RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

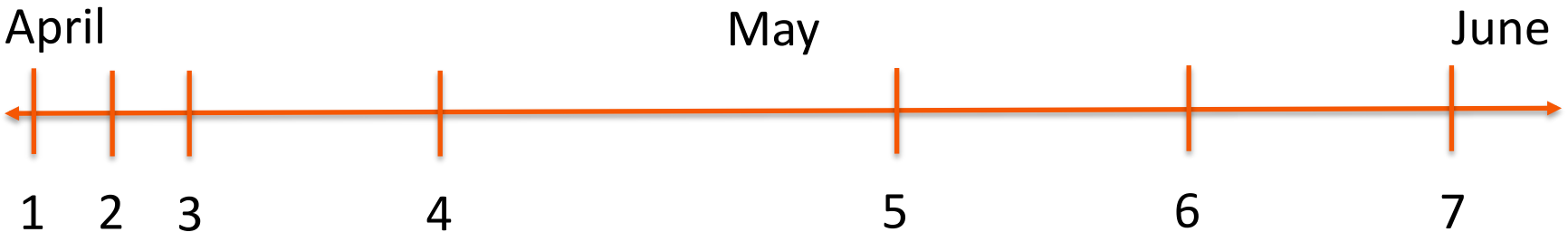
SESSION ID: CXO-W02

BEHIND THE SCENES OF A CYBER INCIDENT: AN APT PR & COMMUNICATIONS CASE STUDY

“WE’VE BEEN HACKED”

“Everyone, pretend to be normal”

PR Case Study: Duqu 2 as it happened

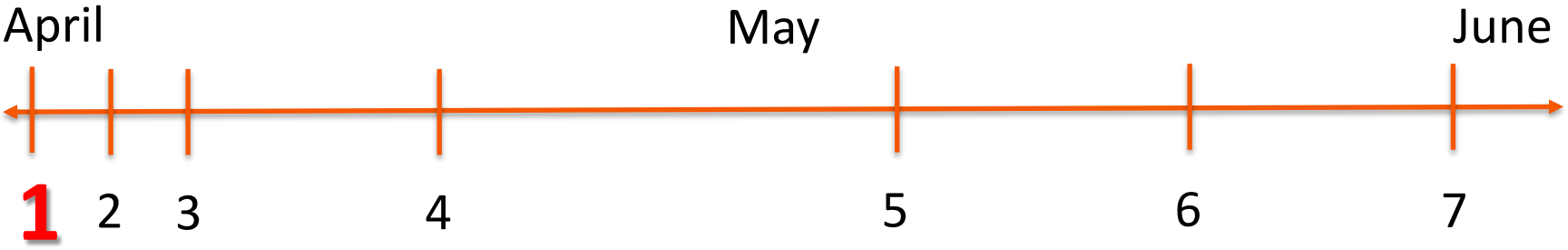


2015

Prelude: *"to disclose or not disclose, that is the question"*

Eugene Kaspersky: *"There is no question, disclose!"*

PR Case Study: Duqu 2 as it happened

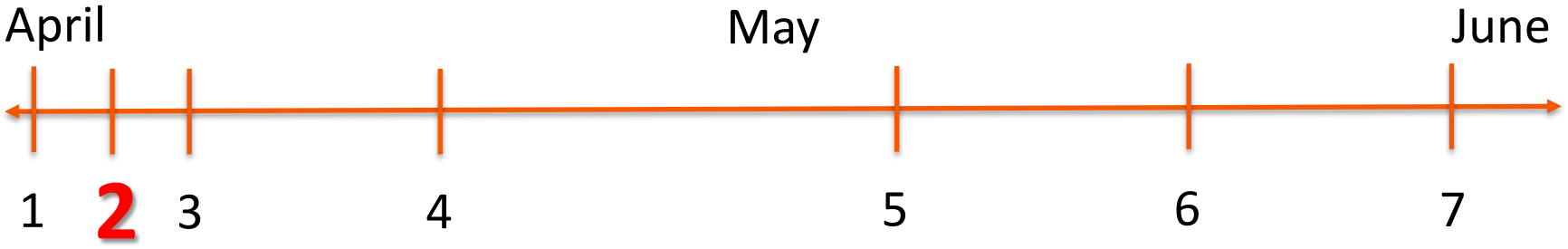


1. April 2015

The James Bond brief: “Everyone, pretend to be normal”

