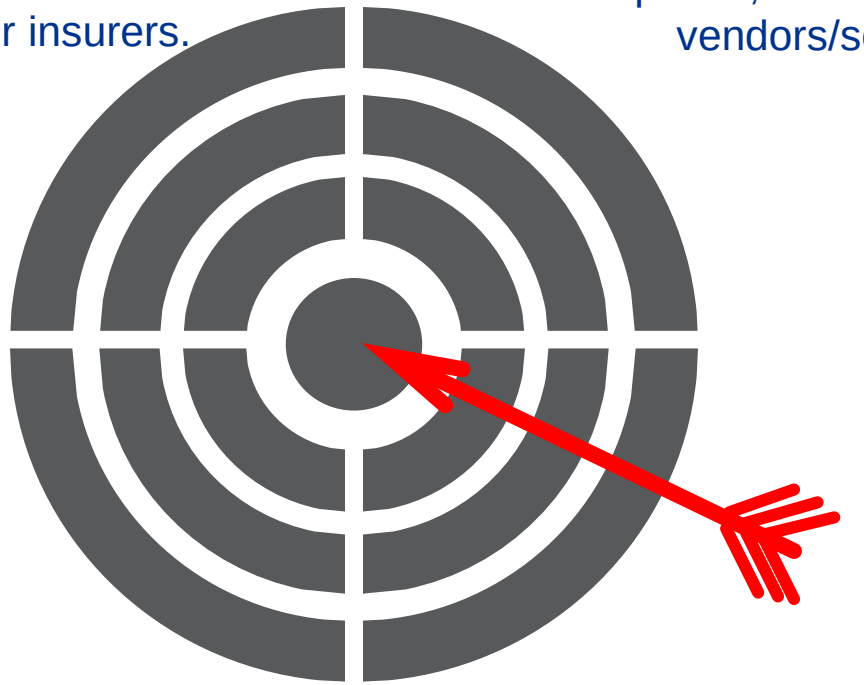
- Introductions
- Objective for Today's Presentation
- The Case for Cyber Security Insurance
- Definitions
- The Cyber Security Insurance Challenge
- Cyber Security Insurance Ownership & Responsibilities
- Considerations when selecting a Cyber Security Insurance Policy
- Tips & Tricks for Favorable Cyber Security Insurance Premiums
- Cyber Security Insurance Application & Review Process
- When the enemy strikes, don't lose your coverage!
- Completing a cyber security insurance application - where to start?
- Walkthrough of typical questions in a Cyber Security Insurance Application Form
- Conclusion

Introductions

Objective for today's presentation

Establish a basic understanding of **key concepts related to cyber security risk treatment** and the **value that Cyber Security Insurance can bring to the organization** in situations where residual risk can be transferred to cyber insurers.

