RSAConference2015

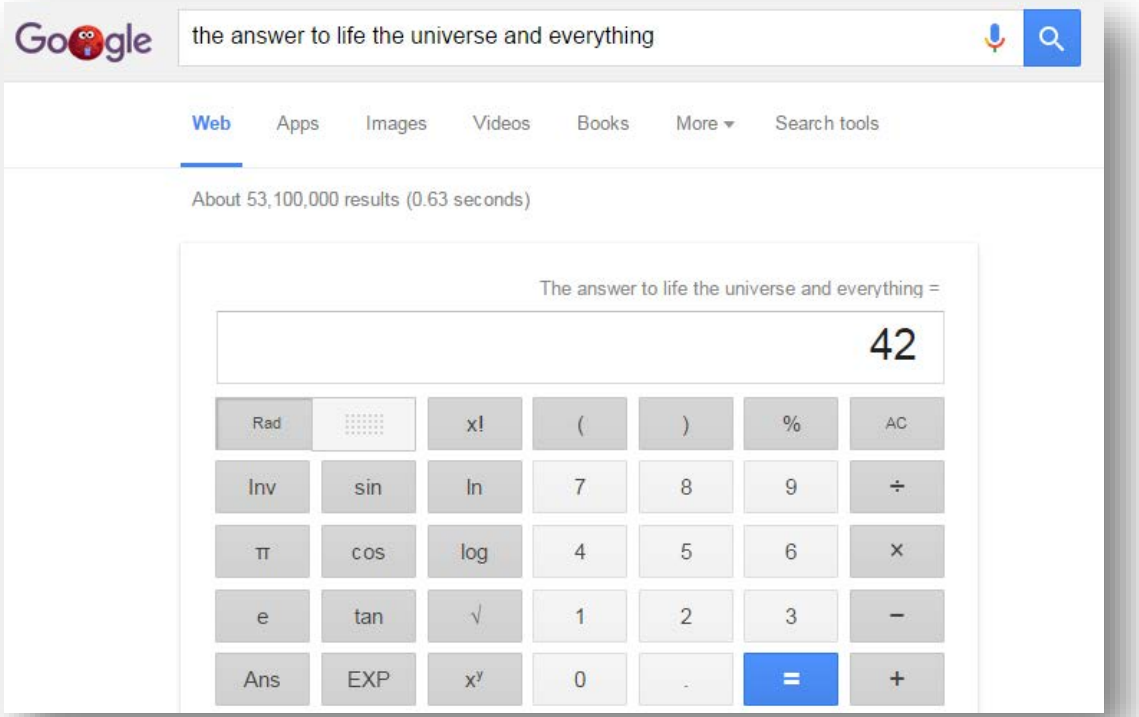
Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: SOP-W07

Do’s and Don’ts of a CISO…

Jason Haward-Grau
Group Chief Information Security Officer
MOL Group

We think we all know the answer is Cyber Security. As a CISO do we know the right question or questions?



In approaching this I had a couple of thoughts as an introduction…

1st Thoughts:

- **How** do you start delivering **Cyber Security in a 'heavy industry'** multinational in Central Europe
- What's **InfoSec** and what's **IT**
- Over 40% of 'large companies' still don't have any proactive Information Security capabilities.

1st Challenges:

- The world is getting more **complex** and **connected**..
- There is a '**Gordian knot**' of things to worry about
- We have to play **catch up**
- Our **industry is** 25 years **young**

