INFORMATION EXCHANGES EXPERIENCE:

THE GOOD, THE BAD, THE UGLY

Financial Sector Cyber resilience Workshop

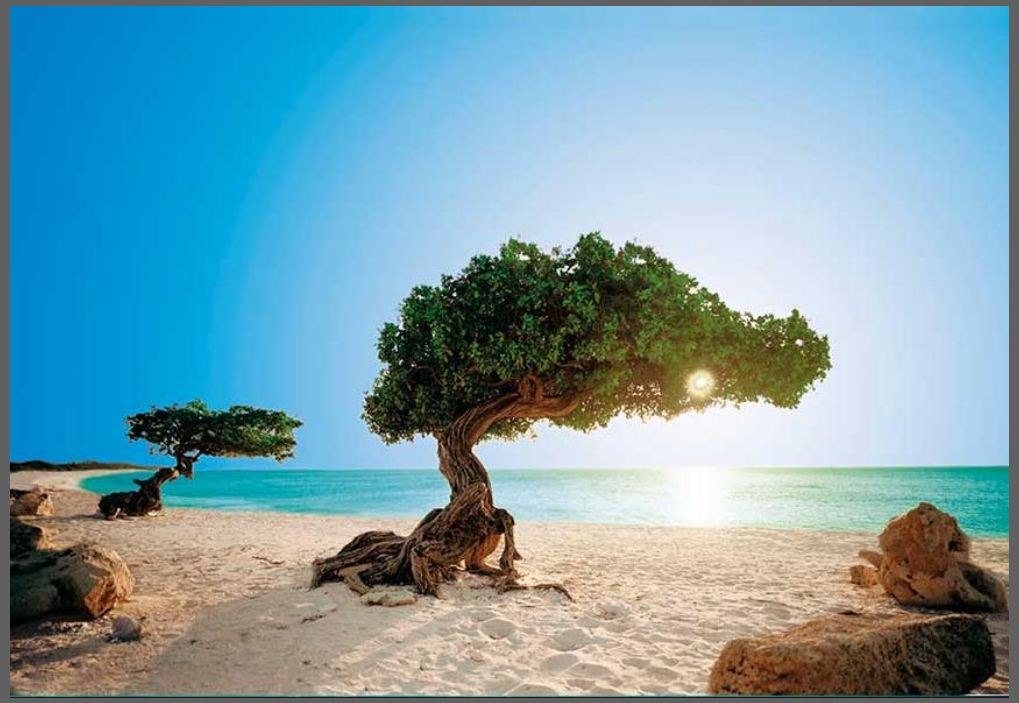
CEMLA- FIGI

Mexico City, 6-7 November, 2019

Kristel de Nobrega

Manager Information Security, Central Bank of Aruba

ARUBA CASE

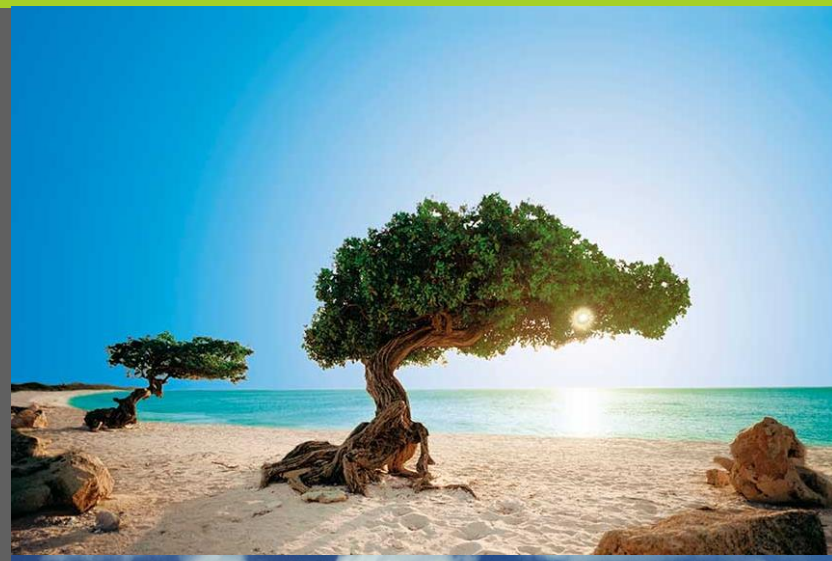


ARUBA THE ISLAND

- 106.000 inhabitants
- Tourism is most important economic pillar
- Expected to rise to 94% of GDP in 2025
- IS/IT development as enabler for financial services, entrepreneurs and tourism
- Microcosm ecosystem
- Logistical hub importance (e.g., harbor, airport, financial services)
- Geo location (e.g., EST time zone)
- Good reputation for Safety is crucial to keep tourists returning

RESOURCES: A CYBER CHALLENGE

- Technological and human resources are constrained
- Large span of responsibility for each stakeholders
- Lack of operational team dedicated to cyber security
- Lack of effective communication
- Work overload: Human processing capacity
- Time constraint



HRO: NEED FOR IX

The Banking and telecom sector are front runners in cyber intelligence sharing on the island.

