CIO EDGE

ADAPT

International Keynote:
How exactly can a CIO mitigate Cyber Risk?

CIO Edge Competing on Experience |
20 – 21 February 2019 | Grand Hyatt, Melbourne

Theo Nassiokas

What will I speak about?

- Defining cyber risk
- Determining cyber risk profile
- Threats, delivery methods and actors
- Disruption by alleged state threat actors (x2)
- Data used to measure cyber risks
- Quantifying cyber risk to business
- Cyber insurance considerations

CIO EDGE

Legal stuff

- All reproduced data is referenced
- Trademarks and images are used under a Creative Commons (CC) License only
- Opinions expressed are the presenter's only; and not those of any past or present employers or clients
- Copyright © 2019 by Theo Nassiokas. All rights reserved

Defining cyber risk

- **Risk of business disruption due to technology, telecommunications or utility failure, causing a loss of service or data**

  - A cyber attack can be performed without a computer and can attack devices that are not computers, e.g. proprietary appliances
  - 2010 Iranian nuclear facility cyber attack caused centrifuges to spin out of control and be destroyed by the Stuxnet malicious code
  - October 2018 "Stuxnet2" attack on Iranian critical networks, as reported by Iranian and Israeli agencies
  - A cyber attack in your office building need not touch a computer. Your building management system can be attacked, placing people at risk

Cyber attacks don't require computers

Ref. *Stuxnet Returns, Striking Iran With New Variant* - https://www.infosecurity-magazine.com/news/stuxnet-returns-striking-iran-with/

CIO EDGE

Determining cyber risk profile

- **Cyber security**
  - Firewalls
  - Intrusion Prevention System
  - Web black/white-listing
  - Lateral network movement
  - Data leakage prevention
  - SIEM monitoring & reporting
  - Vulnerability Assess/Pen Testing
  - DMARC email authentication
  - IEEE 802.1x PNAC
  - Source code review

- **Cyber resilience**
  - Active, active paradigms
  - Running mirrored systems
  - High-availability systems
  - Uninterruptable power supplies
  - Multiple independent power grids
  - Enterprise Cloud strategies
  - Automated response capabilities
  - Red teaming strategy
  - Threat intelligence gathering
  - Cyber threat hunting

You need both in a security strategy!

Threats, delivery methods and actors

Threats (what)

- Malicious code
- Web applications
- Distributed Denial of Service
- Insider and privilege misuse
- Cyber-espionage
- Point of sale terminals
- Payment card copying devices
- Physical theft/loss

Delivery (how)

- Malicious websites
- Legitimate websites
- Online 'Malvertising'
- File sharing networks (P2P)
- Email downloads
- Instant messages
- SMS / WhatsApp / iMessage
- Physical code insertion

Actors (who)

- States (directly)
- State sponsored (indirectly)
- Organised crime
- 'Hacktivists'
- Insider threat
- Internal error
- Opportunistic

Disruption by alleged state threat actors (1):

- GRU – Russian Military Intelligence, Cyber Warfare Unit

4 October 2018

Russian spies have been accused of involvement in a series of cyber-plots across the globe, leading the US to level charges against seven agents.

