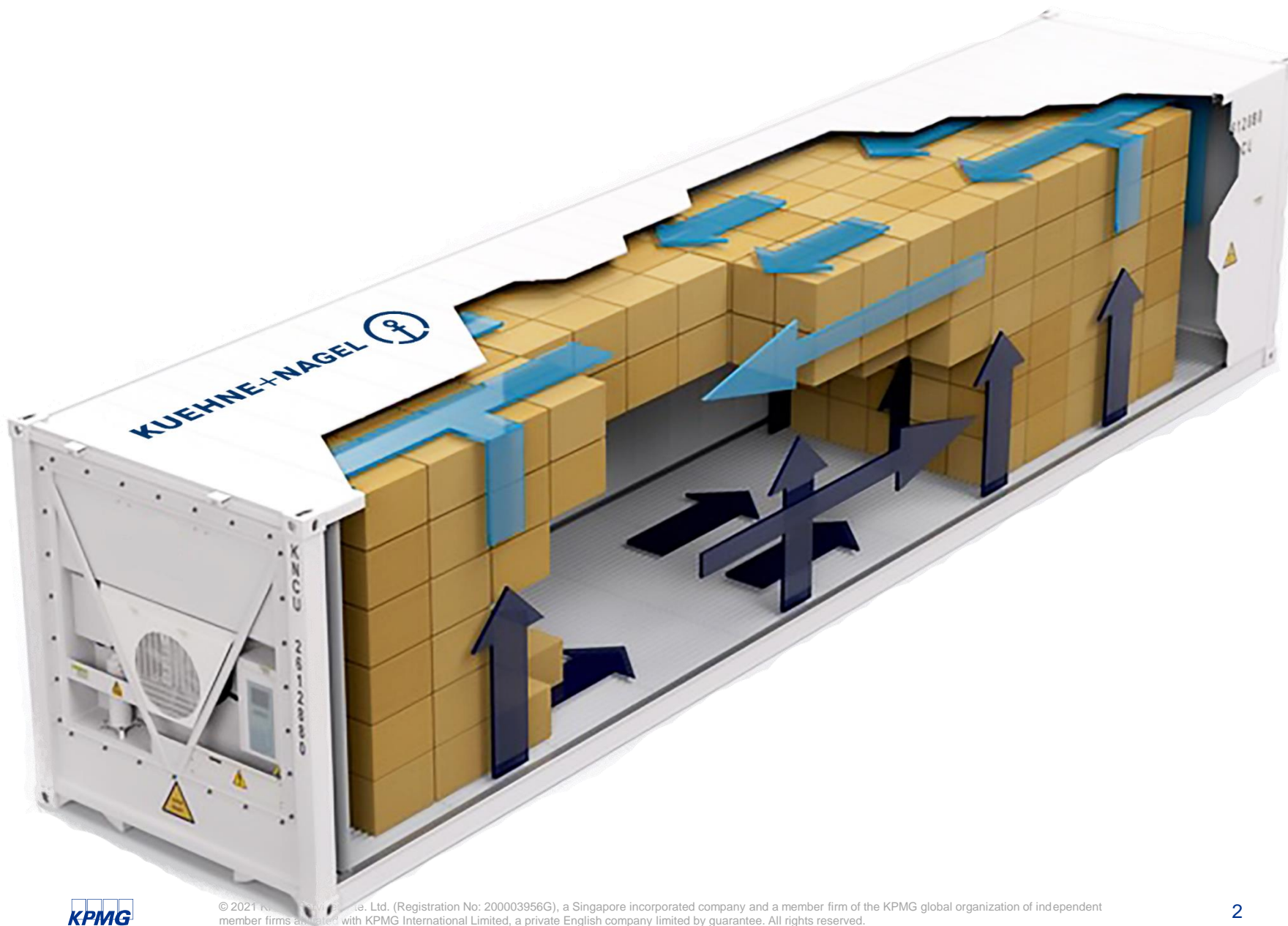


Cyber+crime in the Maritime sector

September 2022



Bananas & drug trafficking

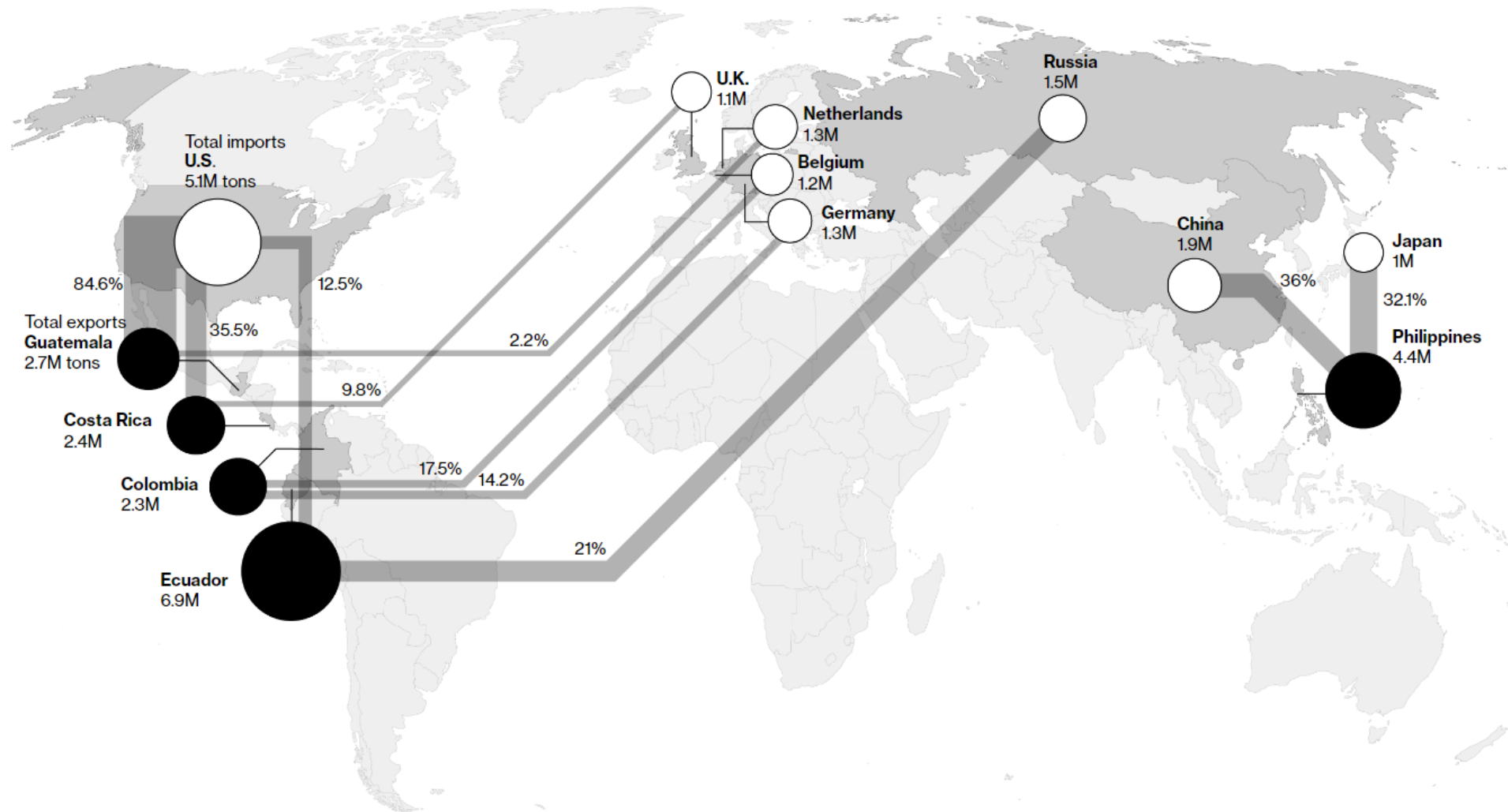


Banana trade routes

International Banana Trade

Some 20 million tons of bananas were exported globally in 2019

● Largest exporters ○ Largest importers ▧ Percent shipped to largest two partners



Source: International Trade Centre

NEWS

Cocaine worth £7.5m found in banana shipment

🕒 14 January

Cocaine with a street value of £7.5m has been discovered hidden in a shipment of bananas from

Border Force officers found 103kg (227lb) of the Class A drug on 6 January while searching a vessel that had arrived at the Port of Southampton.

