Managing cyber risk in JVs
stronger together

COPEX Conference 20th of October 2022

Bas Koch & Luuk Schrandt
Manager Cyber Consultancy Service NOV & Risk & Control Manager

Definitions & cautionary note

Cautionary note

The companies in which Shell plc directly and indirectly owns investments are separate legal entities. In this presentation "Shell", "Shell Group" and "Group" are sometimes used for convenience where references are made to Shell plc and its subsidiaries in general. Likewise, the words "we", "us" and "our" are also used to refer to Shell plc and its subsidiaries in general or to those who work for them. These terms are also used where no useful purpose is served by identifying the particular entity or entities. ''Subsidiaries'', "Shell subsidiaries" and "Shell companies" as used in this presentation refer to entities over which Shell plc either directly or indirectly has control. Entities and unincorporated arrangements over which Shell has joint control are generally referred to as "joint ventures" and "joint operations", respectively. "Joint ventures" and "joint operations" are collectively referred to as "joint arrangements". Entities over which Shell has significant influence but neither control nor joint control are referred to as "associates". The term "Shell interest" is used for convenience to indicate the direct and/or indirect ownership interest held by Shell in an entity or unincorporated joint arrangement, after exclusion of all third-party interest.

Forward-Looking Statements

This presentation contains forward-looking statements (within the meaning of the U.S. Private Securities Litigation Reform Act of 1995) concerning the financial condition, results of operations and businesses of Shell. All statements other than statements of historical fact are, or may be deemed to be, forward-looking statements. Forward-looking statements are statements of future expectations that are based on management's current expectations and assumptions and involve known and unknown risks and uncertainties that could cause actual results, performance or events to differ materially from those expressed or implied in these statements. Forward-looking statements include, among other things, statements concerning the potential exposure of Shell to market risks and statements expressing management's expectations, beliefs, estimates, forecasts, projections and assumptions. These forward-looking statements are identified by their use of terms and phrases such as "aim", "ambition", ''anticipate'', ''believe'', ''could'', ''estimate'', ''expect'', ''goals'', ''intend'', ''may'', "milestones", ''objectives'', ''outlook'', ''plan'', ''probably'', ''project'', ''risks'', "schedule", ''seek'', ''should'', ''target'', ''will'' and similar terms and phrases. There are a number of factors that could affect the future operations of Shell and could cause those results to differ materially from those expressed in the forward-looking statements included in this presentation, including (without limitation): (a) price fluctuations in crude oil and natural gas; (b) changes in demand for Shell's products; (c) currency fluctuations; (d) drilling and production results; (e) reserves estimates; (f) loss of market share and industry competition; (g) environmental and physical risks; (h) risks associated with the identification of suitable potential acquisition properties and targets, and successful negotiation and completion of such transactions; (i) the risk of doing business in developing countries and countries subject to international sanctions; (j) legislative, judicial, fiscal and regulatory developments including regulatory measures addressing climate change; (k) economic and financial market conditions in various countries and regions; (l) political risks, including the risks of expropriation and renegotiation of the terms of contracts with governmental entities, delays or advancements in the approval of projects and delays in the reimbursement for shared costs; (m) risks associated with the impact of pandemics, such as the COVID-19 (coronavirus) outbreak; and (n) changes in trading conditions. No assurance is provided that future dividend payments will match or exceed previous dividend payments. All forward-looking statements contained in this presentation are expressly qualified in their entirety by the cautionary statements contained or referred to in this section. Readers should not place undue reliance on forward-looking statements. Additional risk factors that may affect future results are contained in Shell plc's Form 20-F for the year ended December 31, 2021 (available at www.shell.com/investor and www.sec.gov). These risk factors also expressly qualify all forward-looking statements contained in this presentation and should be considered by the reader. Each forward-looking statement speaks only as of the date of this presentation, July 7 2022. Neither Shell plc nor any of its subsidiaries undertake any obligation to publicly update or revise any forward-looking statement as a result of new information, future events or other information. In light of these risks, results could differ materially from those stated, implied or inferred from the forward-looking statements contained in this presentation.

The contents of websites referred to in this presentation do not form part of this presentation.

We may have used certain terms, such as resources, in this presentation that the United States Securities and Exchange Commission (SEC) strictly prohibits us from including in our filings with the SEC. Investors are urged to consider closely the disclosure in our Form 20-F, File No 1-32575, available on the SEC website www.sec.gov.

