



Navigating a Ransomware Incident: **The Crucial Role of Cyber Insurance**

26 - 28 November 2024 • Riyadh, Saudi Arabia

Organised by Riyadh Alotaibi



الاتحاد السعودي للأمن
السيبراني والبرمجة والدرونز
SAUDI FEDERATION FOR CYBERSECURITY,
PROGRAMMING & DRONES



Who are we?

Cyber Specialists of Munich Re



Asbat El Khairi

Cyber Security Consultant at Munich Re
Cyber Security Researcher – Cloud Security

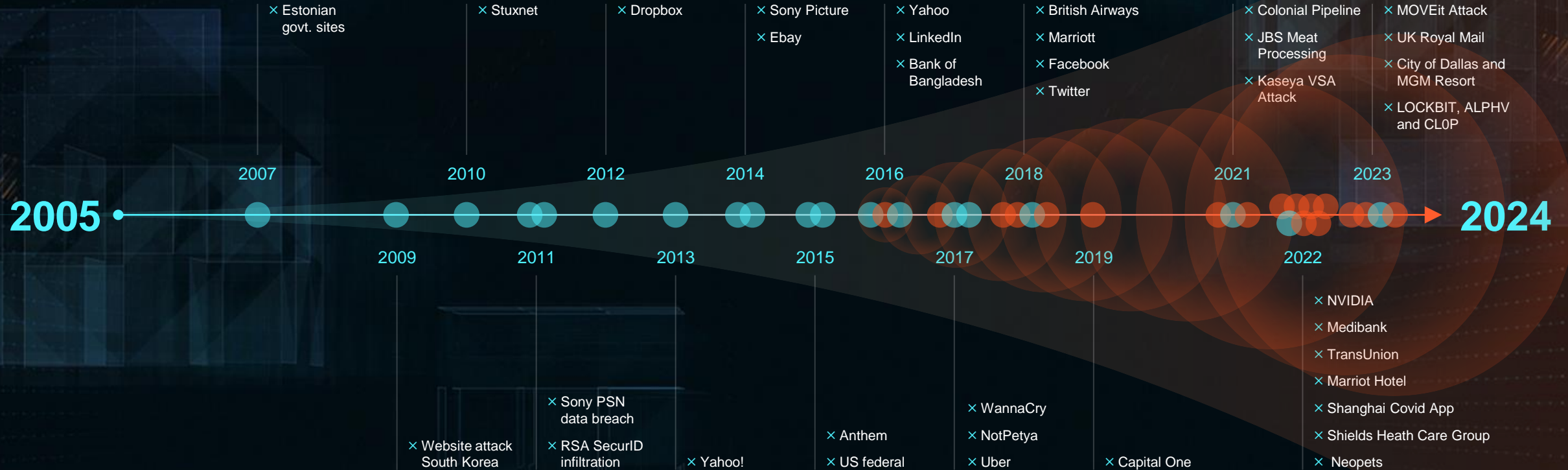


Liam Cattermole-Ward

Senior Cyber Claims Adjuster
at Munich Re

Ransomware on the rise amongst all incidents

Major Cyber Incidents



What is Ransomware?

Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid.

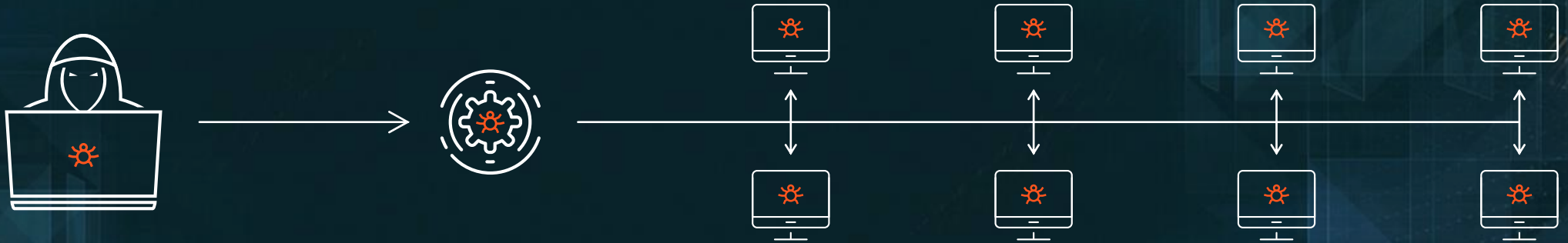
More modern ransomware families, collectively categorized as crypto ransomware, encrypt certain file types on infected systems and force users to pay the ransom through certain online payment methods to get a decryption key.



How has ransomware evolved over time?

From "Shotgun" to "Post-Compromise" Approach

"Shotgun"
Approach



"Post-
compromise"
Approach



How are ransomware attacks performed nowadays?