"organizations that operate hazardous technologies in a nearly error-free manner under trying conditions rife with complexity, interdependence, and time pressure" (p. 2). (Vogel and Stutcliffe 2007)

CYBER THREAT

"Nothing strikes fear in the heart of than organization like the thought of a data breach" (VERIZON)

- Sandbox effect (e.g., mother country)
- Bandwidth increase (e.g., fiber)
- Digital literacy is relatively low (e.g., too many computers, phone and too little knowledge)
- Local policy and legislation is trailing (e.g., data breach not in place)

CONSTRAINTS OF IX

- Risk of exposure
- Lack of centralized information system
- Lack of a trusted community
- Lack of legal obligatory pressure
- Unwillingness to collaborate
- Fears of liability
- Fears of impact to reputation
- Lack of standards to communicate information

WHAT ARE WE DOING THEN?

- Define Cyber defense strategy
- Supervisory framework -Policy Paper on TRM - Highlights
- Local efforts
  - National Cyber Security Task Force
  - ISAC for local critical infrastructure
- Regional initiatives

CBA CYBER Defense VISION

- CBA has modern, resilient information systems that comply to the TRM policy paper, SWIFT CSP, NIST and is a driving force in TIBER-AW, which builds on regional threat intelligence.

- De CBA elevates its cyber resilience posture in 2020 based on ‘best practices’ by means of continuous improvement of its cyber resilience.

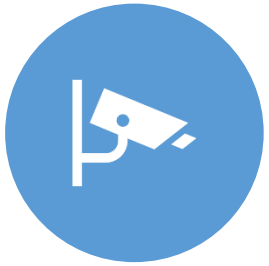
Strategic principles

Continuous improvement

Modern resiliency

“rip and replace”

Security by design – Monitor and Measure



Knowledge Management

MEERKAT/ SURICATA

Suricata →Creation of monitoring rules

Great natural spies

Eat nasty (technical) bugs

Live in clans or gangs (International Threat intelligence sharing communities)

From Cyber Situational Awareness to Cyber Defense

CYBER PHYSICAL RING

CYBER IN THE NEWS:

Sistema WEB victima di virus Zero Day exploit

October 27, 2016 Local

Share this:

Economia

FRONT PAGE POLITICA LOCAL INTERNACIONAL DEPORTE ENGLISH OPINION LIVE Search NoticiaCla

Western Union Aruba ta haci donacion na Mary Joan Foundation GIO'93 un anochi exclusivo den Balas! Enter email address Subscribe

Tweet Recommend Share

Banco Central di Aruba ta alerta pa SMS scam

Posted on 10/4/2019 2:38 pm AST | Updated on 10/4/2019 2:40 pm AST

ORANJESTAD - Banco Central di Aruba (BCA) a tuma nota cu for di ayera 3 october 2019, tin sms-nan cu ta ricibi, cu lo ta pretende di ta for di BCA. Texto di scam manera: "Felicidades por haber ganado 1000$ visite ahora aqui [link] para confirmar su premio este BANCO CENTRALE OF ARUBA"

Segun BCA, e sms-nan aki no ta di BCA y e no ta para responsabel pa nan. BCA ta lamenta e situacion malicioso y ta suplica publico pa no contesta ni yama e number aki, pasobra e sms-nan aki no ta di BCA y esunnan cu a manda nan, no ta liga na ningun operacion relata na BCA.

- No billing for one month
- Only company who reported it
- Scarcity and critical infrastructure
- MIM attack vectors
- SMS Scams

AWEMainta
5 hrs

ADVERTENCIA:
Si bo ricibi un email di CMB cu e subject: "kennisgeving Internetbankieren" no habri e.

Geachte gewaardeerde klant,

Vanwege recente beveiligingsincidenten hebben we nieuwe beveiligingsprotocollen opgesteld.

U moet nieuwe beveiligingsprotocollen valideren om online bankdiensten te kunnen blijven gebruiken.

Klik HIER om nieuwe beveiligingsprotocollen te verifiëren.