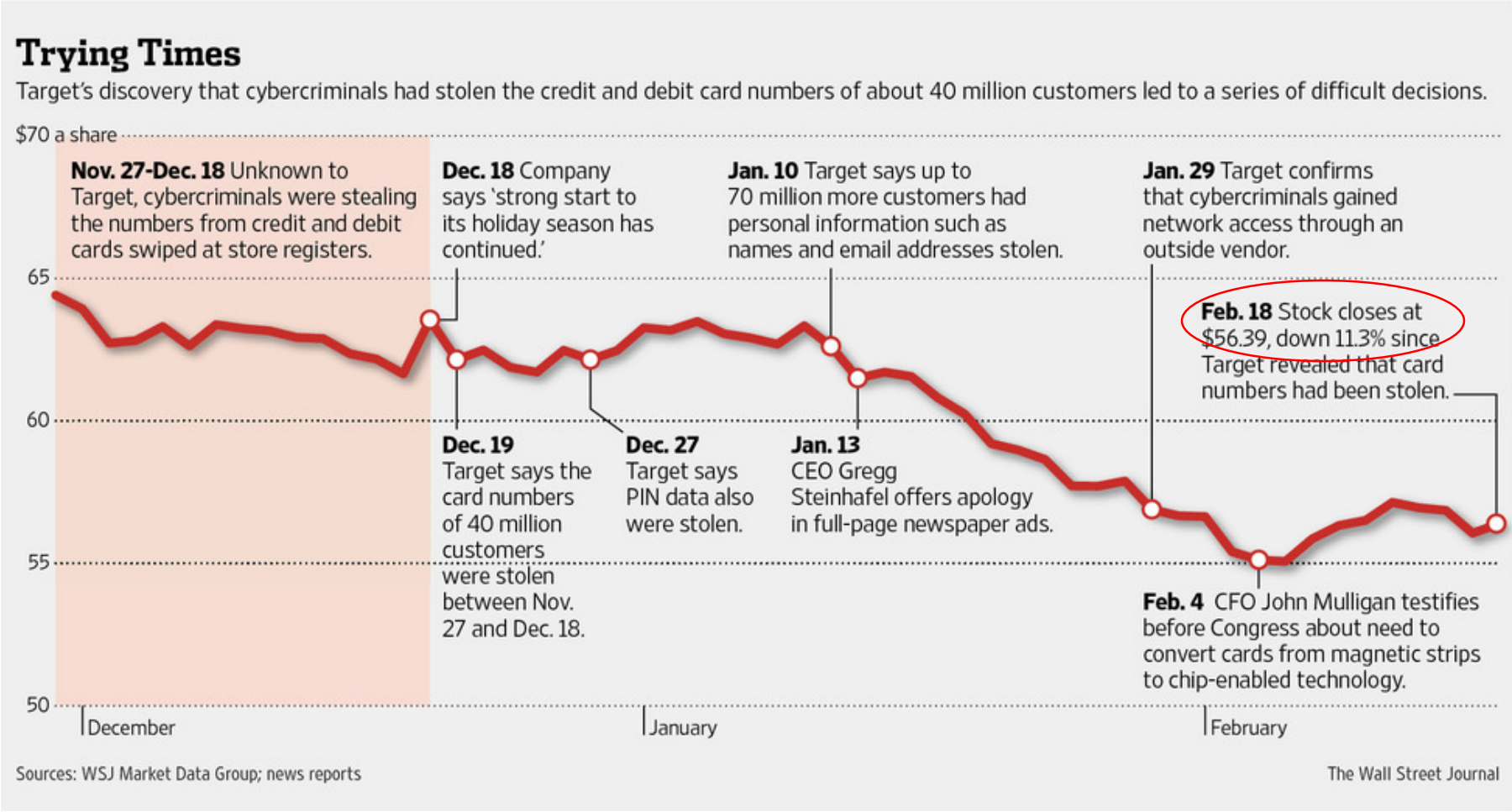
Establish a basic understanding of the **cyber security insurance application process**, **key stakeholders** who need to be involved, and the **challenges** in identifying coverage options, including consideration of vendors/service organizations.



Perform a **practical walkthrough** of a typical **Cyber Security Insurance application form** to establish a basic understanding of the inputs required.

The case for cyber security insurance

A case study “right on target”

