CG Matsunaga's remarks at the opening of seminar "Recent trends in cyber-attacks: mitigating, assessing, and responding to cybersecurity risks" on January 28, 2025

Ms. Molly Reynolds, Partner, TORYS LLP,
Mr. Rohan Dixon, President, and CEO, Sompo Canada,
Mr. Justin Folkerts, Partner and CTO, Supra ITS,
Ms. Julie Himo, Partner, TORYS,
Distinguished business leaders in Toronto,
Dear friends,
Good evening.

Today, we face an increasingly elevated and compounded cyber threat landscape. The tradecraft of perpetrators is evolving. Addressing cyber-attacks is becoming ever challenging. So, I highly value today's seminar, and pay homage to the organizers: TORYS and the Japan Society. Thank you for this opportune initiative.

Today we focus on cybercrime, in particular ransomware. Before speaking about ransomware, however, allow me to take a broader view of recent cyber-attacks.

The aims of cyber-attack perpetrators are not necessarily financial, but also causing disruptions per se, targeting critical infrastructure networks, pursuing auxiliary military goals, or pre-positioning for potential future disruptive or destructive cyber operations, or engaging online information campaigns to intimidate and shape public opinion. Canada's National Cyber Threat Assessment states bluntly that "(c)ritical infrastructure is increasingly at risk from cyber threat activity," "(c)yber threat actors are attempting to influence Canadians, degrading trust in online spaces," and "Canada's state adversaries are using cyber operations to disrupt and divide."

The Spector of similar risks was laid bare in Japan, too, at the end of 2024, when it witnessed large-scale disruptions of networks of a major airline and multiple major banks. The Government of Japan recognizes that the threat of cyber attacks is growing rapidly, cyber attacks have been used constantly to disable or destroy critical infrastructures, interfere in foreign elections, demand ransoms, and steal sensitive information, even in the form of state-sponsored cyber attacks.

Cyber threat actors, including state adversaries and state-sponsored actors, employ diverse mode of

attacks, inter alia, denial of services, deleting or leaking data, and manipulating industrial control systems. They also include scams and fraud, identity theft, exploiting software, hardware or network vulnerabilities, password cracking, and ransomware and other malicious software.

Among all these, ransomeware incident is prevalent and increasing. Notwithstanding major law enforcement actions targeting large ransomeware operations, according to a report, year 2024 recorded 5,414 published ransomware attacks on organizations worldwide, standing for an 11% increase compared to 2023. There was a dramatic spike during Q4.

Toward the end of the year, there was a significant increase in ransomeware incidents targeting the manufacturing sector, which ranked third after business service and retail. Country-wise, in 2024, Canada was again the second most ransomeware targeted country as it was in 2023, second only to the US.

Ransomware attack's average cost was $1.85 million per incident in 2023. The largest ransomware payout was made by an insurance company for $40 million in 2021. In Canada, most ransomware victims did not

make a ransom payment. Of those that did indicate making a ransom payment, the majority paid less than $10,000, while 4% paid more than $500,000. The average downtime a company experiences after a ransomware attack was 24 days.

The Canadian Government states, “ransomware is almost certainly the most disruptive form of cybercrime facing Canadians,” and “(c)ybercriminals deploying ransomware have evolved in a growing and sophisticated cybercrime ecosystem and will continue to adapt to maximize profits.”

How are Canadian companies responding to these cybercrime risks? Spending on recovery from cybercrime incidents has increased: doubling from approximately $600 million in 2021 to $1.2 billion in 2023. In contrast to recovery spending, total spending on prevention and detention of cyber security incidents rose at a a slower pace. The largest cyber security cost for businesses in 2023 was employee salary related to prevention or detection, followed by cyber security software costs and consultation contractor expenses. The cost of providing training to employees, suppliers, customers, or partners was much smaller. Regarding insurance, 22% of businesses

had cyber risk insurance in 2023, up six percentage points from 16% in 2021.

Ransomware attacks have also become a significant concern affecting essential services such as hospitals, schools, municipalities, and utility providers.

Canada's latest assessment states that "(r)ansomware is the top cybercrime threat facing Canada's critical infrastructure." It predicts that "(i)n the next two years, ransomware actors will almost certainly escalate their extortion tactics and refine their capabilities to increase pressure on victims to pay ransoms and evade law enforcement detection." It also draws attention to the Cybercrime-as-a-Service (CaaS) business model, stating that the CaaS "is almost certainly contributing to the continued resilience of cybercrime around the world including in Canada."

To conclude, all these recent analyses both in the private and public sectors appear to attest to the value of today's seminar. We are fortunate today to have highly qualified panelists, with their rich exposures to the latest developments, their direct engagements with diverse stakeholders, and their experiences of providing partners with practically oriented advice. I trust what we are going to listen to in the next hour

will help guide the audience in wading in the precarious terrains of cyber space with added confidence.

Thank you.

REFERENCE:

The National Cyber Threat Assessment 2023-2024 https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024

The National Cyber Threat Assessment 2025-2026 https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf

National Security Strategy of Japan https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf

Ransomware statistics https://cyberint.com/blog/research/ransomware-annual-report-2024/

https://www.varonis.com/blog/ransomware-statistics#top

Biggest ransomware incident payout
https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5

Average cost of ransomware incidents
https://www.getastra.com/blog/security-audit/ransomware-attack-statistics/

Average downtime after a ransomware attack
https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack-us/#:~:text=Length%20of%20impact%20after%20a%20ransomware%20attack%20Q1%202020%2D%20Q3%202021&text=As%20of%20the%20third%20quarter,United%20States%20was%2022%20days.

Impact of cybercrime on Canadian businesses, 2023
https://www150.statcan.gc.ca/n1/daily-quotidien/241021/dq241021a-eng.htm