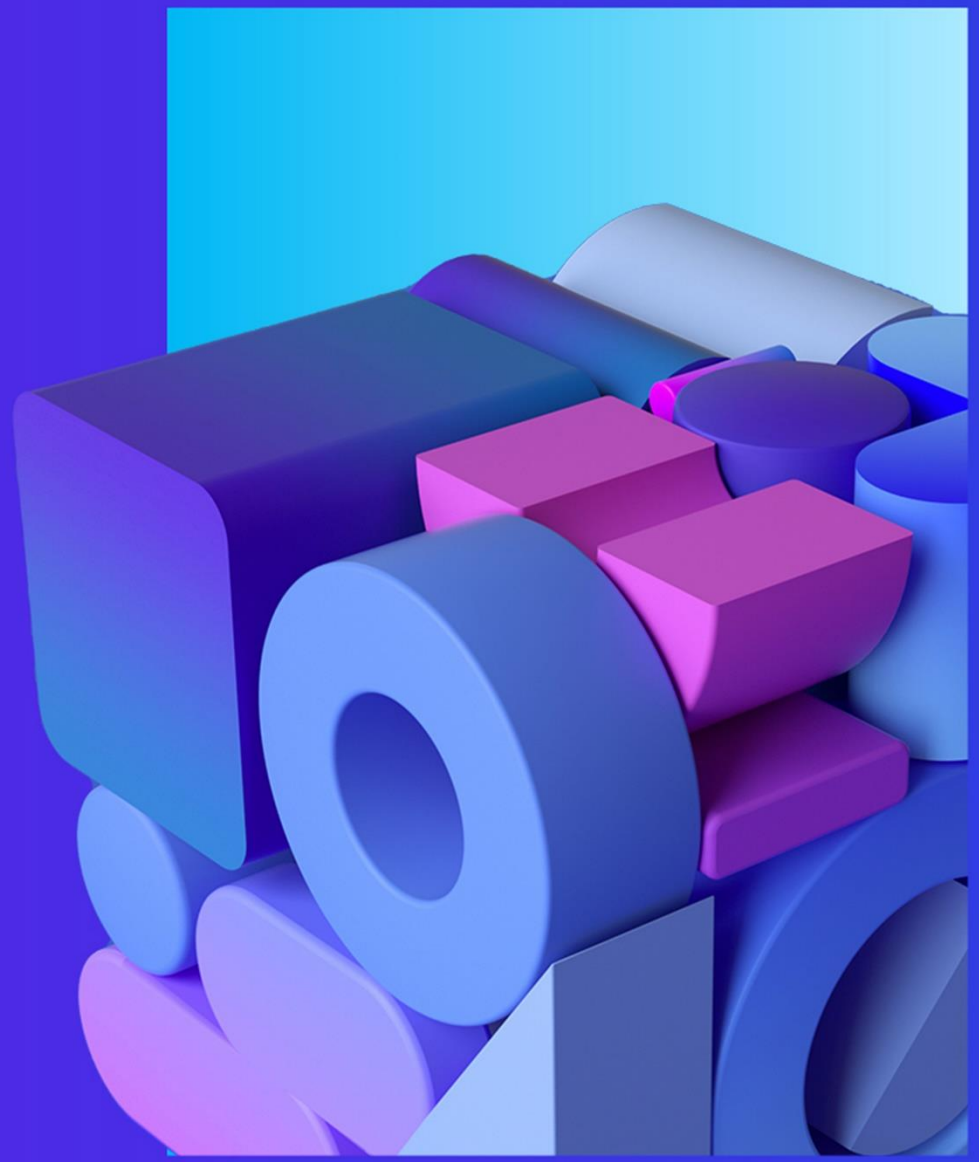
KPMG

Responding to Active Cybersecurity Incidents



Alexander Rau, Partner, Cyber Response

Disclaimer

The statistics, case studies and illustrations we present are based on our work with numerous clients, rather than reflecting the work we have e done for a specific customer or group of customers. We have altered certain details to protect the identities of our clients and the people connected to them.

