SNIA CSTI | CLOUD STORAGE TECHNOLOGIES

Does Your Storage Need a Cyber Insurance Tune-up?

Live Webcast

August 27, 2020

10:00 am PT

Today's Presenters

Paul Talbut
SNIA Regional Program Director

Casey Boggs
President
ReputationUs

Eric Hibbard
CISSP-ISSAP, ISSMP, ISSEP, CIPT, CISA, CCSK
Chair, SNIA Security Technical Working Group

SNIA Legal Notice

- The material contained in this presentation is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

  NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

SNIA-At-A-Glance

185
industry leading organizations

2,000
active contributing members

50,000
IT end users & storage pros worldwide

SNIA CSTI | CLOUD STORAGE TECHNOLOGIES

What We Do

Educate vendors and users on cloud storage, data services and orchestration

Support & promote business models and architectures: OpenStack, Software Defined Storage, Kubernetes, Object Storage

Understand Hyperscaler requirements Incorporate them into standards and programs

Collaborate with other industry associations

Agenda

- Assessing the Business Risk
- What is Cyber Insurance?
  - What is it not?
  - Reasons to consider cyber insurance
- Data breaches
  - Aspects of brand image and reputation
- Cyber insurance considerations
  - Coverage and types of insurance
  - Typical policy exclusions and excesses
- The Panel Discussion
- Summary/Key Takeaways

Business Risk

Cyber Risk

Cyber risk - *risk* caused by a *cyber threat*

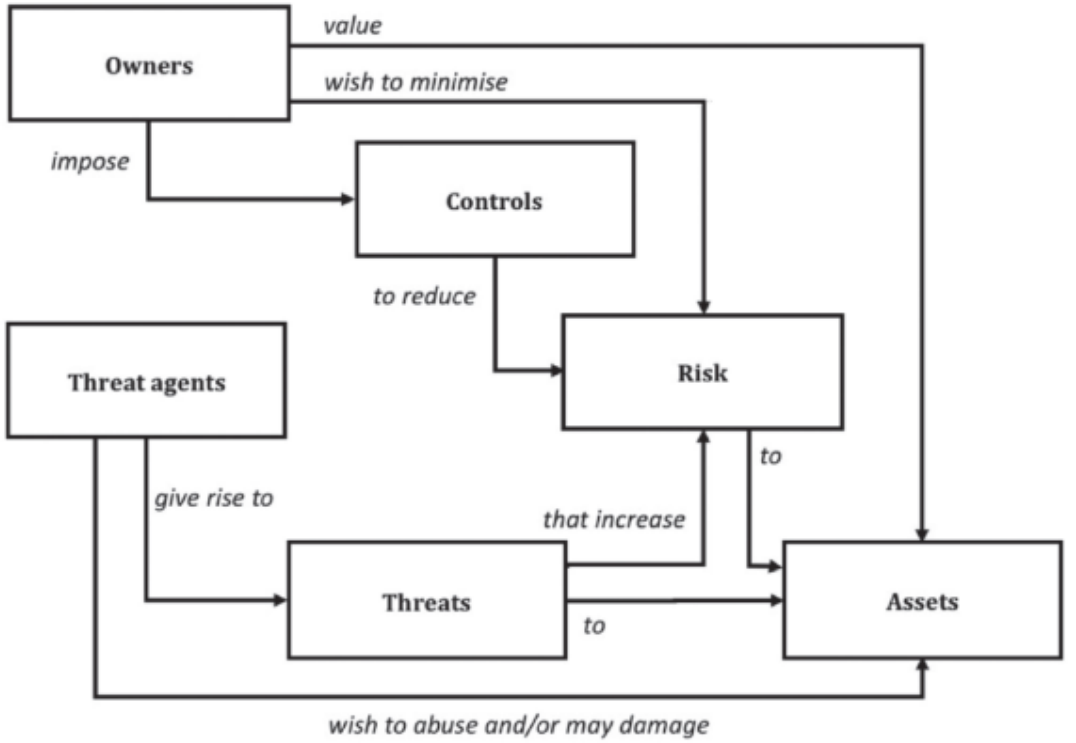
Cyber threat - *threat* that exploits a *cyberspace*

Cyberspace - interconnected digital environment of networks, services, systems, and processes

Risk - effect of uncertainty on objectives

Threat - potential cause of an unwanted incident, which can result in harm to a system or organization

