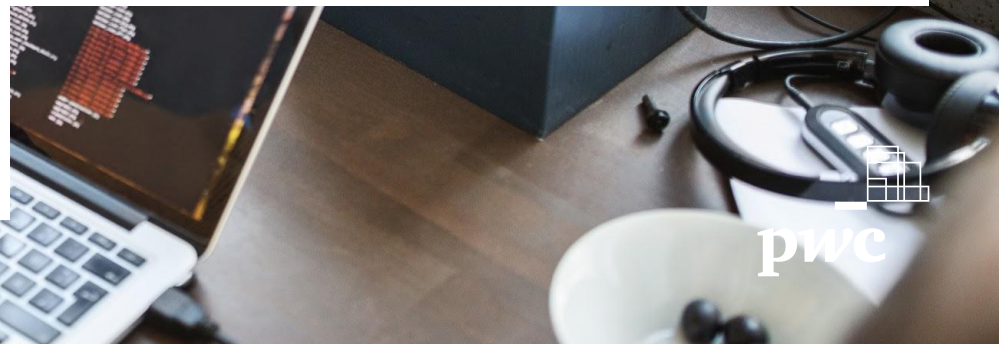


Cyber Risk Management



Cybercrime Landscape

What Cyber crime is...



The frequency of regional cyberattacks have increased

“ I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again. ”

Robert Mueller, Former Director of the FBI

The Royal Bahamas Police Force has reported a 36 percent increase in hacking and extortion in The Bahamas. Between January 1st and June 30th, 2020, there were 118 cyber-crime incidents reported to authorities, compared to the 87 matters reported during the same period in 2019.

Incident Of The Week: Hackers Take Out Caribbean Govt., Access Railway Data

Tags: Cyber Security Incident Of The Week IOTW Cyber-Attacks Sint Maarten Government GWR Great Western Railway Customer Data Accounts Compromised



Dan Gunderman
04/13/2018



Caribbean Cyber-Attacks Increasing

May 18, 2018 | Unallocated Author | 1052 Views | Caribbean, Caribbean cyber attack, cyber-attack, cyber-hack

GUYANA NEWS

Power company still recovering from system hack

By Stabroek News February 28, 2019



Offshore law firm goes after press in Paradise Papers hack

Cayman News | 19/12/2017 | 0 Comments

Vincetian High Commission in UK probes online hack

MELISSA WONG | CREATED : 11 JUNE 2020 | NEWS

Barbados Minister of Health Facebook account hacked

LOOP NEWS | CREATED : 11 APRIL 2020 | COMMUNITY

VM Wealth At Risk Of Civil Suit Over Data Breach, Says Lawyer

Share this Story:

Published: Tuesday | February 18, 2020 | 12:24 AM | Jason Cross/Gleaner Writer

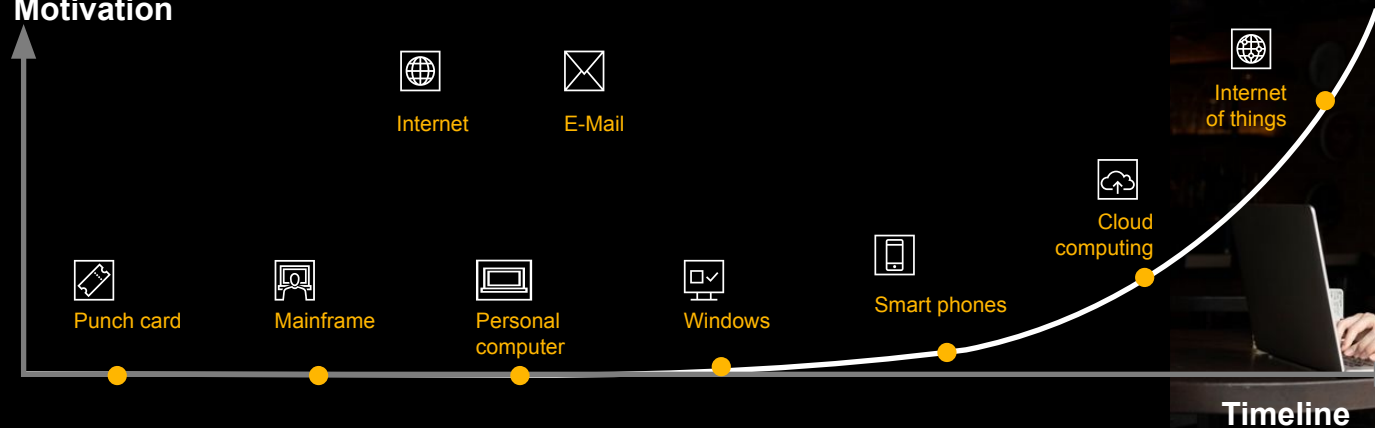
11 government websites were breached by 'VandaTheGod'