The government agency said its officers could be "proud of their work in preventing this drug consignment from reaching our communities".

The Home Office has been asked whether any arrests have been made.



The drugs were hidden among a shipment of bananas from

Hackers facilitated international drug smuggling via major port in Europe 2012

By breaking into the offices of a harbour company, the criminals could install key logger devices to take control of the computers.



Computers of container terminals were hacked so the containers containing drugs could be monitored.



By means of false papers and a hacked pin code, the drivers of the organization were able to pick up the container on a location and time of their choice.



Source: Europol

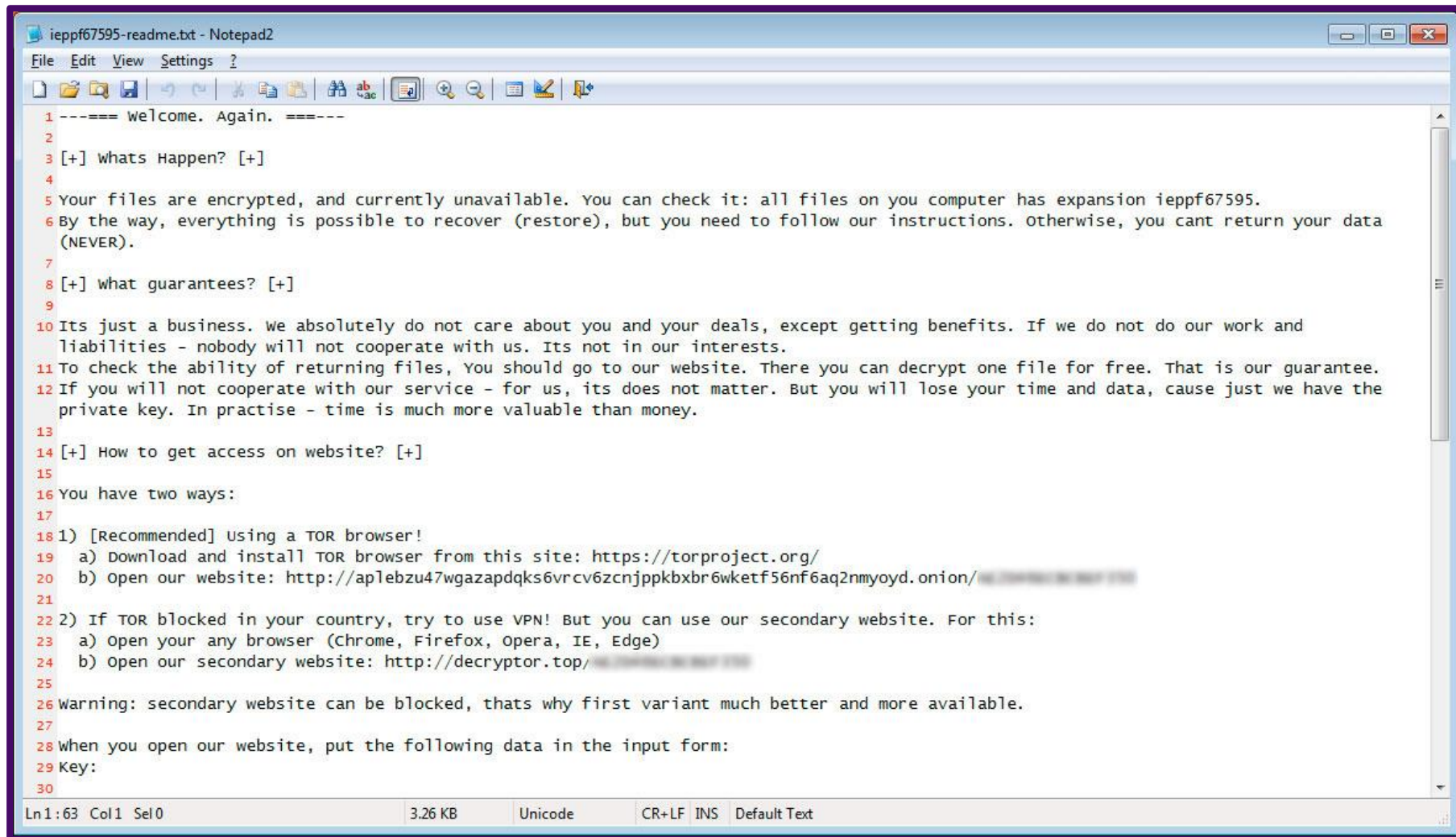


© 2021 KPMG Services Pte. Ltd. (Registration No: 200003956G), a Singapore incorporated company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.



Bananas & ransomware

Most organizations discover that they have experienced a ransomware attack when they find a ransom note like this one

A screenshot of a Notepad2 window titled 'ieppf67595-readme.txt - Notepad2'. The window contains a ransom note with the following text:

```
1 ----- welcome. Again. -----  
2  
3 [+] whats Happen? [+]  
4  
5 Your files are encrypted, and currently unavailable. You can check it: all files on you computer has expansion ieppf67595.  
6 By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data  
  (NEVER).  
7  
8 [+] what guarantees? [+]  
9  
10 Its just a business. we absolutely do not care about you and your deals, except getting benefits. If we do not do our work and  
   liabilities - nobody will not cooperate with us. Its not in our interests.  
11 To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee.  
12 If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the  
   private key. In practise - time is much more valuable than money.  
13  
14 [+] How to get access on website? [+]  
15  
16 You have two ways:  
17  
18 1) [Recommended] Using a TOR browser!  
19 a) Download and install TOR browser from this site: https://torproject.org/  
20 b) open our website: http://ap1ebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/  
21  
22 2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:  
23 a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)  
24 b) Open our secondary website: http://decryptor.top/  
25  
26 Warning: secondary website can be blocked, thats why first variant much better and more available.  
27  
28 When you open our website, put the following data in the input form:  
29 Key:  
30
```

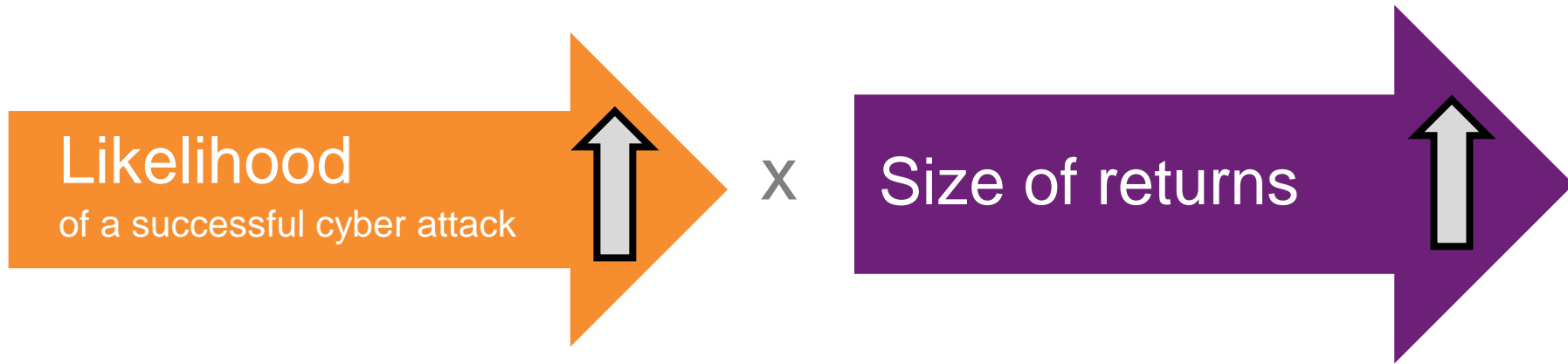
Ln1:63 Col1 Sel0 3.26 KB Unicode CR+LF INS Default Text

The Wannacry (2017) ransomware affected more than 200,000 computers across 150 countries. The scale was tremendous but the amount of ransom collected was relatively small.