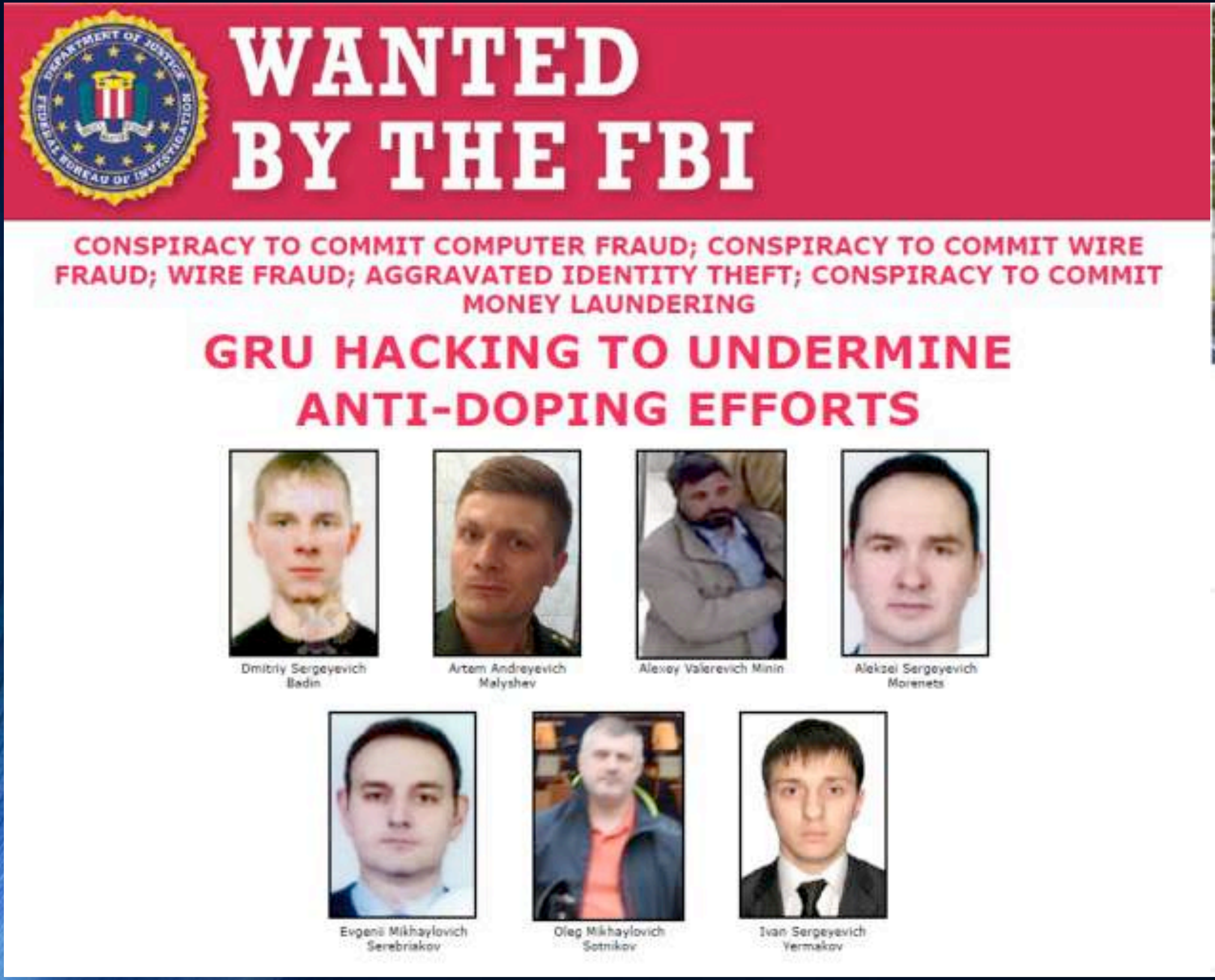
- The US justice department said targets included the global chemical weapons watchdog, anti-doping agencies and a US nuclear company.
- The allegations are part of an organised push-back against alleged Russian cyber-attacks around the world.
- Russia earlier dismissed the allegations as "Western spy mania".

What is Russia accused of?

- The Netherlands has accused four Russians of plotting to hack the Organisation for the Prohibition of Chemical Weapons (OPCW), which had been probing the chemical attack on a Russian ex-spy in the UK
- The UK government accused the GRU of being behind four high-profile cyber-attacks, whose targets included firms in Russia and Ukraine; the US Democratic Party; and a small TV network in the UK
- The US said its anti-doping agency, football's governing body Fifa and the US nuclear energy company Westinghouse were targeted by Russian intelligence
- Canada said "with high confidence" that breaches at its centre for ethics in sports and at the Montreal-based World Anti-Doping Agency were carried out by Russian intelligence

Ref. *Russia cyber-plots: US, UK and Netherlands allege hacking* – BBC World News - https://www.bbc.com/news/world-europe-45746837

Meet alleged members of GRU, Cyber Warfare Unit 26165



WANTED BY THE FBI

CONSPIRACY TO COMMIT COMPUTER FRAUD; CONSPIRACY TO COMMIT WIRE FRAUD; WIRE FRAUD; AGGRAVATED IDENTITY THEFT; CONSPIRACY TO COMMIT MONEY LAUNDERING