PR insight: PR is on the watch list

PR Case Study: Duqu 2 as it happened

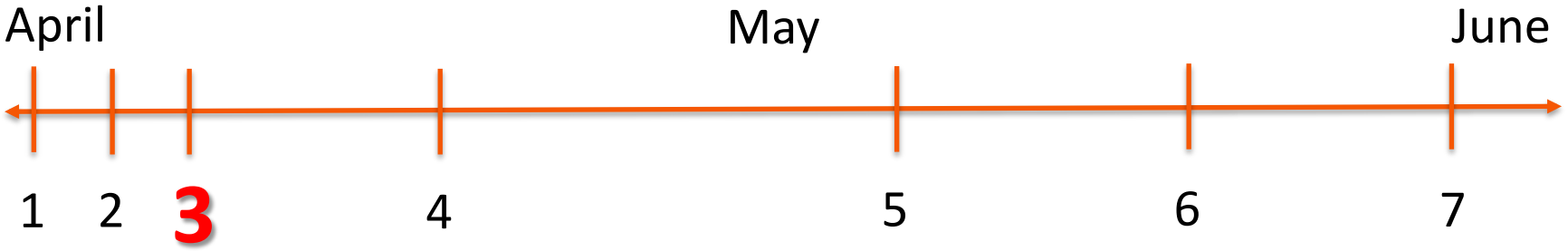


2. April 2015

CTO: No email, no phone, no VOIP, no SMS, no direct messengers, no mobile, no webcams…

PR insight: how do we communicate without communication tools?

PR Case Study: Duqu 2 as it happened

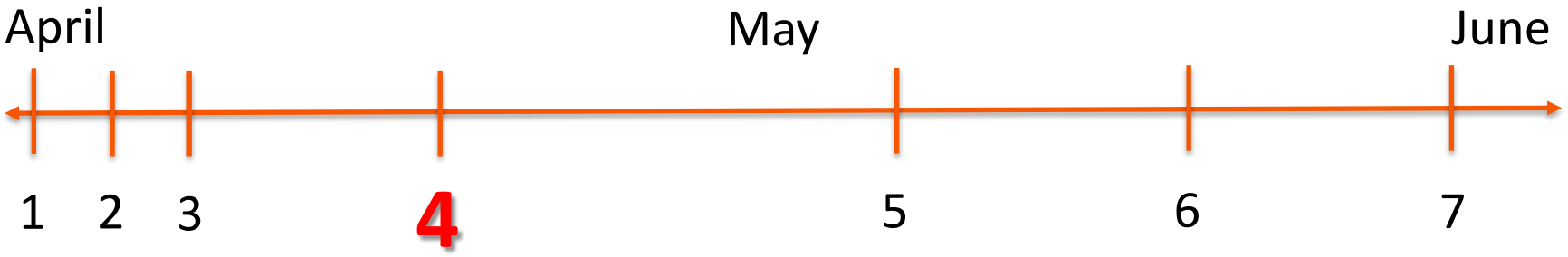


3. April 2015

GReAT: Silent Phone, Threema, PGP & “airgap” laptops

PR insight: Why? I never heard of these things before? IT approves?