Zeit	Über	22:10	DB	Nach	Gleis
22:15 RB61	Dresden Mitte			Dresden Hbf	8
22:20 S1	Dresden Hbf				2
22:25 S2	Dresden-K				1
22:25 RE50	Coswig (b.)				6
22:25 RE50	Dresden M				3
22:29 IC 2045					7
22:32 S2	Dresden Mitte			Dresden Hbf	2
22:37 S1	Radebeul Ost - Coswig (b. Dre)			Meißen Trieb	1

Cyber criminals seek to maximise the likelihood of a success attack and the size of their returns



The returns of an attack depends on the attractiveness of the victim

Likelihood

of a successful cyber attack

x

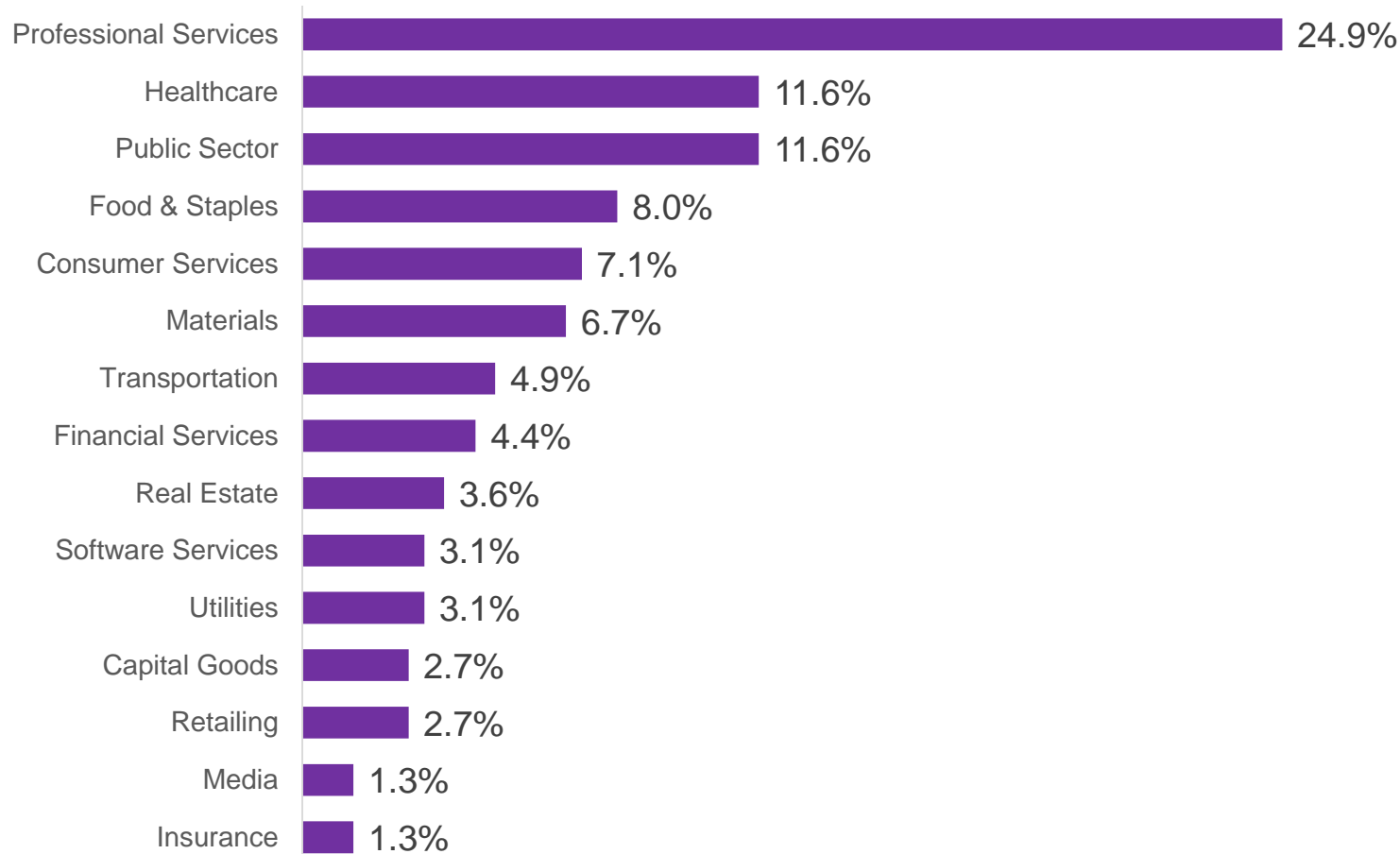
Size of returns



Attractiveness of
target/victim (e.g. willingness
to pay & ability to pay)

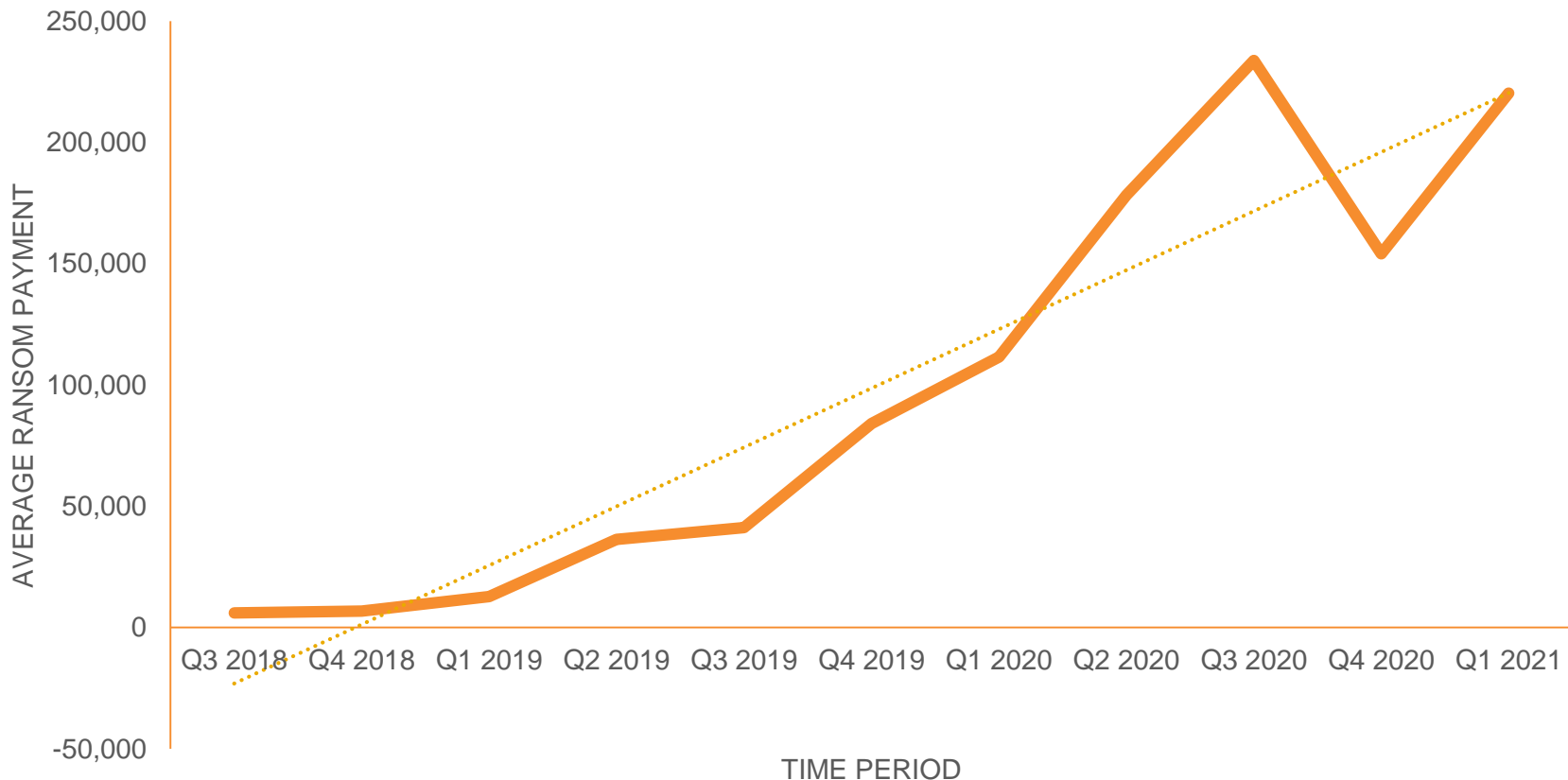
From 2018, many gangs have started to moved away from attacking indiscriminately and selectively choosing their targets.

