CYBER ASSURANCE GROUP

FINANCIAL PROTECTION. LESS TO THINK ABOUT.

White Paper: The Imperative for Insurance Producers to Discuss Cyber Risk and Mitigation Strategies with All Enterprise Clients, Including Small Businesses

Executive Summary

Cyber risk has emerged as one of the most significant threats facing businesses of all sizes. Despite the increasing frequency and severity of cyberattacks, many enterprises—particularly small businesses—remain underinsured and underprepared. For insurance producers, proactively discussing cyber risk and coverage options with every enterprise client is both a professional duty and a commercial opportunity. This paper outlines the rationale for consistently raising the topic of cyber insurance, covering legal compliance prerogatives, commercial benefits, risk management improvements, and the value of deepening client relationships.

1. The Growing Cyber Threat Landscape and Its Impact on All Businesses

According to the *Final 2024 Cyber Report*, cyber insurance claims continued to rise, driven by ransomware attacks, phishing schemes, and data breaches. While large enterprises are often targeted for their scale, small businesses increasingly face cyber threats due to weaker security protocols and limited resources. The Marsh *Cyber Market Update (February 2024)* revealed that SMEs are experiencing the fastest growth in cyber claims, with ransomware attacks and business email compromise being the most common losses.

The misconception that small businesses are less likely to be targeted leaves many uninsured or underinsured. However, insurers and MGAs specializing in cyber coverage understand that businesses of every size can suffer significant operational and reputational damage from a cyber event. Producers must educate their clients on these evolving risks and the critical role of cyber insurance in risk transfer and resilience.

2. Legal Compliance Prerogatives and Duty of Care

Insurance producers have a duty to advise clients of all material risks to their operations. As cyber threats increasingly impact business continuity, failing to address these risks can expose producers to potential errors and omissions (E&O) claims. Multiple state regulatory bodies and industry standards, such as those outlined by the National Association of Insurance Commissioners (NAIC), stress the importance of comprehensive risk assessments, including cyber exposures.

Moreover, sectors such as healthcare, finance, and retail face stringent regulatory requirements for data protection under laws like the *California Consumer Privacy Act (CCPA)*, *New York Department of Financial Services (NYDFS) Cybersecurity Regulation*, and the *General Data Protection Regulation (GDPR)* for international operations. Producers who educate clients on insurance options that help meet these compliance requirements deliver measurable value and risk mitigation.

3. Commercial Opportunity for Producers and Clients

The cyber insurance market represents a rapidly expanding commercial opportunity. The *Marsh Cyber Market Update (February 2024)* reported that cyber insurance premiums have grown by 35% year-over-year, with increased demand across both large enterprises and SMEs. Offering cyber coverage allows producers to:

- **Cross-sell and Upsell Opportunities:** Producers can bundle cyber insurance with general liability or business owner policies, enhancing their value proposition and increasing premium volume.
- **Market Differentiation:** Demonstrating expertise in cyber risk management can position producers as trusted advisors, differentiating them in a competitive market.
- **Support for SMEs:** According to the *Summary of SME Pricing*, small business cyber policies are increasingly affordable, with streamlined underwriting processes, making it a viable and accessible option for smaller enterprises.

4. Deepening Client Relationships and Building Trust

Consistently discussing cyber risk fosters deeper client relationships by positioning the producer as a proactive risk advisor. Cyber insurance discussions can open broader conversations about risk management, incident response, and business continuity planning. Additionally:

- **Frequency of Discussion:** Producers should raise the topic of cyber insurance at every renewal and during any mid-term reviews or risk assessments. According to *Example Risk Mitigation Protocols*, annual cyber risk assessments, combined with regular policy reviews, help ensure that clients' coverage evolves with their risk profile.
- **Value-Added Services:** Offering risk mitigation resources such as cyber hygiene checklists and security awareness training (as recommended in the *Cyber Hygiene Data Points* survey) further demonstrates commitment to clients' long-term success.

5. Addressing Client Objections and Overcoming Misconceptions

Common objections to purchasing cyber insurance include cost concerns and misconceptions about coverage. Producers should address these by:

- **Providing Context with Data:** Highlighting claims trends, such as those in the *HT Cyber 1st January Renewal Report*, which showed that even SMEs face six-figure losses from cyber incidents.
- **Demonstrating ROI:** Explaining how cyber coverage not only transfers risk but can also provide resources for breach response, legal costs, and regulatory fines.

- **Educating on Coverage Scope:** Clarifying coverage aspects such as first-party losses (e.g., data restoration and business interruption) and third-party liabilities (e.g., lawsuits from affected customers).

6. Leveraging Technology and Partnerships for Better Client Outcomes

Producers can leverage tools and partnerships to enhance the client experience and streamline the cyber insurance process:

- **Digital Risk Assessments:** Using third-party risk assessment platforms (e.g., through MGA technology providers) to identify client vulnerabilities.
- **Collaborating with TPAs:** Partnering with Third-Party Administrators (TPAs) specializing in cyber claims to ensure efficient claims handling and incident response.
- **Offering Risk Mitigation Tools:** Through partnerships with cyber security service providers, producers can help clients implement minimum security standards, which are increasingly required for policy eligibility.