Source: ISO/IEC 27102:2019, *Information security management - Guidelines for cyber-insurance*

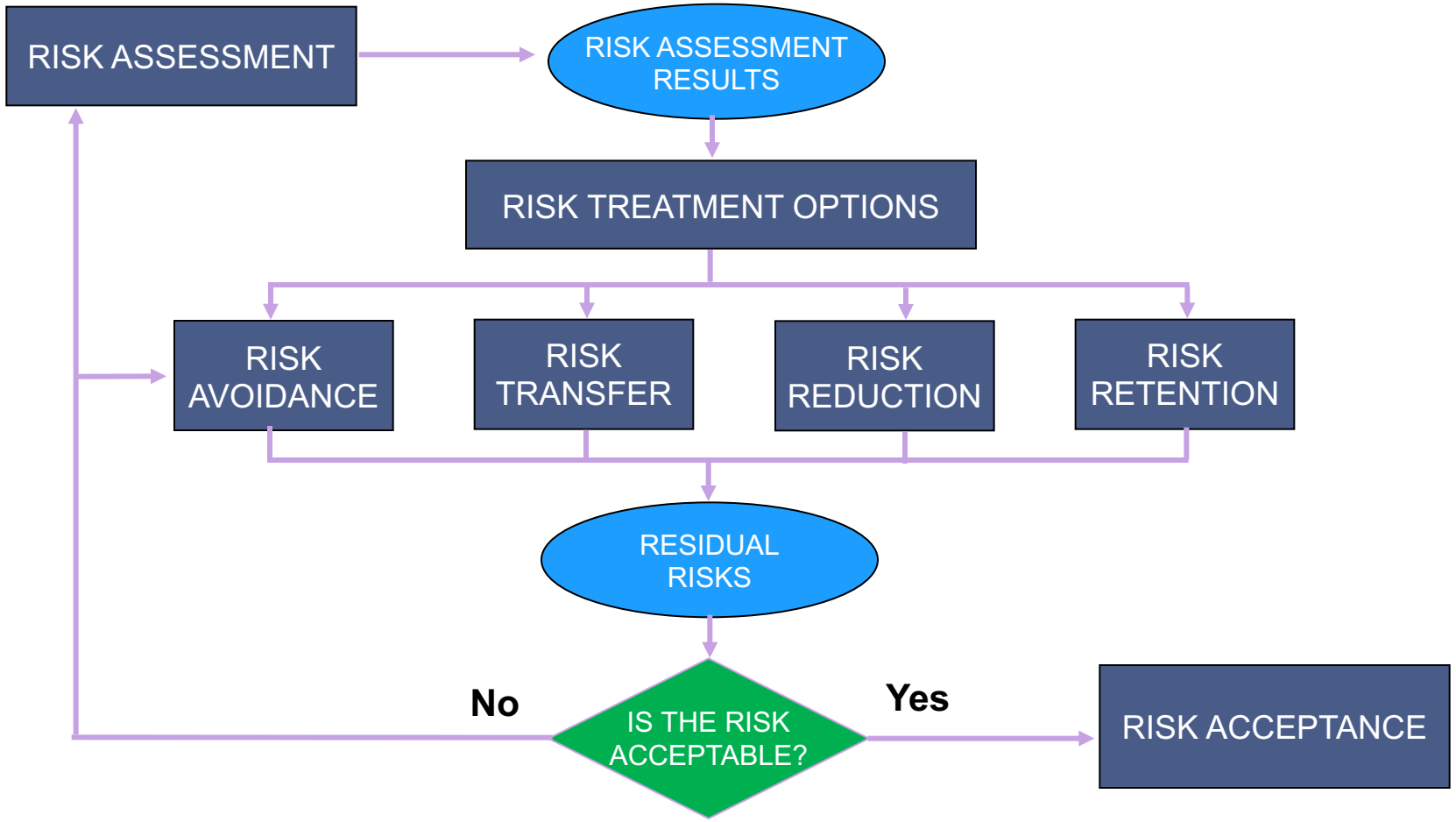


Source: ISO/IEC DIS 15408-1:2020, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model*