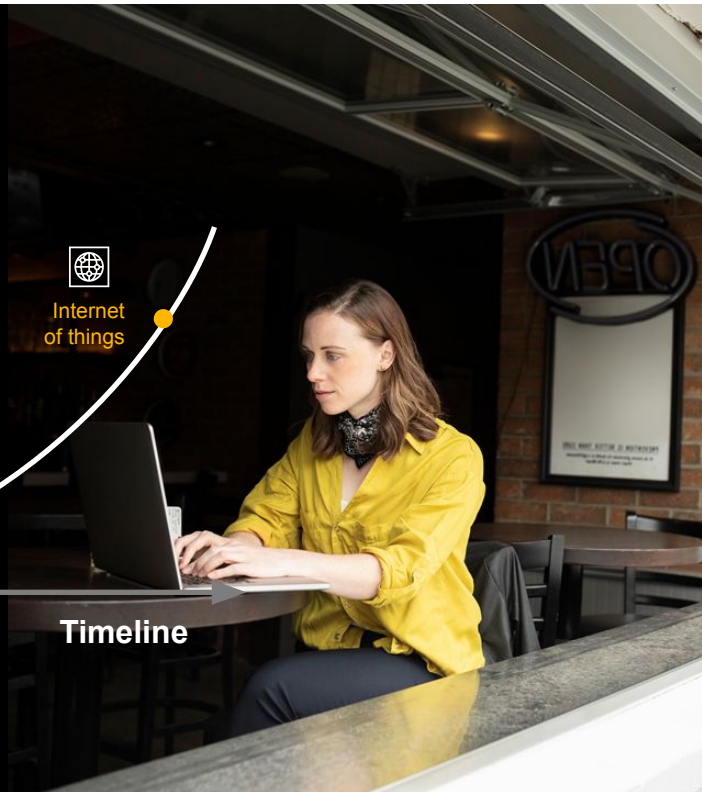
Why is cybercrime a growing concern?

Increasing interconnectivity

Vulnerabilities/
Motivation



Timeline



What is Cybercrime?



Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes).

Cybercrime fits into four (4) categories

1 Cyber-trespassing



Referred to as the act of crossing boundaries of ownership in online environments.

2 Cyber-deception and theft



This category includes all the ways in which individuals may illegally acquire information or resources online and often goes hand in hand with trespassing. **(key threat facing companies)**

3 Cyber-porn and obscenity



Represents a range of sexually expressive content online.

4 Cyber-violence



The sending or access of injurious, hurtful, or dangerous materials online.

Alarming cyber security facts and stats



1

There is a cyber attack every **39** seconds



2

43% of cyber attacks target small businesses



3

The average cost of a data breach in **2020** will exceed **\$150 million**



4

Since **2013** there are **3,809,448** records stolen from data breaches every day



5

Approximately **\$6 trillion** is expected to be spent globally on cybersecurity in **2021**