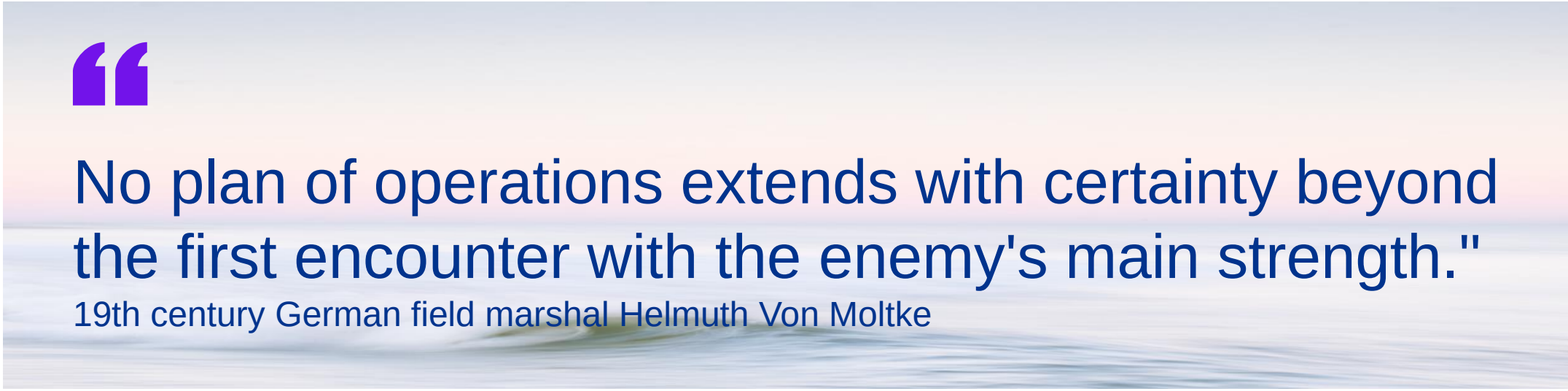
Topics

01 Cyber Trends

02 A closer look at Ransomware

03 To pay or not to pay

04 Tips



No plan of operations extends with certainty beyond the first encounter with the enemy's main strength."

19th century German field marshal Helmuth Von Moltke

Cybersecurity Trends

2021-22 were years of evolution in the incident response space from threat actors adapting their infiltration tactics to organizations and law enforcement shifting their defense strategies. While ransomware continued to dominate headlines, we did notice a number of other significant trends that organizations should be aware of as we move further into 2022, including:

- Zero-day and unpatched vulnerabilities surpassing phishing as the #1 attack vector
- The majority of victims lacking a holistic cyber strategy
- A slowdown on ransomware attacks during Eastern European holidays and summer season

In 2022 (since the beginning of the conflict in Eastern Europe), as an industry, a significant reduction in Ransomware attacks has been observed. “Criminal hacking gangs, usually engaged in corporate ransomware activities, are increasingly being co-opted by the Russian military to launch cyberattacks on Ukraine, according to Digital Shadows[1)].”

Western Intelligence Agencies predict that once the cyber arsenal against the Ukraine is no longer effective or needed, operatives and threat actors may turn their cyber arsenal against the rest of the world, possibly as early as 2023[2)].

1) The Telegraph, October 23, 2022

2) Anonymous source

2022 Cyber Trends observed by KPMG

Rise of Brandless Ransomware groups

Public-sector organizations were targeted with a brandless ransomware (using Alias) to reduce negative media and law enforcement scrutiny. There was limited threat intelligence available for such ransomware operators who used brandless or alias names and did not indicate which group they belong to.

Ransomware activities reduced

Through the Fall and winter of 2022, due to the Russia-Ukraine war and mobilization of military reservists, which included some of the threat actors operating in Russia and Eastern European Regions

Exploitation of Internet facing services

Vulnerability exploitation of internet facing services were one of the top methods on how threat actors gained initial access into an IT Infrastructure. Some of the major vulnerabilities threat actors continue to exploit in the wild include ones associated with organizations running on-premise Microsoft Exchange.