Common Risk Frameworks

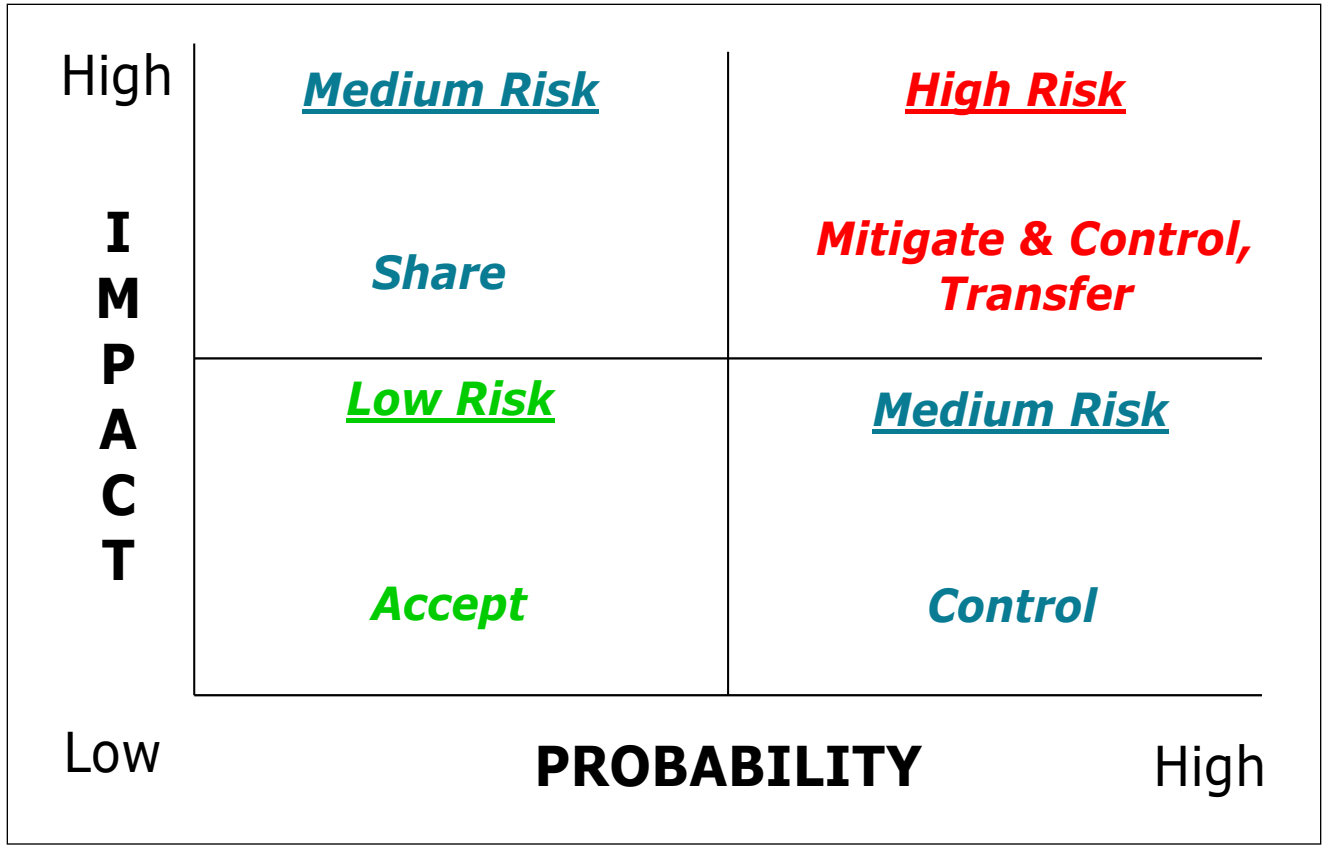
- NIST Risk Management Framework
  - NIST SP 800-39 + NIST SP 800-37 & NIST SP 800-53
- ISO Risk Management Framework
  - ISO 31000, ISO Guide 73, ISO/TR 31004, ISO/IEC 31010
- COSO Enterprise Risk Management—Integrated Framework

Risk Treatment Decision-making Process



SOURCE: ISO/IEC 27005:2018, *Information technology -- Security techniques – Information Security Risk Management*, http://www.iso.org

Risk and Remediation



A simple way of identifying the highest priority risks as well as offering some guidance on what should be done.

What is Cyber Insurance?

…and what is it not?

