CREATING A SUSTAINABLE ENTERPRISE SECURITY ARCHITECTURE

INTRODUCTION

December 2020: Solarwinds Orion Code Compromise

January 2021: CHwapi hospital hit by Windows BitLocker encryption attack

March 2021: Microsoft Exchange Server Remote Code Execution Vulnerability

Continuous: It took more than 14 days to provide that contractor with the necessary access rights

How did it happen?

Do we use the affected solution/version in-house?
Do any of our third-party suppliers use the affected solution/version in-house?

What did the attacker do in our systems?
Do we detect suspicious activity or any of the indicators of compromise?

Who do I have to call to respond to the threat quickly?

By when can we easily get up and running again? In IT terms, this means rebuilding from scratch all hosts that are potentially infected.

How can we prevent this in the future?

INTRODUCTION

December 2020: Solarwinds Orion Code Compromise

~~Protect~~ | Identify | Detect | Respond | Recover

January 2021: CHwapi hospital hit by Windows BitLocker encryption attack

Protect | Identify | Detect | Respond | Recover

March 2021: Microsoft Exchange Server Remote Code Execution Vulnerability

~~Protect~~ | Identify | Detect | Respond | Recover

Continuous: It took more than 14 days to provide that contractor with the necessary access rights

Protect | Identify | ~~Detect~~ | ~~Respond~~ | ~~Recover~~

How did it happen?

Do we use the affected solution/version in-house?
Do any of our third-party suppliers use the affected solution/version in-house?

What did the attacker do in our systems?
Do we detect suspicious activity or any of the indicators of compromise?

Who do I have to call to respond to the threat quickly?

By when can we easily get up and running again? In IT terms, this means rebuilding from scratch all hosts that are potentially infected.

How can we prevent this in the future?

Do you have the necessary capabilities in house to structurally answer these business questions effectively and efficiently?

SPLYNTER

THE BUSINESS ENTERPRISE

IT DEPARTMENT SUPPORTING BUSINESS

KEEP THE BUSINESS RUNNING

- Complex landscape
- Rapid evolution of technologies
- Ruled by IT experts
- Legacy IT is a reality

"It's complicated"

SECURITY OFFICERS MANAGING INFORMATION RISK

KEEP THE BUSINESS SECURE

- Often busy with fire fighting
- Lack of experienced people
- Must cope with resistance
- Technology driven instead of business driven

SPLYNTER

THE BUSINESS ENTERPRISE

IT DEPARTMENT SUPPORTING BUSINESS

KEEP THE BUSINESS RUNNING

How can we better understand the IT landscape?

"It's complicated"

SECURITY OFFICERS MANAGING INFORMATION RISK

KEEP THE BUSINESS SECURE

How can we balance controlling risk and supporting IT?

SPLYNTER

THE BUSINESS ENTERPRISE

IT DEPARTMENT SUPPORTING BUSINESS

KEEP THE BUSINESS RUNNING

How can we better understand the IT landscape?

"Happily married"

SECURITY OFFICERS MANAGING INFORMATION RISK

KEEP THE BUSINESS SECURE

How can we balance controlling risk and supporting IT?

CREATING A SUSTAINABLE ENTERPRISE SECURITY ARCHITECTURE

SPLYNTER

CREATING A SUSTAINABLE ENTERPRISE SECURITY ARCHITECTURE

STEP 1	**ESTABLISHING THE CONTEXT** Define the enterprise information security requirements by understanding the internal and external drivers.
STEP 2	**ASSESSING INFORMATION SECURITY MATURITY** Assess the current maturity of the enterprise information security requirements.
STEP 3	**DEFINING TARGET INFORMATION SECURITY MATURITY** Decide on the roadmap towards a target information security maturity based on industry threats and enterprise risks.
STEP 4	**UNDERSTANDING THE BUSINESS AND IT SERVICE LANDSCAPE** Model the enterprise and translate the enterprise information security requirements to technology security requirements.
STEP 5	**INSTALLING THE INFORMATION SECURITY CAPABILITY** Install the information security capability to support the enterprise in realizing the technology security requirements.