PR Case Study: Duqu 2 as it happened

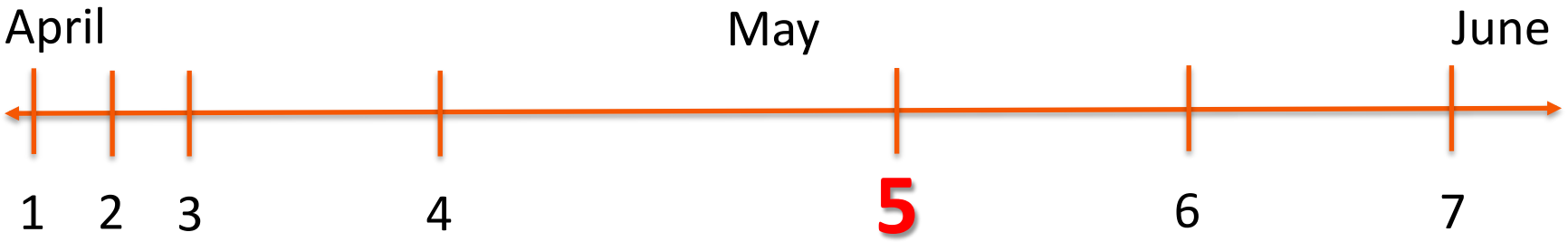


4. May 2015

Activity: Developing the PR assets, under cover…

PR insight: using the tools on the previous page, for the first time, in practice

PR Case Study: Duqu 2 as it happened

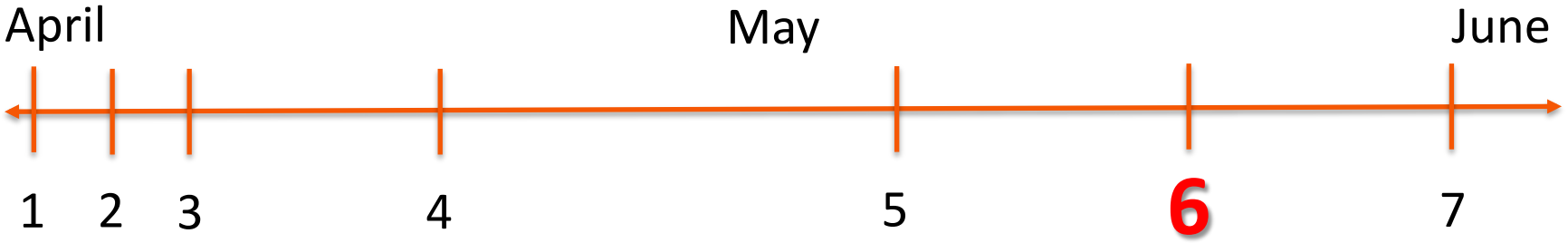


5. May 2015

Activity: Action plan development & involving external PR stakeholders

PR insight: PR Agencies & key journalists also need OpSec tools

PR Case Study: Duqu 2 as it happened

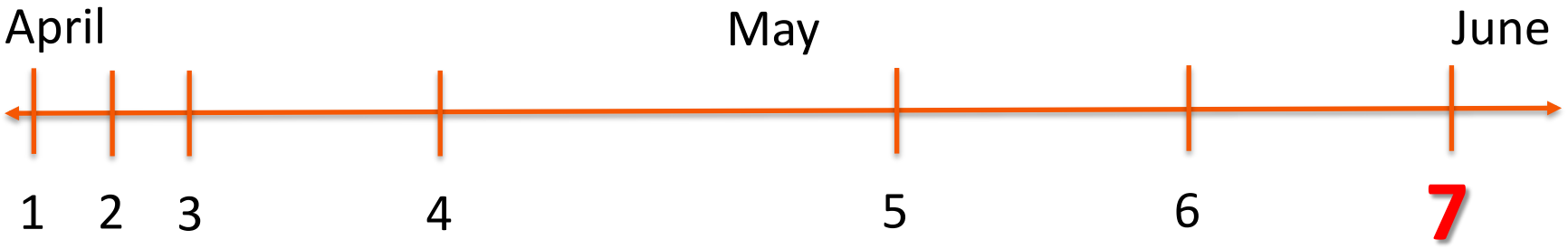


6. June 2015

Activity: Partner briefings, victim briefings & select media briefings

PR insight: Timing, simplification of message & staying calm

PR Case Study: Duqu 2 as it happened



7. June 2015

Announcement: Duqu 2 to the world & “proof of OpSec concept”

PR insight: James Bond style OpSec was worth it!

CYBER INCIDENT AFTERMATH: THREE KEY INSIGHTS

"…most likely, you're not ready"

Insight #1: PR OpSec is technology dependent

The new incident response standard for communicators is defined by high technical OpSec dependency, close collaboration between CISO and CCO (CorpComms) functions – and ongoing real-time updates to the corporate crisis communications manual.