Your CMB Online Banking Support Team
Caribbean Mercantile Bank

E ta purba di hack of hay informacion for di bo persona dor di mandabo na un link cu no ta di CMB "cmbnvcoffecup.com"

Trend in Global Cyber Defense strategies

- The need to protect or enhance “situational awareness”
- Stronger structure for confidential information sharing and analysis
- Effective anticipation and analysis of the environment in order to make appropriate decisions
- Monitor and provide mitigation advice on cyber threats, and coordinate, and coordinate the national response to any cyber security incident

Cyber Situational Awareness

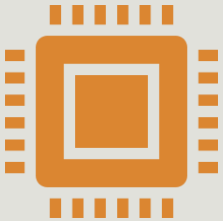
Technology focus: compiling, processing and fusion of data

Cognitive focus: human capacity of being able to comprehend the technical implications and draw conclusions in order to come up with informed decisions (and enhance sensemaking).

Cognitive focus is thus interesting as this can differ per human per task, yet it ultimately defines your cyber defense response.

Both process built upon a foundation of (fusion) data

CSA: [Suspicious Indicators]

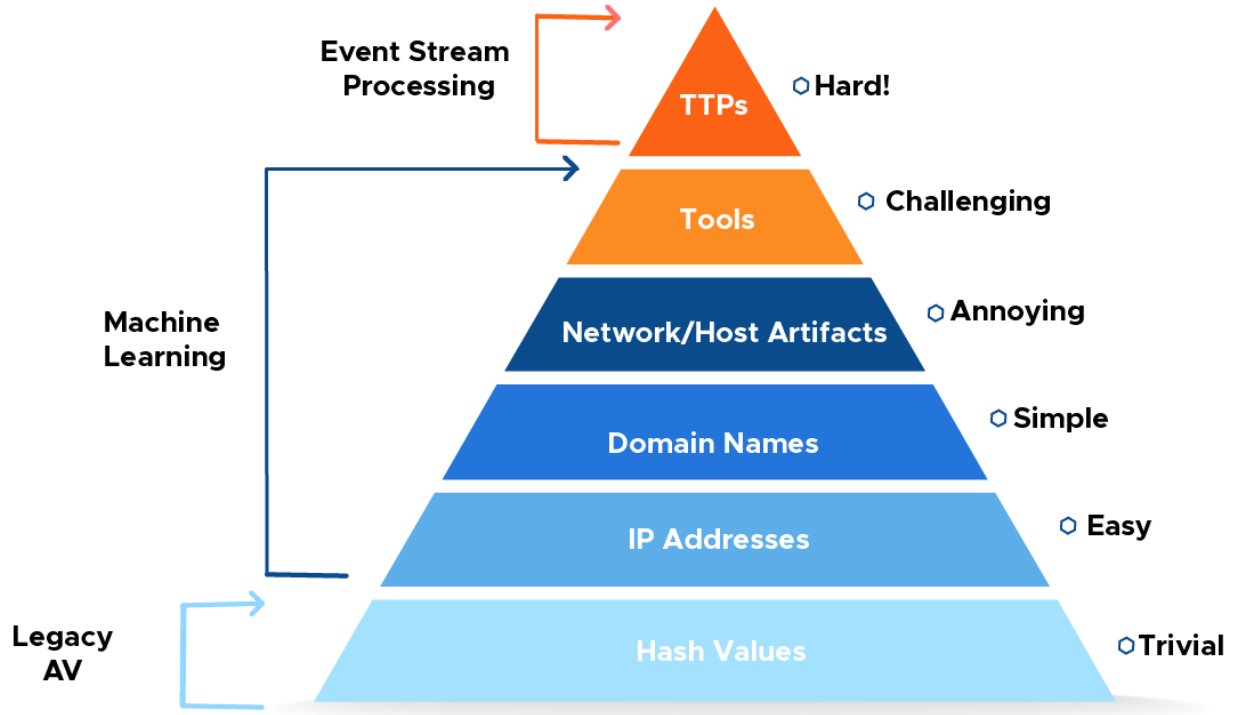


Cyber sensor: IDS alerts, SIEM, IPS, Firewalls etc..