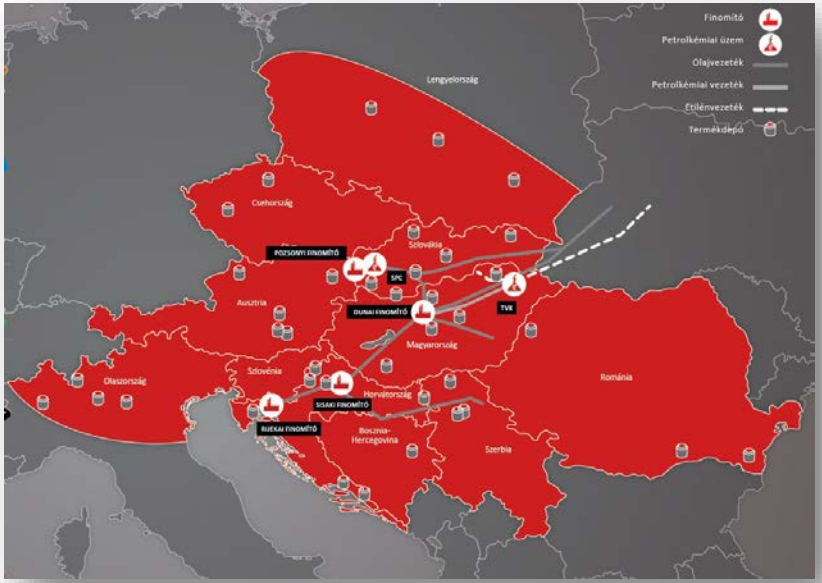
There is a lot to worry about!

Purpose for today's session:

- Provide an **overview of my journey so far** – key challenges, key steps taken
- Outline my approach to '**how**' to deliver InfoSec **from scratch** – the first 6 months,
- Wrestle with working out how to put **strategy into action**
- **Talking the business language** – where the CISO plays

Introducing the challenge - InfoSec in a Modern Multinational is not a simple 'one and done'

- Who are MOL? –
  the largest Oil & Gas Company
  you've never heard of…



Large Regional Retail footprint

Complex Global Reach

Just like everyone else, its complex..

Introducing InfoSec into a Modern Multinational

- Why a CISO and why now?

Is it all about protecting our critical national infrastructure?

Protecting our Critical Infrastructure – challenge accepted

- **Multi-zone protection** and different defence-in-depth strategies: Office + **critical industrial environment** (IT, SCADA, ICS, PI)
- From non-standardized technologies to standardisation

How do we secure all this?

A common challenge?

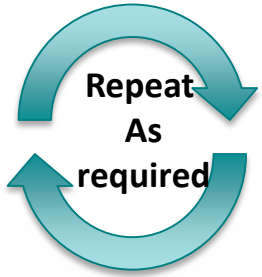
- Ensure **Confidentiality**, **Integrity**, Availability across remote industrial locations and countries, oh and **how do we secure an oil rig?**
- BYOD, M2M, IOT, Cloud?

Securing the enterprise meant starting from scratch. We needed an approach…

- **Key principles**
- **organisation boundaries**
- In **IT or Not**,
- **physical security**.

- **Strategic vision vs Tactical** –famous for & how to get there? Stop it getting worse, focus on quick fixes:
- **Link to the right Organisation**
  - Risk & Compliance
  - Architecture & Design and Assurance
  - Cyber Defence
  - Supported by program delivery

Understand **decision makers**
Use **business language**.
Business challenges.
'Press the flesh'
'**Visibility**' and awareness.



- <u>Stakeholder glue</u>.
- what you need & where:
- InfoSec Board is good, **Executive working group better**.
- **Risk Committee** is a must!

- Organisation - **Commitment** is key
- Get the **right people.**
- **Under promise** its always slower

Meet the right people, Listen & reflect, talk about the right things & Set out your stall early

Delivery is like trying to work out how to take a glass of water from a fire hydrant…. Constant pressure and volume..

We had to focus on tactical and strategic, from day 1.

Challenge: Not a quick fix. Manage the tactical & develop a strategic response
Deploying the basics are key

Establishing a "Baseline" that's applicable to both Tactical and Strategic

Develop a separate plan for tactical fixes, engage the delivery through the IT & business

Identify simple wins to get some traction & start to be visible

Where is the boarder between Tactical & Strategic?

What do you need to drive this?

Delivery needs the right people, structure, processes and then technology.

