SECURITY CHALLENGES AND OPPORTUNITIES FOR DIGITAL TRANSFORMATION IN THE LOGISTICS INDUSTRY

Michael Yip
Chief Innovation Officer
Modern Terminals Limited

IS Summit 2022

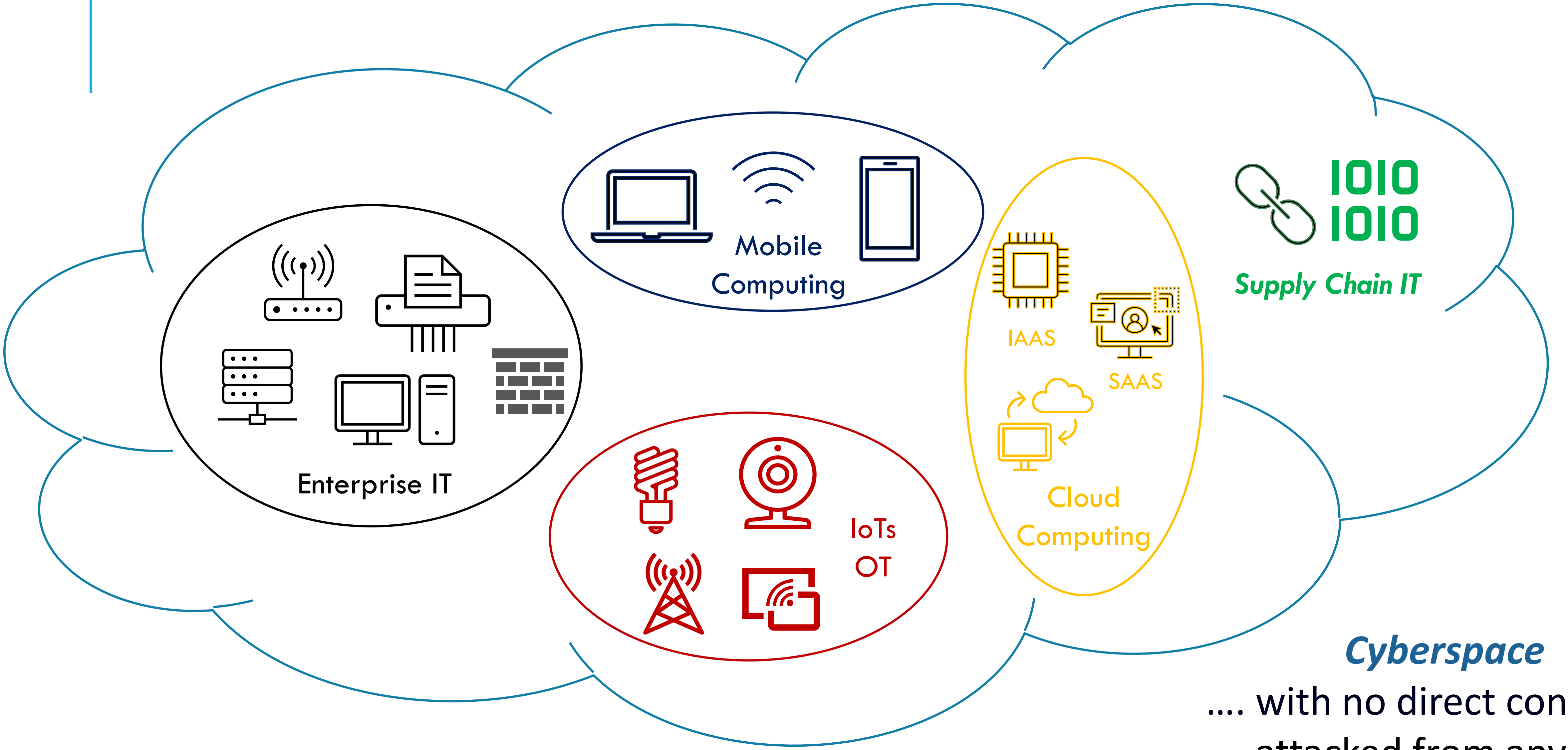
AGENDA

New Normal

Cybersecurity Awareness & Impact

Opportunities for Change

CYBERSECURITY IN A CHANGING WORLD

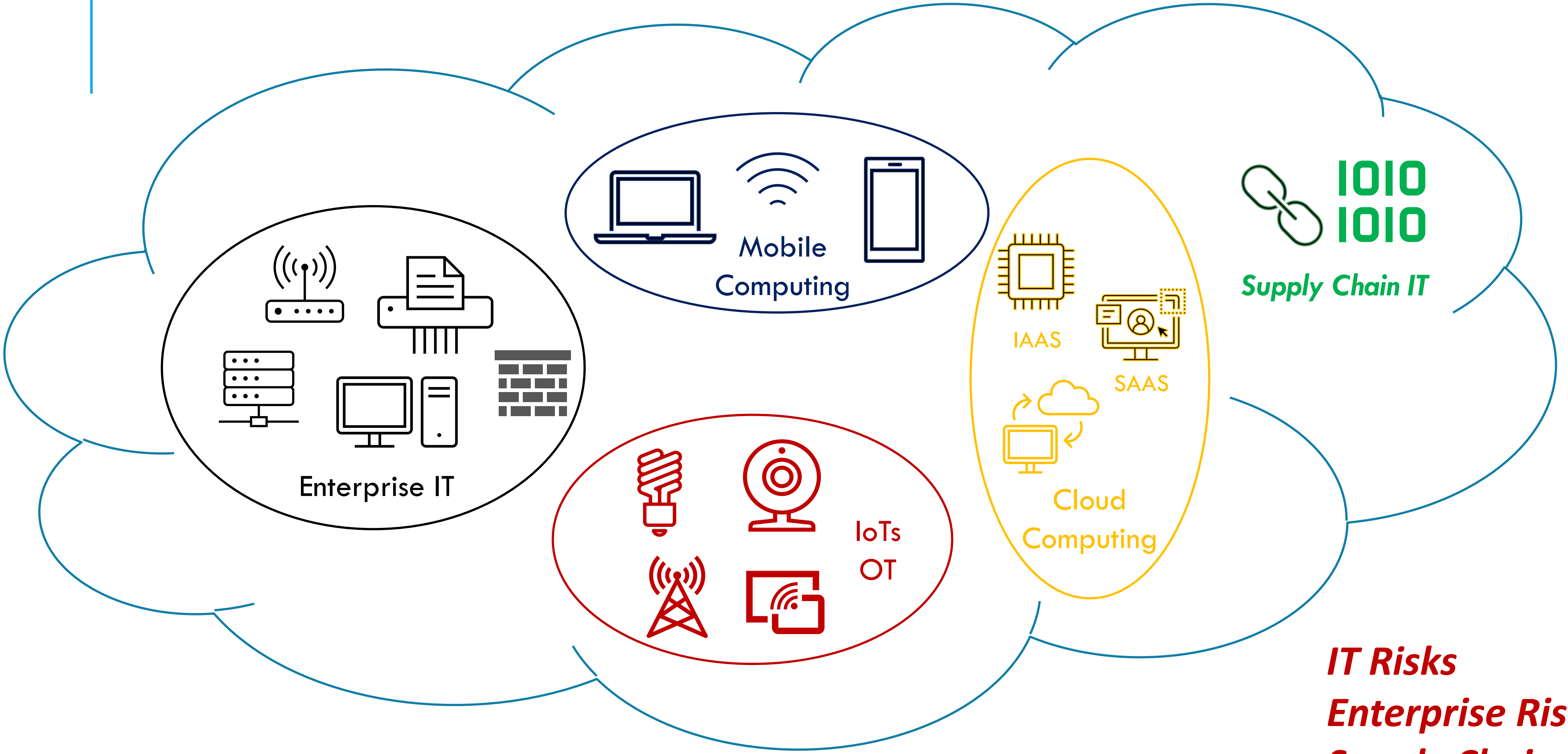


Cyberspace

…. with no direct control

…. attacked from anywhere

CYBERSECURITY IN THE NEW NORMAL



IT Risks

Enterprise Risks

Supply Chain Risks

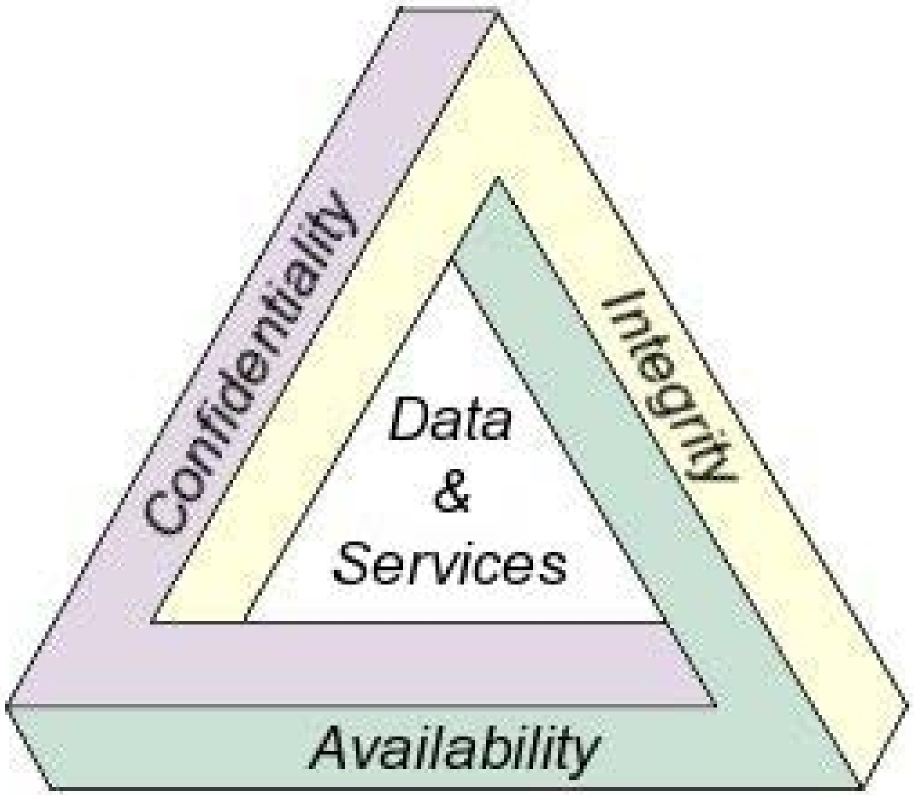
AGENDA

New Normal

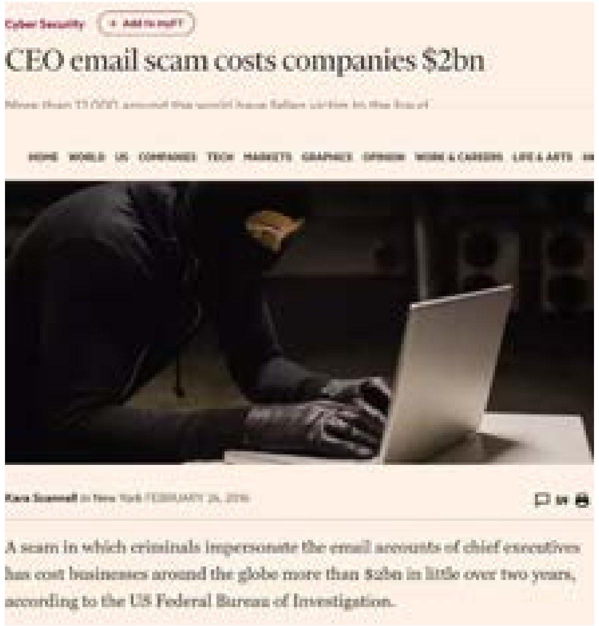
Cybersecurity Awareness & Impact

Opportunities for Change

CIA TRIAD OF INFORMATION SECURITY



