WAVESTONE

Cyber-resilience: bend without breaking

Gérôme BILLOIS
gerome.billois@wavestone.com
(+33) 6 10 99 00 60

Cyber-resilience: 2 concrete public engagements with worldwide IS reconstruction

2017

SAINT-GOBAIN

Not Petya attack

- **Crisis period:** 3 weeks
- Up to **30 consultants** involved
- Steering of the worldwide cybersecurity remediation plan (2 years)

2019

altran

Ransomware

- **Crisis period:** 3 weeks
- Up to **17 consultants** involved

CERT-W run ~4 forensics per month…

What is somehow different in a cyber crisis?

A business crisis, not an IT one

The inverted pyramid: few experts, lot of work to do

Against you, a group of real people

A long term crisis (usually 2 to 3 weeks)

The need for forensics expertise

A strongly regulated topic (GDPR/business specific)

How can **attackers** impact your **resilience**?

Destroy information system
Cyber Warfare, (h)ac(k)tivism…

Corrupt internal system
Steal money, fraud, scams…

Steal data
Trade secrets, personal data…

CYBER-RESILIENCE

In case of a **major cyber-attack,** maintaining **vital activities** in downgraded mode while **regaining trust quickly** in your information system

Specify precisely your **main scenarios**

Precise in details, **adapted** to **context** and **considering** the latest attacks to define **efficient plan**

Massive **destruction** .... Massive **destruction of workstations** & **servers** following a **compromised AD**

Internal system **corruption** .... **Modify securities ownership** in the delivery & settlement process

Fraudulent payments on the payment settlement chain (CBM or commercial money)

Major data leakage .... **Major data leakage** of cash & securities positions

And Quantify the Risks: *What is the value at risk?*

QUANTIFY RISKS

What is the probability of being attacked and how much it will cost

INTERNATIONAL MONETARY FUND

FAIR INSTITUTE

Citalid

How should I do?