"Post-compromise" Approach



What is the impact of ransomware?

Statistics and noteworthy developments

The average downtime experienced from a ransomware attack is **21 days**¹

Total payments reached **\$1.1 billion** in **2023**, up from **\$567 million** in **2022**²

The largest ransom payment recorded is **\$40 million**¹

Affected sectors in 2023 included **healthcare**, **government**, **manufacturing**, and **retail**³

5,070 ransomware incidents were recorded in **2023**, a **55%** increase from **2022**¹

Ransomware-as-a-Service (RaaS) has made it easier for **affiliates** to carry out attacks²

New Trend: Double Extortion

In 2023, over 50% of ransomware attacks included this double-extortion method

¹ Ransomware Trends and Statistics: 2023 Report". Cyberint, 2023

² Ransomware Attacks Surge, Rely on Public and Legitimate Tools". Google Cloud Blog, 2024

³ 2024 Rapid7 Ransomware Radar Report". Rapid7, 2024

⁴ Palo Alto Networks Unit 42 Ransomware and Extortion Report, Zscaler's 2023 ThreatLabz Ransomware Report)

Navigating a Ransomware Incident

Anonymous Case Study based on Real World Scenario & Sequence of Events



- ▶ What is the scope and impact of the attack?
- ▶ How was the attack carried out?
- ▶ What immediate actions should be taken?
- ▶ Has data been exfiltrated?
- ▶ Should the ransom be paid?
- ▶ What is the communication plan?
- ▶ How can future attacks be prevented?

Who is Global Vintage Hotels?

Some key parameters for the case study

140
Properties Globally

1.5 billion US\$
Revenue



65 million
Customers

**Cyber policy
in place**

What is Cyber Insurance?

A modular concept with multiple coverages

1st Party Costs

Business interruption 1

Lost profits and extra expenses incurred due to the unavailability of data and IT systems at the insured or resulting from the IT failure of an external third party (e.g., cloud provider).

Data restoration & recreation costs 2

Reimbursement of costs to restore data and software after a cyber incident.

Incident & breach response costs 3

Reimbursement of cost of responding to an event such as IT forensics, notification, credit-watch services.

Cyber Extortion 4

(Threat of or) loss, leak or destruction of (customer) data.
Includes payment of ransom where legally permissible.

Cyber Crime 5

Reimbursement of loss of funds (e.g., CEO fraud).

PCI DSS 6

Reimbursement for contractual fines and penalties for non-compliance against PCI DSS.
Costs can cover a PCI forensic investigation, PCI-DSS recertification, reissuing of credit/debit cards.

3rd Party Claims

Network security liability 7

3rd-party liabilities arising from security events occurring within the insured's IT network or passing through it in order to attack a third-party.

Privacy & data breach liability 8

Covers 3rd-party claims following a data breach relating to confidential information or personal data of a 3rd-party made against the policyholder.

Media liability 9

Cost for investigation, defense cost and civil damages arising from defamation, libel, slander, copyright/trademark infringement, negligence in publication of any content in electronic or print media.

Global Vintage Hotels has been hacked

A typical ransomware note

>>>> Your network has been penetrated. <<<<

All files on each host in the network have been encrypted with a strong algorithm. Please do not attempt to restore from backups, we have also encrypted these too.

We only have exclusive decryption software for your situation, no decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.

DO NOT RENAME OR MOVE - the encrypted readme file.

DO NOT DELETE readme file.

DO NOT use any recovery software with restoring files overwriting encrypted.

This may lead to the impossibility of recovery of the certain files.

To get info (decrypt your files) contact us at your personal page:

1. Download and install Tor Browser: <https://www.torproject.org/download/>
2. After successful installation, run the browser and wait for initialization.
3. Type in the address bar: DHFMGRERJG*£\$£&\$\$JSLS///azhDHE27383"£\$.onion

YOU NEED TO CONTACT US WITHIN 48 HOURS AND THE ABOVE LINK IS AVAILABLE FOR 7 DAYS!!!!!!

DEMAND IS BTC 559.49 - USD 35M

WildWalruss

No System is Safe

DATA

AQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGFDHRHFNdhfinnrobweb///23843""281923dbdaIGEIBHIWBFBOBCSVSBLZBVZLGBGFAIFHOAHIFGBWQ
EIIBIB87638391ibiebdidbisbidb //zz/sdhhrhrkdhMxJSV

Day 1

Global Vintage Hotels has been hacked

A typical ransomware note

>>>> Your network has been penetrated. <<<<

All files on each host in the network have been encrypted with a strong algorithm. Please do not attempt to restore from backups, we have also encrypted these too.

We only have exclusive decryption software for your situation, no decryption software is available in the public.