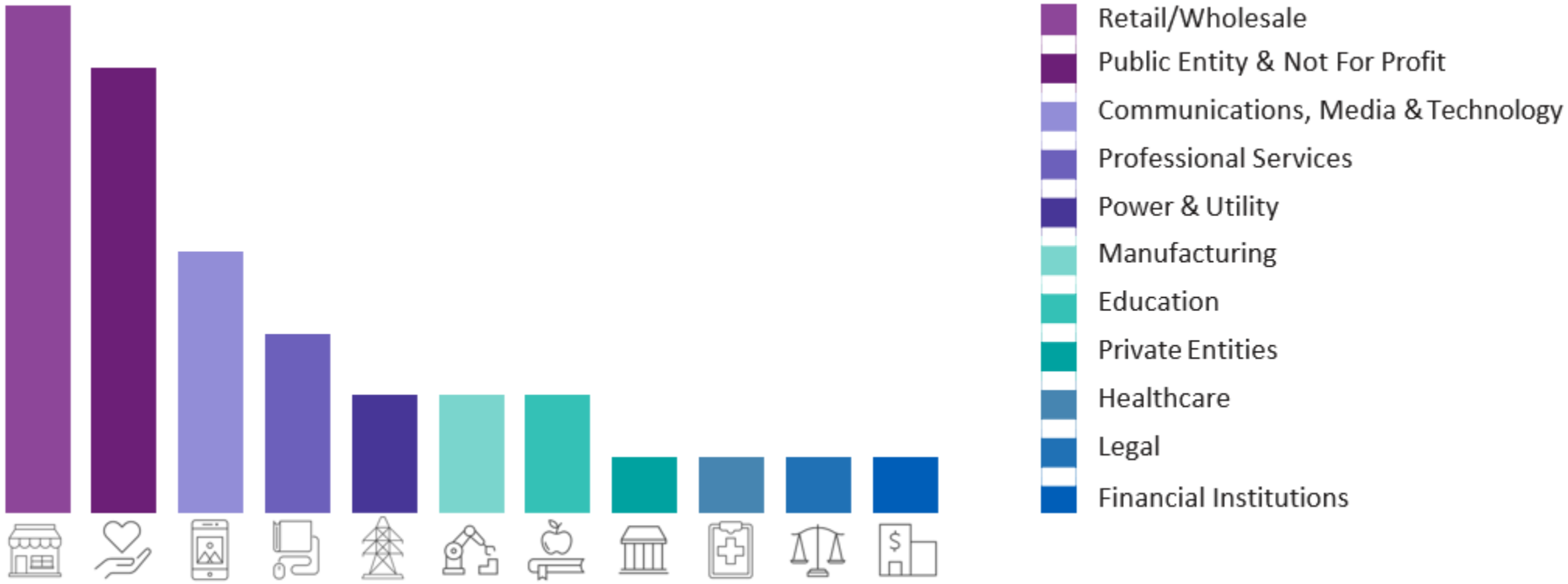
Breaking the human trust

Threat actors seemed to break the human trust by bombing MFA push notifications repeatedly (MFA Fatigue attacks), pushing the limits of human tolerance and forcing them to make a mistake in accepting the push notifications.

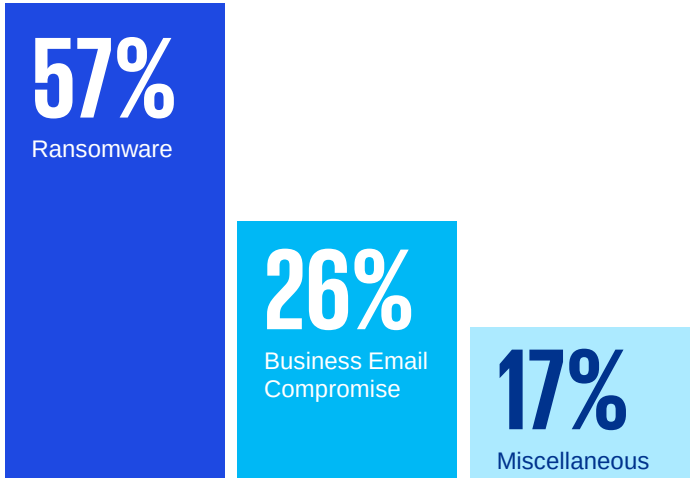
Industries (Global)

1. Healthcare: 15-20%
2. Financial services: 10-15%
3. Retail: 10-15%
4. Government: 10-15%
5. Education: 5-10%
6. Manufacturing: 5-10%
7. Energy and utilities: 5-10%
8. Technology: 5-10%
9. Telecommunications: 3-5%
10. Transportation: 3-5%
11. Other industries: 10-15%