1

Assess your **protection level…** regarding to the selected scenarios

Then **improve** your **cybersecurity protection**

2

Build your **cyber-resilience**

a. Contain the attack

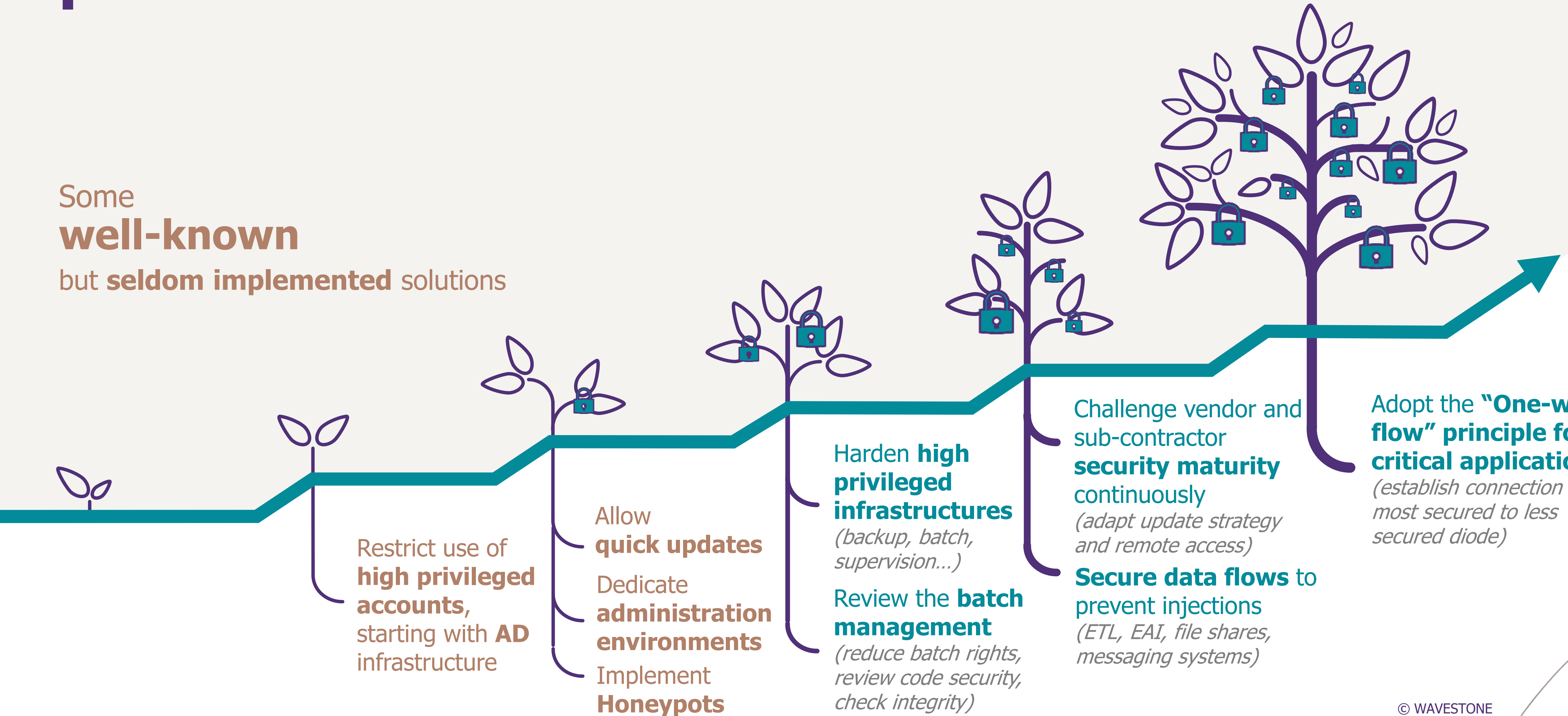
b. Work **without** IT

c. Reconstruction IT fast

1. Improve your cybersecurity **protection**

Some
well-known
but **seldom implemented** solutions

And some
less usual solutions.



Restrict use of **high privileged accounts**, starting with **AD** infrastructure

Allow **quick updates**

Dedicate **administration environments**

Implement **Honeypots**

Harden **high privileged infrastructures** *(backup, batch, supervision…)*

Review the **batch management** *(reduce batch rights, review code security, check integrity)*

Challenge vendor and sub-contractor **security maturity** continuously *(adapt update strategy and remote access)*

Secure data flows to prevent injections *(ETL, EAI, file shares, messaging systems)*

Adopt the **"One-way flow" principle for critical applications** *(establish connection from most secured to less secured diode)*

