3501 Fairfax Drive • Room B7081a • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 562-6446
• http://www.ffiec.gov

Joint Statement

Cyber Insurance and Its Potential Role in Risk Management Programs

The Federal Financial Institutions Examination Council (FFIEC) members[1] developed this statement to provide awareness of the potential role of cyber insurance in financial institutions' risk management programs. This statement does not contain any new regulatory expectations. Use of cyber insurance may offset financial losses resulting from cyber incidents; however, it is not required by the agencies. Financial institutions should refer to the *FFIEC Information Technology (IT) Examination Handbook* booklets referenced in this statement for information on regulatory expectations regarding IT risk management.

BACKGROUND

The increasing number and sophistication of cyber incidents affect financial institutions of all sizes, and remediation of cyber incidents can be costly. Traditional insurance policies for general liability or basic business interruption coverage may not fully cover cyber risk exposures without special endorsement or by exclusion not cover them at all. Coverage may also be limited and not cover incidents caused by or tracked to outside vendors. Cyber insurance may offset financial losses from a variety of exposures, such as data breaches resulting in the loss of sensitive customer information.

The cyber insurance marketplace is growing and evolving in response to the increasing cyber-attack frequency, severity, and related losses. Many aspects of the cyber insurance marketplace, such as terminology, claims history, legal precedents, and risk modeling continue to evolve and are shaping the nature and scope of cyber insurance.

Cyber insurance coverage options vary greatly and may be offered on a stand-alone basis or as additional coverage endorsed to existing insurance policies, such as general liability, business interruption, errors and omissions, or directors' and officers' policies. Further, cyber coverage options may be structured as first-party or third-party coverage. First-party coverage insures against direct expenses incurred by the insured party and may address costs related to customer notification, event management, business interruption, and cyber extortion. Third-party coverage

[1] The FFIEC comprises the principals of the following: the Board of Governors of the Federal Reserve System, Consumer Financial Protection Bureau, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and State Liaison Committee.

protects against the claims made by financial institutions' customers, partners, or vendors as a result of cyber incidents at financial institutions. Understanding the scope of coverage is critical for making an informed risk management decision.

RISKS

Financial institutions face a variety of risks from cyber incidents. These can include financial, operational, legal, compliance, strategic, and reputation risks resulting from fraud, data loss, or disruption of service.

RISK MITIGATION

While cyber insurance may be an effective tool for mitigating financial risk associated with cyber incidents, it is not required by the agencies. Purchasing cyber insurance does not remove the need for a sound control environment. Rather, cyber insurance may be a component of a broader risk management strategy that includes identifying, measuring, mitigating, and monitoring cyber risk exposure. An effective system of controls remains the primary defense against cyber threats.

If institution management is considering cyber insurance, the assessment of cyber insurance benefits should include an analysis of the institution's existing cybersecurity and IT risk management programs to evaluate the potential financial impact of residual risk. As institutions weigh the benefits and costs of cyber insurance, considerations may include:

- **Involving multiple stakeholders in the cyber insurance decision**
  - Include appropriate departments across the institution such as legal, enterprise risk management, operational risk management, finance, information technology, and information security management.
  - Assess the sufficiency of existing control environments to address the potential impact of cyber risk exposures and attestation requirements for the insurance policy.
  - Communicate the cyber insurance decision-making process, including the assessment of cyber insurance options, to the appropriate level of management.

- **Performing proper due diligence to understand available cyber insurance coverage**
  - Review the scope of existing or proposed insurance coverage to identify gaps.
  - Understand insurance policy terms, coverage, exclusions, and costs for cyber events.
  - Consider the potential benefits and costs to assess the insurance coverage appropriateness.
  - Avoid overreliance on insurance coverage as a substitute for sound operational risk management practices.
  - Recognize that policy terms and language may not be standardized. Coverage may be different among insurance providers and tailored for institutions.
  - Consider how the coverage is triggered, if certain types of cyber incidents (e.g., cyber terrorism) are excluded from coverage, and the impact that sub-limits may have in the total coverage and claims process.
  - Assess the financial strength (ratings) and claims paying history of insurance companies providing coverage and their ability to fulfill obligations under the policy if multiple institutions file claims.

- Assess how the proposed policies fit within the business strategies, insurance programs, and risk management programs.
- Understand risk management and control requirements outlined in the policy and ensure the institution would be able to comply.
- As appropriate, engage outside advisors, such as attorneys and brokers, to assist in the due diligence process to assess the benefits of cyber insurance relative to the cost.

- **Evaluating cyber insurance in the annual insurance review and budgeting process**
  - Assessing the benefits of cyber insurance relative to the cost.
  - Determining the sufficiency of existing insurance coverage as cyber risk exposures, insurance products, and the threat landscape evolve.
  - Confirming that any cyber insurance includes coverage expected by the institutions.
  - Engaging the board to assess these factors in insurance program reviews.

Financial institutions ultimately remain responsible for maintaining a control environment consistent with the guidance outlined in the *FFIEC IT Examination Handbook*.

ADDITIONAL RESOURCES

The following cyber insurance resources provide institutions with practical information that may help in understanding cyber insurance.

U.S. Department of Homeland Security:

Cybersecurity Insurance
Cyber Incident and Analysis Working Group White Paper

REFERENCES

FFIEC IT Examination Handbook booklets:

"Audit"
"Business Continuity Planning"
"Development and Acquisition"
"Information Security"
"Management"