FINANCIAL IMPACT OF CYBERSECURITY BREACHES

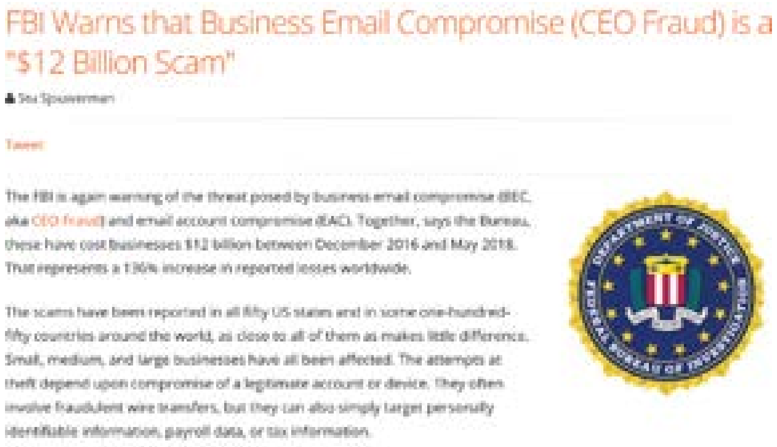

Cyber Security
+ Add to myFT
HOME WORLD US COMPANIES TECH MARKETS GRAPHICS OPINION WORK & CAREERS LIFE & ARTS

CEO email scam costs companies $2bn

More than 12,000 around the world have fallen victim to the fraud

Kara Scannell in New York FEBRUARY 26, 2016

A scam in which criminals impersonate the email accounts of chief executives has cost businesses around the globe more than $2bn in little over two years, according to the US Federal Bureau of Investigation.

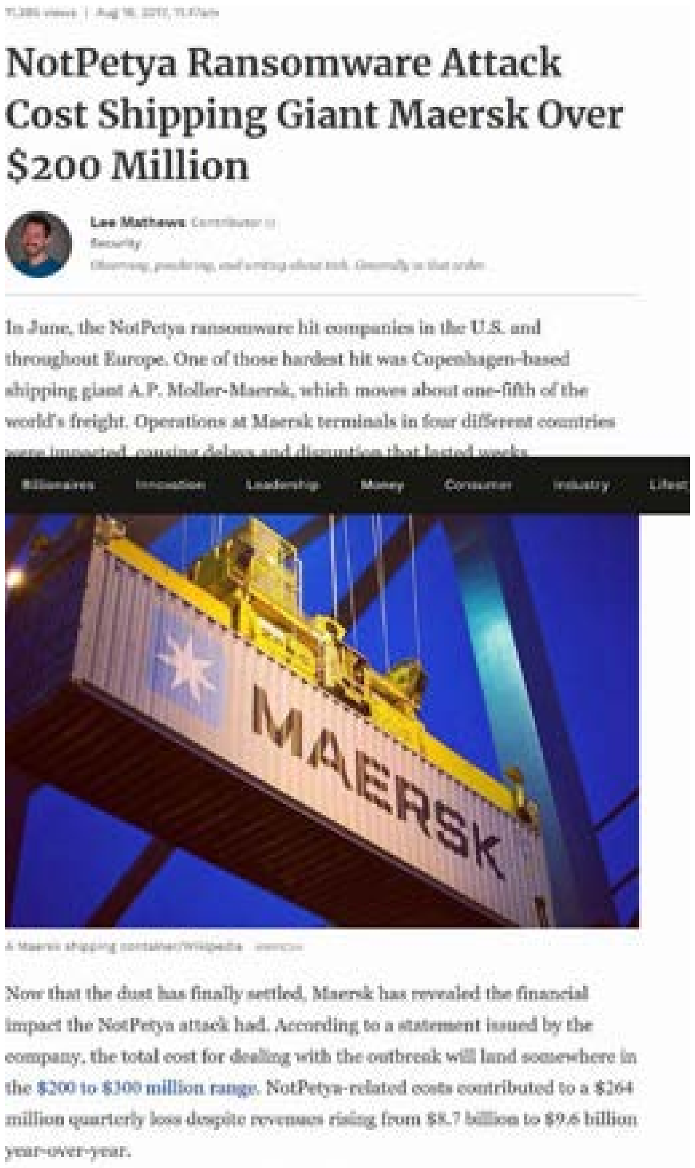


FBI Warns that Business Email Compromise (CEO Fraud) is a "$12 Billion Scam"

Stu Sjouwerman

The FBI is again warning of the threat posed by business email compromise (BEC, aka CEO fraud) and email account compromise (EAC). Together, says the Bureau, these have cost businesses $12 billion between December 2016 and May 2018. That represents a 136% increase in reported losses worldwide.

The scams have been reported in all fifty US states and in some one-hundred-fifty countries around the world, as close to all of them as makes little difference. Small, medium, and large businesses have all been affected. The attempts at theft depend upon compromise of a legitimate account or device. They often involve fraudulent wire transfers, but they can also simply target personally identifiable information, payroll data, or tax information.