Percentage of industries targeted by ransomware in Q1 2021



The strategy of studying various industries and choosing their victims selectively has been associated to the increase in ransom paid

Average ransom payment (USD) by quarter



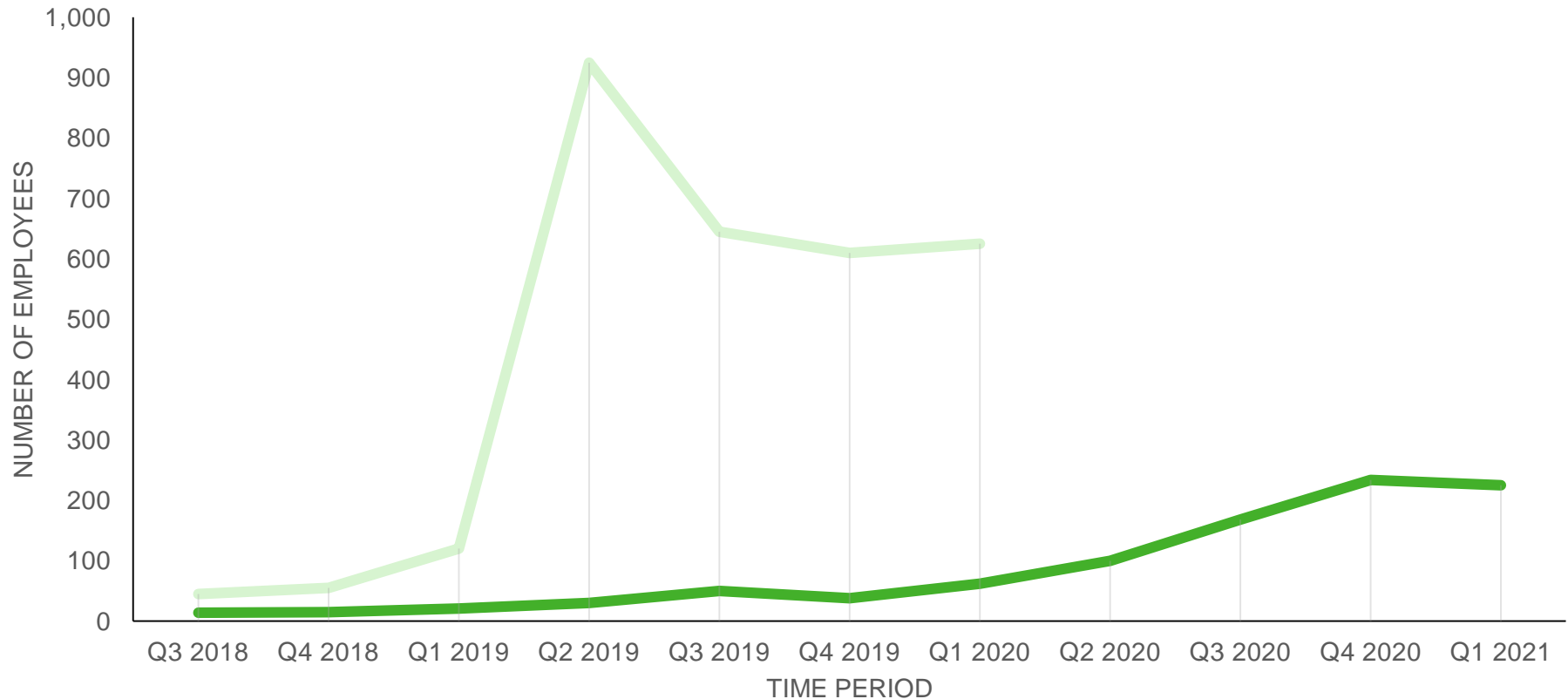
Source: Coveware Ransomware Marketplace



© 2021 KPMG Services Pte. Ltd. (Registration No: 200003956G), a Singapore incorporated company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Although ransomware groups are choosing their targets, victims remain largely small/medium businesses. Why?

Average vs Median size of companies targeted by ransomware

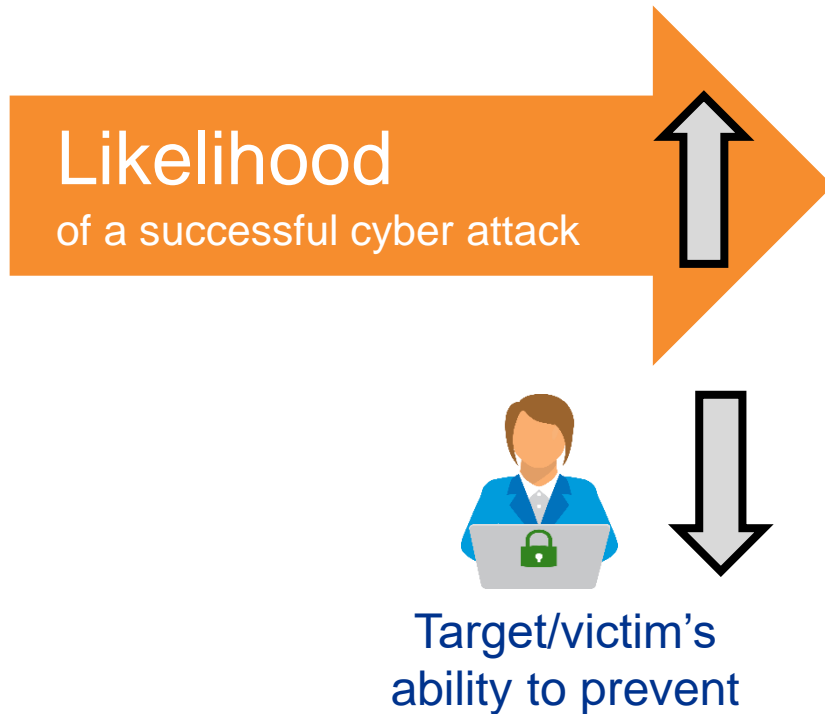


Source: Coveware Ransomware Marketplace



© 2021 KPMG Services Pte. Ltd. (Registration No: 200003956G), a Singapore incorporated company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

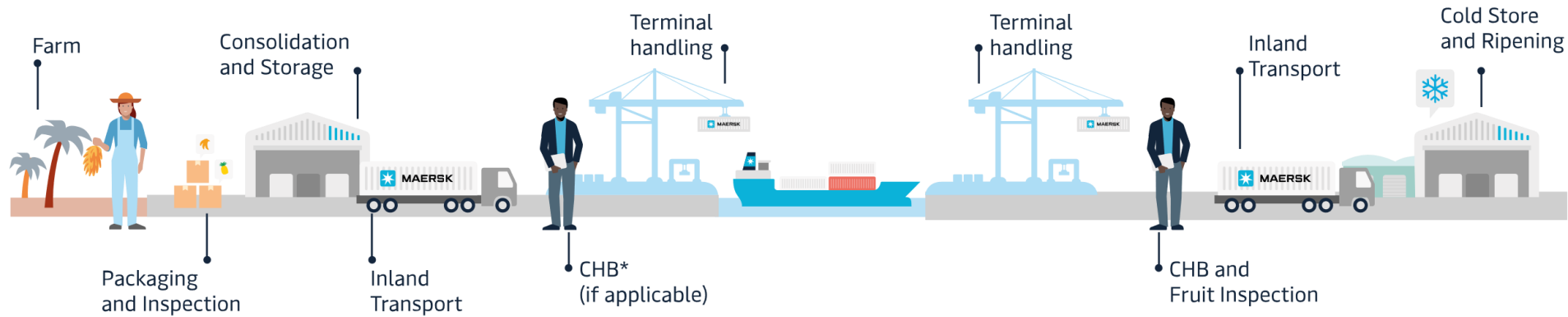
Selectively choosing their victims increases their chance of success.



