# Cyber resilience in the financial systems

Ayse Zoodsma-Sungur,* 7 June 2018

DeNederlandscheBank
EUROSYSTEEM

* Views expressed are those by the presenter

# Agenda

**1. Introduction**

2. Cyber threat landscape

3. Cyber fundamentals and resilience

4. There is a new kid in town: Reducing the risk of wholesale payments fraud related to endpoint security

5. Conclusion

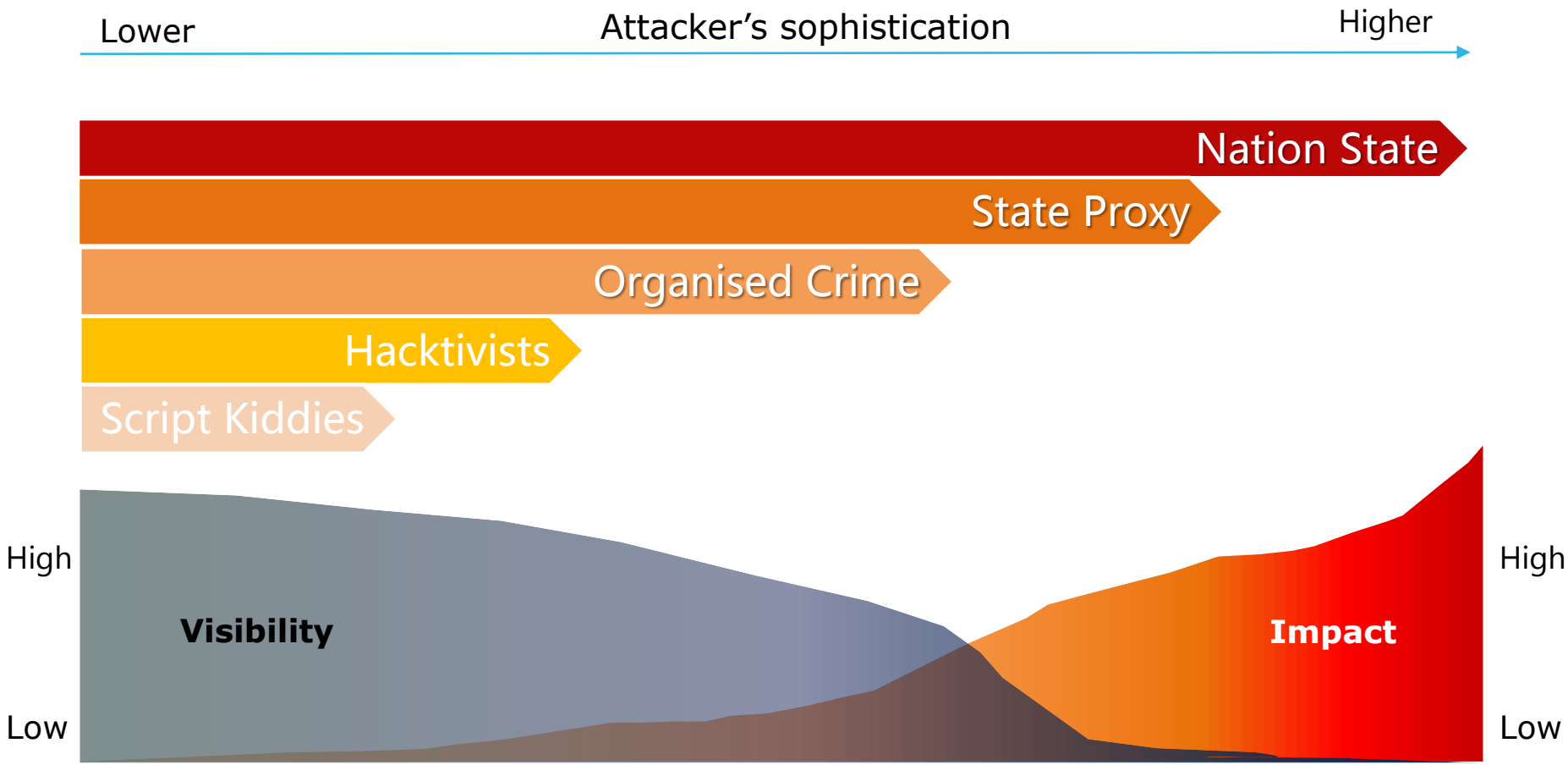
#Bonus material#

# 2. Cyber threat landscape

Threat levels rising


Moving upstream

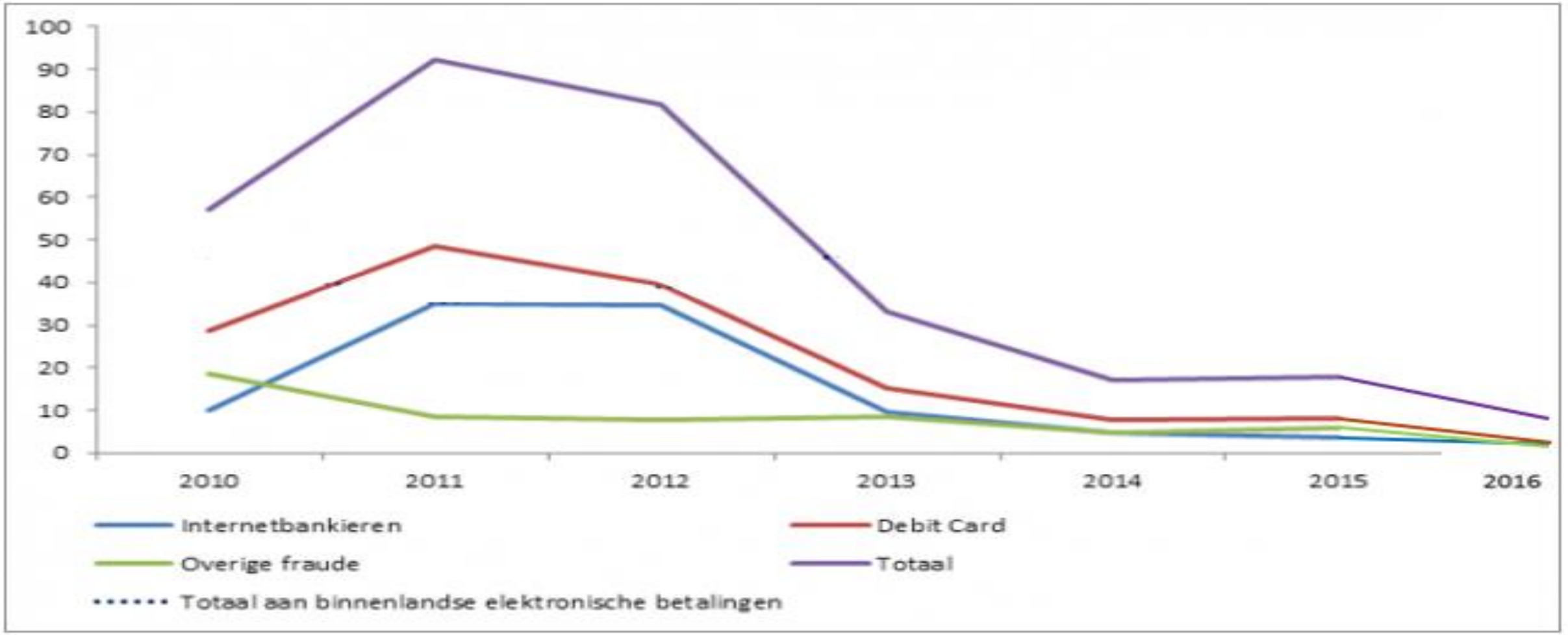
# 2. Cyber threat landscape




Source: DNB, July 2017


I KNOW
HOW TO
HACK INTO
YOUR SIGNS

# Fraud figures NL




Source: Payments Association Netherlands

# Nation states

# A little journey…

## 7. Pigeon camera, 1916–1917

The International Spy Museum

This German pigeon camera was used during World War I for reconnaissance of enemy positions. The camera was placed on a timer and the birds were set free to fly over the battleground. When they returned, the film was processed and the data was used in developing real-time combat strategies.

## 13. Steineck ABC wristwatch camera, circa 1949


*The International Spy Museum*

Developed in West Germany, this tiny camera was situated on an agent's wrist and was capable of snapping eight photos. Since the camera didn't come equipped with a viewfinder, framing a good shot was quite a difficult task.