7,285 views | Aug 16, 2017, 11:47am

NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million

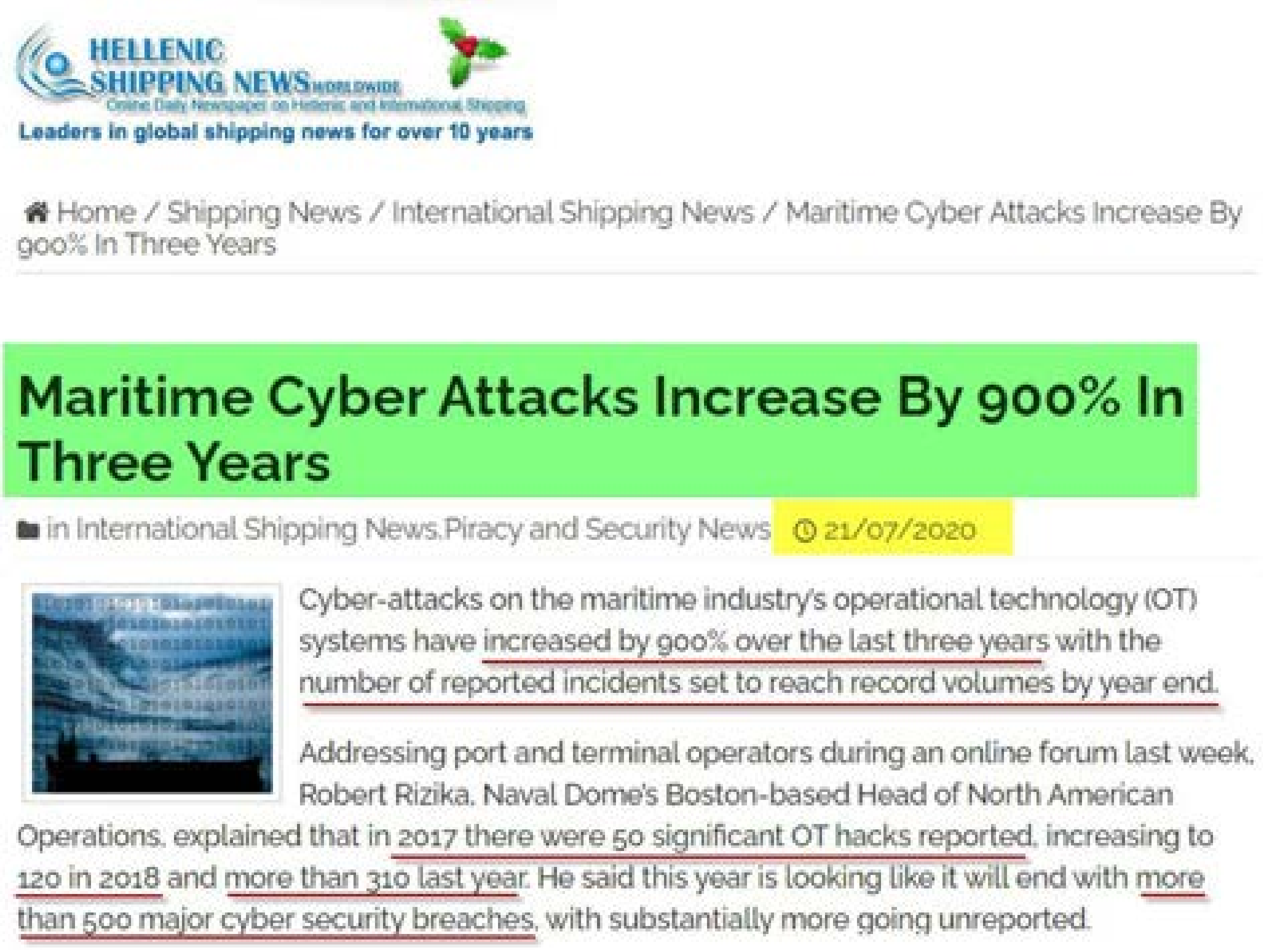
Lee Mathews Contributor
Security
Observing, pondering, and writing about tech. Generally in that order.

In June, the NotPetya ransomware hit companies in the U.S. and throughout Europe. One of those hardest hit was Copenhagen-based shipping giant A.P. Moller-Maersk, which moves about one-fifth of the world's freight. Operations at Maersk terminals in four different countries were impacted, causing delays and disruption that lasted weeks.

A Maersk shipping container/Wikipedia

Now that the dust has finally settled, Maersk has revealed the financial impact the NotPetya attack had. According to a statement issued by the company, the total cost for dealing with the outbreak will land somewhere in the $200 to $300 million range. NotPetya-related costs contributed to a $264 million quarterly loss despite revenues rising from $8.7 billion to $9.6 billion year-over-year.

CYBER ATTACKS IN MARITIME INDUSTRY ARE INCREASING



HELLENIC SHIPPING NEWS WORLDWIDE
Online Daily Newspaper on Hellenic and International Shipping
Leaders in global shipping news for over 10 years

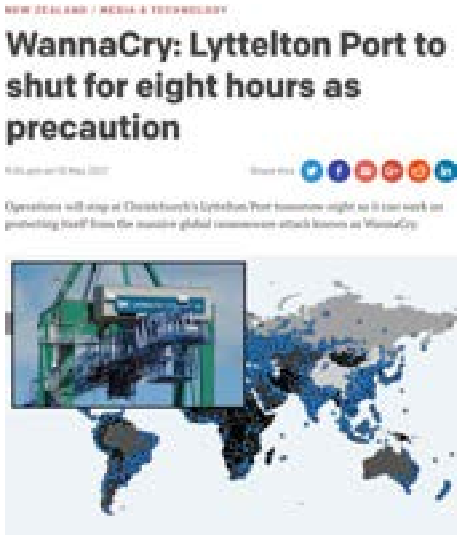
Home / Shipping News / International Shipping News / Maritime Cyber Attacks Increase By 900% In Three Years

Maritime Cyber Attacks Increase By 900% In Three Years

in International Shipping News,Piracy and Security News 21/07/2020

Cyber-attacks on the maritime industry's operational technology (OT) systems have increased by 900% over the last three years with the number of reported incidents set to reach record volumes by year end.

Addressing port and terminal operators during an online forum last week, Robert Rizika, Naval Dome's Boston-based Head of North American Operations, explained that in 2017 there were 50 significant OT hacks reported, increasing to 120 in 2018 and more than 310 last year. He said this year is looking like it will end with more than 500 major cyber security breaches, with substantially more going unreported.