Overview

- The insurance industry has responded to these cyber-based risks with a variety of products collectively referred to as “cyber insurance.”
- A cyber insurance policy can be either a stand-alone policy or be included as special endorsements as a part of general liability, property or other insurance policy.
- Cyber insurance coverage varies quite a lot between different cyber-insurance products, is not standardized and varies depending on:
  - limitations posed by laws and regulations
  - generally accepted market practices
  - business decisions of an insurer
  - needs of the insured

Reasons to Consider Cyber Insurance

- Insurance places a dollar value on an organization's cyber risk.
  - This metric is useful when discussing security budgets with senior management.
- The underwriting process can help organizations identify cybersecurity gaps and opportunities for improvement.
  - In the same way property insurance has helped create safer buildings, cyber insurance can help create safer cybersecurity practices and policies.
- In addition to providing the traditional risk transfer function, many cyber insurance policies bring supplemental value through the inclusion of risk mitigation tools, as well as significant incident response assistance following a cyber incident.
  - Such assistance can be essential, particularly for smaller organizations that lack experience with or the workforce to respond to these issues, when faced with reputational damage or regulatory enforcement.

Possible Coverage

- **Liability:** indemnification for losses to other parties (e.g., damages affecting individuals or other organizations, data breach of personal information, etc.)
- **Incident response costs:** loss, theft, or damage to information; reputational damage; customer or employee notification costs, customer, or employee protection costs; specialist expertise costs; operational cost to manage incidents; staff and personnel costs
- **Cyber extortion costs:** threats to damage or restricting the insured's use of technology (e.g., ransomware), or releasing information copied or stolen. Note: There are jurisdictions where insurance coverage for selected cyber extortion risks is not permitted.
- **Business interruption:** loss of income or loss of profit and increased operating expenses resulting from a cyber incident

Possible Coverage (cont.)

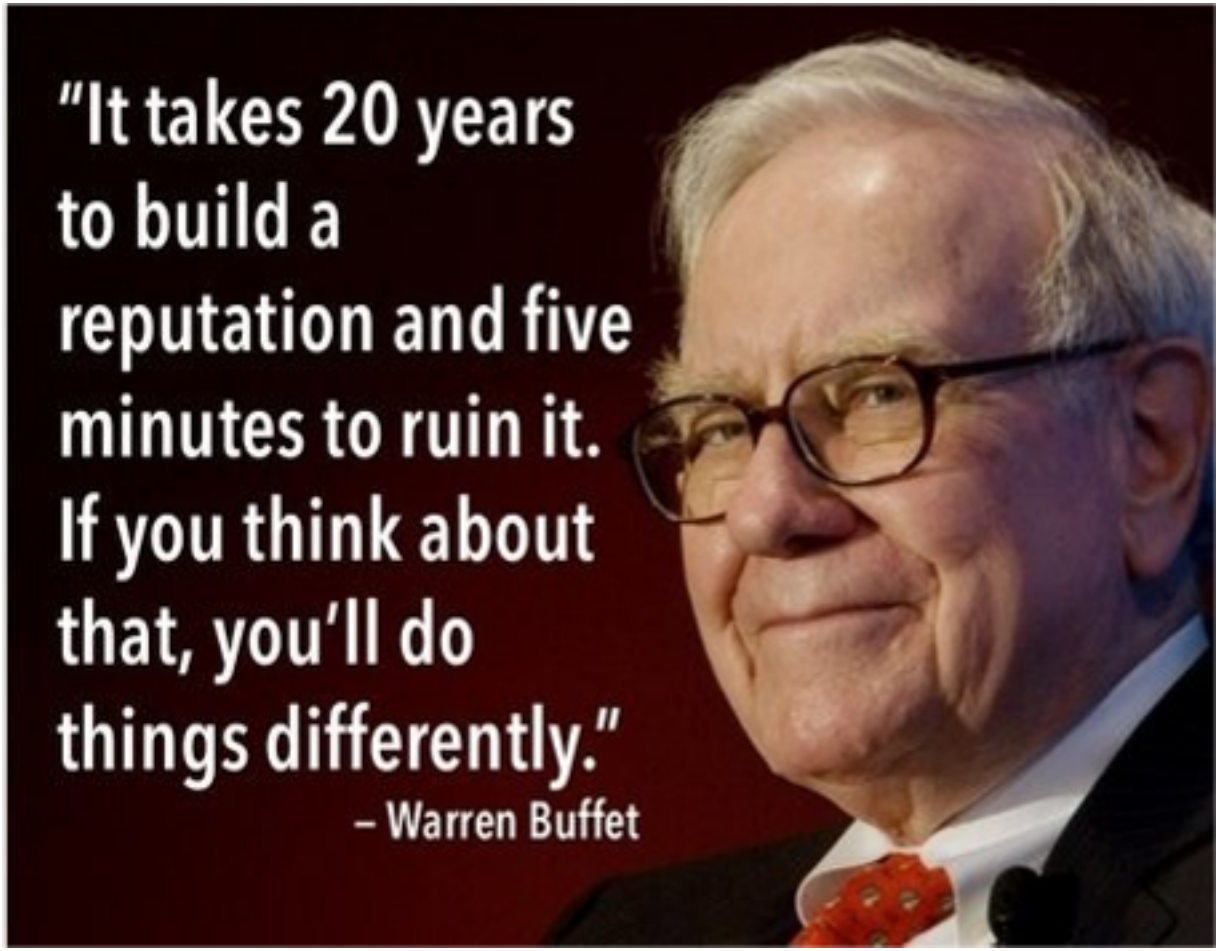
- **Legal and regulatory fines and penalties:** civil penalties; regulatory penalties and fines resulting from an investigation or enforcement action by a regulator; or other compensatory awards decided by a legal system. Note: There are jurisdictions where insurance coverage for certain legal and regulatory fines or penalties is not permitted.
- **Contractual fines and penalties:** A cyber incident can result in the insured not fulfilling contractual obligations, which can result in fines or penalties from these parties.
- **Systems damage:** A cyber incident can result in costs to repair or restore systems, data and software applications not otherwise covered by the insured's existing insurance policies.