Ransomware is not just used for extortion. It can also be used in warfare (with a slight change)



Bananas and Maersk



Source: Maersk



In 2017, Maersk and many companies around the world found themselves part of the collateral damage of a cyber conflict



Impact to Maersk (10 days of pain & estimated 300 millions dollars of loss)



Heroic response and incredible feat from Maersk

While dealing with the issue for 10 days

Maersk maintained transparency and worked closely with partners and customers

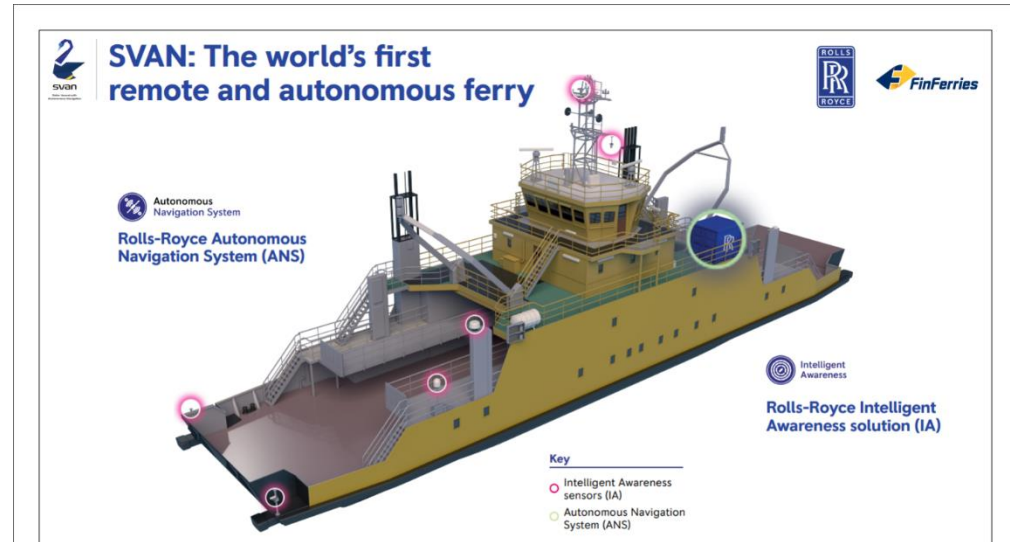
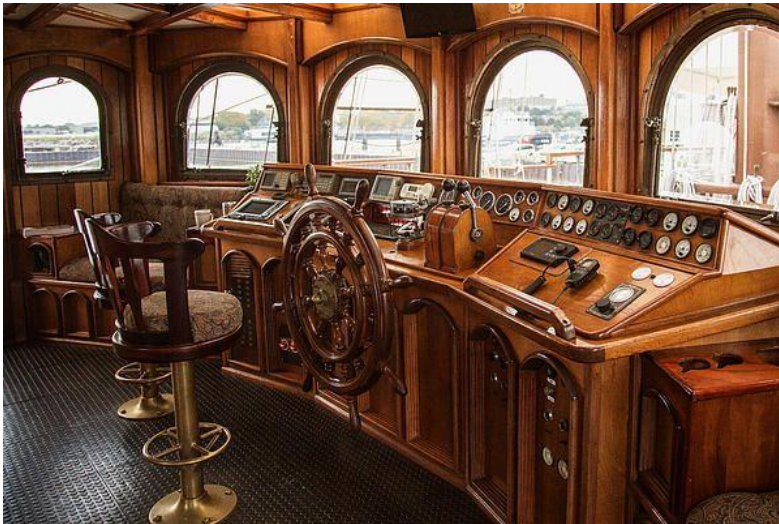
Maersk rebuilt in 10 days

4000 servers

45,000 PCs

2,500 applications

Reliance on digitalisation & automation

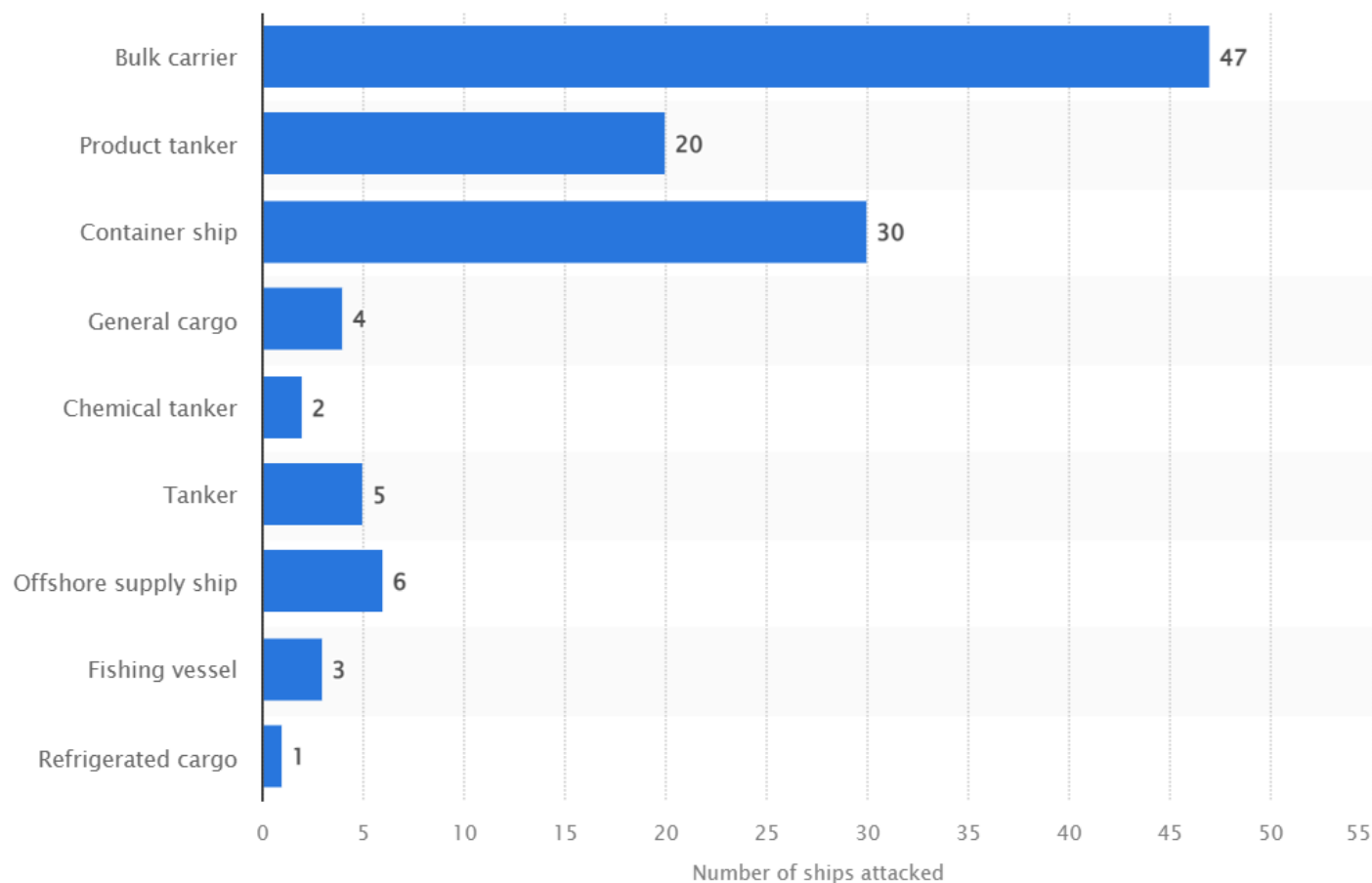




Plantains & pirates

Transportation & Logistics › Water Transport

Number of pirate attacks on ships worldwide in 2021, by ship type



If hackers collaborated with pirates, how might it look like?