NEW ZEALAND / MEDIA & TECHNOLOGY

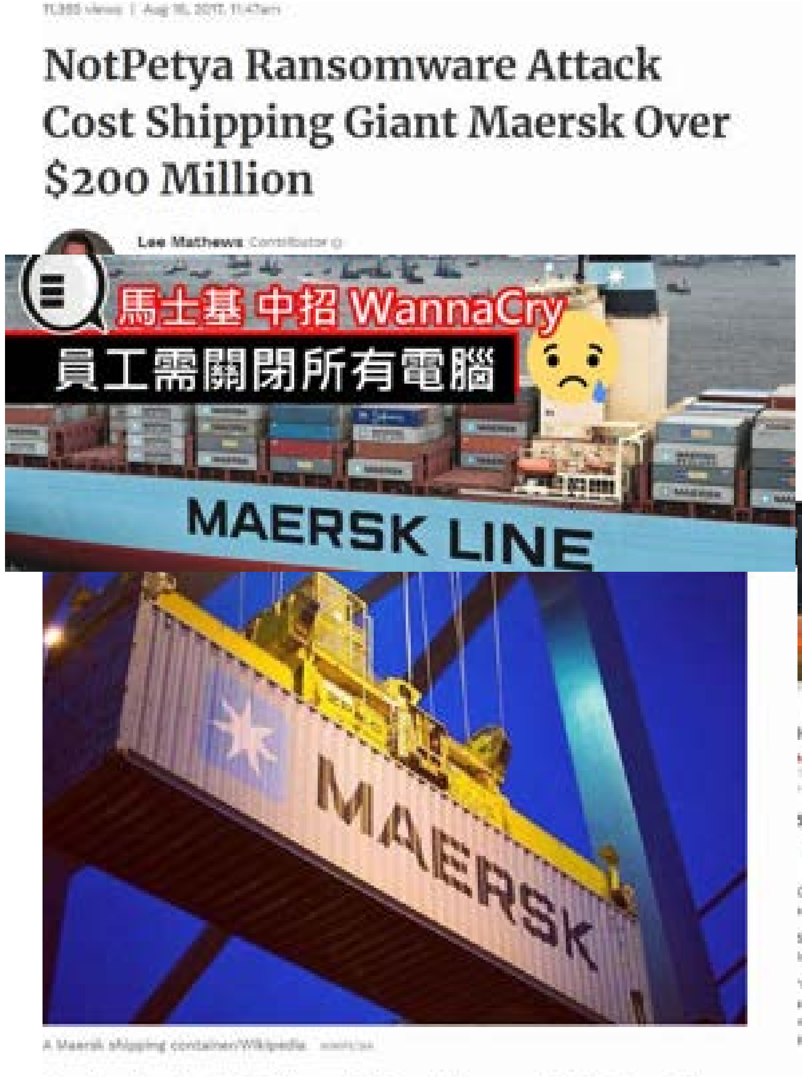
WannaCry: Lyttelton Port to shut for eight hours as precaution

9:05 pm on 18 May 2017

Share this

Operations will stop at Christchurch's Lyttelton Port tomorrow night as it can work on protecting itself from the massive global ransomware attack known as WannaCry.

MAY 2017



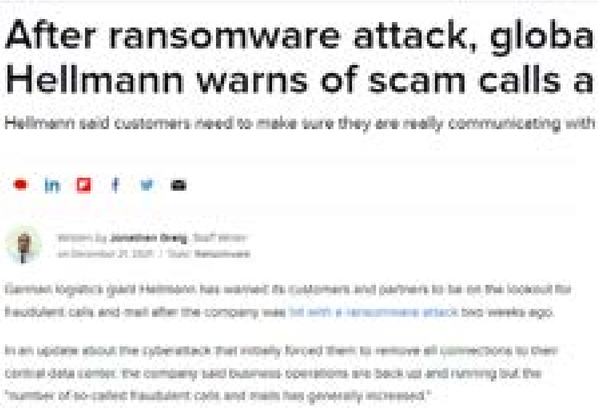
11,355 views | Aug 16, 2017, 11:47am

NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million

Lee Mathews Contributor

A Maersk shipping container/Wikipedia

JUNE 2017



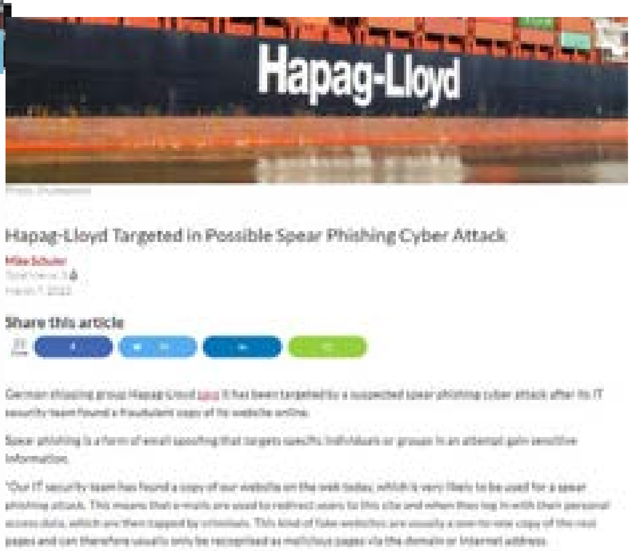
After ransomware attack, global logistics firm Hellmann warns of scam calls and mail

Hellmann said customers need to make sure they are really communicating with an employee through all calls or mail.

Written by Jonathan Greig, Staff Writer on December 21, 2021 | Topic: Ransomware

German logistics giant Hellmann has warned its customers and partners to be on the lookout for fraudulent calls and mail after the company was hit with a ransomware attack two weeks ago.