- Focus on PEOPLE, not technology
- Strong sponsorship, mandate
- Right structure
- Rely on IT, but be impartial

Be able to act as the “Brakes” in the car…

Every journey starts with a single step, getting beyond the tactical needs a map …

VISION

STRATEGIC OBJECTIVES

ENABLERS + KEY INITIATIVES

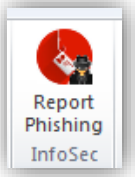
What did we do and how did we start?

Finding business risk & accepting business risk

Establishing our baseline with RED team approach

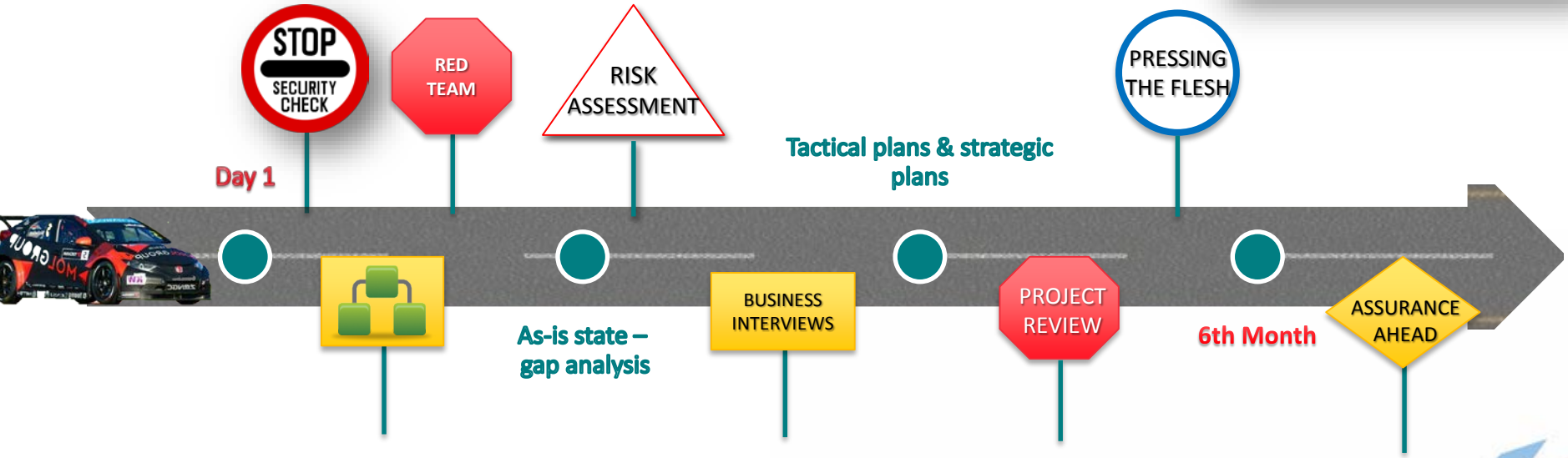
Enable business to excel – where we need urgent development

Developing a real understanding of the InfoSec posture of the organisation



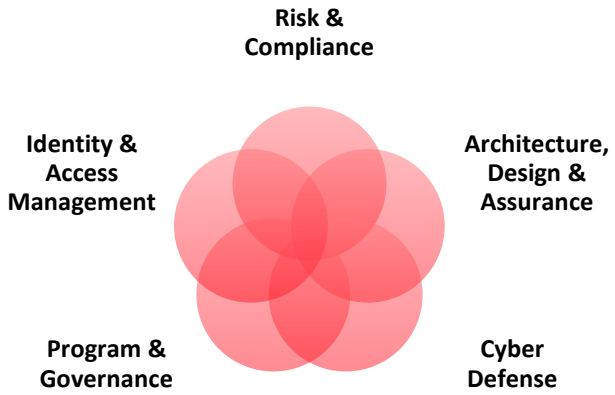
Develop awareness e.g. phishing button, Finance Exec presentation, "shock tactics"?