2a - **Contain** the attack

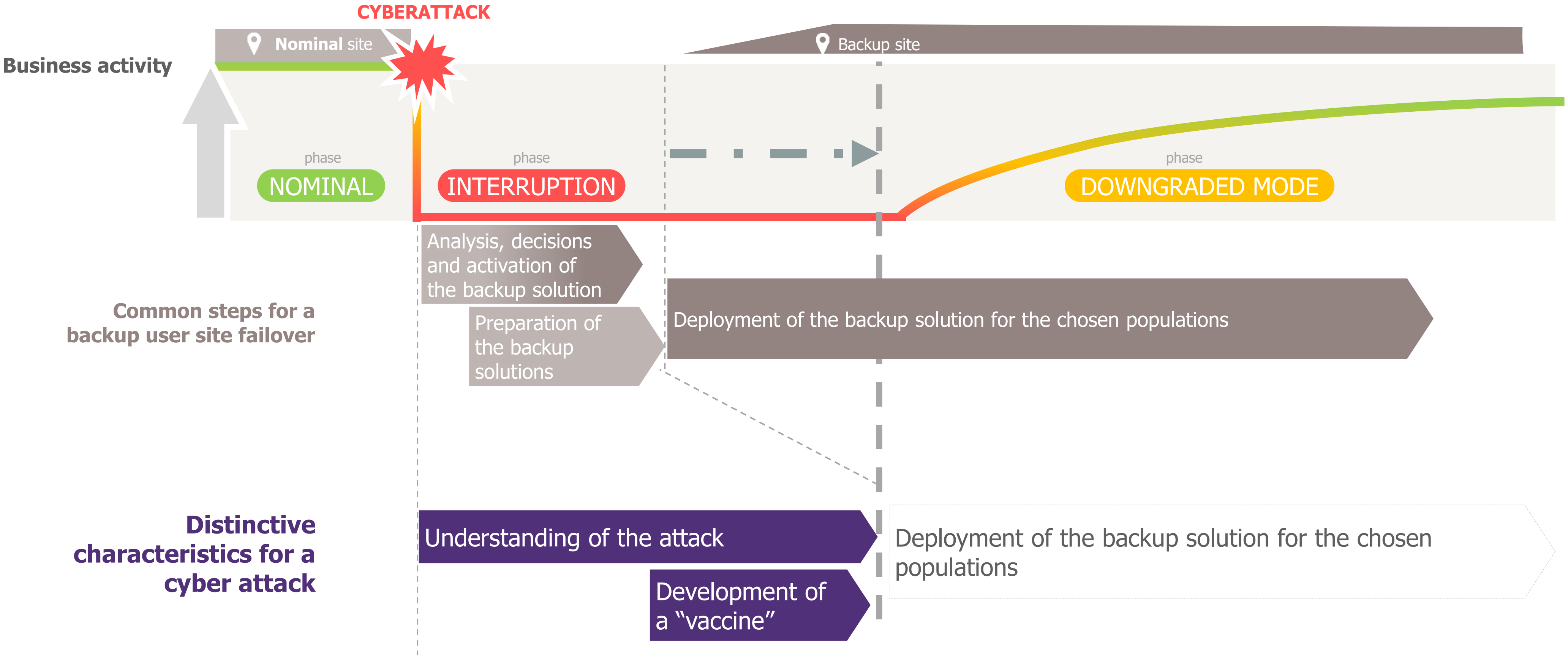
Arm yourself

- Have **forensic expertise** on hand
- Have sufficient, safe and searchable **logs**
- Have safe **crisis management tools**
- **Rethink** crisis **communication**
- Define **floodgates (Red Button) in your network**
- Strengthen **detection with business** processes knowledge (multi-level controls)
- Introduce **technological diversity** when appropriate
- Consider taking out **cyber-insurance**

Respond efficiently

- **Allow quick decisions** from operational teams for threat containment (floodgate activation, systems shutdown…) – *with management delegation of power*
- Be able to rally management, technical **experts**, continuity, HR and communications staff
- Be prepared for **24/7** operations (logistics/HR) over a long time and ensure **rotations**
- **Test** your cyber-crisis management using an ambitious and realistic situation

FOCUS | During a cyber attack, before rebuilding workstations/servers, it is required to understand the attack to develop a "vaccine"



CYBERATTACK

Nominal site

Backup site

Business activity

phase NOMINAL

phase INTERRUPTION

phase DOWNGRADED MODE

Common steps for a backup user site failover

- Analysis, decisions and activation of the backup solution
- Preparation of the backup solutions
- Deployment of the backup solution for the chosen populations