In an update about the cyberattack that initially forced them to remove all connections to their central data center, the company said business operations are back up and running but the "number of so-called fraudulent calls and mails has generally increased."



Hapag-Lloyd Targeted in Possible Spear Phishing Cyber Attack

Mike Schuler

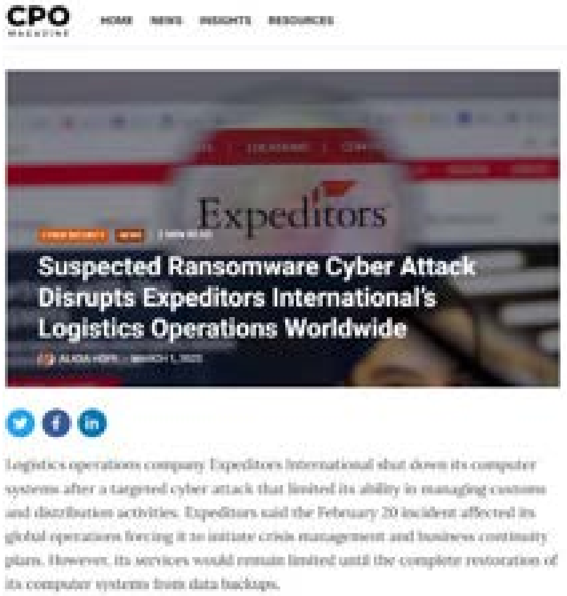
March 7, 2022

Share this article

German shipping group Hapag-Lloyd said it has been targeted by a suspected spear phishing cyber attack after its IT security team found a fraudulent copy of its website online.

Spear phishing is a form of email spoofing that targets specific individuals or groups in an attempt gain sensitive information.

"Our IT security team has found a copy of our website on the web today, which is very likely to be used for a spear phishing attack. This means that e-mails are used to redirect users to this site and when they log in with their personal access data, which are then tapped by criminals. This kind of fake websites are usually a one-to-one copy of the real pages and can therefore usually only be recognised as malicious pages via the domain or Internet address.



Suspected Ransomware Cyber Attack Disrupts Expeditors International's Logistics Operations Worldwide

ALICIA HOPE • MARCH 1, 2022

Logistics operations company Expeditors International shut down its computer systems after a targeted cyber attack that limited its ability in managing customs and distribution activities. Expeditors said the February 20 incident affected its global operations forcing it to initiate crisis management and business continuity plans. However, its services would remain limited until the complete restoration of its computer systems from data backups.

2021 / 2022

MINDSET CHANGE NEEDED….

From IT security to Cybersecurity

Expanded Scope - no longer sufficient to just protect your internal IT

IT & OT - business, operational & consumer technologies

Assess the ***impact*** to both your ***internal operations*** and to your ***supply chain network***