CREATING A SUSTAINABLE ENTERPRISE SECURITY ARCHITECTURE

SPLYNTER

Step 1: establishing the context

Internal factors

Business strategy

Business objectives

Stakeholder's drivers (profit, growth, …)

Risk appetite

External factors

EU regulation (eIDAS, NIS, PSD2, GDPR, …)

Local regulation (usage of SSN, usage of biometrics, NBB BE, …)

Global industry standards (NIST 800-63, ISO27k, PCI DSS, …)

Cyber security frameworks (NIST CSF, …)

Non-regulatory (sector-specific)

Industry threats (ransomware, mobile fraud, …)

EXAMPLE:

***NIST 800-63B**: "Proof of possession and control of two distinct authentication factors is required through secure authentication protocol(s) to provide high confidence about a subject's identity (assurance level 2)."*

Enterprise information security standards

Enterprise information security policies

Enterprise information security standards

Enterprise information security guidelines

Enterprise information security procedures

Enterprise information security **requirements**

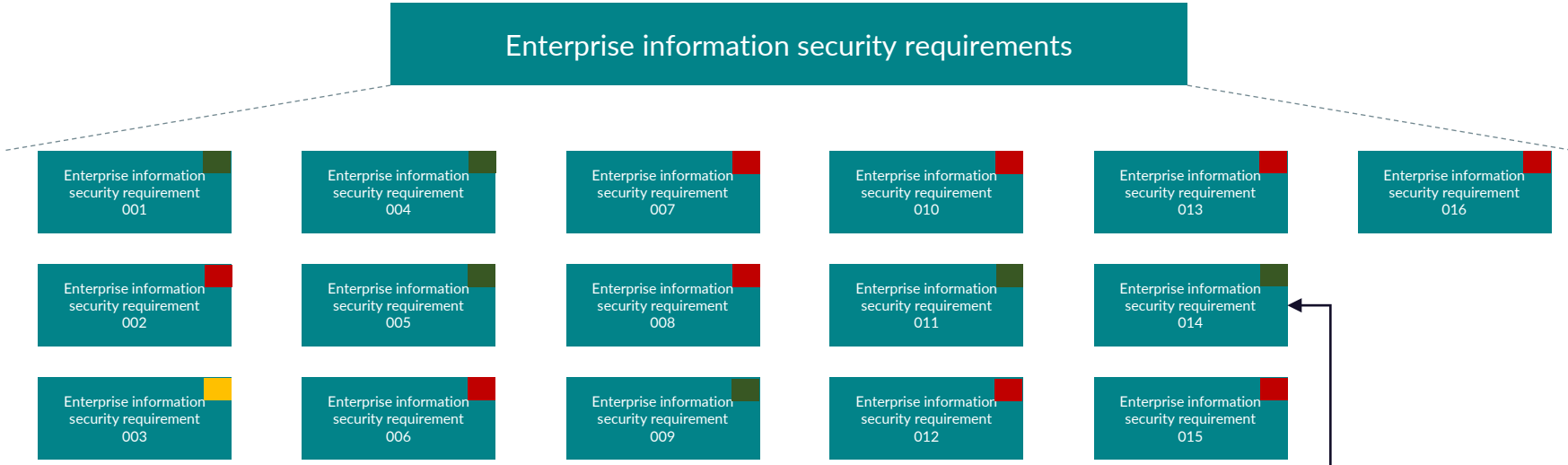
EXAMPLE:

***Requirement**: "Every customer-facing application that provides access to class 3 data must be secured with strong authentication guaranteeing a high level of assurance (≥ Authenticator Assurance Level 2)."*

CREATING A SUSTAINABLE ENTERPRISE SECURITY ARCHITECTURE

SPLYNTER

Step 2: assessing information security maturity



MATURITY ASSESSMENT TOOL

EXAMPLE

		# of applications complying	Align with international standards	Follow standardized patterns	Limit technical depth	Limit technology development)	Prefer to keep knowledge internal		Level of compliancy	Level of alignment with security principles	Grand total / exposure type	Grand total
Every customer-facing application that provides access to class 3 data must be secured with strong authentication guaranteeing a high level of assurance (≥ Authenticator Assurance Level 2).	customer facing	5	3	1	5	5	4		5,00	3,60	4,30	3,20
	employee facing	1	5	5	1	5	4		1,00	4,00	2,50	
	partner facing	3	3	1	1	5	3		3,00	2,60	2,80	