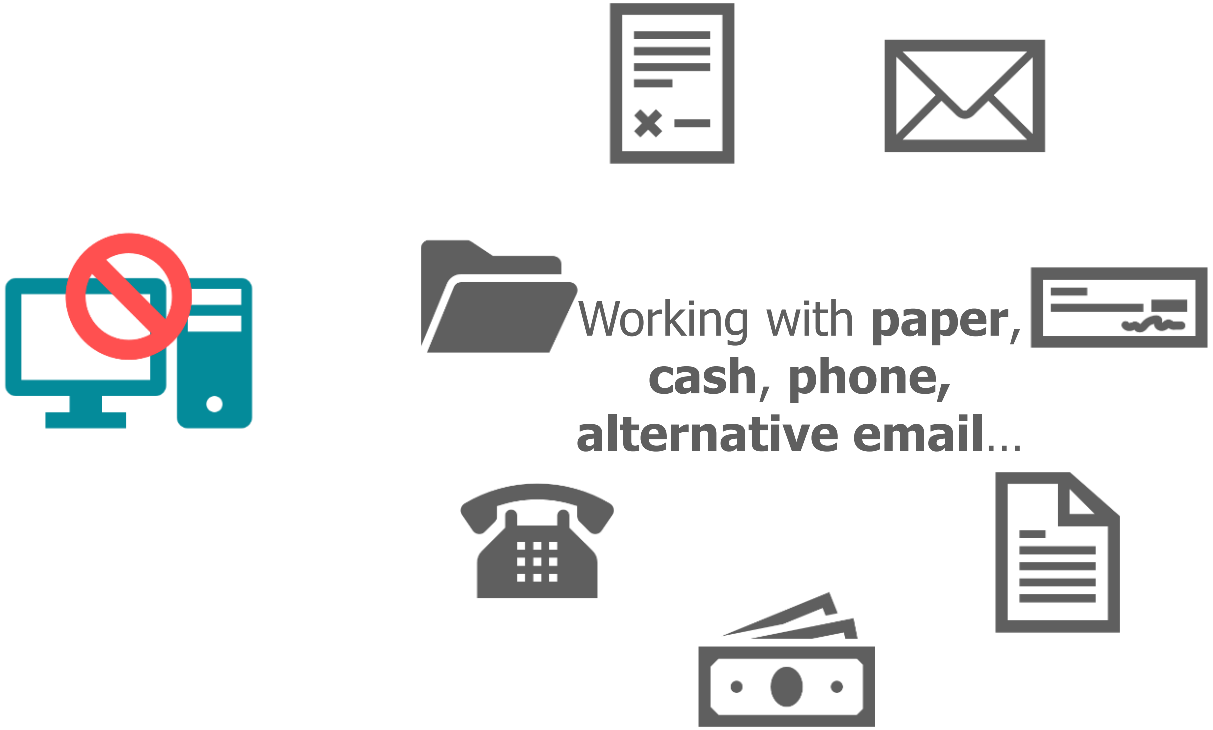
Distinctive characteristics for a cyber attack

- Understanding of the attack
- Development of a "vaccine"
- Deployment of the backup solution for the chosen populations

The time required to understand the attack and to develop the vaccine will delay the activation and deployment of the backup solution

2b. Learn to **work without IT** for a few days.

- Can I work with **manual workarounds?**
- If not, how do I a do **controlled business shutdown**?
- **Which data do I need**? (Clients contacts, contractors or suppliers lists, business data extractions…)
- **Which alternate tools do I need**? (phones, WhatsApp-likes, Gmail-likes, “light” desktop environments…)



Working with **paper**, **cash**, **phone**, **alternative email**…

The keys to fast **IS reconstruction**

ABILITY *TO* ***PARALLELISE***

Standardisation

Define global reconstruction solutions, the specificities are time-consuming!

Automatisation

Accelerate recovery and limit the need for human intervention

Simplicity

Ensure that it is not only experts who can carry out the operations

The keys to fast **IS reconstruction**

Can we **innovate?**

WORKSTATIONS

- / Ready-made **business packages** for workstations
- / **User self remastering** procedure with USB key: *Do It Yourself*
- / Deployed cloud based workstation
- / **Mobile** backup **server** to restore user’s data (drop-shipping)

APPLICATIONS & INFRASTUCTURES

- / **Orderly** applications reconstruction (business prioritization)
- / Ensure **backups and associated infrastructure** are **healthy**
- / **Standalone** mode for vital applications (internal or cloud-based)
- / Key Infrastructures **reconstruction plans** defined and tested
- / **Automated** infrastructure & application **deployment**
- / [High budget] Implement **non-similar facility**