Pirates



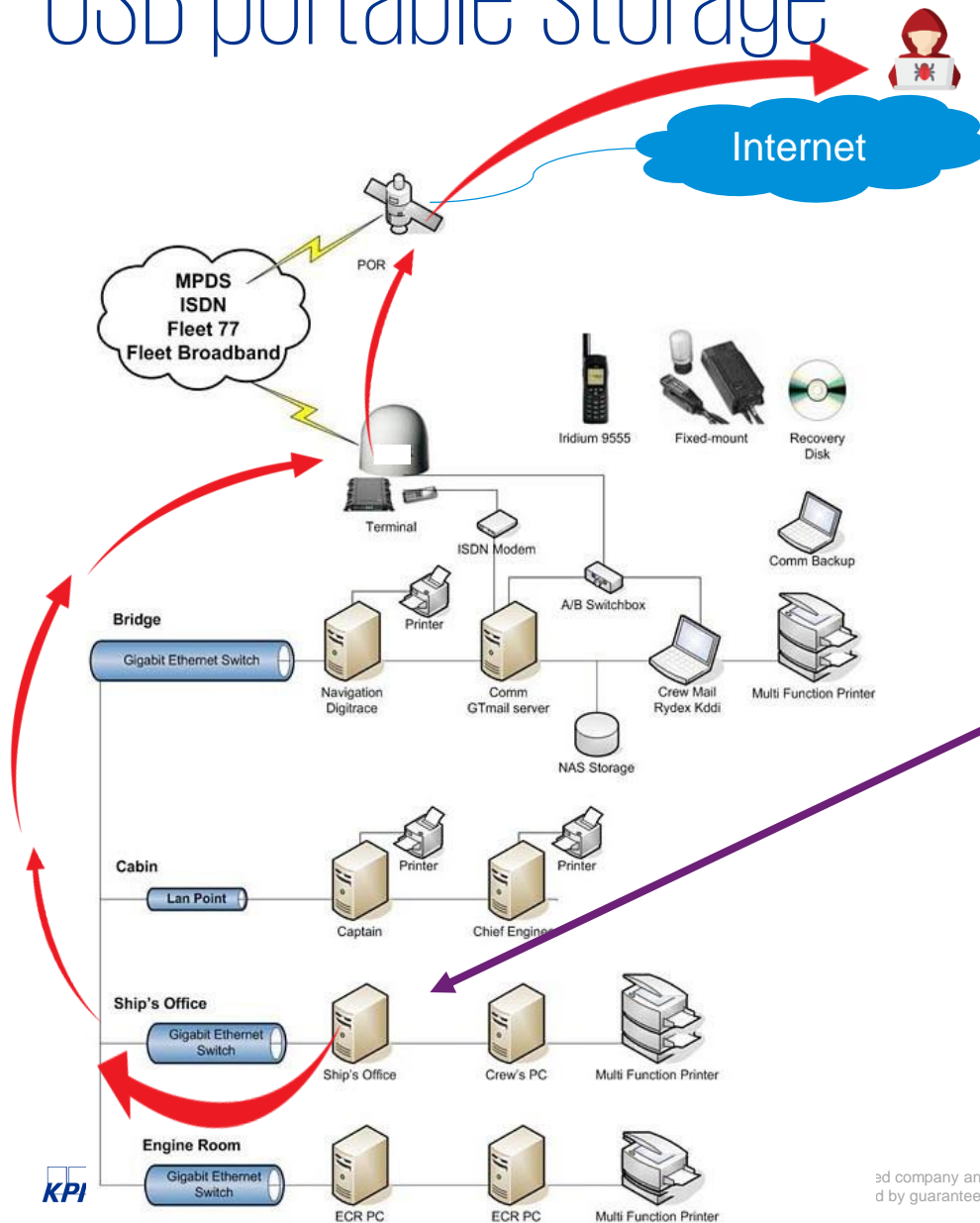
Hackers



① Compromise shipping companies and ships.
Get in and stay hidden.



USB portable storage



- 1 Plugged USB into ship's equipment (e.g. updates to ECDIS, maps)



