News release

Date	**7 October 2022**
Contacts	Marina Mello, Communications marina.mello@pwc.com
Pages	2 pages

One in four companies globally have suffered a data breach that cost them US$1-$20 million or more in the past three years

- Bermuda re/insurers work to deploy more cyber capacity as attacks fuel growing demand for cyber cover

7 October 2022 – One in four companies (27%) globally have suffered a data breach that cost them US$1-$20 million or more in the past three years, according to PwC's annual Global Digital Trust Insights Survey, which surveys more than 3,500 senior executives across 65 countries. The percentage rises to one in three (34%) for companies surveyed in North America, with only 14% of firms globally reporting that no data breaches have occurred during the period.

Despite cyber attacks continuing to cost businesses millions of dollars, fewer than 40% of executives surveyed say they have fully mitigated cybersecurity risk exposure in a number of critical areas. This includes, enabling remote and hybrid work (38% say the cyber risk is fully mitigated); accelerated cloud adoption (35%); increased use of internet of things (34%); increased digitisation of supply chain (32%) and back office operations (31%).

For operations-focused executives surveyed, supply chain security is a major concern. Nine in ten expressed concern about their organization's ability to withstand a cyber attack that disrupts their supply chain, with 56% extremely or very concerned.

"The continued increased prevalence and severity of cyber attacks has fueled a growing demand for cyber coverage, which appears to be far outstripping supply, offering a huge commercial opportunity for specialty insurers and reinsurers," **said Matt Britten, Insurance Partner, PwC Bermuda**. "The rapid evolution of cyber risk does present extreme challenges to underwriting and pricing, but reinsurers risk losing relevance if the demand for cyber cover isn't met."

He added: "During 2021 and this year, there has been an acceleration among Bermuda-based reinsurers towards speciality reinsurance with several carriers and brokers establishing dedicated cyber teams and units. This trend is expected to continue as they work to deploy more capacity to the market."

Most organizations are increasing cyber budgets

The majority of executives surveyed said their organizations are continuing to increase their cyber budgets – 69% said the budget increased in 2022 and 65% plan to spend more on cyber in 2023. Increasing budgets reflect the fact that cybersecurity tops the agenda for resilience planning.

Concern with cyber extends to the top of organizations. Most CEOs surveyed are planning to ramp up action to address cybersecurity in the coming year - 52% said they will drive major initiatives to improve their organisation's cyber posture. Many CFOs surveyed are also planning to increase their cyber focus, including cyber technology solutions (39%), focus on strategy and coordination with engineering/operations (37%) and upskilling and hiring of cyber talent (36%)

It's not hard to see why cyber continues to move up the corporate agenda. The cost of cyber breaches goes much further than direct financial costs, according to marketing-oriented execs surveyed. The range of harm organizations have experienced due to a cyber breach or data privacy incident over the past 3 years include loss of customers (cited by 27%), loss of customer data (25%) and reputational or brand damage (23%)

Bruce Scott, Cyber Leader, PwC in the Caribbean, said, "According to PwC's survey – a catastrophic cyber attack is the top scenario in 2023 resilience plans. It ranks *higher* than global recession, a new health crisis or inflationary environment. As cyber threats continue to increase in frequency and sophistication, a holistic approach to cybersecurity has become a top priority for the C-suite and boards."

To improve cyber resilience and build public trust, it's clear from PwC's survey that a higher level of public-private collaboration is needed to address the increasingly complex cyber threat landscape – companies are calling for increased information sharing and transparency as well as a consistent format for mandatory disclosure of cyber incidents.

Anthony Zamore, Cyber director, PwC in the Caribbean, said: "The good news is cyber has progressed on many fronts as CISOs and cyber teams rise to the challenge, and other C-suite executives join forces with them."

While progress has been made, **Zamore cautions**, there are three things that need to be put in place to keep pace with digital transformation and help build public trust:

- A strategic risk management programme
- Continuity and contingency planning
- Clear, consistent external reporting

Mandatory disclosure of cyber incidents is favoured

Four in five organisations (79%) surveyed state that a comparable and consistent format for mandatory disclosure of cyber incidents is necessary to gain stakeholder confidence and trust. Three-quarters (76%) agree that increased reporting to investors will be a net benefit to the organisation and entire ecosystem. Further, the same percentage agree that governments should be expected to use the knowledge base from mandatory cyber attack disclosures to develop cyber defence techniques for the private sector.

While there is a clear preference for mandatory disclosure of cyber incidents, fewer than half (42%) of executives surveyed are fully confident their organization can provide required information about a material/significant incident within the specified reporting period. There is also a hesitance to

share too much information – 70% said greater public information sharing and transparency poses a risk and could lead to a loss of competitive advantage.

Ends

About the Global Digital Trust Insights Survey

The Global Digital Trust Insights Survey captures the views of senior executives on the challenges and opportunities to improve and transform cybersecurity within their organisation in the next 12-18 months. The Survey includes 3,522 respondents across 65 countries. Companies with revenues greater than US$1bn make up 52% of those surveyed; 25% have revenues greater than US$5bn.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 152 countries with nearly 328,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.