
Cyber Threat Intelligence
Sharing Network

Objectives

- **Identify whether there is an appetite amongst community members to be a part of a Cyber Threat Intelligence Sharing Network**
  - **Survey (50 minutes)**
    - **Identify what the barriers are for community members to be a part of the cyber threat intelligence sharing network**
    - **Identify the incentives and benefits of sharing cyber threat intelligence**
- **Provide an overview of the available cyber threat intelligence sharing networks in SA, courtesy of SARB (20 minutes)**
  - Who?
  - What?
  - Legal
  - Platform
  - **Lesson learned and best practices**
- **Next Steps (5 minutes)**

State of Cybercrime

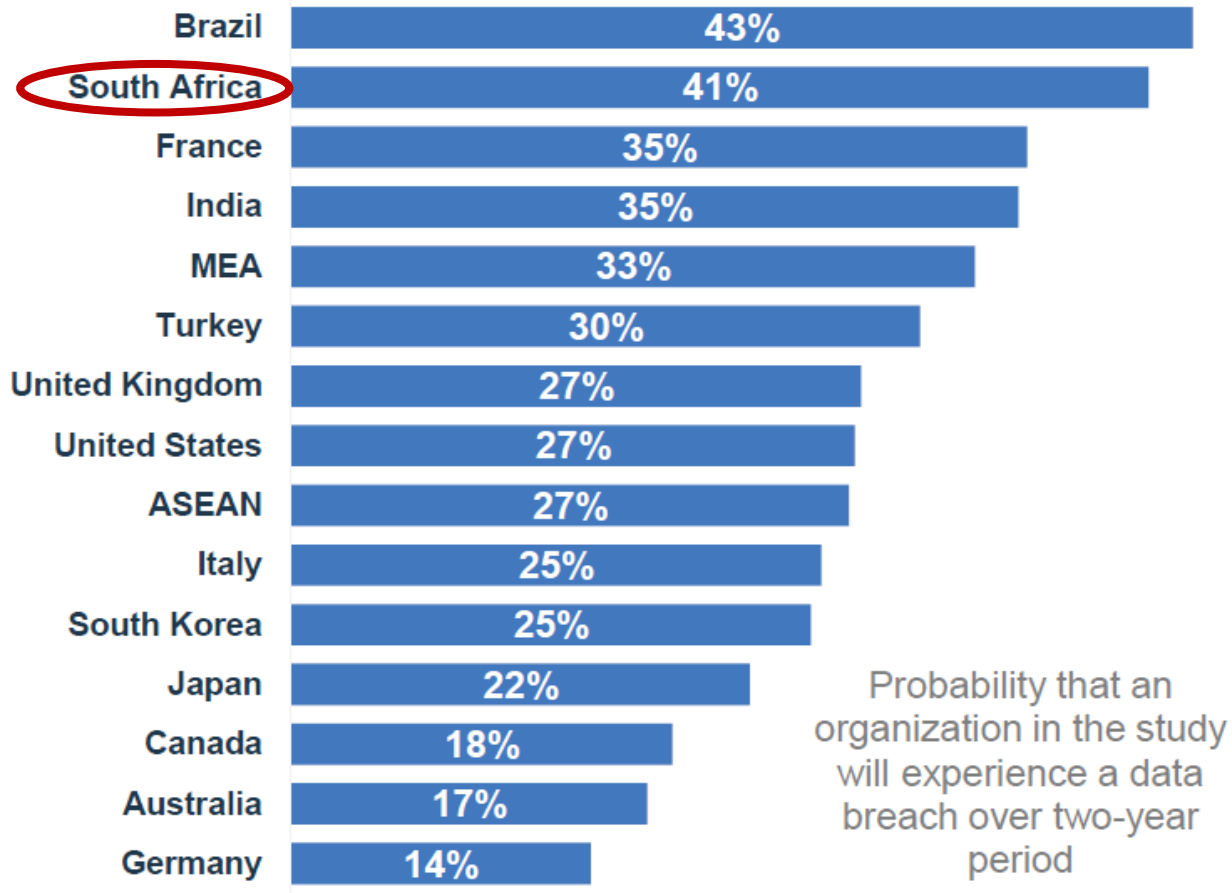
A quick overview

The odds of experiencing a data breach

Experiencing a data breach?