6

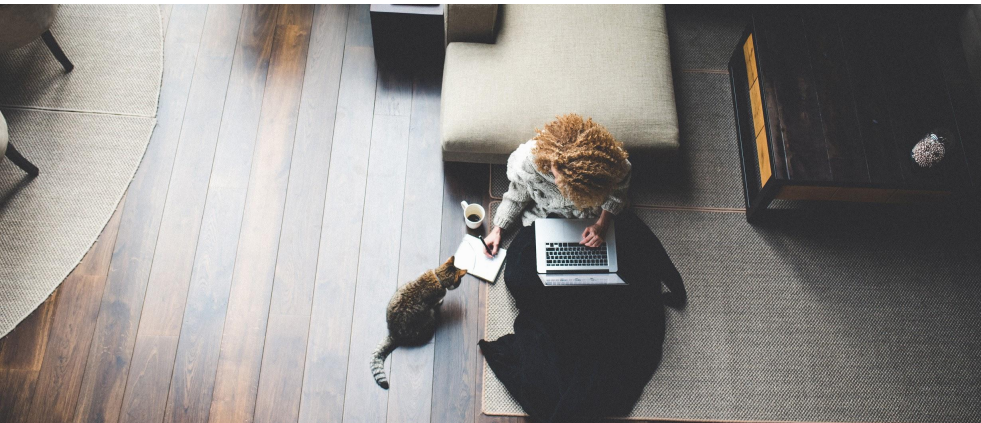
Only **38%** of global organizations claim that they are prepared to handle a sophisticated cyber attack

Cybercrime profits amounted to approx. \$1.5 trillion in 2018

Crime	Annual revenues-\$
Illegal online markets	\$860 billion
Trade secret, IP theft	\$500 billion
Data Trading	\$160 billion
Business Email Compromise	\$1.2 billion
Crime-ware/CaaS	\$1.6 billion
Ransomware	\$1 billion

Notable Breaches

3-billion	Yahoo!
Users compromised (2013 – 14)	
150-million	Under Armour
Users compromised (2018)	
145-million	ebay
Users compromised (2014)	
143-million	Equifax
Users compromised (2017)	
110-million	Target
Users compromised (2013)	
87-million	Facebook
Users compromised (2018)	
76-million	JP Morgan Chase
Households, 7-million	
Small business compromised (2014)	



How much do cyber criminals earn for an individual job?



A

\$6,000



B

\$10,000



C

\$30,000



How much do cybercriminals earn?



While individual hackers may earn around \$30K per month for an individual job. Platform managers for online data forums can earn up to \$2 million

Top tier cyber criminals earn \$167k per month, medium tier \$67K and low skilled \$3.5K

A typical cyber criminal can earn 10% to 15% more than traditional criminals.



Ross Ulbricht of Silk Road reputedly made a personal fortune of over \$1 billion

The new trend is cybercrime as a service

In **2018**

Dutch police shut down the world's largest Distributed Denial of Service DDoS-for-hire service, "webstressor.org" and arrested

6 people behind it.

The site had over

136,000 registered users and allowed customers with little or no technical knowledge to launch a DDoS attack for around









\$14.+

Cybercrime product or Service	Price (US Dollars)
SMS Spoofing	\$20/month
Custom Spyware	\$200
Hacker-for-Hire	\$200+
Zero-Day Adobe Exploit	\$30,000
Zero-Day iOS Exploit	\$250,000

“ Buying malware is currently not a problem: it's easy to find them on various hacker forums, and they are relatively cheap, making them attractive. A cybercriminal following this illegal path doesn't even need any skills – for a fixed price they can get an off-the-peg package to launch their attacks at will. ”

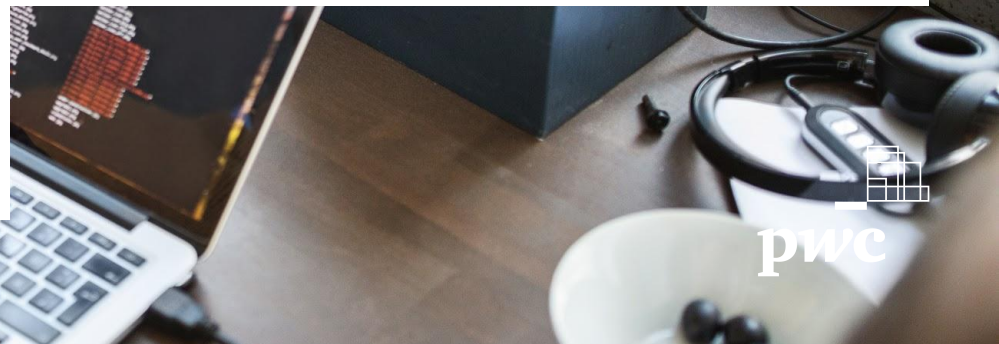
says Alexander Gostev, Chief Security Expert at Kaspersky Lab.