Insight #2: PR needs incident classification too

A cyber incident PR classification can be downgraded, but never upgraded, and it needs to be aligned with the internal, technical incident classification system

Insight #3: CCO & CISO need synchronization

- *Agreeing on shared terminology*
- *Understanding all stakeholder audiences' role in the bigger picture*
- *Mitigating brand reputation is a shared responsibility*

THE AFTERMATH:
A NEW STANDARD

“CCO and CISO must stay connected happily ever after”

Solving the terminology gap: CISO & CCO Communications

CISO ⟷ **CCO**

Solving the terminology gap: CISO & CCO Communications

CISO ⟷ **CCO**

ROOTKIT

PHISHING

DDOS

0-DAY

RANSOMWARE

APTs

SOCIAL ENGINEERING

Core of the challenge?
Disconnected internal stakeholders

Core of the challenge?
Disconnected internal stakeholders

CISO ⟷ **CCO**

- Technical jargon, details & accuracy

Core of the challenge?
Disconnected internal stakeholders

CISO ⟷ **CCO**

- Technical jargon, details & accuracy
- Would prefer to call everything "*a virus*"

Core of the challenge?
Disconnected internal stakeholders

CISO ⟷ **CCO**

- Technical jargon, details & accuracy
- Educated audiences, understands nuances

- Would prefer to call everything "*a virus*"

Core of the challenge?
Disconnected internal stakeholders

CISO ⟷ **CCO**

- Technical jargon, details & accuracy
- Educated audiences, understands nuances

- Would prefer to call everything "*a virus*"
- Most audiences would prefer if it was all "*a virus*"

Core of the challenge?
Disconnected internal stakeholders

CISO ⟷ CCO

- Technical jargon, details & accuracy
- Educated audiences, understands nuances
- Why does the CCO think everything is ”*a virus*”???

- Would prefer to call everything “*a virus*”
- Most audiences would prefer if it was all “*a virus*”

Core of the challenge?
Disconnected internal stakeholders

CISO ⟷ CCO

- Technical jargon, details & accuracy
- Educated audiences, understands nuances
- Why does the CCO think everything is ”*a virus*”???

- Would prefer to call everything “*a virus*”
- Most audiences would prefer if it was all “*a virus*”
- Why can’t the CISO just call it “*a virus*”???

Core of the challenge?
Disconnected internal stakeholders

CISO ⟷ Two-way communications ⟷ **CCO**

- Technical jargon, details & accuracy
- Educated audiences, understands nuances
- Why does the CCO think everything is *"a virus"*???

To properly manage advanced cyber incident communications, both sides need to **understand** each other & **continuously** work together **pragmatically**

- Would prefer to call everything *"a virus"*
- Most audiences would prefer if it was all *"a virus"*
- Why can't the CISO just call it *"a virus"*???

Three connected layers of cyber incident communications stakeholders

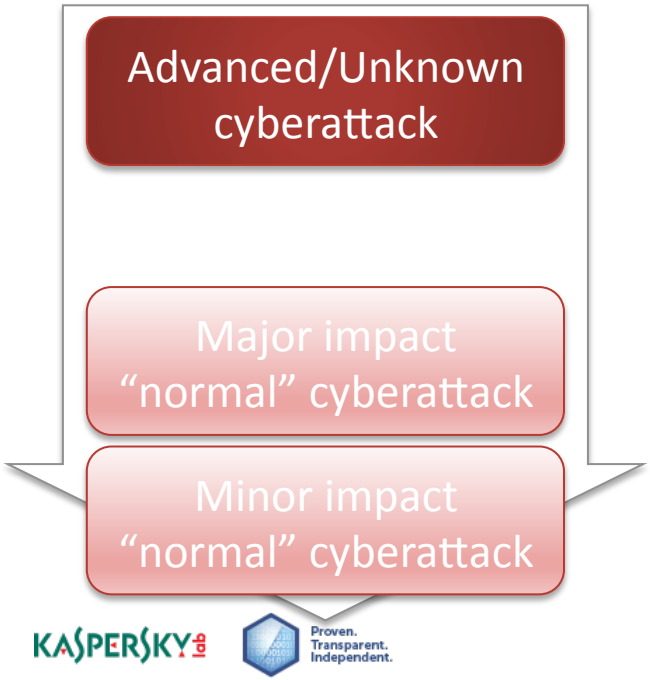
The new standard in cyber incident classification for professional communicators