IR engagements by industry –KPMG Canada



Incident Types

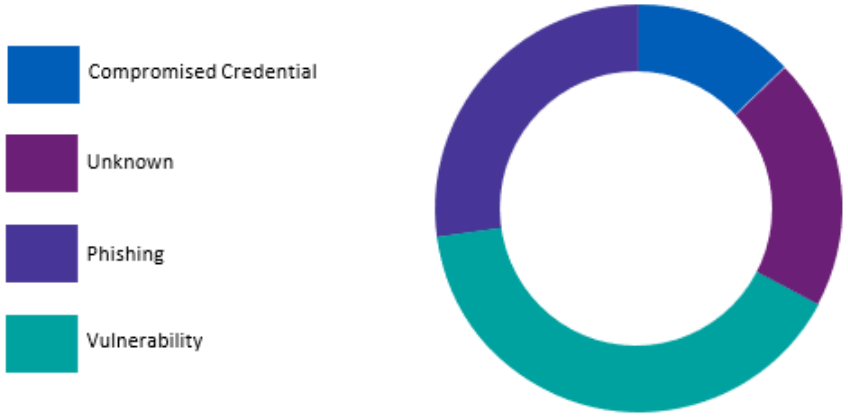


A closer look at ransomware

Ransomware continued to be the dominant driver behind cyber incidents. Not only did the number of ransomware incidents increase versus prior years, but the average ransom amount increased significantly. Significant trends from ransomware include:

- The emergence of ransomware as a platform
- Large corporations and government entities being increasingly targeted by threat actors
- Threat actors focusing more on data exfiltration in an effort to ensure ransom payments are made.