CREATING A SUSTAINABLE ENTERPRISE SECURITY ARCHITECTURE

SPLYNTER

Step 3: defining target information security maturity

Enterprise information security requirements

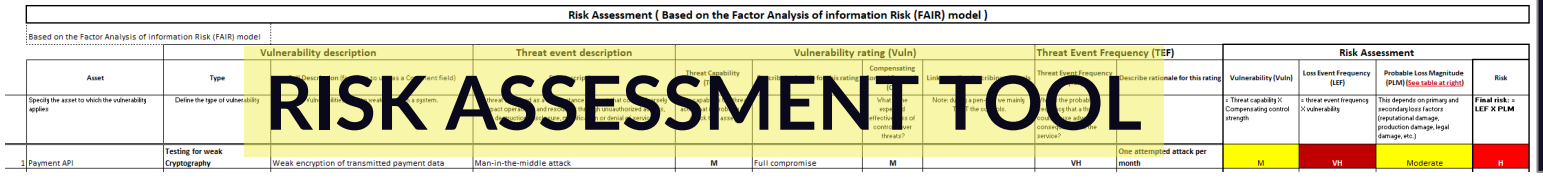
Level 1: Initial	Level 2: Compliance driven	Level 3: Risk-informed and repeatable	Level 4: Adaptive
Enterprise information security requirement 001	Enterprise information security requirement 002	Enterprise information security requirement 006	Enterprise information security requirement 007
Enterprise information security requirement 005	Enterprise information security requirement 004	Enterprise information security requirement 011	Enterprise information security requirement 008
Enterprise information security requirement 009	Enterprise information security requirement 010	Enterprise information security requirement 013	Enterprise information security requirement 012
Enterprise information security requirement 003		Enterprise information security requirement 014	Enterprise information security requirement 015
		Enterprise information security requirement 016	
TARGET Y	**TARGET Y+1**	**TARGET Y+2**	**TARGET Y+5**

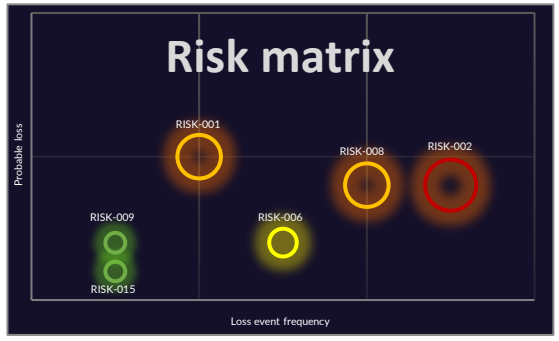
EXAMPLE:

Risk: *"Unauthorized disclosure of personal information due to weak access control mechanisms [leads to high monetary fines]"*

Decision*: "IAM enterprise information security requirements must be realized* ***within the year****"*

