CYBER LIABILITY INSURANCE: A CONCISE INTRODUCTION

This document outlines the salient points raised in AMCHAM TT's Tech Hub Islands Sumit 2026 Panel discussion: "***Cyber Resilience & Risk Transfer***", on 30th June 2026.

1. WHAT DOES A "CYBER LIABILITY" POLICY ACTUALLY COVER?

A cyber policy operates on two tracks: protecting your own business and protecting you from claims by others.

First-Party (Your Own Losses)

- Incident response & digital forensics
- Business interruption and extra operating expenses during recovery
- Data restoration costs
- Ransomware / cyber extortion payments (where legally permissible)
- Mandatory breach notification costs, both regulatory and customer
- Crisis communications and PR management

Third-Party Liability (Claims Against You)

- Privacy liability from affected individuals or regulators
- Network security liability, where your breach affects third parties
- Regulatory fines and penalties (where insurable at law)
- Media liability: defamation or IP infringement in digital content

Common Extensions to the policy

- Social engineering / funds-transfer fraud
- Contingent business interruption (cloud or vendor outage)
- Reputational harm cover
- Deepfake fraud, AI-assisted phishing, AI-generated malware and cyber attacks involving the insured's use of AI tools

> *"A cyber policy doesn't just pay for the breach: it pays for everything that happens after the breach, which is usually where the real damage lives."*

2. HOW DOES THE APPLICATION PROCESS WORK?

- **First, a proposal form is completed**, which covers network architecture, multi-factor authentication, backup strategy (frequency and air-gapping), endpoint detection, email security, employee training, and prior incident history.
- **Larger risks** typically require an underwriter call and/or an external scan of your digital attack surface.
- **Timelines:** SME risks can bind within days. Mid-market risks with security review: 2 to 4 weeks. Complex placements with remediation conditions: 4 to 6+ weeks.

> *"The application itself is often the first cybersecurity audit a company has ever had — and sometimes the only one until something goes wrong."*

3. HIDDEN VALUE #1: FREE THREAT INTELLIGENCE

The underwriting process is more than a form. It is a genuine security consultation even before you place cover and at no charge.

- **Underwriters review your actual control environment,** not just your policies on paper.

Brokerslink Partner

5 ARIAPITA DRIVE, WOODBROOK 170511
TRINIDAD & TOBAGO, WEST INDIES

VOICE +1 868 628 7732
BESPOKEBROKING.COM

- **Their feedback reflects live claims data across thousands of businesses**, what is actually causing breaches right now, not generic guidance from 18 months ago.
- **Better security controls translate directly into better premium terms,** a real financial incentive to improve your posture.

> *"Your insurer has seen more breaches this month than your IT team will see in a career. That underwriting call is genuinely free threat intelligence."*

4. HIDDEN VALUE #2 - 24/7 EMERGENCY RESPONSE ON RETAINER

Included in most cyber policies at no additional cost: instant access to a pre-vetted panel of specialists, usually through a smartphone app that is shared with policyholders once cover is in place, and that means your response team are available around the clock.

- Digital forensics firms
- **Specialist breach counsel** (legal advice from day one)
- PR and crisis communications experts
- **Panel relationships are negotiated at insurer scale -** better response times and rates than any individual business could secure alone, mid-crisis, at 2am.

> *"When a breach hits, the worst time to start Googling 'forensic IT firm near me' is during the breach. The policy means that number is already in your phone."*
>
> *"It's not just claims money — it's a SWAT team on retainer."*

5. HOW CYBER INTERACTS WITH YOUR OTHER POLICIES

- **Fidelity Guarantee and/or Commercial Crime:** Traditional crime policies respond poorly to funds-transfer fraud, business email compromise, and social engineering, which is how most theft happens today. Cyber policies fill this gap with purpose-built cover.
- **Directors & Officers:** Directors face growing personal liability for inadequate cyber governance. A major breach can trigger regulatory scrutiny and derivative actions against the board. Cyber and D&O policies must be reviewed together to ensure no gap falls between them.

> *"A phishing email doesn't care whether your policy calls it a 'cyber event' or a 'crime loss' — but your insurer might. That's why these policies need to talk to each other."*
>
> *"Boards used to worry about cyber risk. Now they need to worry about being personally liable for not worrying about it enough."*

6. SHOULD YOU PAY A RANSOM? THE FULL PICTURE.

This is one of the most misunderstood decisions in a cyber incident. Here is what you need to know before you even consider it.