Cyber Incident Types

- **System malfunction:** the insured's system or network is malfunctioning or creating damage to a third-party system or a supplier's system is not functioning, impacting operations;
- **Data confidentiality breach**: data stored in the insured's system (managed on premise, hosted or managed by a third party) has been stolen or exposed;
- **Data integrity or availability loss:** data stored in the insured's system (managed on premise, hosted or managed by third party) has been corrupted or deleted;
- **Other malicious activity:** misuse of a technology system to inflict harm (such as cyber-bullying over social platforms or phishing attempts) or to illicitly gain profit (such as cyber-fraud); and
- **Human error:** where something unintentional has been done by a human resulting in harm to a system, network or information.

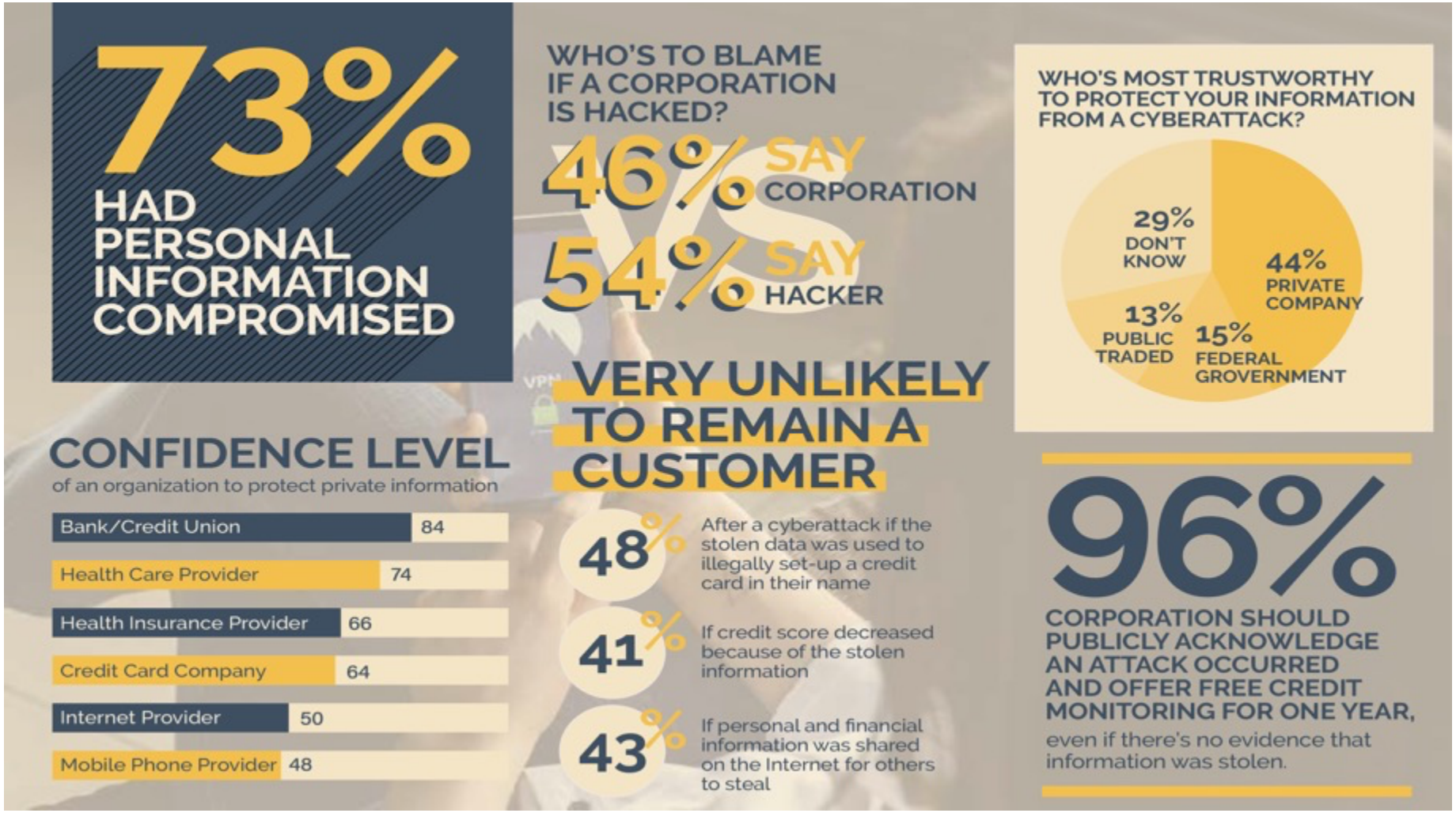
Impact on Reputation

Reputation Risks



Cybersecurity/Reputation Study

Customer Confidence/Corporate Reputation



Cybersecurity Study

Who is to blame for cyber attack?

Cybersecurity Study

Customer Confidence/Corporate Reputation

Reputation Protection Steps

1. Plan For Attack
2. Simulate Attack
3. Communicate to Mitigate

Cyber Insurance Considerations

The fine print…

Policy Triggers

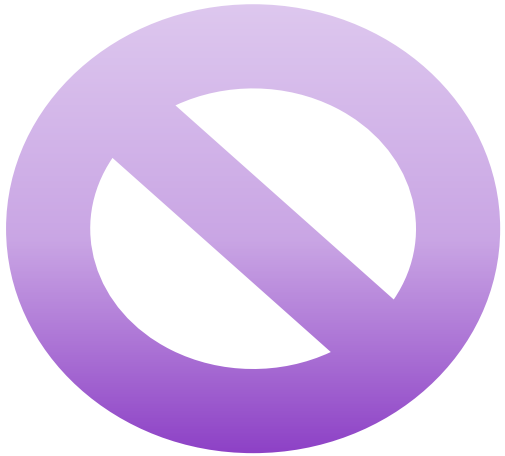
- A typical policy is ***triggered*** when a claim is first made against the insured (in the form of a demand letter, lawsuit, or other document) that their product, service, or property has caused a third party some type of harm, loss, or damage.
- This can be a problem, because such claims often occur after the insured issues notifications of a data breach (i.e., prior to a claim), leaving the insured organization to pay for many costs associated with a cyber breach they may have thought were covered.
- To resolve this situation, look closely at how the policy is constructed, especially the insuring agreement.
- The element of time is critical to ensuring coverage is triggered appropriately.

Pre-approval of Experts/Vendors

- In the critical moments of responding to a potential data breach, the last thing an organization should be worried about is whether their insurance provider will approve their selected breach counsel and forensics firm.
- Typically, cyber insurance policies require underwriter approval of the use of breach vendors.
- Include selected breach counsel and vendors (e.g., forensics firm, public relations, crisis management firms, etc.) in the incident response plan.
- Discuss the selected breach vendors with the insurers prior to policy purchase to ensure they will approve the use of those vendors if there is an incident.