## 14. Tessina camera and cigarette case concealment, 1960s

*The International Spy Museum*

What at first glance looks to be a fancy cigarette case was actually a hidden camera developed by the German Stasi during the 1960s. An operative was able to grab a real smoke and covertly snap pictures at the same time.

## 12. Shoe with heel transmitter, 1960s–1970s


*The International Spy Museum*

This shoe was stolen from a US diplomat by the Romanian Secret Service and outfitted with a hidden microphone and transmitter.

## 11. Hollow coin, 1950s–1990s


*The International Spy Museum*

Hollow coins are quite prevalent in espionage, offering clandestine storage for microdots and microfilm. The coin is opened by inserting a needle into a tiny hole on its face.

## 1. Buttonhole camera, model F-21, circa 1970


*The International Spy Museum*

Known by the codename "Ajax," this hidden camera was concealed within a regular coat and was widely used in the Soviet Union, Europe, and the US. The camera's trigger was held in the pocket and, when activated, would snap a picture from a lens that resembled a button.

Source: Buzzfeed.com, Top secret devices from the dangerous world of spies, 12 Feb 2017

## 2. Dog poop transmitter, circa 1970

*The International Spy Museum*

This hidden transmitter was disguised by the one thing nobody wants to touch: poop. This device was issued by the CIA during the 1970s and transmitted a radio signal to coordinate airstrikes and reconnaissance.

## 5. Tree stump listening device, early 1970s

*The International Spy Museum*

Designed by the CIA, this tree stump would be placed near a Soviet base and used to intercept secret radio transmissions. The data would be relayed back to the CIA via satellite.

*The International Spy Museum*

This ordinary-looking lipstick was designed and used by the KGB during the Cold War and was capable of firing a deadly .177-caliber round.

Take away:

‘Anything that can be used, will be used’