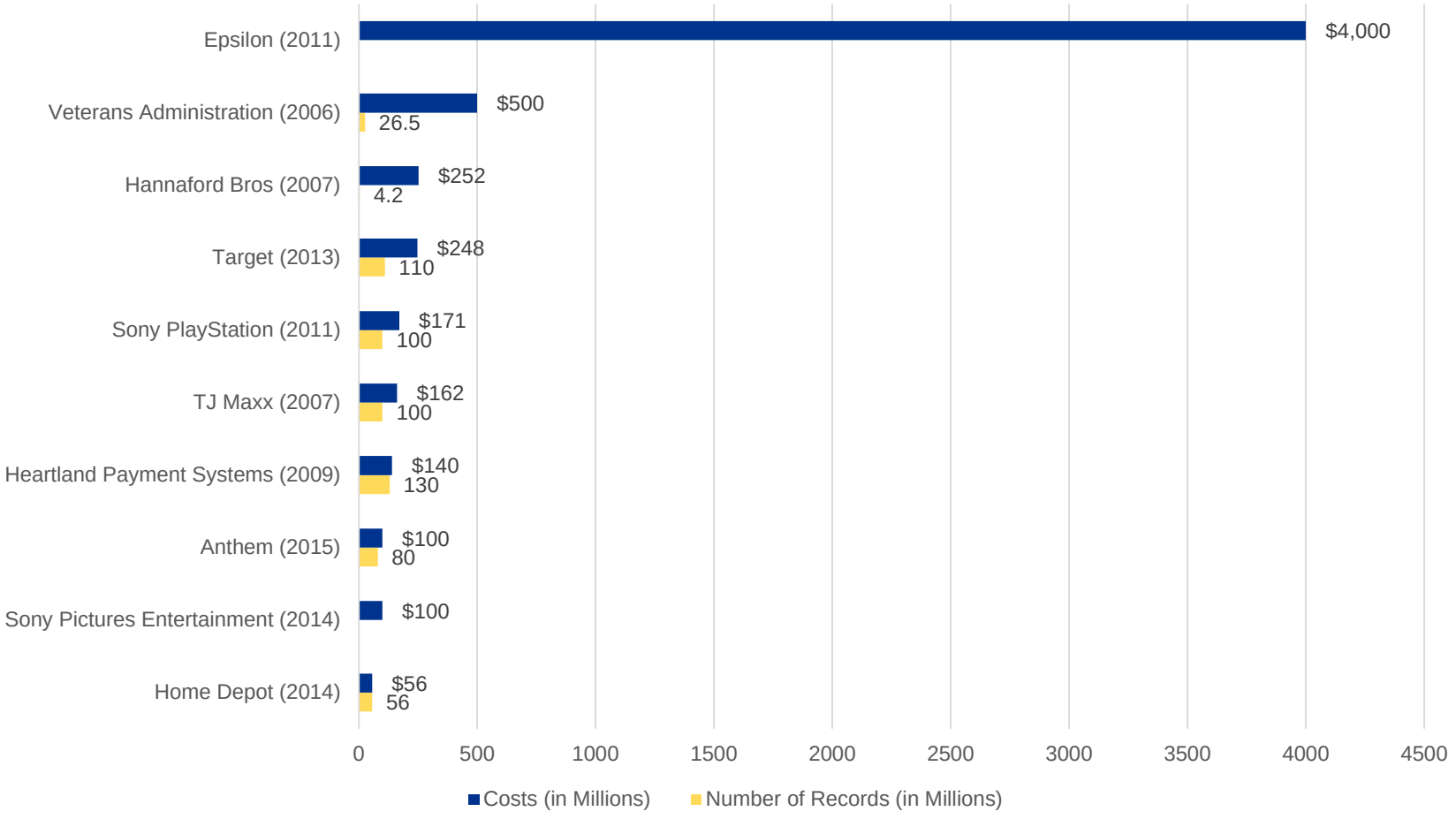


May 5th 2014: CEO Gregg Steinhafel was removed by the Board of Directors.
May 28th 2014: Institutional Shareholder Services (ISS) recommended that Target shareholders vote out 7 of its 10 board members including members of the Audit and Corporate Responsibilities committees.