Who are the threat actors?

 Adversaries	 Motives	 Targets	 Impact
Nation State 	<ul style="list-style-type: none"> Economic, political and/or military advantage 	<ul style="list-style-type: none"> Trade secrets Sensitive business information Emerging technologies Critical infrastructure 	<ul style="list-style-type: none"> Loss of competitive advantage Disruption to critical infrastructure
Organised Crime 	<ul style="list-style-type: none"> Immediate financial gain Collect information for future financial gains 	<ul style="list-style-type: none"> Financial/payment systems Personally identifiable information Payment card information Protected health information 	<ul style="list-style-type: none"> Costly regulatory inquiries and penalties Consumer and shareholder lawsuits Loss of consumer confidence
Hackers 	<ul style="list-style-type: none"> Influence political and/or social change Pressure business to change their practices 	<ul style="list-style-type: none"> Corporate secrets Sensitive business information Information related to key executives, employees, customers & business partners 	<ul style="list-style-type: none"> Disruption of business activities Brand and reputation Loss of consumer confidence
Insiders 	<ul style="list-style-type: none"> Personal advantage, monetary gain Professional revenge Patriotism 	<ul style="list-style-type: none"> Sales, deals, market strategies Corporate secrets, IP, R&D Business operations Personnel information 	<ul style="list-style-type: none"> Trade secret disclosure Operational disruption Brand and reputation National security impact

Managing Cyber Risk

Risk Management



What is a cybersecurity risk?

Imagine that the bald tire is tied to a frayed rope hanging from a tree branch.

A High Risk

B Medium Risk

C Low Risk



How much risk is there?

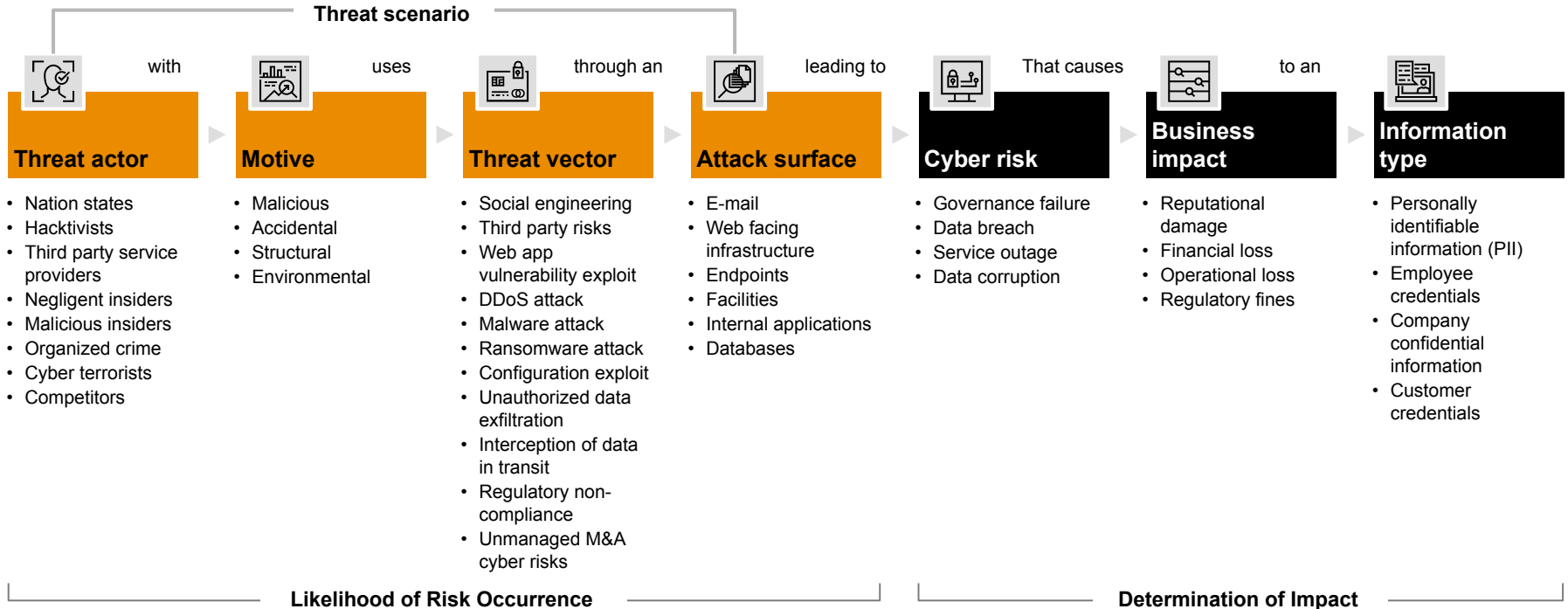
What is a cybersecurity risk?