RISK ASSESSMENT TOOL

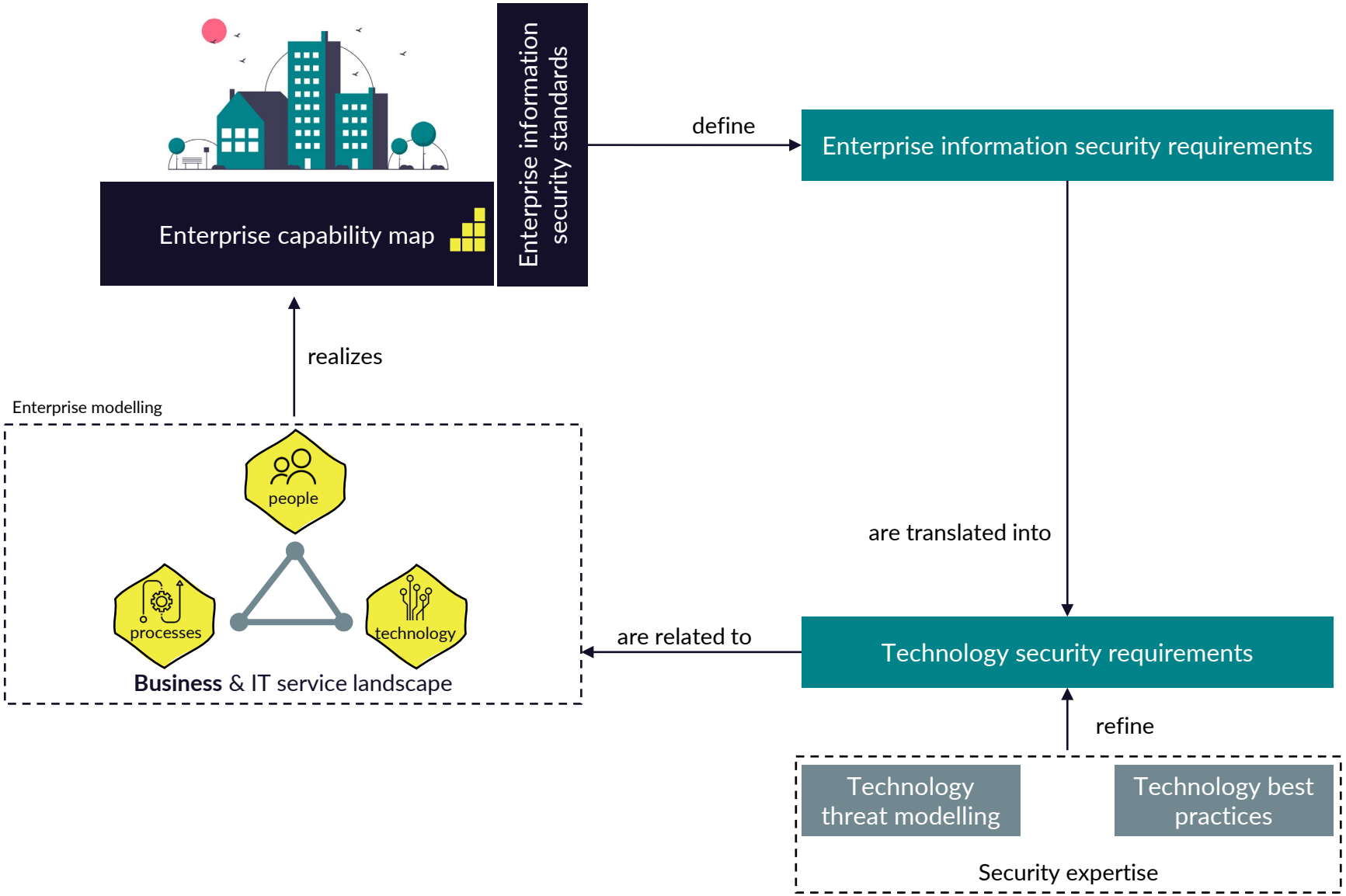




CREATING A SUSTAINABLE ENTERPRISE SECURITY ARCHITECTURE

SPLYNTER

Step 4: understanding the business and IT service landscape and defining the technology security requirements



CREATING A SUSTAINABLE ENTERPRISE SECURITY ARCHITECTURE

SPLYNTER

Step 5: installing the information security capability

Enterprise capability map

Enterprise information security standards

define

Enterprise information security requirements

realizes

Enterprise modelling

people

processes

technology

Business & IT service landscape

supports realizing security requirements

are translated into

are related to

Technology security requirements

refine

people

processes

technology

Identify

Detect

Protect

Respond

Recover

Information security capability

Technology threat modelling

Technology best practices

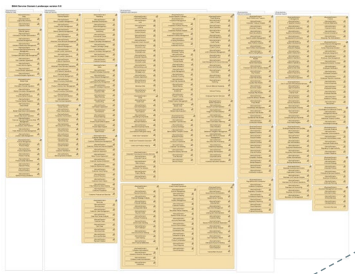
Security expertise

CREATING A SUSTAINABLE ENTERPRISE SECURITY ARCHITECTURE

SPLYNTER

EXAMPLE

EXAMPLE
***Capability map**: based on BIAN*



Enterprise capability map

Enterprise information security standards

define

EXAMPLE
***Requirement**: "Every customer-facing application that provides access to class 3 data must be secured with strong authentication guaranteeing a high level of assurance (≥ Authenticator Assurance Level 2)."*

Enterprise information security requirements

realizes

Enterprise modelling

people

processes

technology

Business & IT service landscape

supports realizing security requirements

are related to

are translated into

EXAMPLE
***Requirement**: "Customers must authenticate using the central cIAM system before being granted access to the mobile app."*

Technology security requirements

refine

Identify | Detect | Protect | Respond | Recover

people

processes

technology

Information security capability

EXAMPLE
***Capability**: cIAM*

Technology threat modelling

Technology best practices

Security expertise

We assist you executing your activities with confidence, helping you achieve your objectives in a risk-managed way.

Interested? Book an online call now.

SPLYNTER

Combatting your adversaries with structure.