GRU HACKING TO UNDERMINE ANTI-DOPING EFFORTS

Dmitriy Sergeyevich Badin

Artem Andreyevich Malyshev

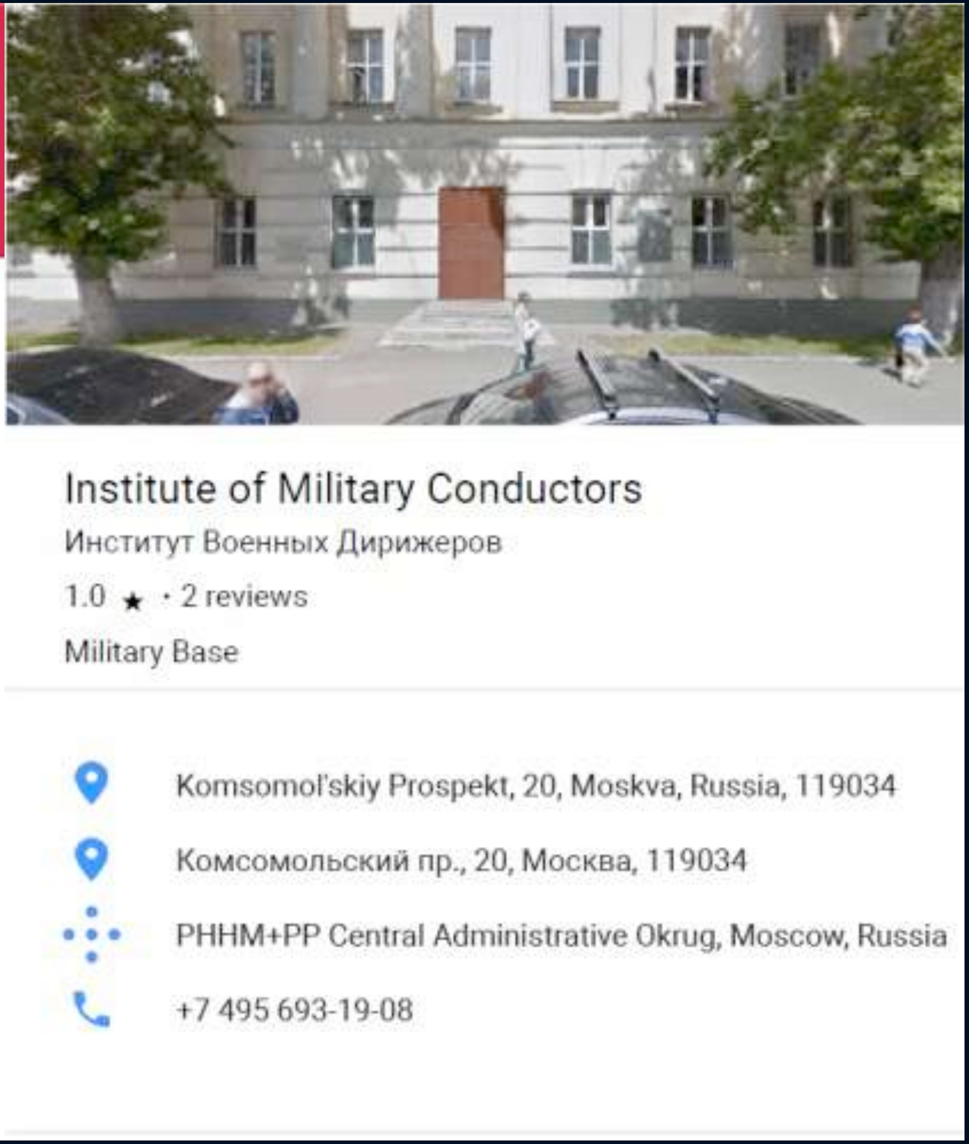
Alexey Valerevich Minin

Aleksei Sergeyevich Morenets

Evgenii Mikhaylovich Serebriakov

Oleg Mikhaylovich Sotnikov

Ivan Sergeyevich Yermakov



Institute of Military Conductors

Институт Военных Дирижеров

1.0 ★ · 2 reviews

Military Base

Komsomol'skiy Prospekt, 20, Moskva, Russia, 119034

Комсомольский пр., 20, Москва, 119034

PHHM+PP Central Administrative Okrug, Moscow, Russia

+7 495 693-19-08

Ref. *GRU Hacking to Undermine Anti-Doping Efforts* - https://www.fbi.gov/wanted/cyber/gru-hacking-to-undermine-anti-doping-efforts