The threat of quantifiable damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be mitigated through preemptive action



Defining risks and threats

The following outlines the construct that is used to define threats, threat vectors, attack surfaces, and cyber risks.



Alignment with industry leading practices

The Cyber Risk Management is recommended by several leading frameworks.

	FFIEC	ISO/IEC 27005	ISO 31000	COSO ERM	NIST SP 800-30*
Cyber Risk Assessment Methodology	Information Security Program Management	Information Security Risk Management	Risk Management	Enterprise Risk Management	Risk Management for Information Technology Systems
Identify risks	Risk Identification	Risk Identification	Identify Risks	Event Identification	System Characterisation
Identify threats					Threat and Vulnerability Identification
Assess risks	Risk Measurement	Risk Estimation	Analyze Risks	Risk Assessment	Control Analysis
		Risk Evaluation	Evaluate Risks		Likelihood Determination
					Impact Analysis
					Risk Determination
					Control Recommendation
					Results Documentation

* NIST 800-30 is bottom up focused.

Enterprise Risk Management and Cybersecurity

Enterprise Risk Management

The IT Security Policy Scope provides the guidance on **'What'** the IT Security Risk Management Policy should be managing



IT Security Risk Management Program



The GC provides the guidance on **'Who'** IT security should be managed by.



The framework provides the guidance on **'How'** IT security should be managed.

Cyber risk assessments

Cyber risk assessments are broadly categorized into two types: Top Down and Bottom Up

Focus of this methodology

Top Down Risk Assessment (Strategic)



Identify and assess macro risks

Drive identification and prioritization of strategic remediation initiatives

Performed on an annual basis (typically) or based on changes in the internal/external environment

Intended for consumption by senior/executive management

Bottom Up Risk Assessments (Asset Level)



Identify and assess micro risks Drive tactical app level remediation

Perform when new app is on-boarded or as part of periodic monitoring

Intended for consumption by operational level stakeholders



Risk Assessment Process

1. Risks & Impacts

2. Likelihood

3. Controls

4. Residual Risk



Cyber Risk Assessment Considerations

1. Identify Cyber Risks & Business Impacts



Cyber Risk Identification

Threat Vectors and Scenarios

Business Impacts and Cyber Risk Assessment

2. Determine Likelihood



Cyber Threat Identification and Assessment

Threat Vectors

Attack Surfaces

Threat Likelihood

3. Identify & Score Cyber Controls



Control Identification

Control Assessment Review

Control Target Setting

4. Determine Residual Risk & Risk Target



Control Strength

Residual Risk Determination

Target Risk Level Determination

- Focus on the alignment of business risks to relevant cyber threats and controls:
 - What are our business risks (i.e., data incident, fraud)?
 - What are the potential impacts (i.e., monetary, legal)?
 - What are the potential threat vectors, attack surfaces, and threat scenarios?
 - What can we do to mitigate the risks?
- Effective risk management capabilities require the alignment of the cyber risk assessment approach with the organization's broader operational and enterprise risk management programs