Advanced/Unknown cyberattack

Major impact "normal" cyberattack

Minor impact "normal" cyberattack

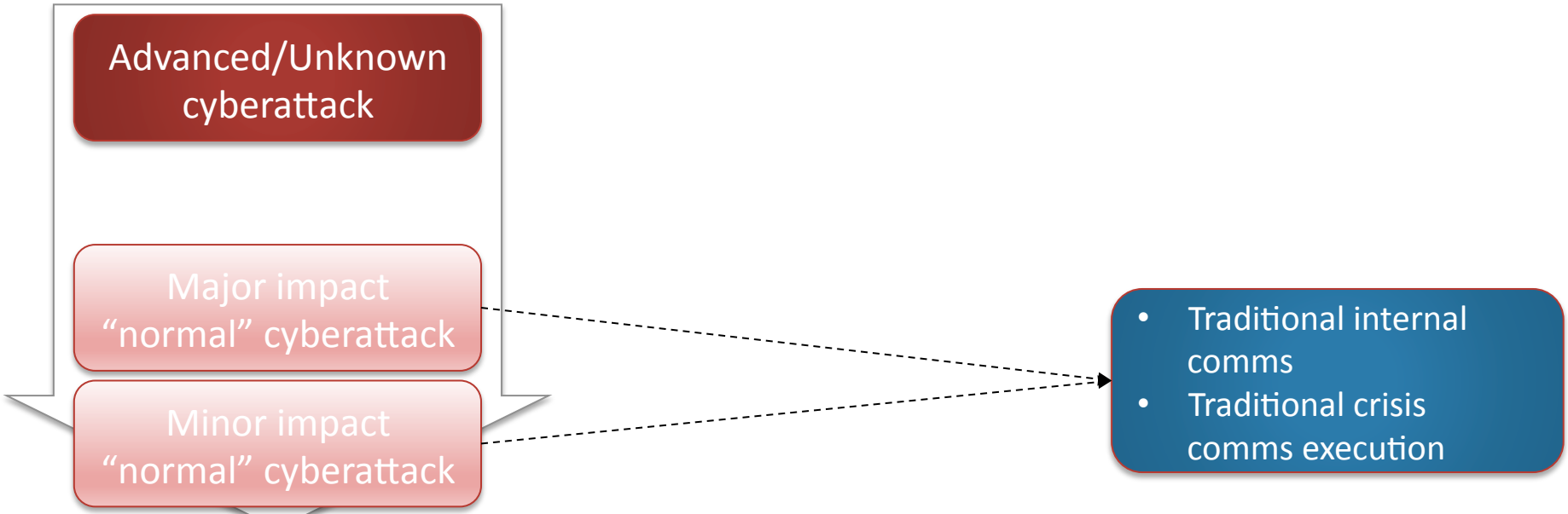
The new standard in cyber incident classification for professional communicators