Ref. *305 Car Registrations May Point to Massive GRU Security Breach* - https://www.bellingcat.com/news/2018/10/04/305-car-registrations-may-point-massive-gru-security-breach/

CIO
EDGE

Disruption by alleged state threat actors (2):

- RGB – North Korean Clandestine Operations

Who’s the RGB?

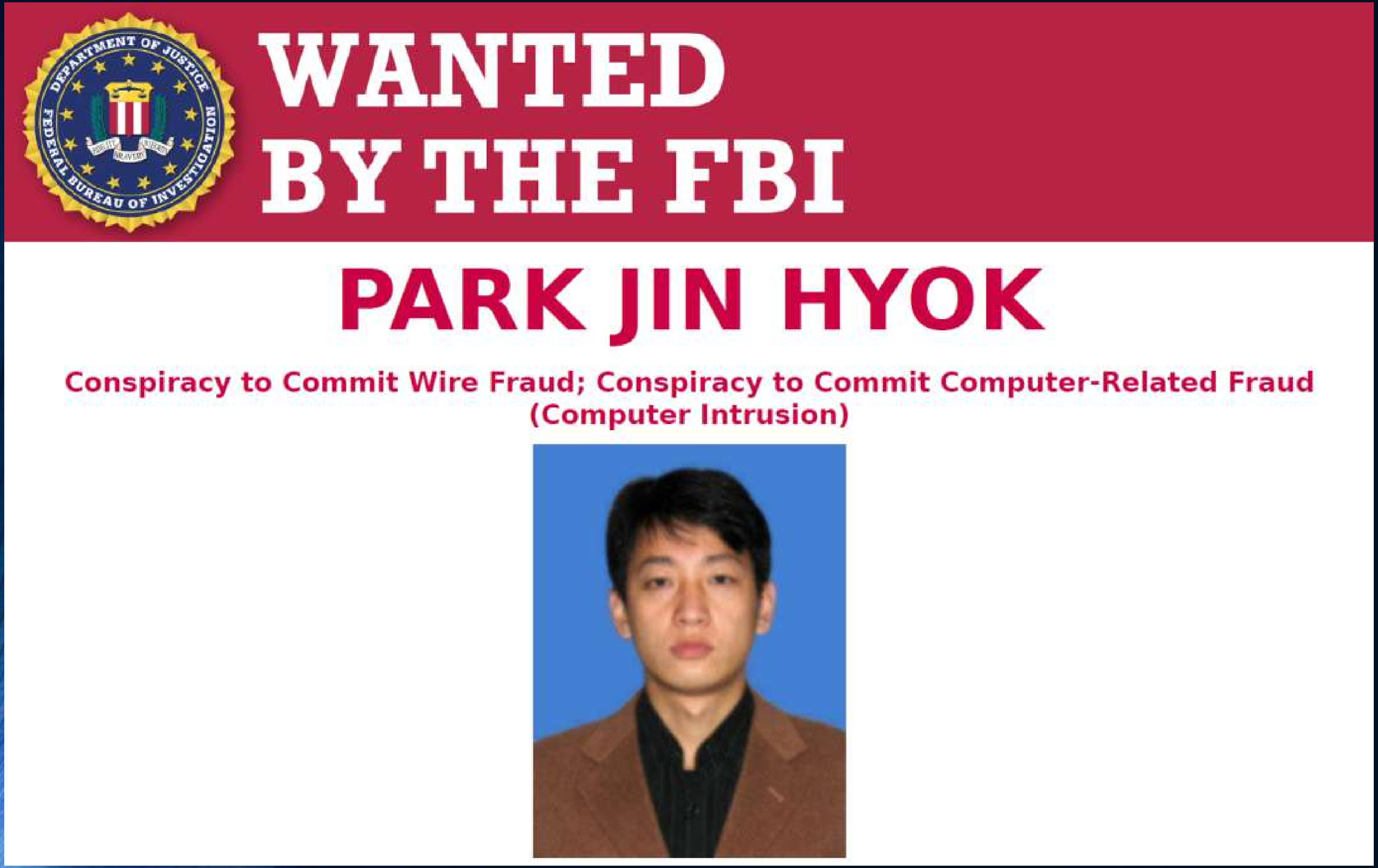
- Reconnaissance General Bureau [RGB] which is equivalent to the US Directorate of National Intelligence, is involved in the collection and analysis of military intelligence on South Korea.
- RGB Sixth Bureau (Technical Bureau) is also involved in some special activities and has been implicated in numerous cyberwarfare activities targeting South Korean government and financial institutions.