1 in 4

(Global average 28%)



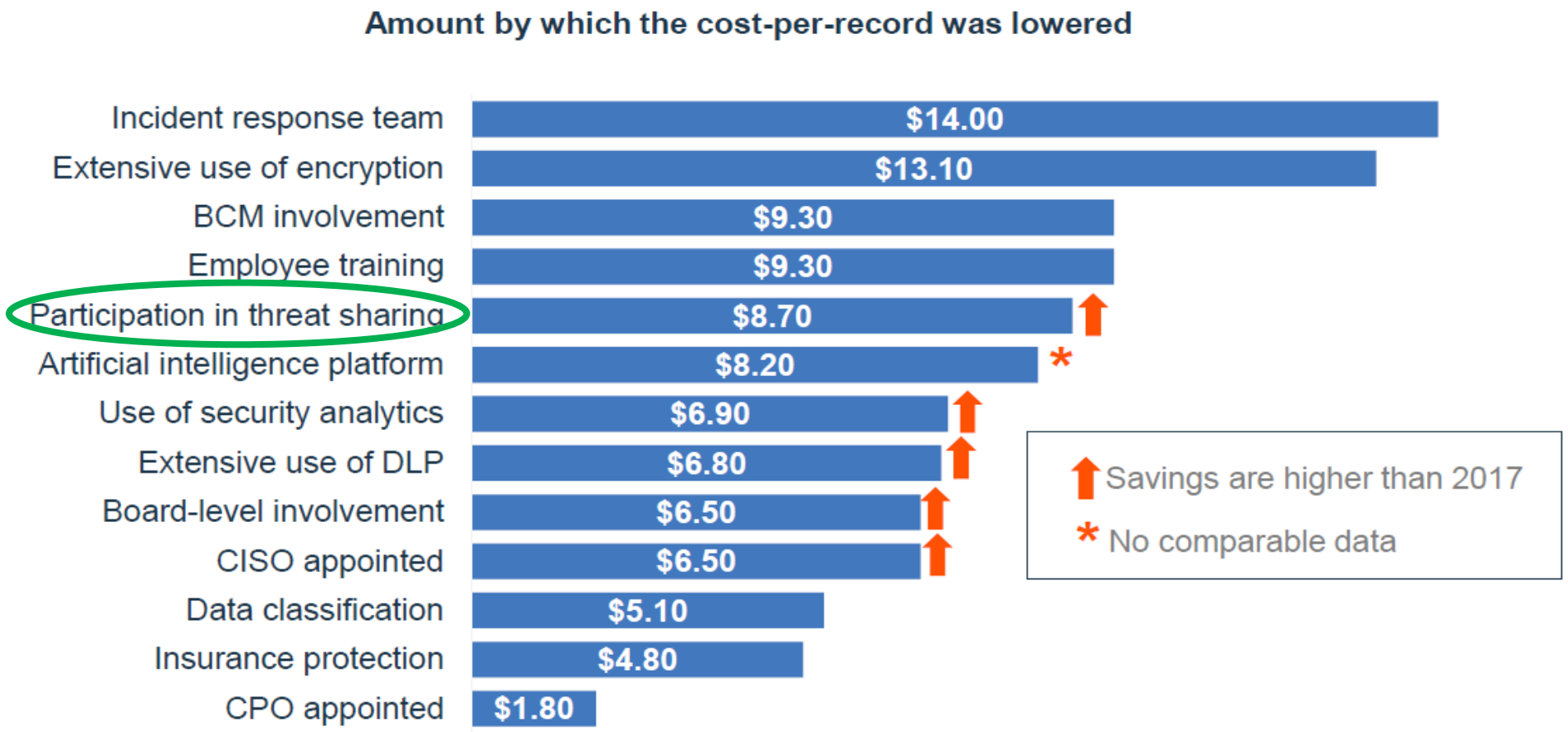
Source: Ponemon

The biggest cyber crime trends for 2019

- **Advanced phishing attacks**
  - 345600 new malware kits created every day
  - Phishing sites are online on average 4-5 hours
  - Only 17% of phishing attacks are reported
  - Only 35% of URLS are trusted
  - 2020 will be known as year of advanced phishing attacks
- **Remote access Attacks**
  - Cryptojacking
  - Perimeter devices (like cameras, storage devices, access points, routers
- **Smartphone attacks**
  - Unsafe browsing
  - Phishing, spear-phishing and malware
  - More than 60% of online fraud is committed through smartphones
  - Smartphones used for 2FA, and contains lost of personal information. It is a major source of risk if lost or stolen
- Vulnerabilities in home automation and **IOT**
  - Is growing threat, even though users do not interact with them directly for e.g. foot counters, music systems, cameras etc.
  - Attack vector likely to be DDOS
- **Artificial Intelligence**