# … And is commercially available

amzn.to

Just in *case?*

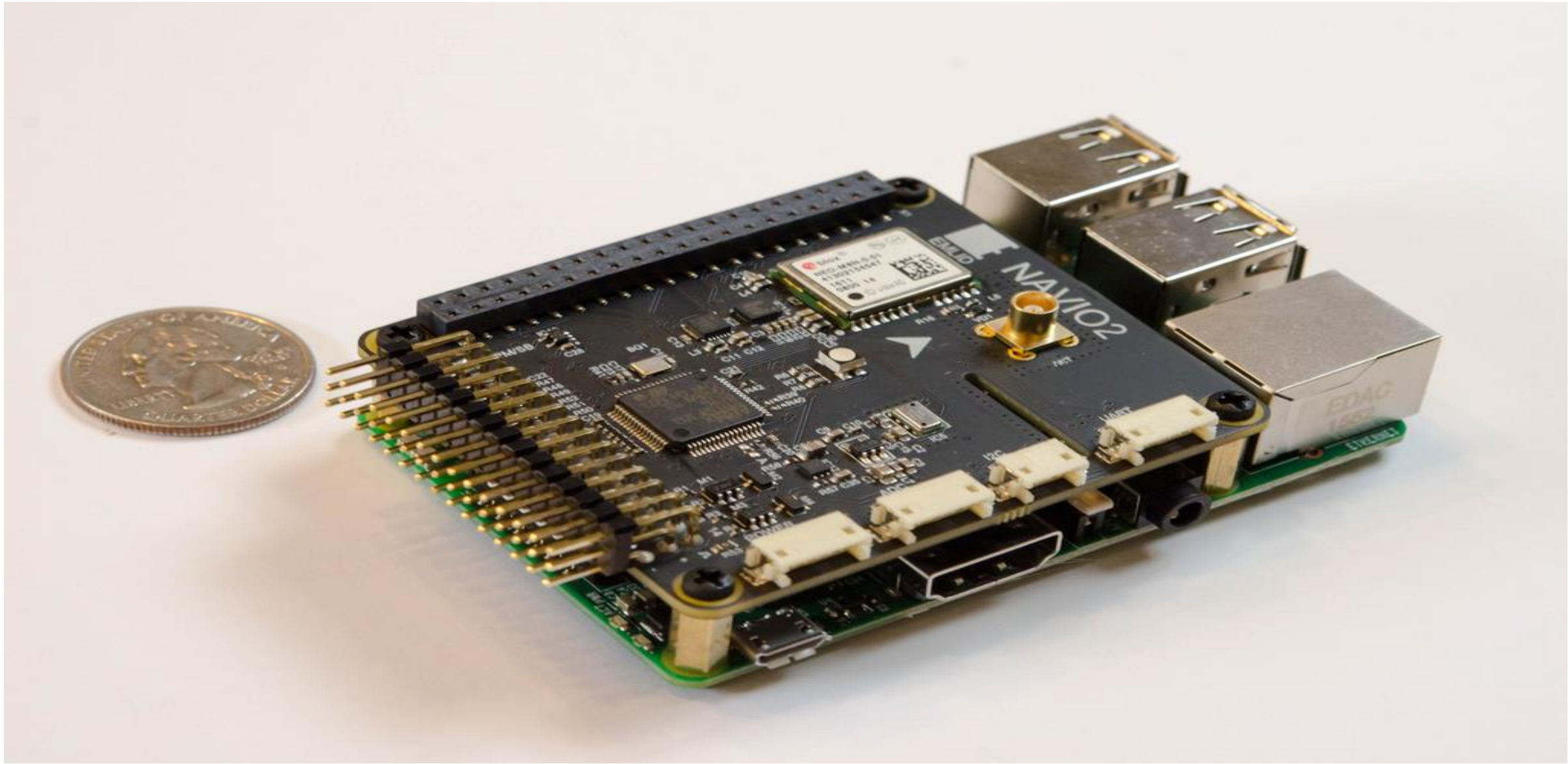
**Price:** $24 to $50

# At your service☺


amzn.to

Makes *cents*.