What is North Korea accused of?

- **WannaCry** – On May 12, 2017, organizations across the world reported ransomware infections. WannaCry was delivered using phishing and built using the NSA’s “EternalBlue”.
- **Bangladesh Bank** – In February 2016, a series of cyberattacks on banks in Bangladesh and Southeast Asia resulted in the theft of $81 million involving the global SWIFT system.
- **Sony Pictures Entertainment** – On November 24, 2014, Sony Pictures Entertainment experienced a cyberattack that disabled its technology, and leaked compromised data.
- **South Korean Banks** – In March 2013, several South Korean banks and news broadcasters experienced network disruption. “DarkSeoul” malware rendered computers unusable.

Ref. *Kim Yong Chol, A Biography* by Michael Madden, May 29, 2018 https://www.38north.org/2018/05/mmadden052918/
Ref. *North Korean Cyber Capabilities: In Brief* by Congressional Research Service, August 3, 2017 https://fas.org/sgp/crs/row/R44912.pdf
Ref. *38 North Special Report*, June 11, 2010 https://www.38north.org/wp-content/uploads/2010/06/38north_SR_Bermudez2.pdf

Meet an alleged member of RGB, Technical (6th) Bureau



WANTED BY THE FBI

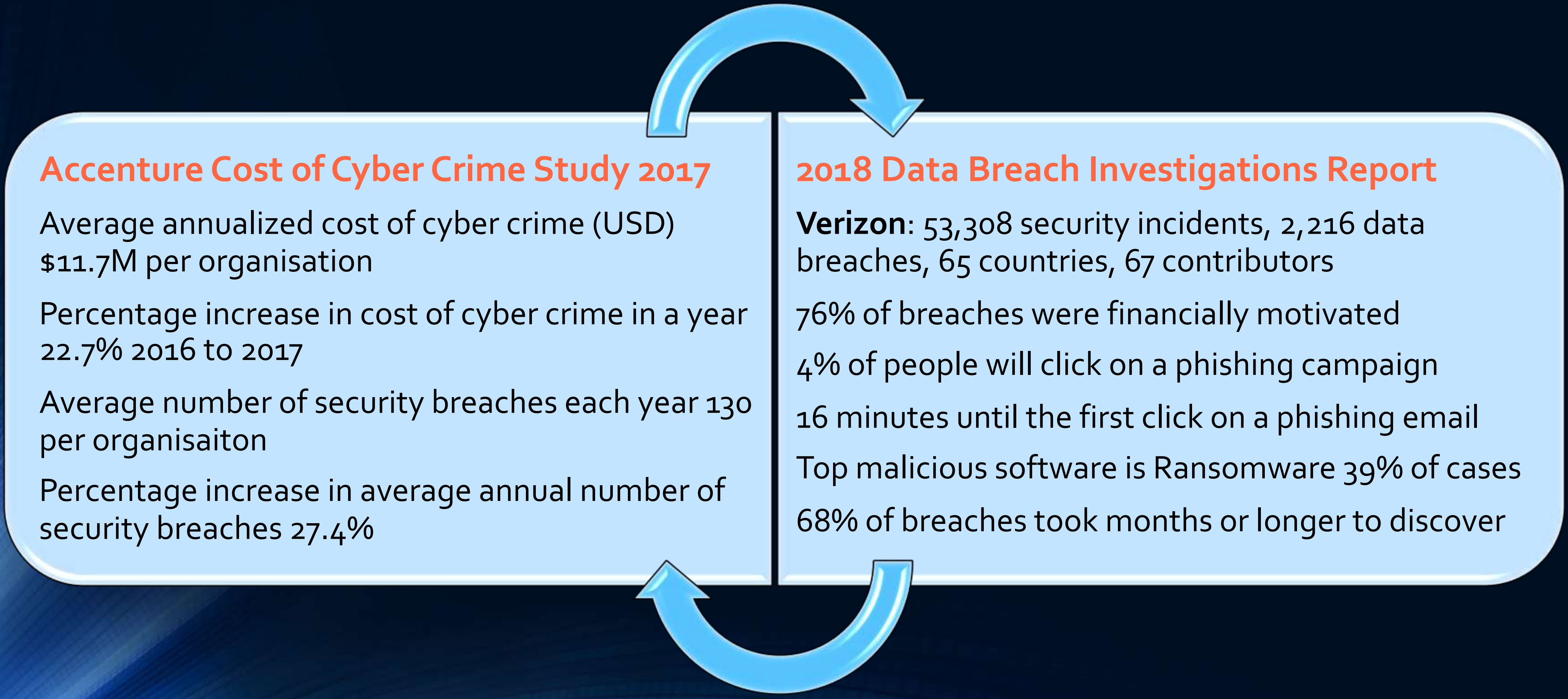