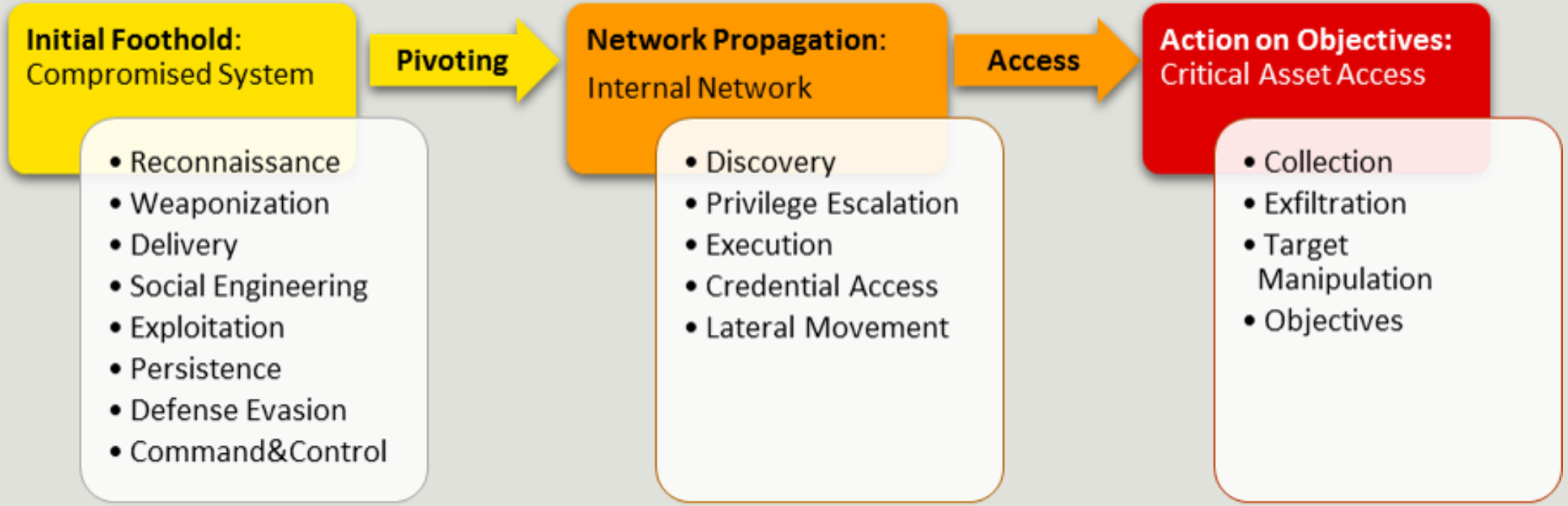
Traditional sensor :Human intelligence, Insider leaking information, Information Exchanges

Physical sensor: Natural events, Power outages, Acts of God etc.

Pyramid of Pain



Recent Developments in attack vectors that affect network defense



SUPERVISION FRAMEWORK - POLICY PAPER ON TRM - HIGHLIGHTS

POLICY PAPER ON TRM - HIGHLIGHTS

- In July 2018 the final Policy Paper on TRM was issued, after several consultation rounds

- TRM Policy Paper is based on international standards and best practices
  - All banks under CBA's supervision are required to comply with the guidelines contained in this policy paper on a comply or explain basis
  - Grace period granted: 1 year

POLICY PAPER ON TRM - HIGHLIGHTS

- Structure of the Policy Paper on Technology Risk Management

- The TRM Guidelines set out risk management principles and best practices to guide banks in:
  - Establishing a sound and robust TRM framework
  - Deploying strong authentication to protect customer data, transactions and systems
  - Strengthening system security, reliability, resiliency and recoverability

LOCAL INITIATIVE -NCSTF

CYBER [RE]ADINESS IS NOT A CHOICE, It IS OUR DUTY

- *Ministrerieel Besluit waar het Nationale Cyber Security Taskforce in leven is geroepen op 21 Sept 2018*

"Het doel van de beoogde samenwerking zal zijn bij te dragen aan bescherming van de vitale informatie infrastructuur op Aruba (Critical Information Infrastructure Protection)"

- *"Gezien de vitale rol van de Centrale Bank van Aruba (CBA) in de veiligheid van de Arubaanse betalingsinfrastructuur is besloten om de CBA als samenwerkingspartner bij te voegen aan deze initiele groep"*

REGIONAL INITIATIVES -

- The goal of this working group is to establish a regional IT/ cyber risk supervisory framework.
- The published Technology Risk Management (TRM) Framework and self-assessment tool with all members of the working group.
- Regional information sharing

THE FUTURE IS CHALLENGING!

- Cyber Security nor justice can keep you safe
- Cyber readiness index of a country depends on digitalization, which goes hand in hand with cyber security
- Public and private partnership is the way to go
- Don’t depend on the enemy not coming, depend rather on being ready for him
- Holistic approach
- Balance short term and long term initiatives
- Simulate, practice and engage when encountering mistakes
- IX build trust lead by example, trust makes the Suricata clan stronger