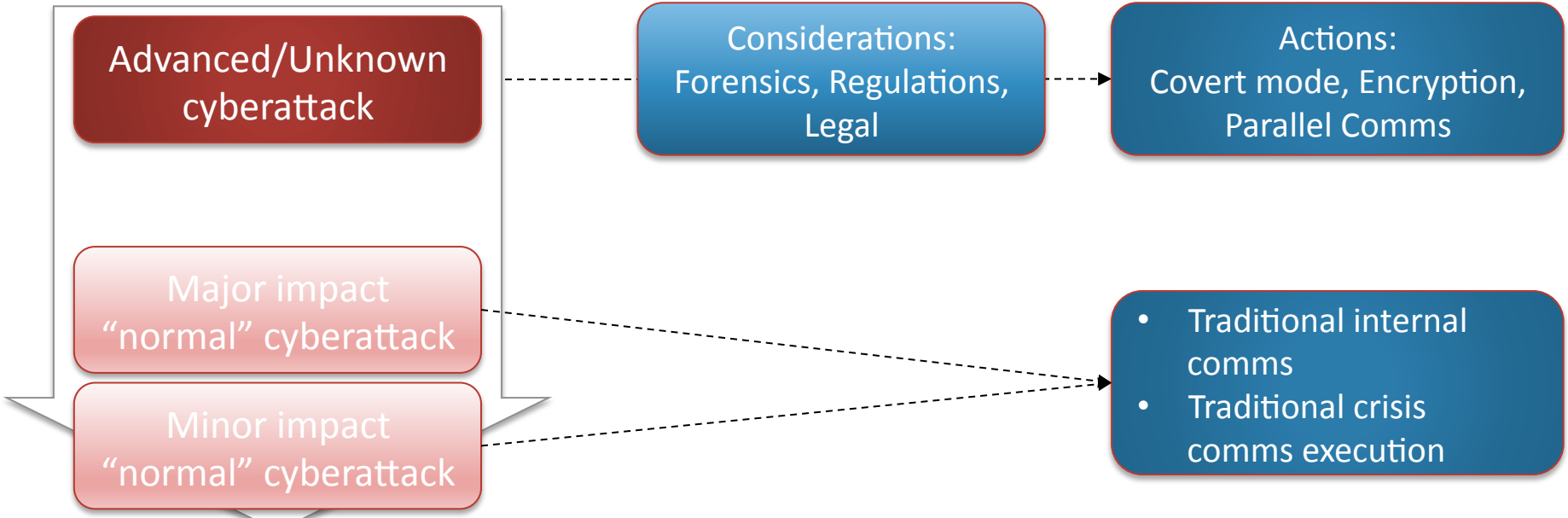
KASPERSKY lab

Proven. Transparent. Independent.

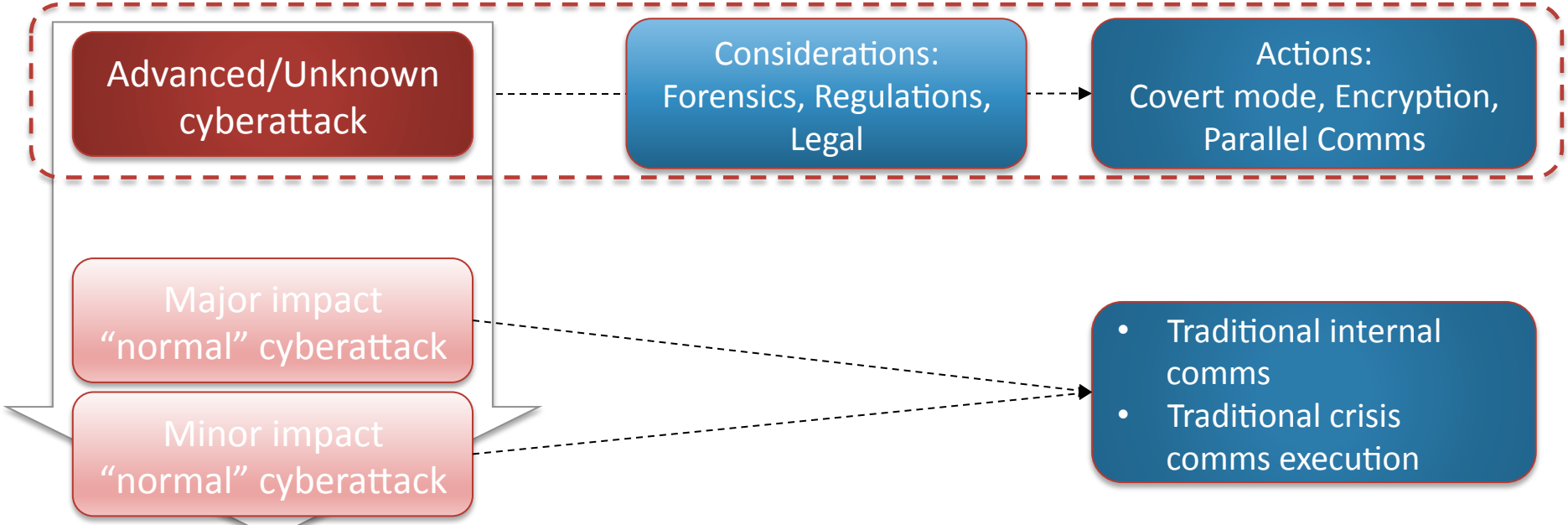
The new standard in cyber incident classification for professional communicators