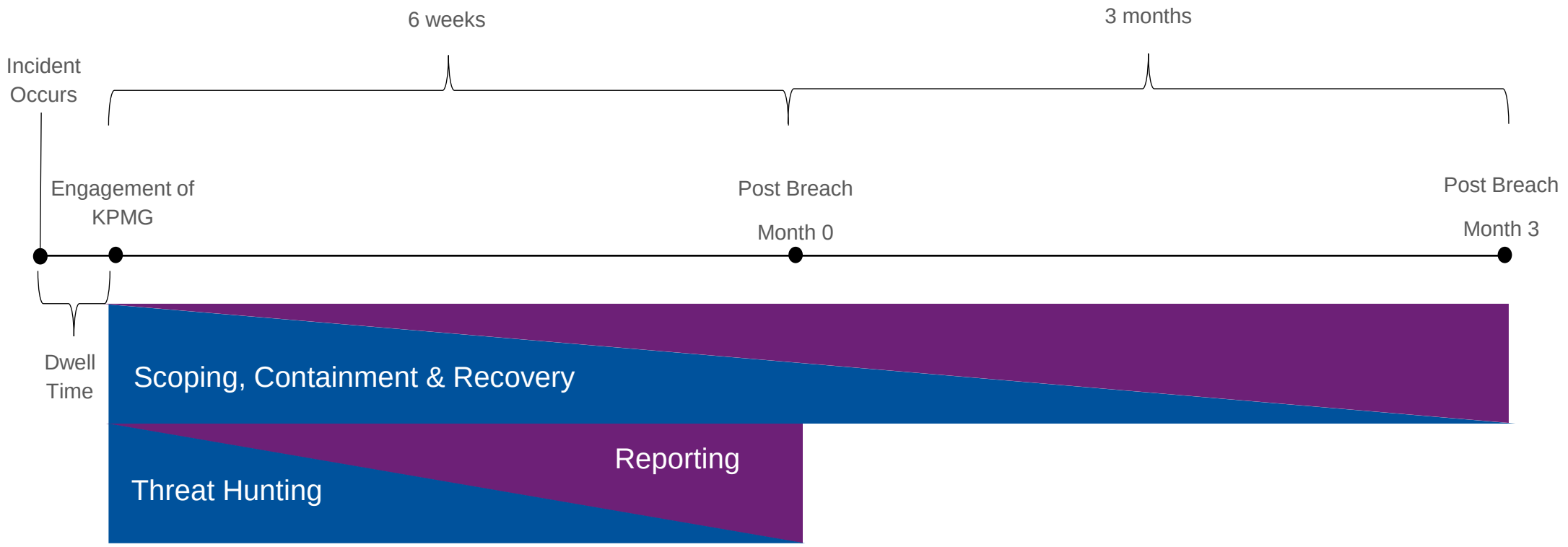
Ransomware root cause



Ransomware paid vs. not-paid

To pay or not to pay

Factor 1: Recovery and Restoration Time



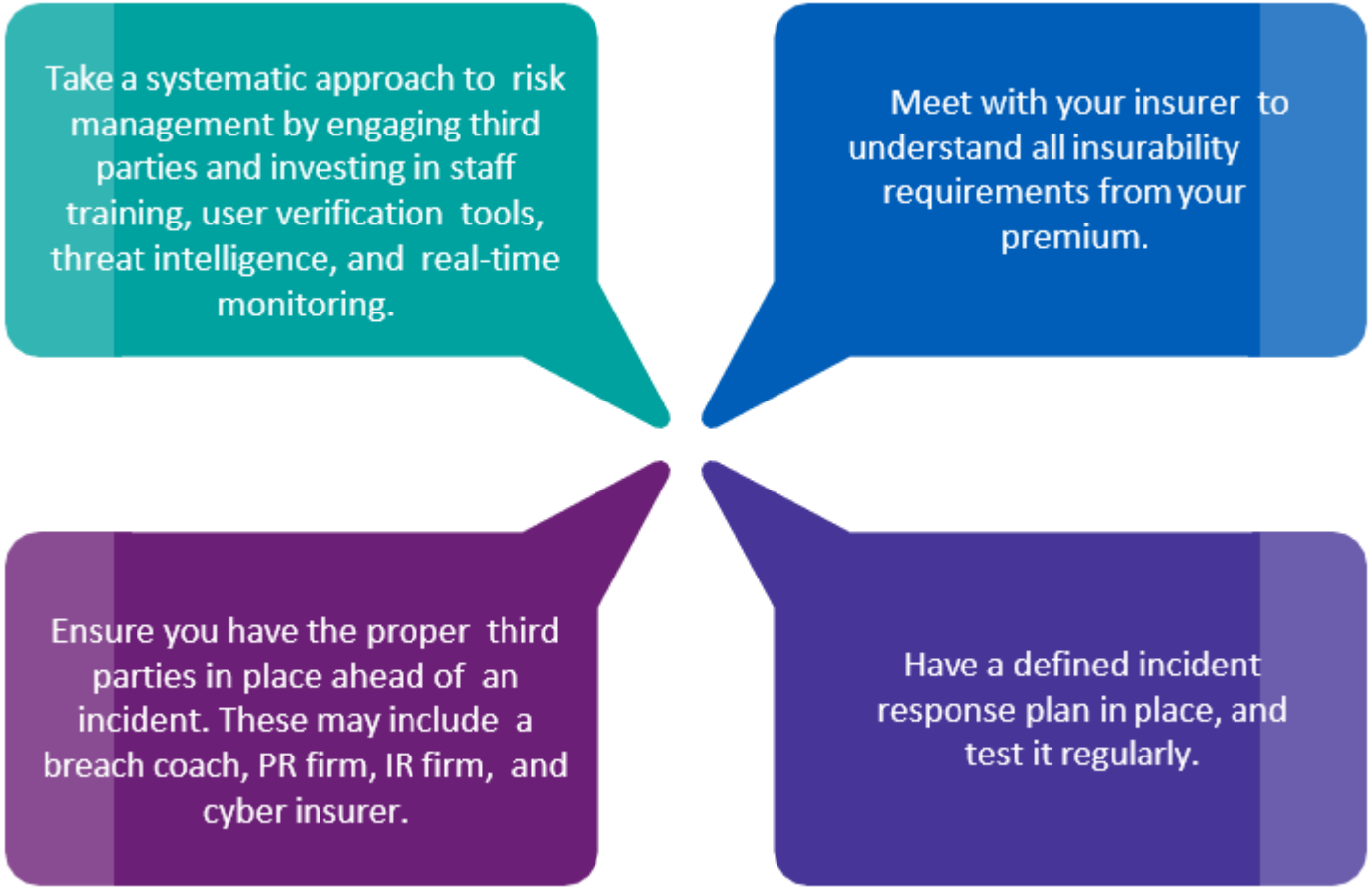
Factor 2: 'Value' of the exfiltrated Data

- Personal Identifiable Information (PII) of customers and/or employees
- Personal Health Information (PHI) of customers and/or employees
- Other sensitive data of customers and/or employees
- Intellectual Capital and confidential business information

Other thoughts on paying for Ransom

- Threat actor on sanctions list?
- Will the decryption keys work?
- Law enforcement is getting more effective in shutting down treat actors – shut down after payment before decryption key is received
- Data is out – who guarantees threat actors will not release and/or come back for future extorsion?
- Legislation to notify victims may have an impact on the decision to pay or not to pay
- Other mitigating, risk reducing ways to protect victims such as credit monitoring and identity theft insurance – possibly cheaper

Tips to enhance your cyber defenses



Q&A

Alexander Rau
Partner, Cyber Response
alexanderrau@kpmg.ca

home.kpmg/ca