**Price:** $25


NAVIO2

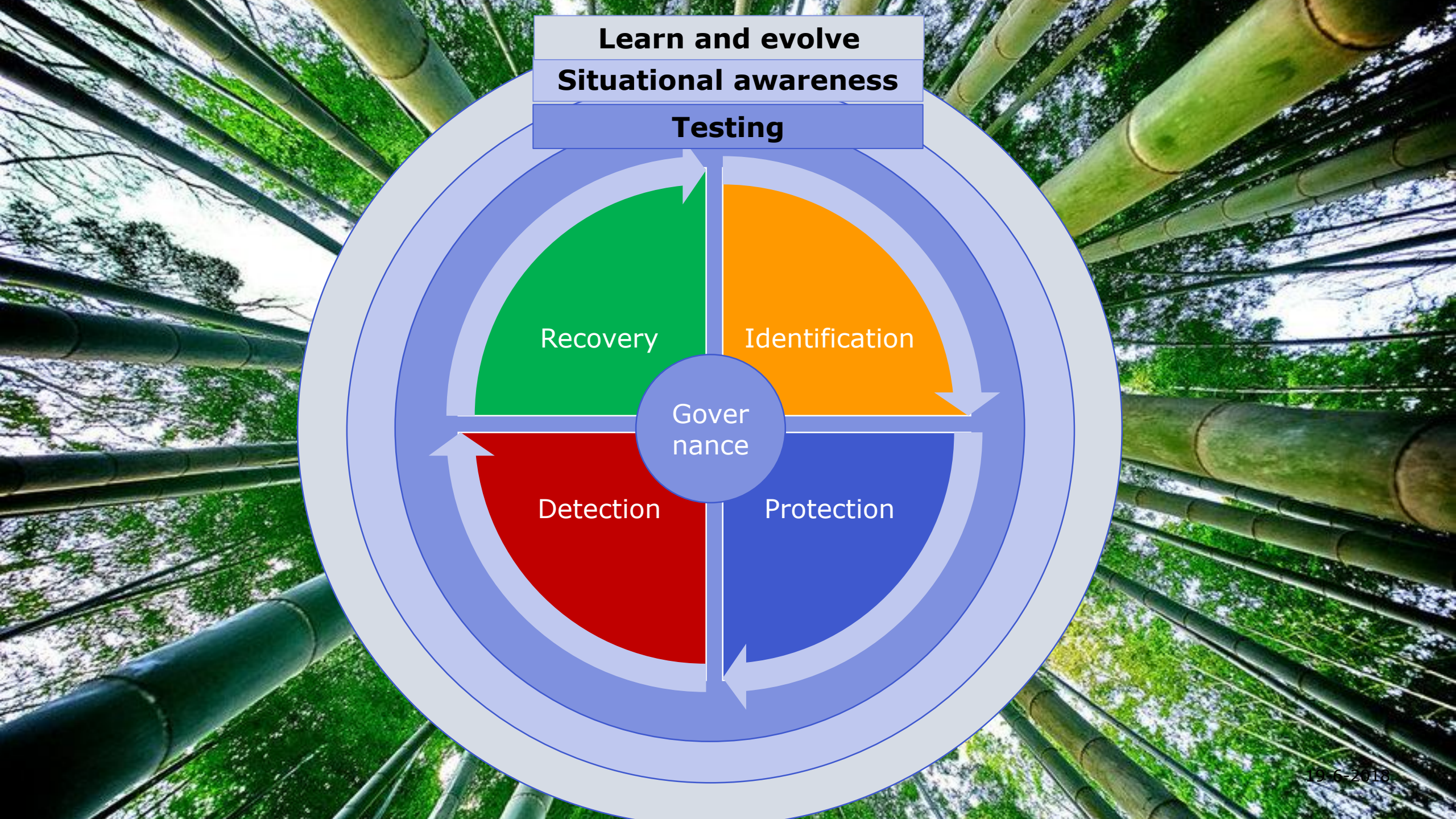
# Agenda

1. Introduction
2. Cyber threat landscape
3. **Cyber fundamentals and resilience**
4. There is a new kid in town: Reducing the risk of wholesale payments fraud related to endpoint security
5. Conclusion

# 3. Fundamentals

# 3. Fundamentals and resilience

# 3. Fundamentals and resilience


Learn and evolve
Situational awareness
Testing
Recovery
Identification
Gover
nance
Detection
Protection

# 3. Fundamentals and resilience

Key messages guidance:

1. Board and governance is critical
2. Understand the battlefield
3. Safe and quick resumption
4. Collective endeavour
5. Learn and evolve


# Agenda

1. Introduction

2. Cyber threat landscape

3. Cyber fundamentals and resilience

4. **There is a new kid in town: Reducing the risk of wholesale payments fraud related to endpoint security**

5. Conclusion

# There is a new kid in town: Reducing the risk of wholesale payments fraud related to endpoint security

CPMI developed a strategy to encourage and help focus industry efforts to reduce the risk of wholesale payments fraud related to endpoint security.

The strategy is composed of seven elements*:

designed to work holistically to address all areas relevant to preventing, detecting, responding to and communicating about fraud.

* #Bonus material#

# There is a new kid in town:

Benoît Cœuré - Chair, Committee on Payments and Market Infrastructures:

"The success of this plan depends on clear ownership and active engagement by all stakeholders, public and private sector alike".

# There is a new kid in town: Reducing the risk of wholesale payments fraud related to endpoint security

The strategy's primary aim is to encourage and help focus industry efforts to reduce the risk of wholesale payments fraud and, in doing so, support financial stability. T

This report discusses the wholesale payment ecosystem and endpoints, and the risk of wholesale payments fraud, stressing the need for a holistic approach and coordination It then presents the strategy, which comprises seven elements

.

# There is a new kid in town: Reducing the risk of wholesale payments fraud related to endpoint security

CPMI plans to promote, support and monitor local and global progress in operationalising the strategy with due recognition of the need for flexibility to reflect the uniqueness of each system and jurisdiction, including the:

- legal, regulatory,
- operational and technological structures,

and

- constraints under which they may operate

# Agenda

1. Introduction
2. Cyber threat landscape
3. Cyber fundamentals and resilience
4. There is a new kid in town: Reducing the risk of wholesale payments fraud related to endpoint security
5. **Conclusion**

# #Bonus material#

## Points for consideration for operationalising the strategy:

**Element 1 – Identify and understand the range of risks**
**Element 2 – Establish endpoint security requirements**

**Element 3 – Promote adherence**

**Element 4 – Provide and use information and tools to improve prevention and detection**

**Element 5 – Respond in a timely way to potential fraud**

**Element 6 – Support ongoing education, awareness and information-sharing**

**Element 7 – Learn, evolve and coordinate**

# Useful links

**CPMI-IOSCO guidance on cyber resilience for financial market infrastructures**
https://www.bis.org/cpmi/publ/d146.pdf


**Committee on Payments and Market Infrastructures (CPMI)**
**Reducing the risk of wholesale payments fraud related to endpoint security**
**May 2018**
https://www.bis.org/cpmi/publ/d178.htm