7. Conclusion: The Imperative for Proactive Cyber Risk Conversations

Discussing cyber risk and insurance options with all enterprise clients, including small businesses, is no longer optional—it is a fundamental component of comprehensive risk management. From regulatory compliance to commercial opportunity, the benefits of proactively addressing cyber risk are clear. Insurance producers who embed cyber risk discussions into their client engagement strategies not only protect their clients' businesses but also position themselves as indispensable partners in an evolving risk landscape.

To fully capture this opportunity, producers should:

- Raise the topic of cyber insurance at every policy review and renewal.
- Provide educational resources and risk assessment tools.
- Offer tailored solutions that match clients' industry and risk profile.
- Continuously update clients on evolving threats and coverage trends.

In doing so, producers will not only drive business growth but also foster long-term, trust-based relationships that position them as essential advisors in an increasingly digital economy.

Addressing the Top 5 Client Objections to Cyber Risk Mitigation and Transfer Options

When discussing cyber risk mitigation and insurance with enterprise clients, producers often face objections rooted in misconceptions, cost concerns, or lack of understanding about coverage value. Proactively addressing these objections is crucial for closing coverage gaps and positioning the producer as a trusted advisor. Below are the five most common objections and effective responses for insurance producers.

A. "Cyber Insurance is Too Expensive"

Client Concern:
Clients, especially SMEs, often perceive cyber insurance premiums as cost-prohibitive, particularly if they have not experienced a cyber incident firsthand.

Producer Response:

- **Cost-Benefit Framing:** Emphasize the high cost of cyber incidents versus the cost of coverage. For example, according to the *HT Cyber 1st January Renewal Report*, the average cost of a ransomware attack for SMEs exceeds $200,000, while typical premiums for SMEs range from $1,500 to $5,000 annually.
- **Coverage Value:** Explain that cyber policies often include valuable risk management services such as incident response teams, forensic investigations, and legal support, which alone can justify the premium cost.
- **Tailored Coverage Options:** Highlight the availability of scalable policies designed for smaller enterprises with lower premiums and coverage limits that match their needs, as outlined in the *Summary of SME Pricing*.

B. "Our Business is Too Small to Be a Target"

Client Concern:
SMEs often assume they are not significant enough to attract cybercriminals.

Producer Response:

- **Dispelling the Myth:** Share industry data, such as from the *Final 2024 Cyber Report*, which indicates that SMEs are increasingly targeted because they are perceived to have weaker security defenses. Over 60% of cyberattacks in 2024 targeted businesses with fewer than 500 employees.
- **Automation of Attacks:** Explain that many cyberattacks, such as phishing and ransomware, are automated and indiscriminate, meaning size does not protect against risk.
- **Regulatory Risk:** Emphasize that data privacy laws apply regardless of business size, and a data breach could result in fines and lawsuits.

C. "We Already Have Strong Cybersecurity Measures in Place"

Client Concern:
Clients with robust security controls may believe they do not need cyber insurance.

Producer Response:

- **Complementary Role of Insurance:** Emphasize that even with strong cybersecurity, human error, supply chain vulnerabilities, and zero-day exploits pose significant risks. Insurance acts as a financial backstop when controls fail.

- **Risk of Business Interruption:** Highlight that cyber insurance can cover business interruption losses, which security measures alone cannot prevent or compensate for.

- **Contractual and Compliance Needs:** Point out that many vendors and partners now require cyber coverage in contracts, and it may be necessary to comply with industry regulations (e.g., *NYDFS Cybersecurity Regulation*).

D. "Cyber Insurance Won't Cover the Risks We Actually Face"

Client Concern:
Clients may be skeptical about policy exclusions or believe cyber policies are too narrow to address their specific risks.

Producer Response:

- **Policy Clarity:** Offer to walk through sample policy wording, such as from the *Aviva Cyber Insurance Policy Documents*, explaining coverage for:
  - First-party losses (e.g., data recovery, notification costs, crisis management)
  - Third-party liabilities (e.g., lawsuits from customers or partners)
  - Regulatory fines and penalties (where permitted)
- **Customization Options:** Explain that policies can be tailored to their industry and specific risk profile, including coverage for supply chain attacks, system failures, and social engineering fraud.
- **Improved Policy Terms:** Share insights from *Marsh's Cyber Catalyst Program*, which highlights carriers that offer broader and more innovative coverages.

E. "We're Not Sure How to Evaluate or Implement Cyber Insurance"

Client Concern:
Clients may find cyber insurance confusing and may not know how to compare policies or ensure they meet their needs.

Producer Response:

- **Educational Approach:** Offer a structured cyber risk assessment and coverage comparison using tools such as *Example Risk Mitigation Protocols* and cyber hygiene checklists.
- **Simplified Options:** Present coverage tiers (e.g., basic, standard, comprehensive) to simplify decision-making.
- **Ongoing Support:** Emphasize that your role is not only to place coverage but to support risk management continuously, including assistance with claims and annual policy reviews.

Conclusion

By anticipating and effectively responding to these common objections, insurance producers can overcome client hesitations, educate their clients, and reinforce the value of cyber insurance as a critical component of comprehensive risk management. This approach not only drives policy uptake but also builds long-term, trust-based client relationships, positioning the producer as an essential partner in navigating the complex landscape of cyber risk.

February 2024
Cyber Assurance Group Incorporated

This white paper is based on data from industry-leading reports, including the *Marsh Cyber Market Update (February 2024)*, *Final 2024 Cyber Report*, *HT Cyber 1st January Renewal Report*, and the *Summary of SME Pricing*.