6 ways employees can help to avoid phishing attacks

Remember! Phishing Awareness is a good start, but it is vital to make Phishing Reporting a habit.

THINK SECURE

KNOW THE COMMON TYPES OF ATTACKS

SPEAR PHISHING

Attackers send a tailored email to an individual or a group using personal details

VISHING

Attackers call you on your phone to trick you into revealing information

SMISHING

Attackers send text messages via SMS, WhatsApp etc. to trick you into clicking a link

WHALING

Attackers target Senior Executives with personalised phishing emails

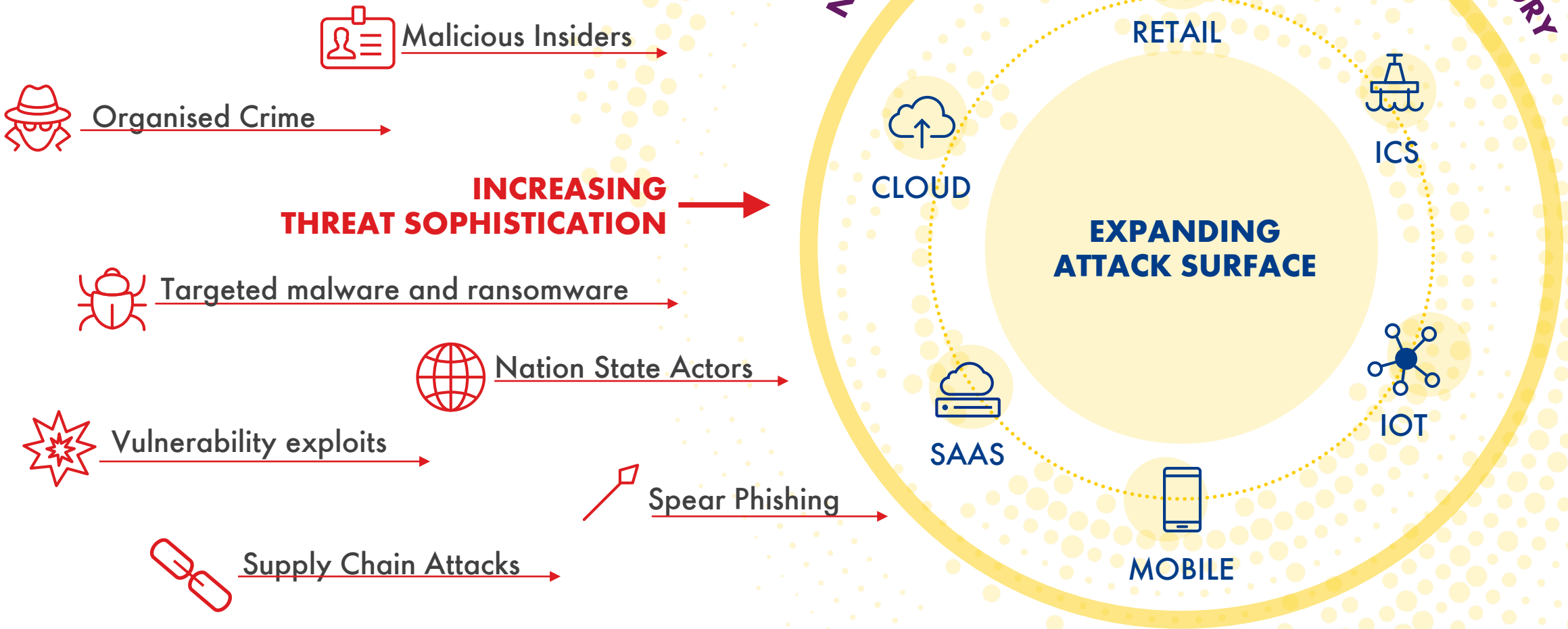
Managing cyber risk in JVs

Bas Koch
Manager Cyber Consultancy
Service NOV

Luuk Schrandt
JV Risk & Control Manager

Agenda

Changing threat landscape



Enterprise Impact

CNN BUSINESS

The Log4j security flaw could impact the entire internet.