The case for cyber security insurance

The Cost of Data Breaches

Top 10 Most Expensive Data Breaches*

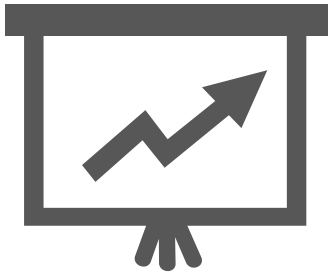


Article Reference: http://www.lifehealthpro.com/; Published June 18th, 2015

The case for cyber security insurance

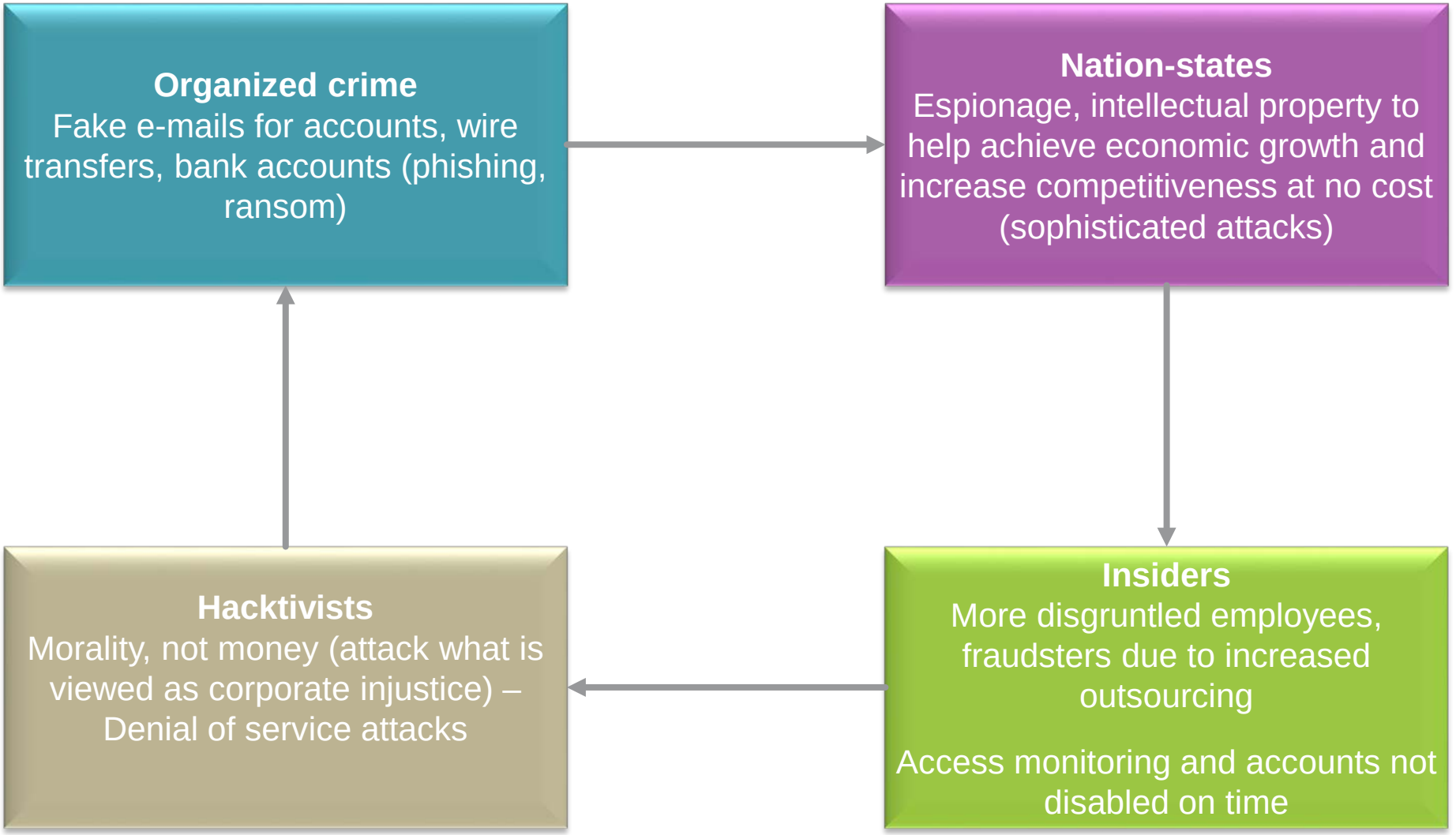
Costs related to a Cyber Security Incident

- **Business interruption (loss of revenue)**
- **Crisis event management,** including establishing a call center
- **Credit monitoring**
- **Data and system restoration**
- **Cyber extortion or cyber terrorism**
- **Forensics**
- **Notification to customers (**account holders, patients, providers, etc**.) via letter, media, web, email, etc. depending on state & federal laws**
- **Notification message content preparation**
- **Cost related to tracking of effort**: Hours and invoices for credit monitoring, data & system restoration, legal, privacy, etc.
- **Regulatory fines and penalties**