Delivery roadmap!



Whilst we attempted to contain the tactical we need to focus on “what’s next”… What about Risk management??

A Structured approach



With the right domains

- Detection and Response
- Network Security
- Endpoint Security
- Data Center and Server Security
- Awareness, Assurance and Governance
- Data Security
- Identity and Access Security

Tackling Risk and driving Awareness

- You can **start awareness** quickly, at Exec level, in IT, etc.
- **Develop Fact based cyber risk**, structure risk with the business, in business language.
- **Quantify the potential impact** in with other risks in a structured risk framework.
- **Fear works once, facts every time**, understanding business implications is key, especially when you are cost not profit.

Use RISK to establish the potential exposure and as a tool for awareness.

People and Awareness

- Awareness is cheap & effective
- Key topics:
  - Separation business and personal P455w0Rd$
  - SPAM & Phishing
  - Sensitive data handling
  - Encryption

Summary

- Summary lessons I have learned:
  - **All about PEOPLE**, right org. & aligned business strategy.
  - Position the strategy properly, don't overcommit, focus on tactical & strategic
  - Technology – final consideration, not final importance
  - Visibility – **talk the business language** – not IT, not InfoSec

It's all about people & communication and expect the unexpected….

Learnings 6 months in.. Things to think about

Next week you could ask yourself:

- Take a look at your InfoSec strategy, does it tie to the right things? (Risk? Compliance? Regulation? Technology?)
- Make sure the business understand your strategy?
- Have you got the right people? Is the organization structure still meeting your needs?
- How can I articulate the cyber risks, and are you at the right table, to discuss the risks the and the InfoSec posture?
- Is my architecture, design & assurance healthy and doing what it needs to?
- Where is my cyber defense today is it the right mix of technology, people & processes?
- How complete are your processes? (and can you measure success?)

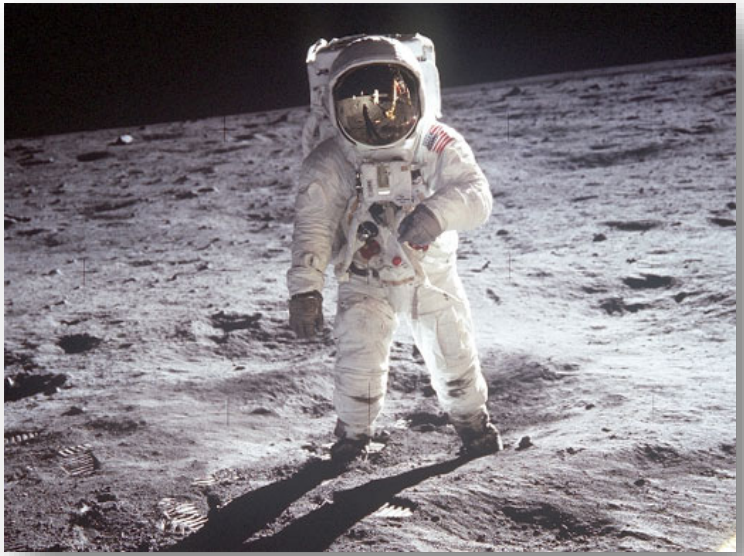
Looking forward – where to go from here!

In the next three months following this presentation you could:

- Have a regular discussion with Business Leaders about the challenges found and seen from InfoSec perspective
- Debate the ‘value add’ components of InfoSec – not efficiency per se, but effectiveness
- Schedule regular meetings with Business units – if you are not at the table you wont have a conversation...

Within six months you could:

- Review that you have the right people at the right places, doing the right things (and retain them!)
- If you haven’t already you should ensure Cyber Risk is in your enterprise risk *structure* and regularly update your leaders on the changing landscape inside and out
- Update your ‘crown jewels’ inventory and apply processes to ensure this is core to your business..
- Review your strategic roadmap and vision, is it relevant? What is changing? How



It’s all about right people with the right mentality