# AccumeView: Executive Cybersecurity Pulse

In April, the Federal Financial Institutions Examination Council (FFIEC) published a joint statement on the potential role of cyber insurance in financial institutions' risk management programs. It is important to note that the FFIEC pointed out that the statement does not contain any new regulatory expectations and, therefore, there is no requirement to purchase cyber insurance.

In reality, whenever the FFIEC publishes joint statements, financial institutions would be wise to discuss and review the content at the senior management and board level. There is no debate on the increasing number and sophistication of cyber incidents affecting institutions of all sizes. Each week brings examples of how cyber threats have evolved and increased.

Bill Kane, Manager
Cybersecurity and
Technology Risk

646.375.9500 x151

wkane@accumepartners.com

**Background**

The cyber insurance industry has been growing and evolving in response to the increase in cyber threats. Cyber insurance may be an effective tool for mitigating financial risk associated with cyber incidents. Every institution needs to weigh the benefits and costs of obtaining cyber insurance. If this has not been discussed at your institution, we recommend you do so as soon as possible. The statement contains many examples of things to consider including:

- Involving multiple stakeholders
- Performing proper due diligence
- Evaluating cyber insurance in annual budgeting process

**Reputation and Compliance Risk Considerations**

Obtaining cyber insurance may indeed lower financial losses from a variety of exposures such as data breaches. It is imperative, however, to remember that purchasing cyber insurance does not eliminate the need for a sound control environment, nor should obtaining cyber insurance be considered a control that reduces your institution's inherent risk. Cyber insurance can neither adequately cover the reputation and compliance risk related to your customer relationships and privacy concerns, nor will it shield you from the negative publicity that results from cyber events. In risk management practice, there are 4 "t's" that are considered effective options for responding to risk – Treat, Tolerate, Transfer and Terminate. Insurance is a strategy to transfer risk; however it does little to address the other "t's."

**Steps to take today**

Here are some questions that should be addressed by your board and senior management today:

- Is your institution focusing on risk management, instead of compliance, as part of your cybersecurity framework?
- Have you determined the sufficiency of existing insurance coverage as the threat landscape evolves?
- Beyond insurance, is your incident response capability appropriate to the rising cyber threat and has it been tested?
- Have you established robust governance strategies, including sufficient expertise and training to manage cyber risks?
- How often is the management of internal and external threats and vulnerabilities and your supporting infrastructure reviewed?
- Does your institution routinely monitor, maintain awareness of, and discuss cyber threats, vulnerabilities, and events?

Obtaining cyber insurance is not a substitute for an effective cybersecurity program. Establishing an enterprise-wide approach to manage cyber risks with a strong cybersecurity culture as its foundation is the best approach.

*Bill Kane, Manager of Cybersecurity and Risk, has served as a Federal regulator and has more than 25 years' experience.*

*Don't know where to start? Contact Accume Partners and we will get you on the proper path to risk management and compliance.*