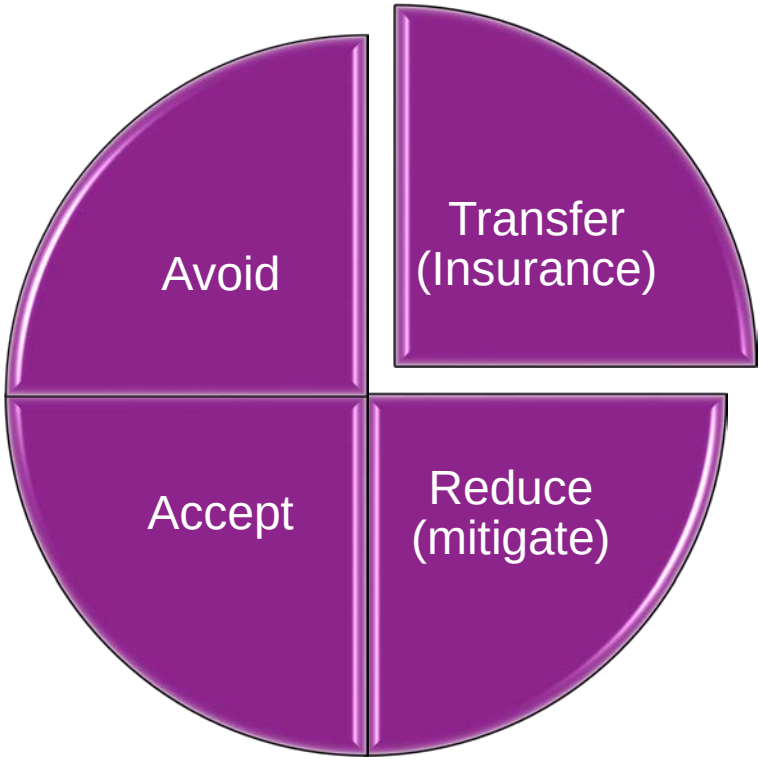
The case for cyber security insurance

Cyber threats and how they materialize in organizations



The case for cyber security insurance

Why Do We need Cyber Insurance – Risk Treatment



Definitions

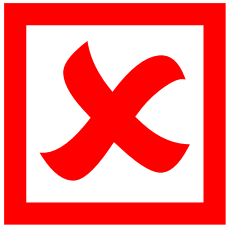
What Cyber Security Insurance IS

Risk Management Strategy i.e. cyber security insurance transfers some of the financial risk of a security breach to the insurer.

What Cyber Security Insurance IS NOT

Cyber Security Insurance doesn't do a good job of covering the reputation damage and business downturn that can be triggered by a security breach.

Having Cyber Security Insurance is not an excuse to neglect the design and implementation of good cyber security controls.



The Cyber Security Insurance Challenge

- **Limited regulation and frameworks** available to guide selection of insurance options out of numerous cyber insurance products
- **Executive management** does not see the value of Cyber Security Insurance
- **Determining the likely financial impact** on the organization as a result of a cyber security breach
- Unable to get insurance underwritten because of **current risk profile**
- Too many **exclusions, restrictions and defined uninsurable risks**
- **Applications** are challenging to complete, compare, and can be confusing
- **Ownership** (CIO/CTO? CISO? CFO? CLO?)
- **Premiums** increase annually or are too expensive

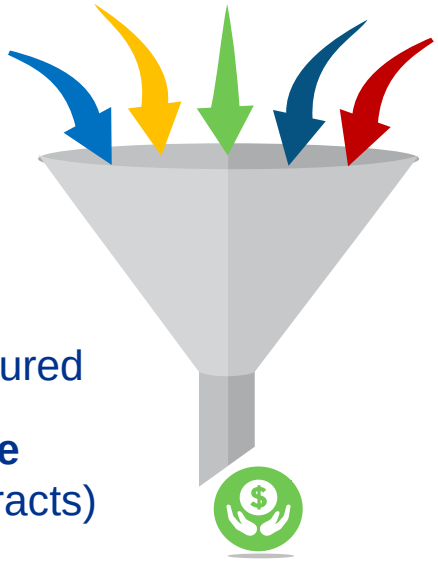
Cyber Security Insurance Ownership & Responsibilities

- Insurance falls within the duties of the Chief Financial Officer (CFO)
- Completion of the application is often delegated to the IT Officer/Director or CISO office, who may feel it is an ‘indictment’ on them
- **Combination of CFO, IT, and Risk Officer required for completing different sections of application**
- **Privacy and Legal may provide inputs**
- Other members of management

Considerations when selecting a Cyber Security Insurance Policy

Identifying insurance scope

- Identify and secure the company's "**crown jewels**", then quantify and insure the remaining risk
  - Personally Identifiable Information (**PII**) or electronic identifiable Protected Health Information (**ePHI**)? **PCI**? **Intellectual Property**?
  - **Volume** of data
  - Data **Location** (i.e. in-house, hosted (cloud)), structured & unstructured
  - Who has **access** to the data and from where (also consider **outside vendor access** into network and their coverage when signing contracts)