- 2 Malware activated



A utilities plant vs a commercial ship

Not a lot of changes

More changes to the people & environment



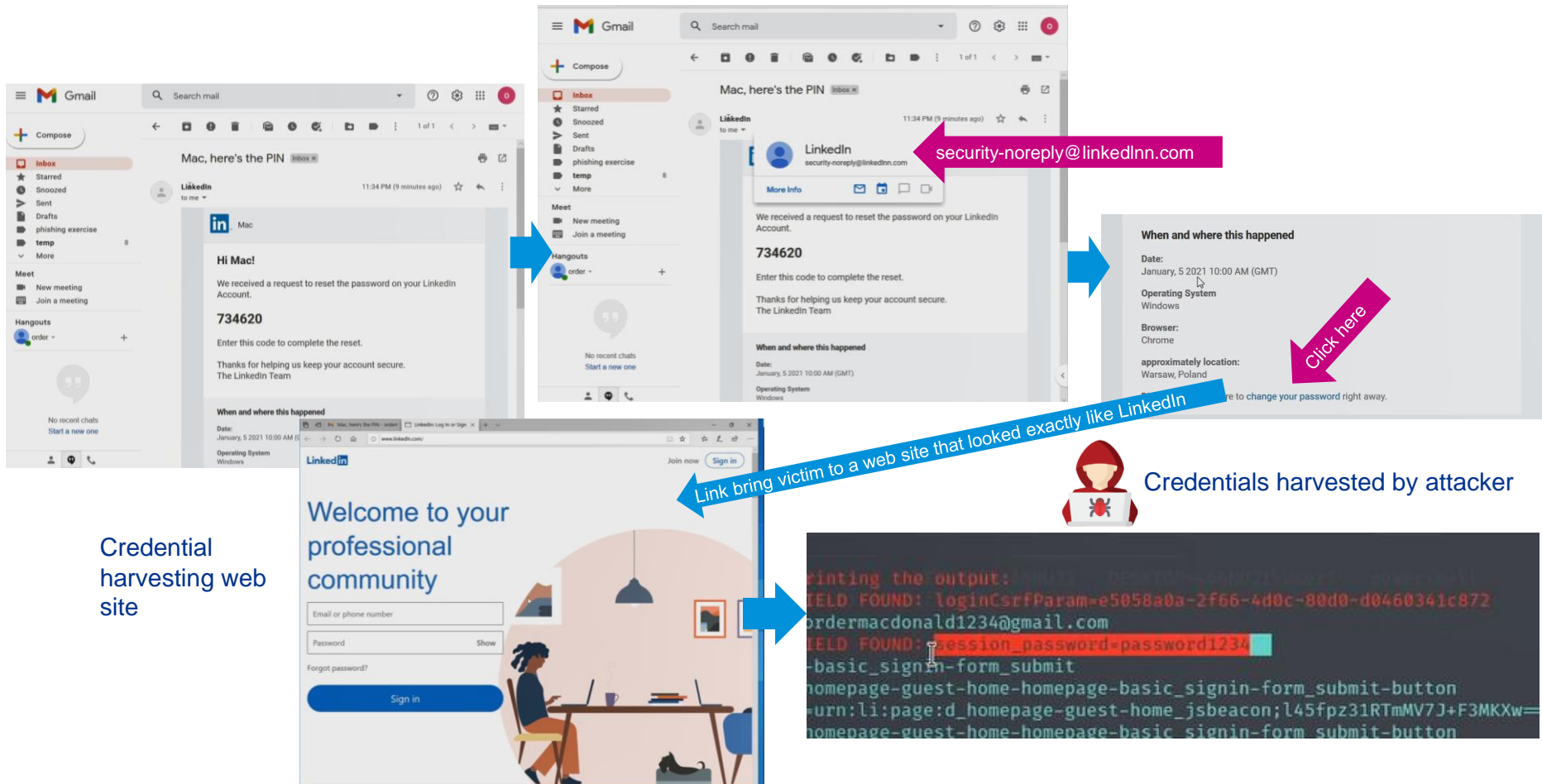
VS



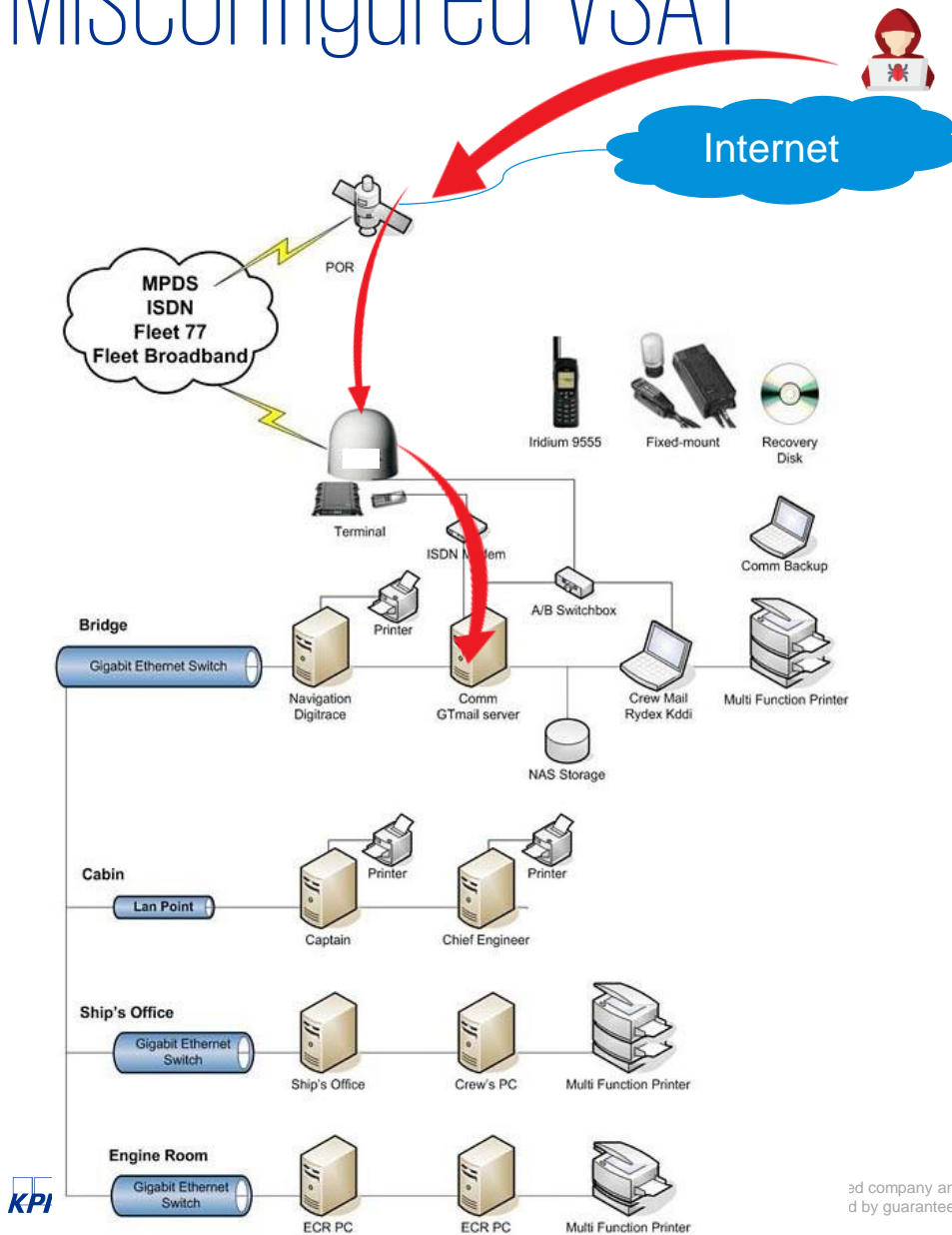
Passenger ships



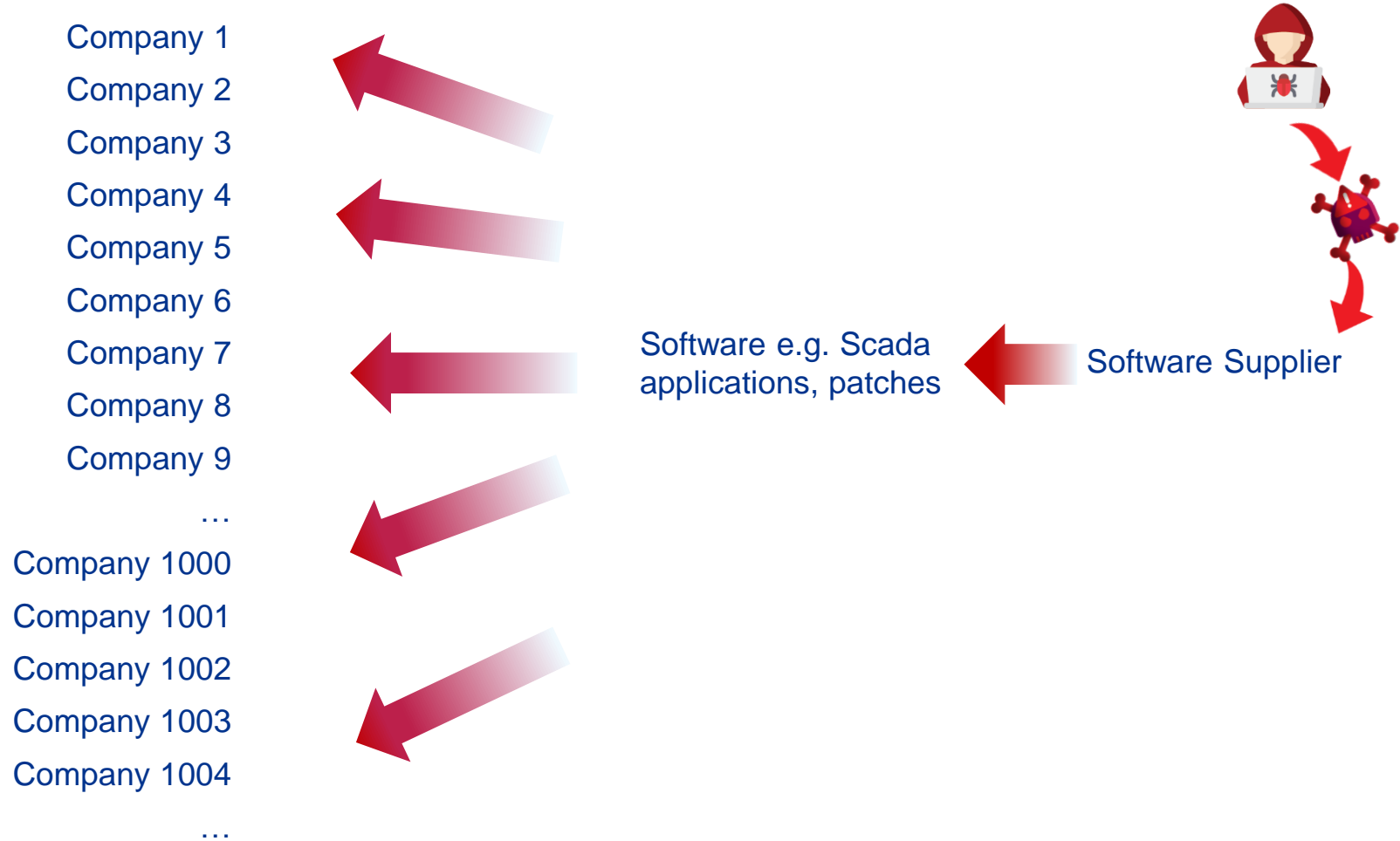
Phishing: Crew or passengers could be click on a malicious link or open an attachment in an email



Misconfigured VSAT



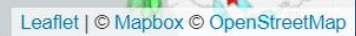
Attacking the software supply chain



② Stay hidden & study the internal processes.



Gather intelligence from AIS and shipping companies onshore system. Identify location and cargo on ship. Evaluate and selectively target ships/cargo.

