M&T Insurance Agency, Inc.

Insurance • Surety • Group Benefits

Managing Cloud and Supply Chain Risk: A Security and Insurance Roadmap

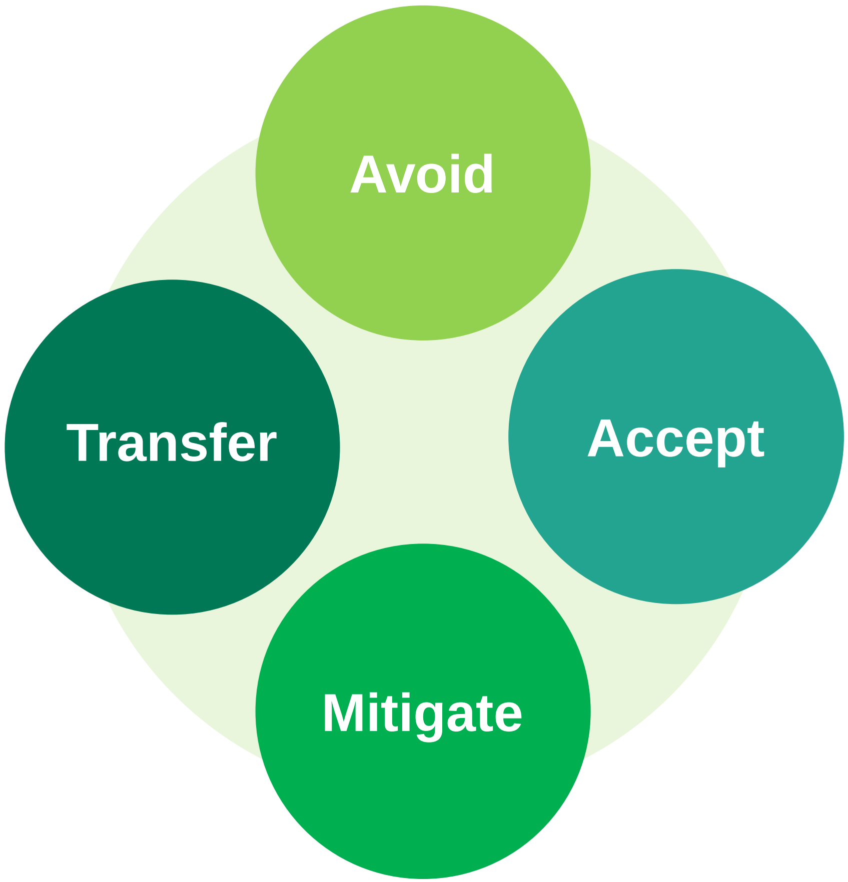
Jeffrey Batt
Cyber Insurance Practice Leader

June 25, 2020

Cloud Computing – Cyber Risk

- Cloud-related cyber risks are widespread. Can include sensitive and personal data, as well as business continuity.
- Cloud-service provider (CSP) security is widely regarded to be robust, but – like all entities – they are vulnerable. The Capital One data breach is a case in point.
- Entities across industry segments are becoming increasingly more reliant on cloud computing. Public cloud acceleration.
- Blending of cyber and privacy risk considerations (GDPR, CCPA)

Cyber Risk Responses



Vendor Management – Risk Acceptance, Avoidance, and Mitigation Recommendations

- Identify data criticality and reliance levels. Cloud / logistics / supply chain risk.
- Audit and vet cybersecurity and privacy practices at least annually. Utilize frameworks and assessments to track.
  - Ex. **NIST CSF / Privacy Framework**
- Learn and retain information around “fourth-party vendor risk” (i.e., any vendors that your cloud service provider might be using).
- Stay informed on regulatory requirements, especially with respect to privacy.
- Re-assess contractual indemnity language and other duties / obligations articulated.

Threat and Vulnerability Assessment

How seriously would I be impacted if most of my network was inoperable for several days?

What if one of my core suppliers was taken offline?

How would I financially assess it?

How much – and what types – of sensitive data do I have?

What are some key challenges and changes that my business is facing?

Am I subject to any cyber or privacy regulations (such as 23 NYCRR 500 or the GDPR)? What do they require?

What initiatives or investments do I have planned over the upcoming year?

What has been going on in the cyber threat landscape, specific to my industry?

How frequently do I audit my vendors' cyber security controls?

Do I currently transfer any cyber or privacy risk through vendor contracts, or am I actually assuming more risk through such agreements?

Risk Mitigation and Transfer: Quantification and Insurance Solutions

Cyber Risk Quantification

Measures the frequency and severity of a cyber event.

Includes first and third party costs, as well as category-specific estimates

Analytical capabilities offered either by security consultants or cyber insurers

Cyber Insurance

Covers losses related to a wide range of cyber events, including data breaches, ransomware, social engineering, privacy regulatory fines, and business interruption.

Policies are global in scope. Key part of cyber risk governance, works alongside policy, personnel and technology solutions.

Questions???

Contact Info:

Jeffrey Batt
Cyber Insurance Practice Leader
M&T Bank
jbatt@mtb.com