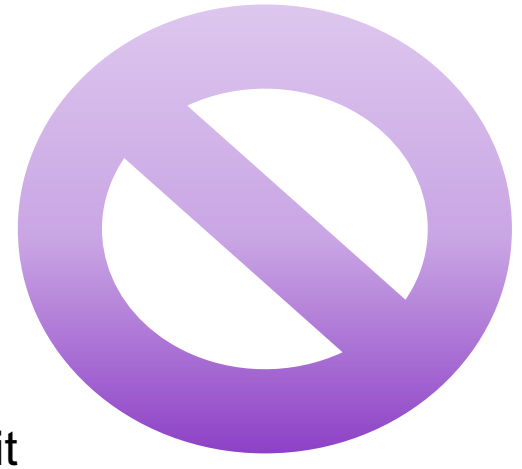
Common Policy Exclusions

- **Bodily injury and property damage.** First-party and third-party bodily injury and property damage arising from a cyber incident are usually excluded under a cyber insurance policy.
- **Terrorism.** A cyber loss caused by hacking groups that are classified as terrorist organizations in some countries, or by internationally recognized organizations.
  - Clearly define Act of Terrorism or Cyber Terrorism and limit any exclusion so it only applies where the U.S. Government officially declares an incident as an act of Terrorism or Cyber Terrorism.
- **Acts of war and other hostile acts.** There is no generally recognized definition of cyber war. The definition is expected to be linked to actors, for example nation state, and to the level of disruptive or destructive impact, whether war is declared or not.
  - Limit Nation/State exclusions to those recognized by the U.S. Government or United Nations.
- **Insider threats.** Coverage for incidents of insider malfeasance can be excluded.
  - If such incidents are not covered, request an exclusion (applies only to the company's highest ranking directors or officers) and make sure the exclusion applies only after a finding of intentionality has been fully adjudicated on the merits in a court of law.



Common Policy Exclusions (cont.)

- **Territorial limits.** Some coverage is limited only to incidents that occur in the United States, and an organization may need additional coverage depending on where data is stored.
- **Intellectual property.** Impacts due to loss of intellectual property, for example, patents, copyrights or trade secrets.
- **Confidential information.** Theft or loss of confidential information where the information is not directly owned by the insured.
- **Acts of God.** Review “Acts of God” exclusions carefully in cyber policies, negotiate to limit exclusions as much as possible.
- **Devices.** Some policies do not cover devices that are unencrypted or non-company-owned devices as well as portable devices in general. Request removal of the exclusion from the policy.
- **Loss of reputation.**



Possible Excesses or Deductibles

- The amount of money the insured should pay before a claim can be made against the cyber insurance policy.
- There can be an aggregate limit either as a policy whole or an aggregate for a single event per annum.
- Cyber insurance policies can also include a waiting period of several days before business interruption cover begins to apply.
- Further, the length of business interruption coverage in a cyber insurance policy can be limited. Most policies cover lost income resulting from a cyber incident only for a certain period of time.

Miscellaneous Considerations

- Organizations can do a lot to shore up their information security policies and practices to increase the availability of coverage and reduce the cost of coverage.
- Keep in mind that the underwriting process and communications with an insurance broker or agent are not privileged communications and could be discoverable in litigation, so it is important to think about what is put in writing to underwriters, brokers, or agent.

Panel Discussion

Summary

- Knowledge of the risks and business consequences allows a cyber insurance policy to be in alignment with the security risk management strategy and risk acceptance criteria of the organization
- It is important to keep in mind that a cyber insurance policy cannot cover all types of losses, so it is critical to understand what risks are excluded from a cyber insurance policy
- An insurer can require a level of security as a precondition of coverage, and the insured may need to meet these conditions during the validity of the contract
- Cyber insurance policies can have an excess or deductible applied, which impacts payout amounts as well as the cost of the cyber insurance
- Organizations should consult with knowledgeable professionals before placing coverage

After This Webcast

- Please rate this webcast and provide us with feedback
- This webcast and a copy of the slides will be available at the SNIA Educational Library https://www.snia.org/educational-library
- A Q&A from this webcast will be posted to the SNIA Cloud blog: www.sniacloud.com/
- Follow us on Twitter @SNIACloud

Thank you!

Q & A