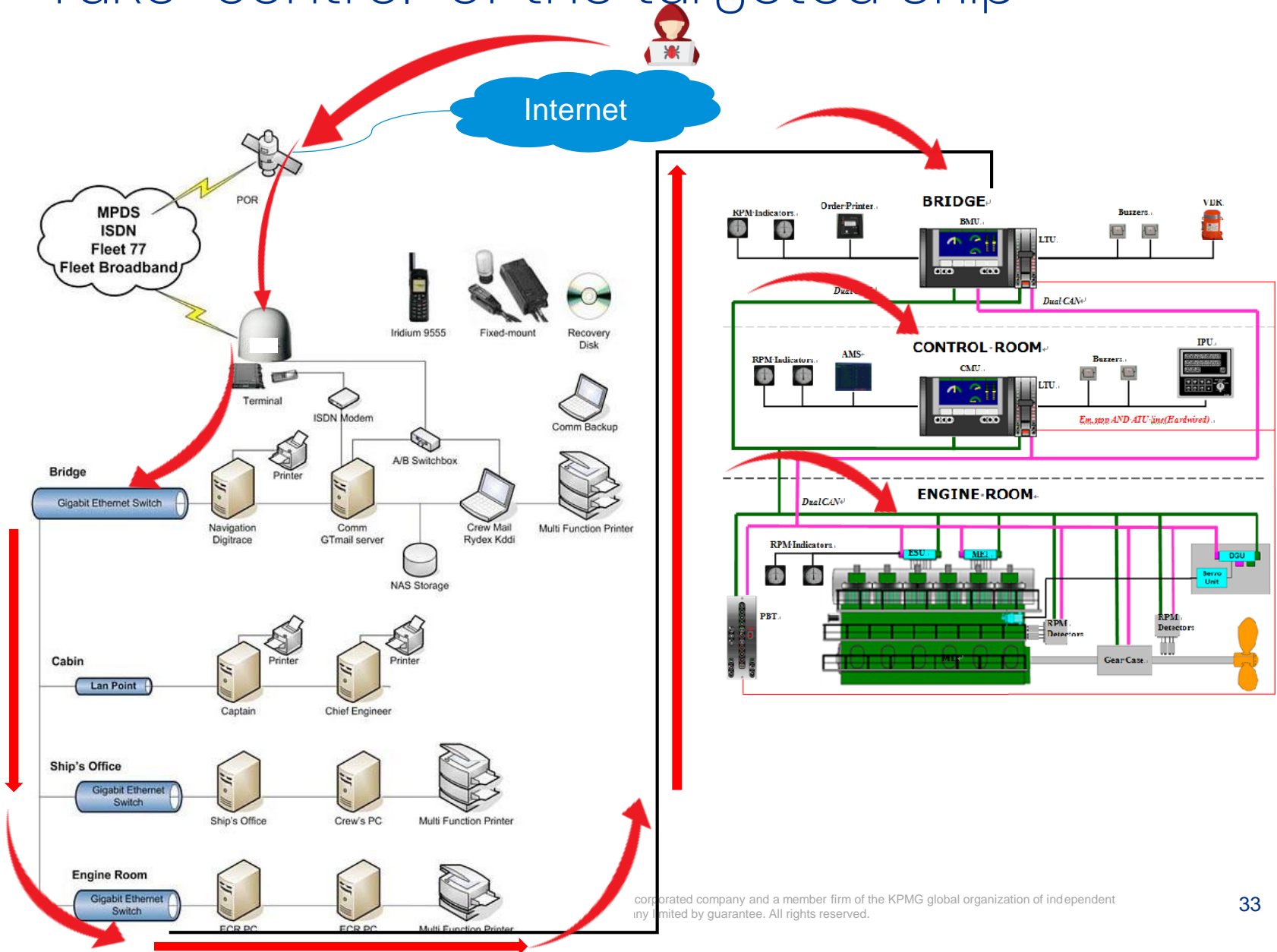


Cargo manifest and bills of lading tells someone what cargo is onboard



Source marineinsight.com

④ Take "control" of the targeted ship



Electronic Chart Display & Information System (ECDIS)

Electronic navigation charts (ENC)



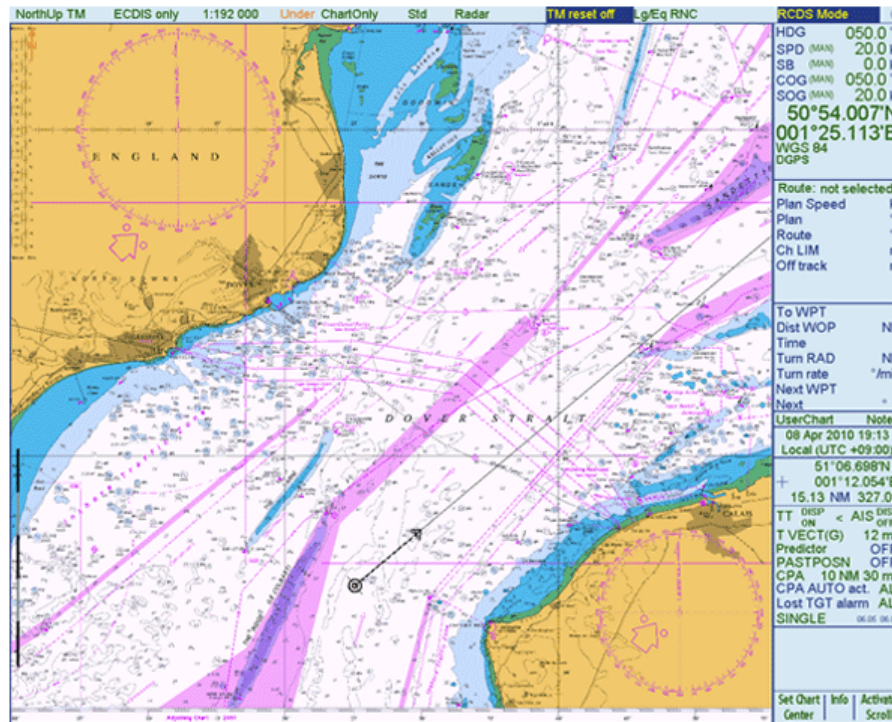
Automatic Identification System (AIS)



External GPS Antenna



Gyro Compass



Source: Furuno

Voyage Data Recorder (VDR)



Autopilot



Navigation decisions



⑤ Tamper with data that might influence navigation decisions. Steer the ship away from law enforcement and to somewhere I can board easily

Electronic navigation charts (ENC)



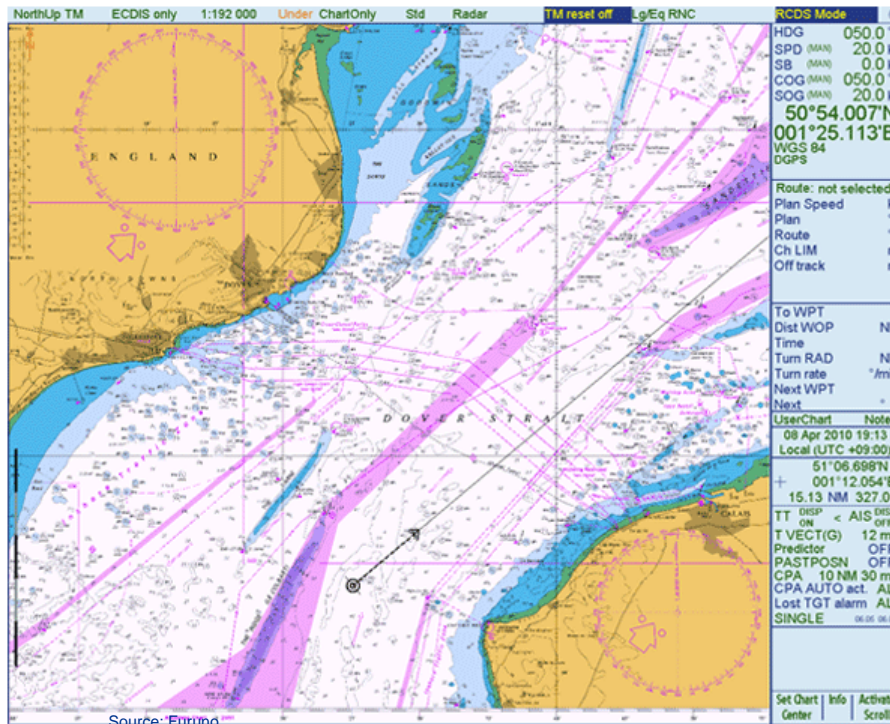
Automatic Identification System (AIS)



GPS data



Gyro Compass



Voyage Data Recorder (VDR)



Autopilot



Navigation decisions



⑥ Find the cargo in the least time (stow position) and extract the cargo

BAY 13

12	10	08	06	04	02	01	03	05	07	09	11	
												92
												90
												88
F	F	F	F	L	L	L	L	F	F	F	F	86
F	F	F	F	L	L	L	L	F	F	F	F	84
A	A	A	A	L	L	L	L	F	F	F	F	82

H	H	L	R	L	L	R	R	H	H			12
H	H	R	R	L	L	R	R	H	H			10
H	H	R	R	L	L	R	R	H	H			08
	H	R	R	L	L	R	R					06
		R	R	L	L	R	R					04
			R	L	L	R	R					02

12 10 08 06 04 02 01 03 05 07 09 11



Summary

- Increased reliance on digitalization and automation
- Cyber capabilities can greatly enhance the “performance” of criminals
- Cyber attack can affect not just IT systems but also physical things/processes
- Need to strengthen maritime sector’s resilience against cyber attacks