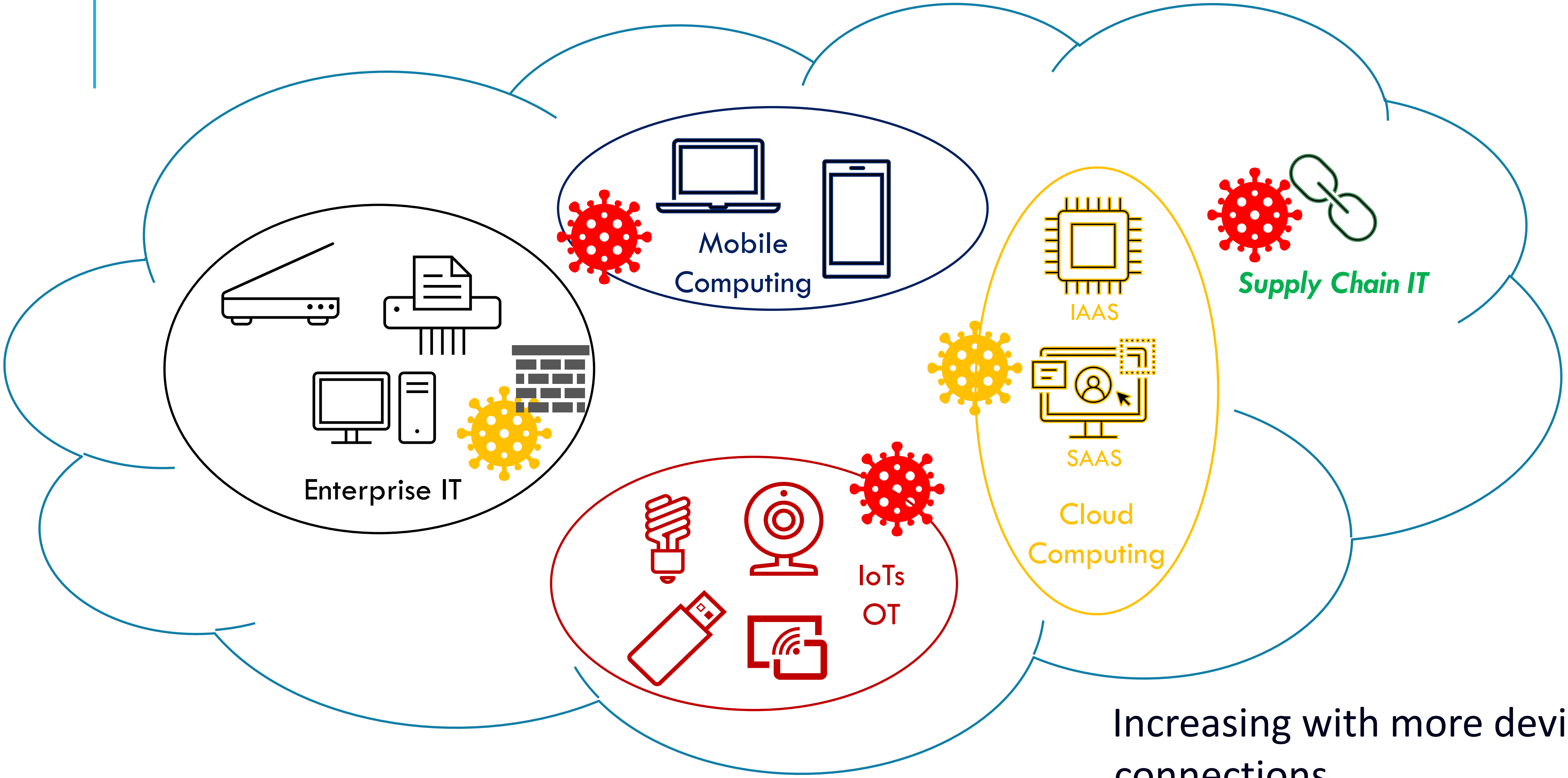
CYBERSECURITY AWARENESS

Cybersecurity incidents are more frequent, harder to prevent, and with potential of significant financial impact

More holistic approach to Cybersecurity is required

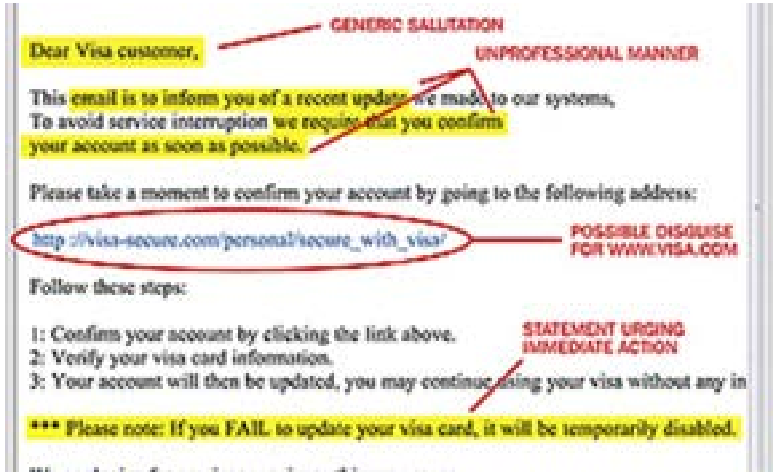
- Understand your Vulnerabilities
- Strengthen your weaknesses
- Be prepared to React and Respond

SYSTEM VULNERABILITIES



Increasing with more devices & connections....

HUMAN VULNERABILITIES



Dear Visa customer,

This email is to inform you of a recent update we made to our systems.
To avoid service interruption we require that you confirm your account as soon as possible.

Please take a moment to confirm your account by going to the following address:

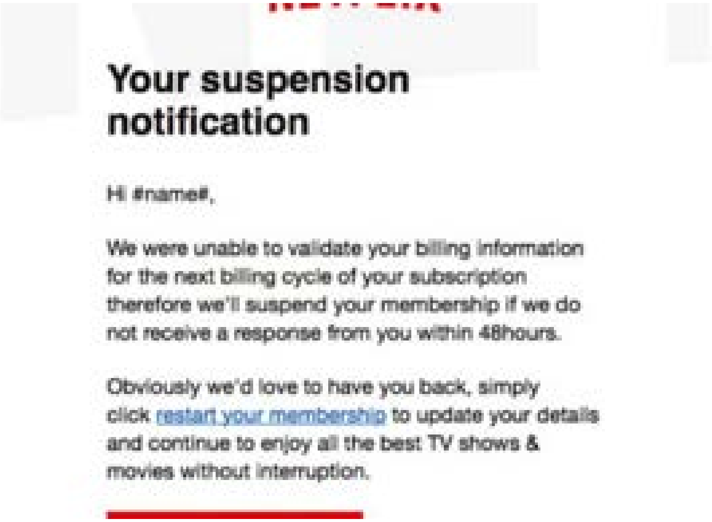
http ://visa-secure.com/personal/?secure_with_visa/

Follow these steps:

1: Confirm your account by clicking the link above.
2: Verify your visa card information.
3: Your account will then be updated, you may continue using your visa without any in

*** Please note: If you FAIL to update your visa card, it will be temporarily disabled.

GENERIC SALUTATION
UNPROFESSIONAL MANNER
POSSIBLE DISGUISE FOR WWW.VISA.COM
STATEMENT URGING IMMEDIATE ACTION



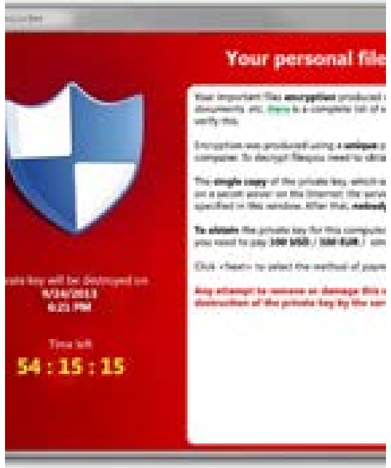
NETFLIX

Your suspension notification

Hi #name#,

We were unable to validate your billing information for the next billing cycle of your subscription therefore we'll suspend your membership if we do not receive a response from you within 48hours.

Obviously we'd love to have you back, simply click restart your membership to update your details and continue to enjoy all the best TV shows & movies without interruption.