PARK JIN HYOK

Conspiracy to Commit Wire Fraud; Conspiracy to Commit Computer-Related Fraud (Computer Intrusion)

- June 8, 2018, a federal arrest warrant was issued for Park Jin Hyok in the United States District Court in California.
- Park allegedly conducted illegal computer intrusion activities on behalf of North Korea's RGB.
- Park has been linked to "Lab110" a.k.a. "Lazarus Group"; one of the North Korean Government's alleged hacking organisations.
- September 18, 2018, North Korea denied the existence of Park Jin Hyok.

Ref. *Park Jin Hoyk* - https://www.fbi.gov/wanted/cyber/park-jin-hyok
Ref. *The Washington Times* - *https://www.washingtontimes.com/news/2018/sep/14/north-korea-disputes-existence-park-jin-hyok-suspe/*

Data used to measure cyber risks



Accenture Cost of Cyber Crime Study 2017

Average annualized cost of cyber crime (USD) $11.7M per organisation

Percentage increase in cost of cyber crime in a year 22.7% 2016 to 2017

Average number of security breaches each year 130 per organisaiton

Percentage increase in average annual number of security breaches 27.4%

2018 Data Breach Investigations Report

Verizon: 53,308 security incidents, 2,216 data breaches, 65 countries, 67 contributors