Recovery Strategy

Three layers to consider in order
to **define** the **Recovery Strategy**

OS

Restore, Clean-up & Patch

or

Reinstall

Applications

Restore, Clean-up & Patch

or

Reinstall

Data

Restore, Clean-up

or

Recreate data

or

Accept the loss

Usually the malware is located in the OS part or sometime in Application part

We need to work together

Continuity

and cybersecurity teams must work

👍 *in* 👍

Businesses

must be onboarded

in cyber crisis management

Suppliers

must be considered

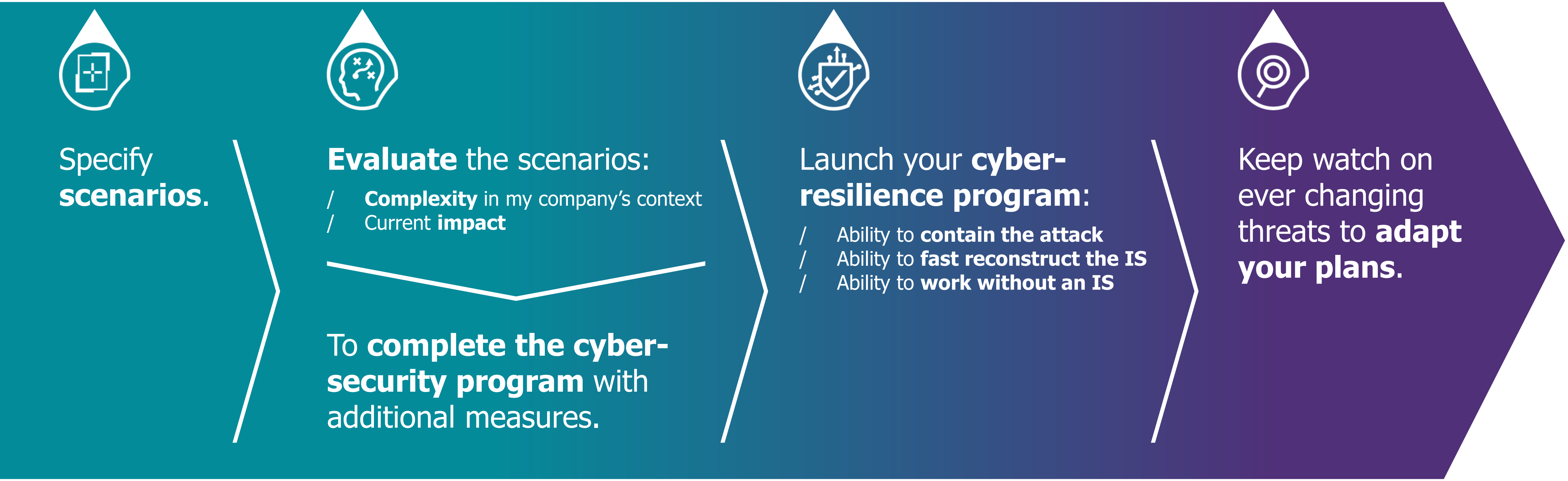
in your cyber-resilience strategy

Rundown:

The road **towards cyber-resilience**.

From completing your **cyber-security** program…

…to building your **cyber-resilience** program.



Specify **scenarios**.

Evaluate the scenarios:

/ **Complexity** in my company's context
/ Current **impact**

To **complete the cyber-security program** with additional measures.

Launch your **cyber-resilience program**:

/ Ability to **contain the attack**
/ Ability to **fast reconstruct the IS**
/ Ability to **work without an IS**

Keep watch on ever changing threats to **adapt your plans**.

WAVESTONE

RISKINSIGHT

LA LETTRE DES CONSULTANTS RISK MANAGEMENT
ET CYBERSÉCURITÉ DE WAVESTONE

CYBER-RESILIENCE

A NEW PILLAR OF CYBERSECURITY STRATEGY

SUMMARY

EDITORIAL

Summer 2017 has shown how global cyber attacks unfold in practice, especially with NotPetya. Although the full consequences of the "ransomworm" are still to be determined, Merck group already announced in late November 2017 that they expected the cyber attack to cost them more than 600 million dollars over the 2017 period!

Adding together the latest announcements, the 2 billion dollars threshold in lost revenues is clearly within reach. This is the first time such a high impact is measured following a cyber incident. This unprecedented escalation is rallying C-level executives who are looking for the means to limit the impacts of such attacks but also for the positions to adopt during an actual attack. We hope that the articles below will help you get a clearer view and plan the required actions.

Gérôme BILLOIS
Partner Cybersecurity & Digital Trust

WAVESTONE

Gérôme BILLOIS

gerome.billois@wavestone.com

@gbillois

@Risk_Insight

Credits Icons Thenounproject: Ben Davis, Anbileru Adaleru, Anil, Nikita Kozin, Rodrigo Ramirez, David Courey