Your personal file

Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key generated for this computer. To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody

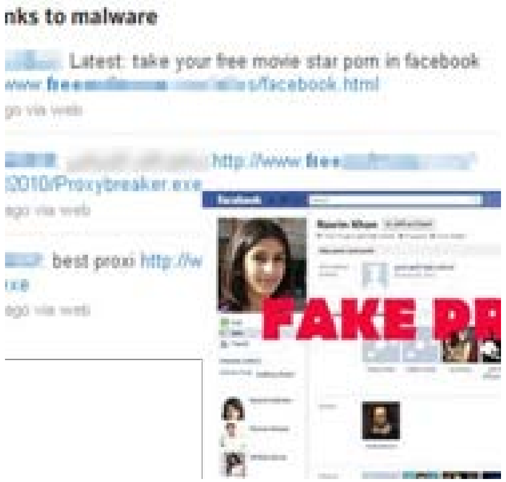
To obtain the private key for this computer you need to pay 300 USD / 300 EUR /

Click <Next> to select the method of payment

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

ate key will be destroyed on
9/24/2013
6:21 PM

Time left
54 : 15 : 15



nks to malware

[redacted] Latest: take your free movie star porn in facebook
www free[redacted]s/facebook.html
go via web

[redacted] http://www.free[redacted]
2010/Proxybreaker.exe
ago via web

[redacted] best proxi http://w
xe
ago via web

AGENDA

New Normal

Cybersecurity Awareness & Impact

Opportunities for Change

CYBERSECURITY PROTECTION

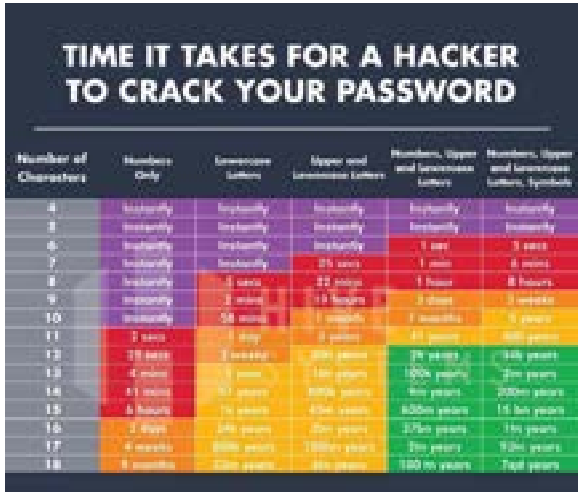
STEPS TO TAKE…

1. Build Organizational Awareness
2. Strengthen Cybersecurity Protection
3. Establish Risk Mitigation & Crisis Response Plans

BUILD AWARENESS

Employee Training & Awareness

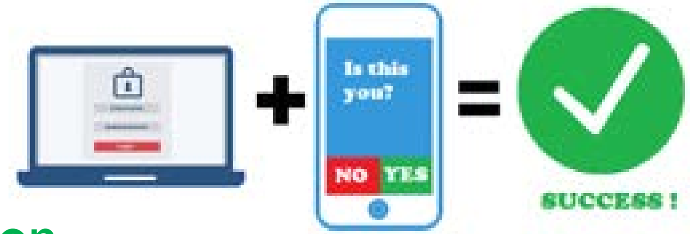
- Simulations and “Friendly Hacks”


TIME IT TAKES FOR A HACKER TO CRACK YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

Strong Passwords – simple but effective

- Balance inconvenience & security
- Multi-Factor / Biometric Authentication



Keep hardware & software up-to-date

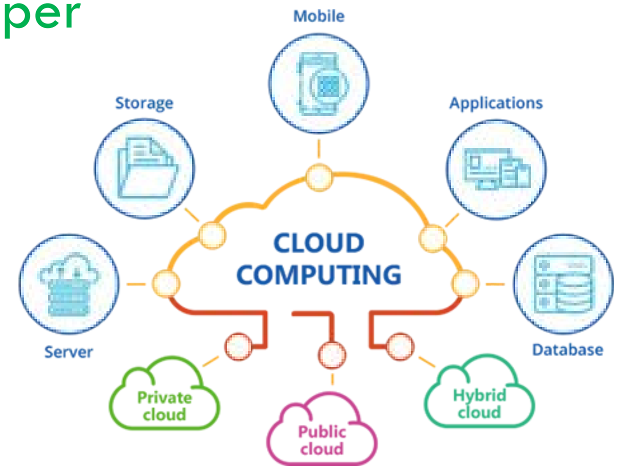
- Work with Engineering teams on OT security

STRENGTHEN PROTECTION

- Invest in security protection hardware & software
  - Traditional firewalls, endpoint protection, email security, etc.
  - Cybersecurity services & partnerships; Virtual CISOs

- Identify the key IT assets that require hardening or building redundancies
  - Business Systems & Technology Services – IT & OT
  - Data – Financial, Customer, Operational, HR, etc.
  - Information Flow – Digital or Analog/Paper

- Moving from "backup & restore" to…
  - ➢ Availability of Service
  - ➢ Data Replication & Synchronization



RISK MITIGATION / CRISIS RESPONSE

Think end-to-end processes - within your organization; across your supply chain

- Business continuity plans are across organizational units
- Develop plans or define requirements with your key supply chain partners
- Key partners – require proven cybersecurity strategies or certifications

Develop crisis response plans against your “high risk” scenarios

- Can be specific – i.e. if a certain scenario occurs
- Or more generic – disruptions to labour, facilities, technology, suppliers/partners
- Include external communications & reputation management aspects
- Identify the necessary organizational changes/teams to manage the crisis

INCIDENT RESPONSE

CRISIS MANAGEMENT

Nothing is 100% secure, despite all the investment devoted to prevent cybersecurity events, you still need to be prepared to respond and act….

IT will have service continuity and Disaster Recovery Plans in place to respond to cybersecurity incidents – including data backup/restoration plans

Business operations will need to develop mitigation measures during systems disruptions, and crisis communications plans for both internal and external stakeholders

BUILD ORGANIZATIONAL FIREWALL

….. Strong Culture of Security

- Everyone will be treated the SAME in a cyber-attack!!!
- Cybersecurity awareness training, security drills & exercises
- Business units take accountability
- Build with Security in mind
- Opportunity for change

THANK YOU

Michael Yip
Chief Innovation Officer
Modern Terminals Limited
michael.yip@modernterminals.com