Calculate Residual Risk

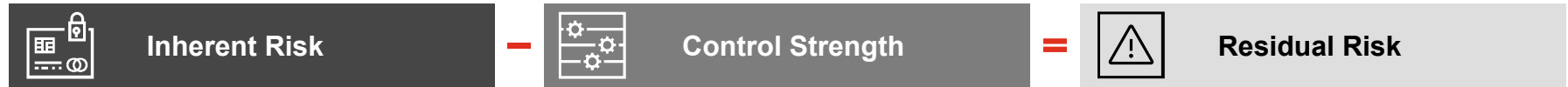
1. Risks & Impacts

2. Likelihood

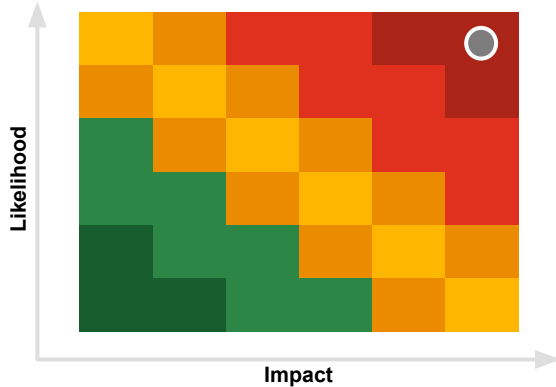
3. Controls

4. Residual Risk

Residual risk is calculated using the formula provided below:



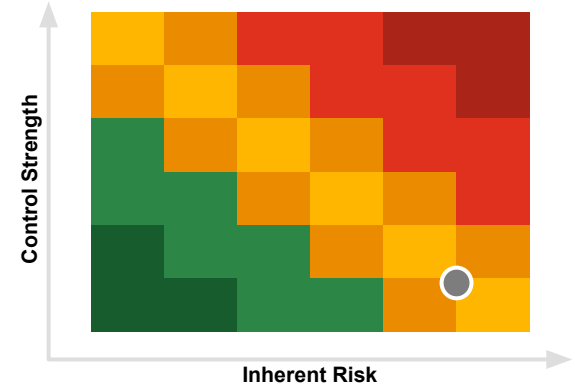
Impact (determined by data type) × **Inherent Likelihood** (determined by threat vectors)



Multiple sources of obtaining control strength

- Controls Testing
- Metrics
- Open Issues
- NIST Capability Maturity

Optimizing	Repeatable
Managed	Ad-hoc
Defined	



Example Risk Calculation

L1 Risk	Business impact levels (1-5)					Total Impact (Weighted Average)
	Financial (40%)	Regulatory (30%)	Reputational (20%)	Operational (10%)		
Theft of Employee Credentials & PII	3 - Medium	4 - High	3 - Medium	2 - Low		3.2

	TVo1	TVo2	TVo3	TVo4	TVo5	...	TV23	Total
Avg. Likelihood (across various threat scenarios)	4.8	3.0	4.0	2.7	5.0	...	3.0	4.1
Applicability	3 High	2 Medium	1 Low	2 Medium	0 N/A	...	1 Low	

Inherent Risk = (Impact x Likelihood)/5 = (3.2 x 4.1)/5 = 2.6



Questions?

Thank you

Contact our team



Myra Lundy-Mortimer
Assurance & Risk Assurance Partner
Connect with Myra on LinkedIn
myra.lundy-mortimer@pwc.com



Anthony Zamore
Director - Risk Assurance Services
Connect with Anthony on LinkedIn
anthony.l.zamore@pwc.com



Nestle Maullon
Senior Manager - Risk Assurance Services
Connect with Nestle on LinkedIn
nestle.maullon@pwc.com

Thank you

[pwc.com/bs](https://www.pwc.com/bs)

© 2020 PricewaterhouseCoopers. All rights reserved. PwC refers to The Bahamas member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. © 2020 PwC. All rights reserved.