link

BBC

Honda's global operations hit by cyber-attack

link

THE NEW YORKER

AFTER THE SOLARWINDS HACK, WE HAVE NO IDEA WHAT CYBER DANGERS WE FACE

link

Bloomberg

Marriott Shares Fall After Hit From Cyber Fine Crimps Earnings

link

ComputerWeekly.com

Data of thousands of Dutch citizens leaked from government Covid-19 systems

link

REUTERS

travel giant CWT pays $4.5 million ransom to cyber criminals

link

DIGITAL GUARDIAN

Tesla Data Theft Case Illustrates the Danger of the Insider Threat

link

The New York Times

Google Is Fined $57 Million Under Europe's Data Privacy Law

link

mortgagebusiness

LandMark White CEO resigns following data breach

link

Cyber Threats Recent Examples | 2021

Exchange Server

Microsoft Exchange e-mail server vulnerabilities were being exploited in-the-wild, giving attackers full access to user emails and passwords. ~250K organisations were affected, like the European Banking Authority, the Norwegian Parliament, and Chile's Commission for the Financial Market.

Codecov

The updating mechanism of the software testing and developing platform Codecov was manipulated. Sensitive data like customer tokens and credentials were exposed. Once customers updated the malicious Codecov version malware was installed at their network and data exfiltrated.

Colonial Pipeline

Threat actors linked to the DarkSide ransomware organization had gained access to an outdated VPN account. The compromise, leveraged to encrypt data on the company's systems, left Colonial's massive operational technology (OT) network, including a 5,500 mile pipeline, at risk of remote takeover.

PrintNightmare

Critical vulnerability for Windows systems whereby attackers could use a print spooler to remotely execute commands on IT devices. In Shell the patch for the vulnerability released by Microsoft was quickly applied to the relevant devices.

Fortinet

Threat actors published a list of hundreds of thousand Fortinet VPN login credentials from exploited devices in the past. This poses a major risk to organizations with weak or unchanged passwords as it gives threat actors an opportunity to gain a foothold.

Log4j

A vulnerability in a widely used logging library has become a full-blown security meltdown, affecting digital systems across the internet. Hackers are already attempting to exploit it, but even as fixes emerge, researchers warn that the flaw could have serious repercussions worldwide.

JAN — FEB — MAR — APR — MAY — JUN — JUL — AUG — SEP — OCT — NOV — DEC

Strategic Imperatives to manage the cyber landscape

To increase our security capability maturity and reduce the systemic risks Shell's Information Risk Management organization has identified eight strategic imperatives to strengthen cybersecurity capabilities.

Systemic Risks

- Evolving cyber threat landscape
- Risks in industrial control systems
- IT supply chain and 3rd party risks
- Geopolitical and national legal and regulatory pressure
- Reliance on legacy cyber access models
- Risks related to evolving business models