DO NOT RESET
DO NOT RENAME
DO NOT DELETE
DO NOT use
This may I

DO NOT RESET OR SHUTDOWN – files may be damaged.
DO NOT RENAME OR MOVE – the encrypted readme file.
DO NOT DELETE readme file.

DO NOT use any recovery software with restoring files overwriting encrypted.

To get info

1. Download
2. After s
3. Type in

YOU NEED TO CONTACT US WITHIN 48 HOURS AND THE ABOVE LINK IS AVAILABLE FOR 7 DAYS!!!!!!

DEMAND IS BTC 559.49 – USD 35M

WildWalruss

No System is Safe

DATA

AQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGFDHRHFNDhfinnrobweb///23843""281923dbdaIGEIBHIWFBFOBCSVSBLZBVZLGBGFAIFHOAHIFGBWQ
EIIIBIB87638391ibiebdidbisbidb //zz/sdhhrhrkdhnMxJSV

Day 1

Global Vintage Hotels has been hacked

A typical ransomware note

>>>> Your network has been penetrated. <<<<

All files on each host in the network have been encrypted with a strong algorithm. Please do not attempt to restore from backups, we have also encrypted these too.

We only have exclusive decryption software for your situation, no decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.

DO NOT RENAME OR MOVE - the encrypted readme file.

DO NOT DELETE readme file.

YOU NEED TO CONTACT US WITHIN 48 HOURS AND THE ABOVE LINK IS AVAILABLE FOR 7 DAYS!!!!!!

DEMAND IS BTC 559.49 – USD 35M

YOU NEED TO CONTACT US WITHIN 48 HOURS AND THE ABOVE LINK IS AVAILABLE FOR 7 DAYS!!!!!!

DEMAND IS BTC 559.49 – USD 35M

WildWalruss

No System is Safe

DATA

AQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGFDHRHFNDhfinnrobweb///23843""281923dbdaIGEIBHIWFBFOBCSVSBLZBVZLGBGFAIFHOAHIFGBWQ

EIIBIB87638391ibiebdidbisbidb //zz/sdhhrhrkdhnMxJSV

Day 1

Global Vintage Hotels has been hacked

What do we know so far?

Threat Actor:
"Wild-
Walruss"

Initial entry:
Vishing
Attack

35m USD
Demand in BTC

1TB of Data
Exfiltrated

Backups
have been encrypted

48h time
to respond

Day 1

Global Vintage Hotels has been hacked

What is the potential impact?

Website



Key Cards



Payment



Telephone



Emails



Restaurant POS Systems



Payroll



Day 1

The Role of an Incident Response Manager

Example: Lawyer Led Model



Day 1

Profiling the Threat Actor

What can we find out about their behavior?

What is their operating model?



How many victims and datasets are leaked?

Do they have defined demand patterns?

Are decryptors known or available?

Day 2

Contacting the Threat Actor

Who and when in case you cannot restore from backups?

Do not nominate
a decision
maker



Don't let the
threat actors be in
the driving seat

Independent
and unrelated to
the business

Contact 24 hours
after the deadline is
usually advisable

Day 3

Contact with Threat Actor established

How to prepare for negotiations?

"WildWalruss"
reiterate the demand
of USD 35 million



It is advised
to request a
proof of life

They have not yet
leaked the data, despite
the 48-hour deadline

The crisis team held
numerous meetings, the
board has budgeted a limit
of USD 20 million

Day 4

Day 5

Negotiation phase

How to conduct negotiations?

After proof of life
process is complete,
negotiation on the
price begins



You do not hold
Bitcoin as a company, so
you need to engage a specialist
payment broker

You want to start negotiations
close to your given budget
(f.i. USD 14,550,000),
don't expect many rounds

Make clear all avenues
have been exhausted,
there is no alternative

Day 7

Settlement agreement achieved

What to consider and what are the next steps?

Even if Threat Actor fulfills settlement and makes good on the agreement, ultimately you cannot trust them
(double extortion)



You receive a decryptor via dark web portal after payment
(in our case settlement of USD 17,500,000)

System restoration takes additional 10 days, core functionality restored within 2 days

Incident Response
Costs USD 6 million leading to Estimated Loss of Revenue of USD 70 million

System restoration completed

Day 17

Are you now safe and can rest? What happened in reality?



after **18** Months

EU Regulators
launch investigation

after **24** Months

US Regulators
issue USD 10 million fine

after **36** Months

Litigation with
customers ongoing

Key Take Aways from the Case Study

What do you need to remember?

1

First 24 hours
is critical

2

Knowing the
profile of the
threat actor

3

Paying a
ransom is not
advisable

4

Right person
& right time

5

Insurance plays
a crucial role

6

Know your
business
continuity plan

The Role of Cyber Insurance

What influences the decision making?