- **Payment of a cyber ransom is not explicitly illegal in T&T — but far from safe.** There is no statute that directly criminalises paying a ransom. The danger lies in what surrounds the payment.
- **Terrorism financing risk.** T&T's Anti-Terrorism Act and AML/CFT regulations criminalise providing funds to designated entities, knowingly or recklessly. Many major ransomware groups are formally sanctioned under US, UK, and Australian law. Paying them in crypto may constitute terrorism financing under T&T law, regardless of intent.
- **International sanctions exposure.** US OFAC sanctions apply extraterritorially and carry strict liability - you can be penalised even without knowing you paid a sanctioned group. If your payment touches a US bank or clears through New York, you have a potential OFAC problem. That describes most businesses in T&T.

Brokerslink Partner

5 ARIAPITA DRIVE, WOODBROOK 170511
TRINIDAD & TOBAGO, WEST INDIES

VOICE +1 868 628 7732
BESPOKEBROKING.COM

- **Payment doesn't extinguish regulatory duties.** Every breach notification obligation that arose at the moment of the attack remains fully in force after payment. Modern ransomware almost always involves double extortion (data stolen before it's encrypted) so paying for a decryption key does nothing to retrieve the exfiltrated copy.
- **T&T's Data Protection Act - the sleeping giant.** Passed in 2011 but never fully proclaimed into force. Full private sector obligations remain pending a Presidential Proclamation that can happen at any moment, with no further parliamentary process required. Businesses without a compliance plan are already behind.
- **Where your data lives matters.** Cloud infrastructure in the EU, UK, or US can expose a T&T company to GDPR, UK GDPR, and US state data laws simultaneously, regardless of where the business is incorporated. A single breach can trigger multiple notification regimes at once, each with different deadlines.
- **The practical case against paying is strong.** 84% of those who paid ransoms in Q4 2024 failed to fully recover all data, and 80% of the total were attacked again within 12 months. Three quarters of victims now refuse to pay — and most recover anyway through backups and expert IR support.

Here are some takeaways to keep in mind:

> *"Paying the ransom buys a decryption key. It does not buy regulatory absolution, guarantee data recovery, or prevent the next attack."*

> *"The Data Protection Act has been asleep for over a decade — but it can be awakened overnight. Is your business ready for the morning it comes into force?"*

> *"In T&T, paying a ransom isn't a crime. But depending on who you're paying and how you pay them, it very well may become one."*

7. CHOOSING THE RIGHT SUM INSURED — A CRITICAL DECISION

Selecting an appropriate sum insured is one of the most consequential, and most frequently underestimated, decisions in the cyber insurance process. Buying the right cover at the wrong limit is not much better than having no cover at all.

- The sum insured must reflect the realistic total cost of a major incident, not simply a round number or an estimate based on the ransom demand alone. **The ransom is often the smallest component of the overall loss**.
- Key variables to consider include: the volume and sensitivity of data held, reliance on digital systems for revenue generation, the regulatory environment applicable to that data, contractual liability to third parties, the cost of forensic investigation, legal fees, notification obligations, and the duration of potential business interruption.
- Multi-jurisdictional exposure can dramatically increase the appropriate limit - a business subject to both T&T data obligations and GDPR faces a very different maximum loss scenario than one operating in a single jurisdiction.
- Underinsurance is a real and common risk. Many businesses set limits based on premium comfort rather than exposure analysis and discover the gap only at the point of claim - when it is too late to close it.

> *PRFC Limited has developed detailed guidance on how appropriate cyber sums insured should be calculated across a range of business types and risk profiles. If you would like a structured conversation about the right limit for your business, we would welcome the opportunity to walk you through our approach. Get in touch with our team to arrange a no-obligation discussion.*

IN CLOSING

Cyber liability insurance protects against an exposure that, unlike a building or a vehicle, has no physical form and did not exist in its current shape a decade ago for most organisations. PRFC Limited is available to work through this exercise with you, category by category, using your organisation's own details, and to review the exposures a cyber liability policy is intended to address.

Rodney B. Farah, ACII, ARM, CBCI
Managing Director - PRFC Limited
Regional Manager, Americas - Brokerslink

Brokerslink Partner
5 ARIAPITA DRIVE, WOODBROOK 170511
TRINIDAD & TOBAGO, WEST INDIES
VOICE +1 868 628 7732
BESPOKEBROKING.COM