  - Unethical use of AI
  - Cyber detection evasion
  - AI based phishing
  - AI in social engineering

Source: WEF

Factors or controls to reduce the cost of a data breach

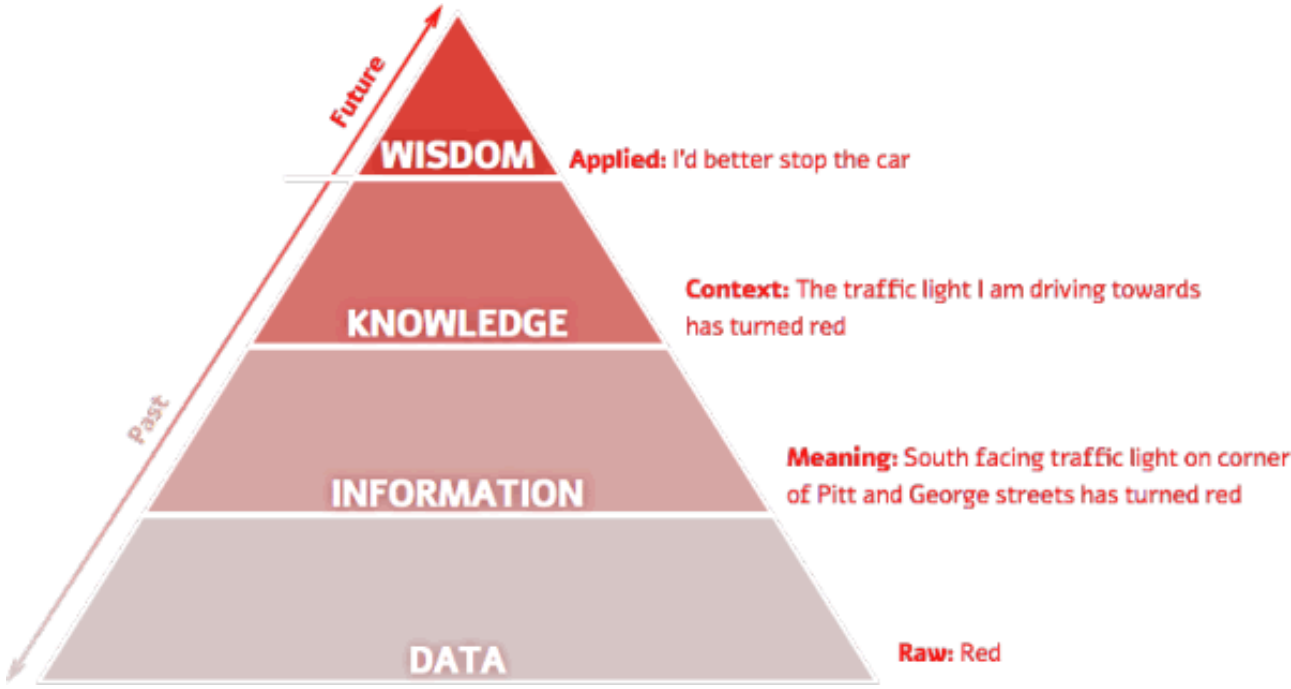


Source: Ponemon

What is Threat Intelligence?

"Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard." (Gartner)

Example: if a 3rd party vendor informs you that a North Korean, cyber crime organisation is attacking companies in your vertical, and provides a list of tools and techniques that are being used to execute these attacks.



Characteristics to identify threat intelligence;

1. ***Relevance:*** Can it or does it impact your organisation in some way?
2. ***Actionable:*** Can concrete steps be taken by security teams to protect the organisation?
3. ***Contextual:*** Is there enough information to enable the Security Analyst to effectively rank the threat and or risk

Source: The Handbook of Cyber Threat Intelligence

Problem Statement

Cyber crime is a global issue and everyone is exposed to it in some shape or form.