76% of breaches were financially motivated

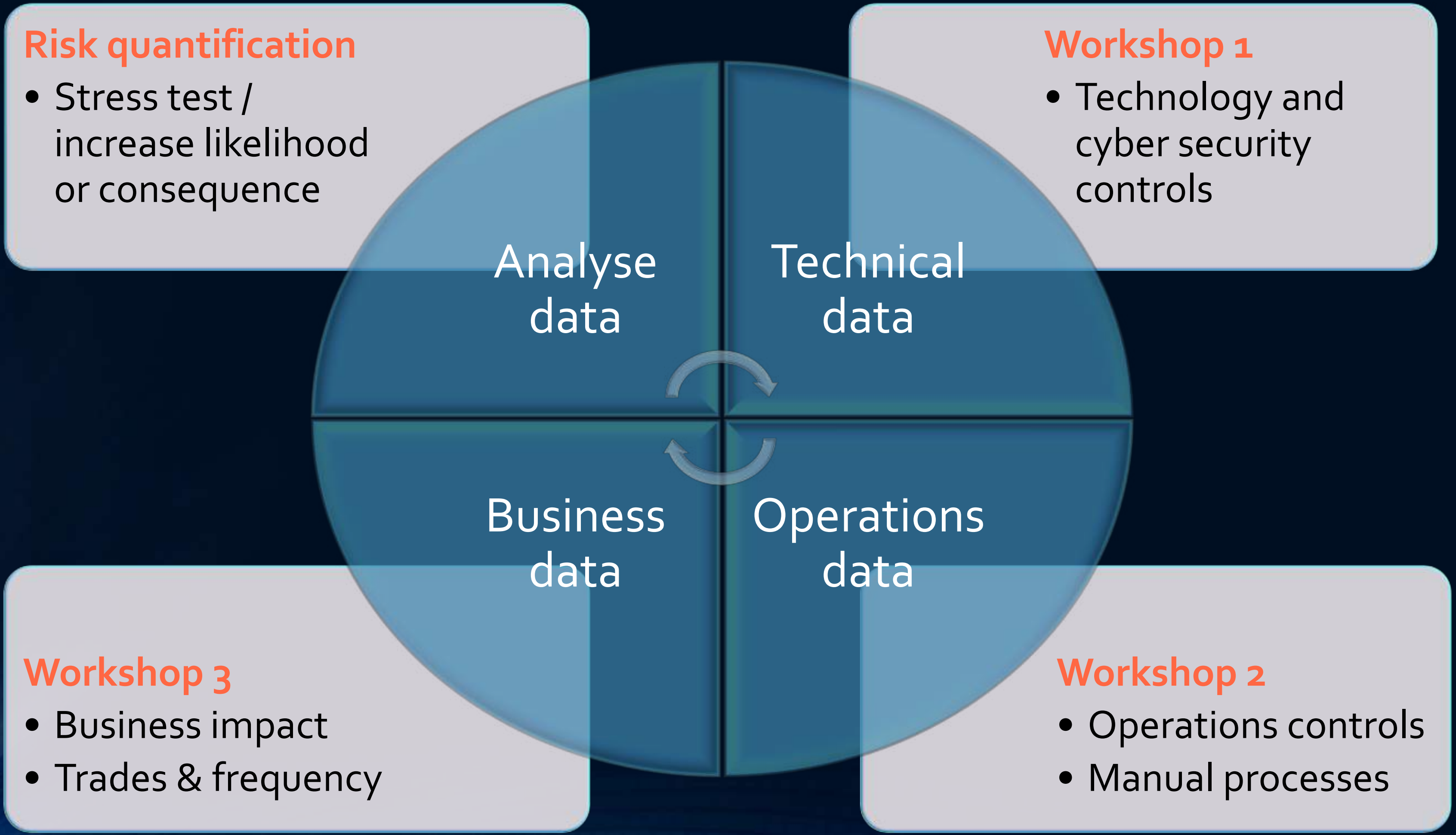
4% of people will click on a phishing campaign

16 minutes until the first click on a phishing email

Top malicious software is Ransomware 39% of cases

68% of breaches took months or longer to discover

Quantifying cyber risk to business



Risk quantification

- Stress test / increase likelihood or consequence

Workshop 1

- Technology and cyber security controls

Analyse data

Technical data

Business data

Operations data

Workshop 3

- Business impact
- Trades & frequency

Workshop 2

- Operations controls
- Manual processes

Cyber insurance considerations

7 Key elements to cyber liability coverage

- Forensic Expenses
- Legal Expenses
- Notification Expenses
- Regulatory Fines and Penalties
- Credit Monitoring and ID Theft Repair
- Public Relations Expenses
- Liability and Defense Costs

Other key cyber insurance considerations

- Quantify your cyber risk in business terms
- Understand cyber risk you will (i) mitigate (ii) accept & (iii) transfer
- Use your exposure to determine scope and value of coverage
- Scope of liabilities to be covered:
  - 1st party and 3rd party liabilities
  - Response costs

AIG

CHUBB INSURANCE

HISCOX

Liberty Mutual INSURANCE

Ref. *7 Key Coverage Elements of Cyber Liability Insurance* – R&R Insurance Blog - https://www.myknowledgebroker.com/blog/business-insurance/7-key-coverage-elements-of-cyber-liability-insurance/

Thank you for your time

SAY NO

TO CYBER BULLYING

Theo Nassiokas

https://sg.linkedin.com/in/theonassiokas