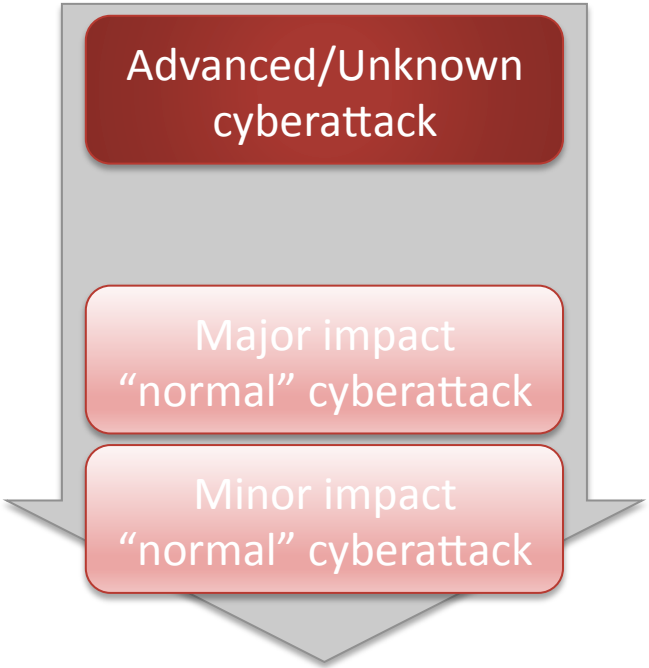
The new standard in cyber incident classification for professional communicators



The new standard in cyber incident classification for professional communicators



The new standard in cyber incident classification for professional communicators



"The one-way street"

Insight: communicators must understand the new modus operandi to manage **advanced/unknown** cyber incident communications

APPLYING THE NEW STANDARD

“Redefining and engaging with your reputational stakeholder map”

What you should do today

- CCO and CISO need to connect, and stay connected
- Stakeholder and technology audit – is **everyone** OpSec ready?
- Accept that this won't go away – and it's ever changing, just like cyber threats

THE SOLUTION: OPSEC TRAINING FOR PROFESSIONAL COMMUNICATORS

"Sharing what we learned benefits the industry collectively, we should all do the same"

Offer training that complements the technical cyber incident reputation solution

New industry standard

Current industry solutions

In-house Corporate Communications team:

- Generic crisis comms manual
- Crisis comms strategy
- Top level execution

External Communications Consultant:

- PR/Communications Agency
- Crisis comms training
- Mid/low level execution

Offer training that complements the technical cyber incident reputation solution

New industry standard

New training components:

- OpSec/Technical training workshop
- Insert for crisis comms manual
- Real-time cyber incident advice & updates for communicators

Current industry solutions

In-house Corporate Communications team:

- Generic crisis comms manual
- Crisis comms strategy
- Top level execution

External Communications Consultant:

- PR/Communications Agency
- Crisis comms training
- Mid/low level execution

Essential training components

- Offering training at different levels
  - **Basic:** educational / awareness keynotes for the PR industry
  - **Mid:** generic, practical training industry workshops
  - **Premium:** company specific training/workshop and ongoing cyber updates
- Real-time updates are essential (Telegram/Threema example)
- Cross-functional stakeholder involvement

Summary and final thoughts

- **Regulation** is giving companies less choice regarding disclosing incidents
- **Reputation** is the responsibility of the whole C-suite
- **Reputational damage** cost often exceeds the physical/IT damage cost

"Education and industry collaboration is key – together we're stronger"

THANK YOU!