- Consider **costs** related to the following for coverage scope:
  - Business interruption
  - Crisis event management (e.g. establishing a call center)
  - Credit monitoring
  - Data and system restoration
  - Forensics
  - Cyber extortion
  - Notifications to customers (account holders, patients, providers, etc.) via letter, media, web, email, etc. depending on state & federal laws
  - Media, privacy, legal costs
  - Regulatory fines and penalties
  - Soft costs

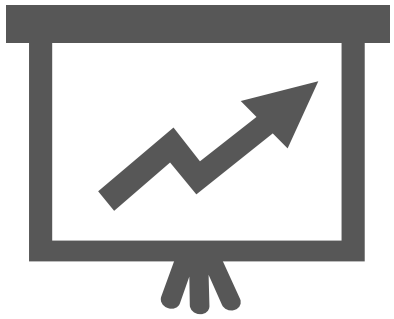
Considerations when selecting a Cyber Security Insurance Policy

Cyber Security Insurance Policy Options & Limit Considerations

- **Understand various types of coverage** (Data breach coverage, Business Interruption coverage, Network damage, etc.)
- **Standalone** policies or **combined** with Professional Liability/Error & Omissions (E&O) Insurance (e.g. Doctors & Hospitals - cyber with medical malpractice)
- Don't just increase limit on a standalone E&O policy for cyber coverage. It won't cover it.
- Buy insurance from **same carrier** as other insurance policies to keep premiums low
- Cyber & Privacy Insurance are often packaged together
- **Customer contracts** can influence insurance limits and duration. The bigger and longer the contract, the higher the liability.
  - Professional services companies should look at average size of their contract and capping liability.

Tips & Tricks for Favorable Cyber Security Insurance Premiums

- **Four "pillars" of an effective cyber risk culture** that results in favorable premiums:
  - engaged executive leadership;
  - targeted cyber risk education and awareness;
  - cost-effective technology investments; and
  - relevant information sharing.
- **Review** premiums & coverage quarterly at a minimum
- Conduct an **independent audit** of cyber security controls at least annually



Tips & Tricks for Favorable Cyber Security Insurance Premiums

Conduct an Independent Cyber Maturity Assessment

Legal and compliance

Regulatory and international certification standards relevant to the organization.

Leadership and governance

The board, their due diligence, ownership, and effective management of risk.

Operations and technology

The level of control measures implemented within the organization to address identified risks, and minimize the impact of compromise.

Human factors

The level of security-focused culture that empowers and ensures the right people, skills, culture and knowledge.

Business continuity and crisis management

The organization's preparations for a security event and its ability to prevent or minimize the impact through successful crisis and stakeholder management.

Information risk management

Approach to achieve comprehensive and effective risk management of information throughout the organization and its delivery and supply partners.

The Cyber Security Insurance Application & Review Process

Select a Cyber Insurance Policy Broker who…

- Can get **multiple quotes** in the market to balance price with coverage
- **Specializes** in offering coverage **in your industry** and is knowledgeable on attacks experienced by that industry
- **Understands** state and federal regulatory **compliance**
- Can help compare the company capabilities with other similar companies
- Can **clarify cyber risk coverage vs. other insurance** policies' coverage
- Can help identify incident breach types **too expensive to insure**
- Can help **scrutinize incident response** workflow capabilities
- Can clearly outline the **forensic analysis and incident response conditions and process**
- Can help **find policies** that include **breach drill assistance and training**

When the enemy strikes, don’t lose your coverage!

- **Notify Cyber Security Insurer first** in a breach incident unless pre-authorized to contact Forensic firm first
- Forensic Firm and Cyber security provider must be both involved simultaneously
- Create procedures with **contract requirements** in mind
- Notify the **credit card brand companies**
- **Don’t wait too long** before notifying legal, public relations, privacy, executive management

Establish a **Cyber Security Breach Incident Communications Policy and**

Conduct **Annual Training for EVERYONE** in the organization

Completing a cyber security insurance application - where to start?