As a community, we represent some of the leading organisations in South Africa, with a common interest **of "protecting our brands"** as well as protecting our business stakeholders and communities at large.

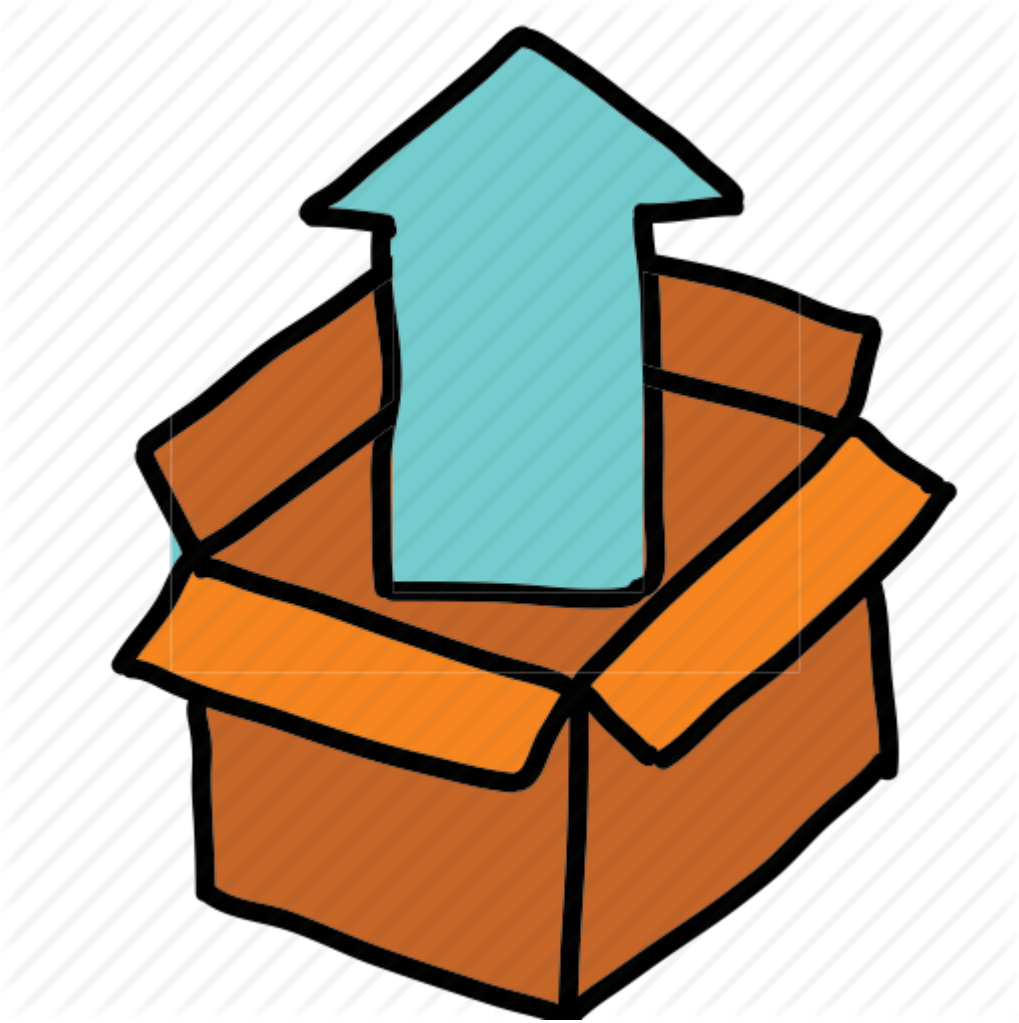
"Doing good never goes out of fashion"

One of the ways in-order for us to deal with our common enemies, is to utilise **cyber threat intelligence to better "protect our houses" and communities.**

"Are you willing to be part of a cyber threat intelligence sharing network?"

Survey

Let’s unpack the survey



Proposed Next Steps

- Follow up survey to establish interest

- Interested parties will be contacted for a webinar with the SARB team with regards to the following;
  - How do we formalise your enrolment into the network?
  - On-boarding process
  - Platforms
  - Costs
  - Etc.