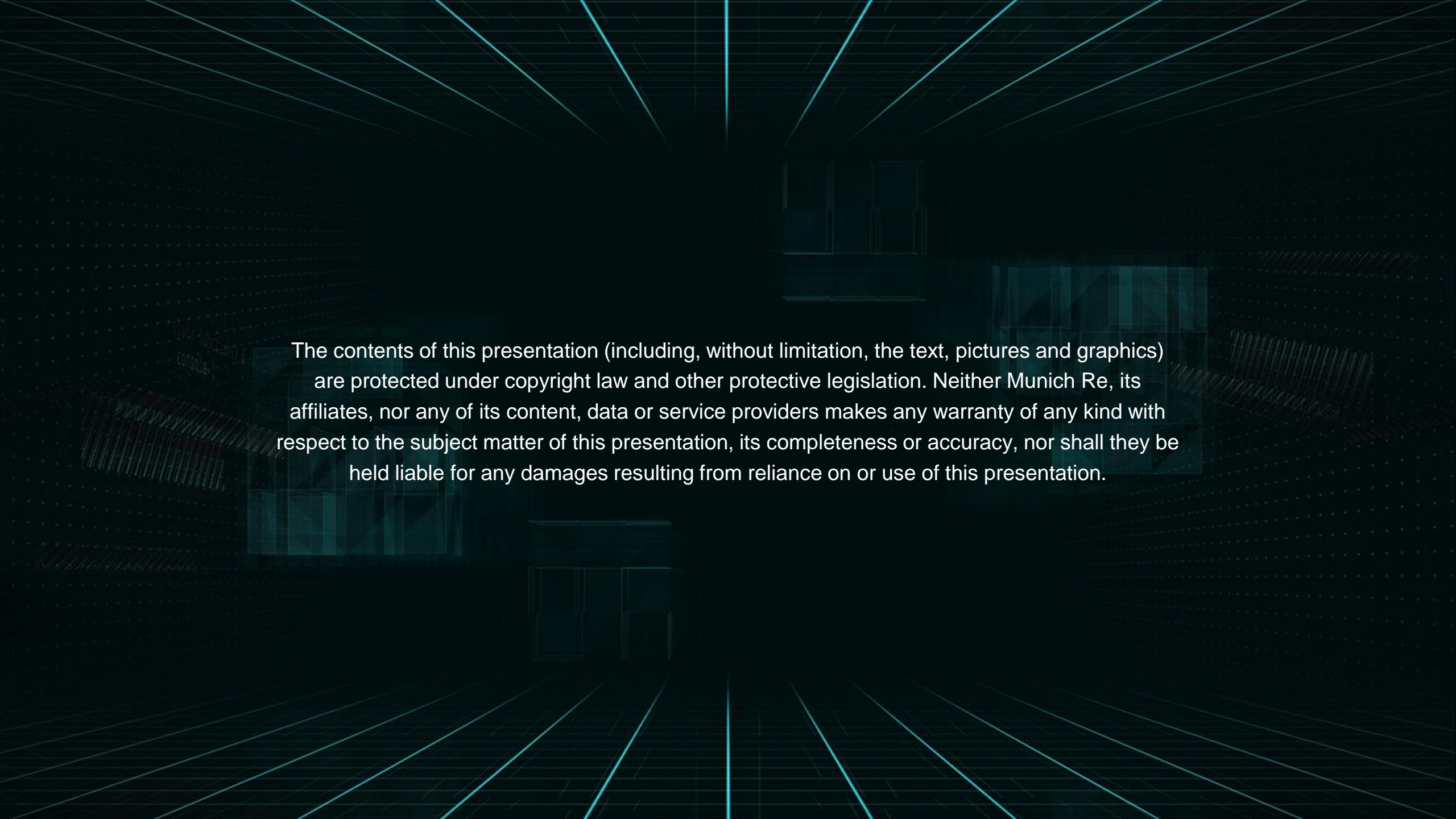
Thank you!
Questions?

Organised by Riyadh Alotaibi



الاتحاد السعودي للأمن
السيبراني والبرمجة والدرونز
SAUDI FEDERATION FOR CYBERSECURITY,
PROGRAMMING & DRONES



The background is a dark teal color with a subtle grid pattern. Overlaid on this are several bright teal lines that radiate from the center towards the corners, creating a sense of depth and perspective. There are also some faint, darker teal rectangular shapes scattered across the background.

The contents of this presentation (including, without limitation, the text, pictures and graphics) are protected under copyright law and other protective legislation. Neither Munich Re, its affiliates, nor any of its content, data or service providers makes any warranty of any kind with respect to the subject matter of this presentation, its completeness or accuracy, nor shall they be held liable for any damages resulting from reliance on or use of this presentation.