Prepare to complete the application

- **Build relationships** ahead of time
- **Communicate** in advance to stakeholders (6 + months)
- Update the **annual cyber security plan** narrative
- Update the **listing of available protection & prior-year control enhancements**
- Use the **prior year application** (if you have one)
- **Compare** multiple applications
- Allow for **40+ hours of work**
- Develop an **approach** and set a **realistic timeline**
- Do not submit application without **legal review**
- **Update the board** on outcome

Walkthrough of cyber security insurance application questions

MICKEYMOUSE INC. Cyber security insurance application

<The Controller's Office or CFO's office completes this portion of the application>

Applicant Full Name: Acme, Inc.

Business Address:

Nature of Business/Business Description including products/services offered: Acme Inc. is a national health insurance provider operating in 4 states: Arizona, Massachusetts, California, and New York

State of Incorporation

# of Employees

US Prior Year Revenue and Current Year Estimated Revenue

Overseas Prior Year Revenue and Current Year Estimated Revenue

Main Website Address

State of Incorporation

Date Established

) ist the largest 5 contracted vendors

Authorized Officer name and contact information:

Main Contact for Risk Manager, Privacy and Information Security officer or designee

A. BUSINESS CHANGES	
Are significant changes in the nature or size of the Applicant's business anticipated over the next twelve (12) months? Or have there been any such changes in the past twelve (12) months?	x☐ Yes ☐ No
If yes, please explain: The company has acquired 5 (five) health insurance providers in the state of NY, divested 1 (one) of its 21 (twenty one) subsidiaries, consolidated 3 of its 12 claim processing systems, decommissioned 2 of its 4 ERP systems that process employee HR and payroll data, and underwent a significant restructuring process as a result of which 2,499 (twenty four hundred ninety nine) employees were laid off. As a result of these changes, the number of employees increased almost twofold to approx. 29,500 (twenty nine thousands five hundred).	
Has the Applicant in the past twelve (12) months completed or agreed to, or does it contemplate within the next twelve (12) months, a merger, acquisition, consolidation, whether or not such transactions were or will be completed?	x☐ Yes ☐ No
If yes, please explain: Mickey Mouse Inc. will continue its mergers and acquisitions strategic initiative in the next 12 months and divest lines of business that are not aligned with minimal profitability threshold requirements approved by the board of directors.	

Conclusion

- Cyber Security Insurance can be used as a **tool to transfer some of the risk related to a cyber security incident** and soften the financial impact on the organization
- There are many **challenges** in obtaining Cyber Security Insurance, however with **adequate buy-in from Executive Management** and the help of a **good broker**, the battle is half won
- The Cyber Security Insurance application form completion should be a **collaborative effort** between the CFO, CIO, CISO and Legal Officers
- More favorable Cyber Insurance Premiums are possible by providing **evidence of a mature cyber security posture** across all levels of the organization (people, process & technology)
- A **good Cyber Security Insurance broker** is **critical** in helping to understand policy options, exclusions, restrictions and uninsurable risks
- A tested and communicated **Incident Communication, Response and Handling Policy** is vital to help ensure coverage payout in the event of a cyber security breach and limit financial and reputational damage.

References

https://www.dhs.gov/publication/cybersecurity-insurance-reports

http://www.ponemon.org/blog/managing-cyber-security-as-a-business-risk-cyber-insurance-in-the-digital-age

http://www.cybersecuritydocket.com/2015/04/09/cyber-insurance-a-pragmatic-approach-to-a-growing-necessity/

https://www.fbi.gov/news/testimony/cyber-security-terrorism-and-beyond-addressing-evolving-threats-to-the-homeland

http://www.csoonline.com/article/2835274/cyber-attacks-espionage/cyber-insurance-worth-it-but-beware-of-the-exclusions.html

http://www.inc.com/will-yakowicz/does-your-company-need-cybersecurity-incurance.html

http://www.welivesecurity.com/2013/09/16/nist-cybersecurity-framework-your-insurance-company-is-watching/

Google various cyber insurance providers

Google ‘target data breach timeline”

What Questions Do You Have?

Thank you

Alex Branisteanu
Director, IT Advisory
abranisteanu@kpmg.com

Sumari Witt
Director, IT Advisory
switt@kpmg.com