Strategic imperatives

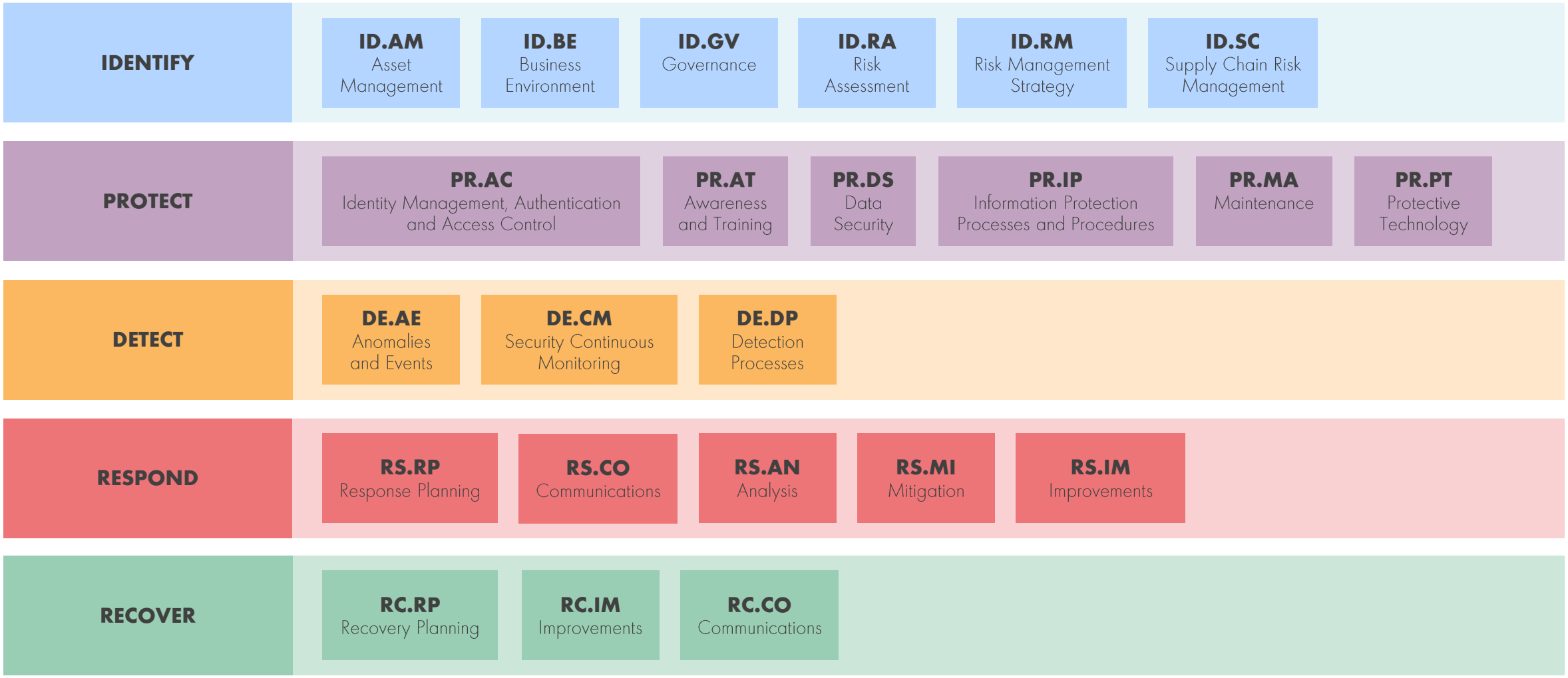
Imperatives reducing specific systemic risks

- Cyber Resilience
- Strengthen PCD
- Supply Chain, 3rd Parties & JV-NOVs
- Identity is key
- Next Generation IRM

Foundational imperatives addressing all systemic risks

- Brilliant Basics
- Zero Trust Unless
- Data Protection

The NIST Framework is an industry standard framework to manage cybersecurity risk. It consists of 5 functions and is based on a 'bow-tie' model



Fit-for-purpose cybersecurity services are offered

With the aim to protect business value the focus is on key services with strategic intent

Strategic	**Open-Source Intelligence (OSINT Scan)**		External perimeter scan assessing the company's digital footprint from a hacker's perspective
	Cyber Security Maturity Assessment		Extensive insight into the current maturity of the cybersecurity and IRM organization of the venture. Assessment is done against the industry standard NIST framework
	Target Cyber Maturity and Roadmap		Based on GAP between the current and target maturity, a comprehensive roadmap is defined to help ventures increase their maturity
	IT Control Framework Assessment		Formalized fit for purpose reviews of Design and Operating effectiveness of NOV IT Control framework
	Senior Management Awareness Workshop		Bring awareness to senior management on their role towards addressing cyber risk and the importance of IT to successfully execute on their business strategy
	CISO Bootcamp		A personalized training workshop to support CISO's in building their strategic plan
Specialist	**Penetration Testing**		Testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit
	Breach Assessment		Assessing past and/or current attacker activity in your network or systems
Best Practice & Community	**NOV Cybersecurity Forum**	F	Community of practitioners in the field of cyber security between Shell and the JV/NOV partners
	Phishing Campaign Service		Phishing simulation campaign service. NOVs/JVs can opt-into Shell's global service
	Think Secure	F	Best practice materials in support of any security awareness program. Content is generalized (no Shell logo's etc) and updated/shared on a quarterly basis
	Cyber Threat Advisory Reports	F	Threat intelligence report is provided on a quarterly basis. NOV/JV partners can sign up to receive it.
	Custom		Any request for which there is no predefined service can be taken into consideration

Conversations you can have in your business

How is your **leadership** creating a **security culture**?

Do you do the **cyber foundations** well?

How secure is your vendor and **supply-chain** ecosystem?

Are you buying technology from fewer and more **secure vendors**?

How do you know your **mission critical systems are secure**?

How would you **detect, investigate** and **recover** in the event of an **incident**?

Q&A