

Cyber Crime

The Known Unknown Emerging Exposure

Peter Hacker, Cyber Security Expert and Thought Leader

Nigel Phair, Cyber Security Expert

ADB Workshop

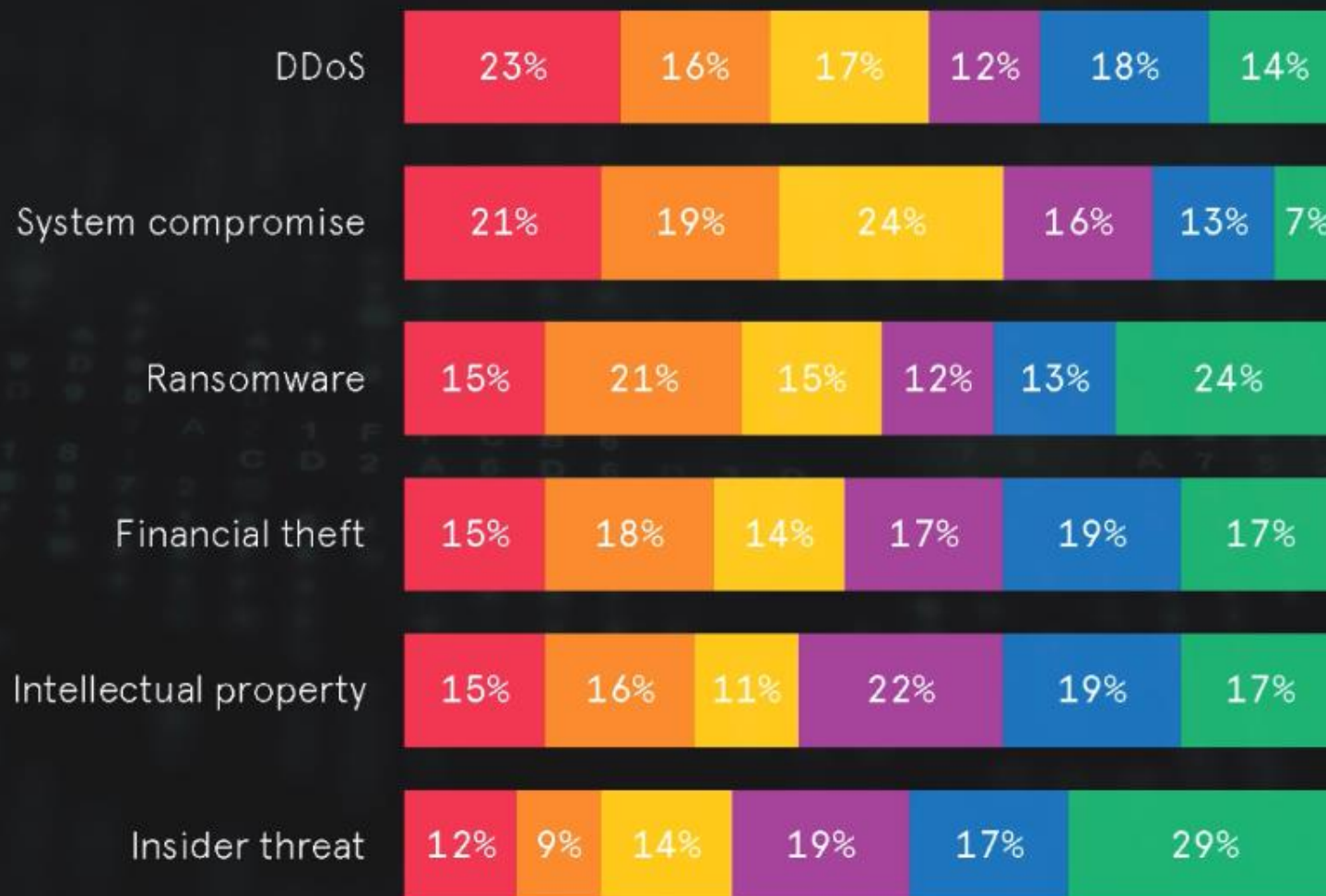
Manila, 4th November 2019

Cyber Security Board Report

Cyberthreats ranked
in order of concern,
January 2019 NISC report

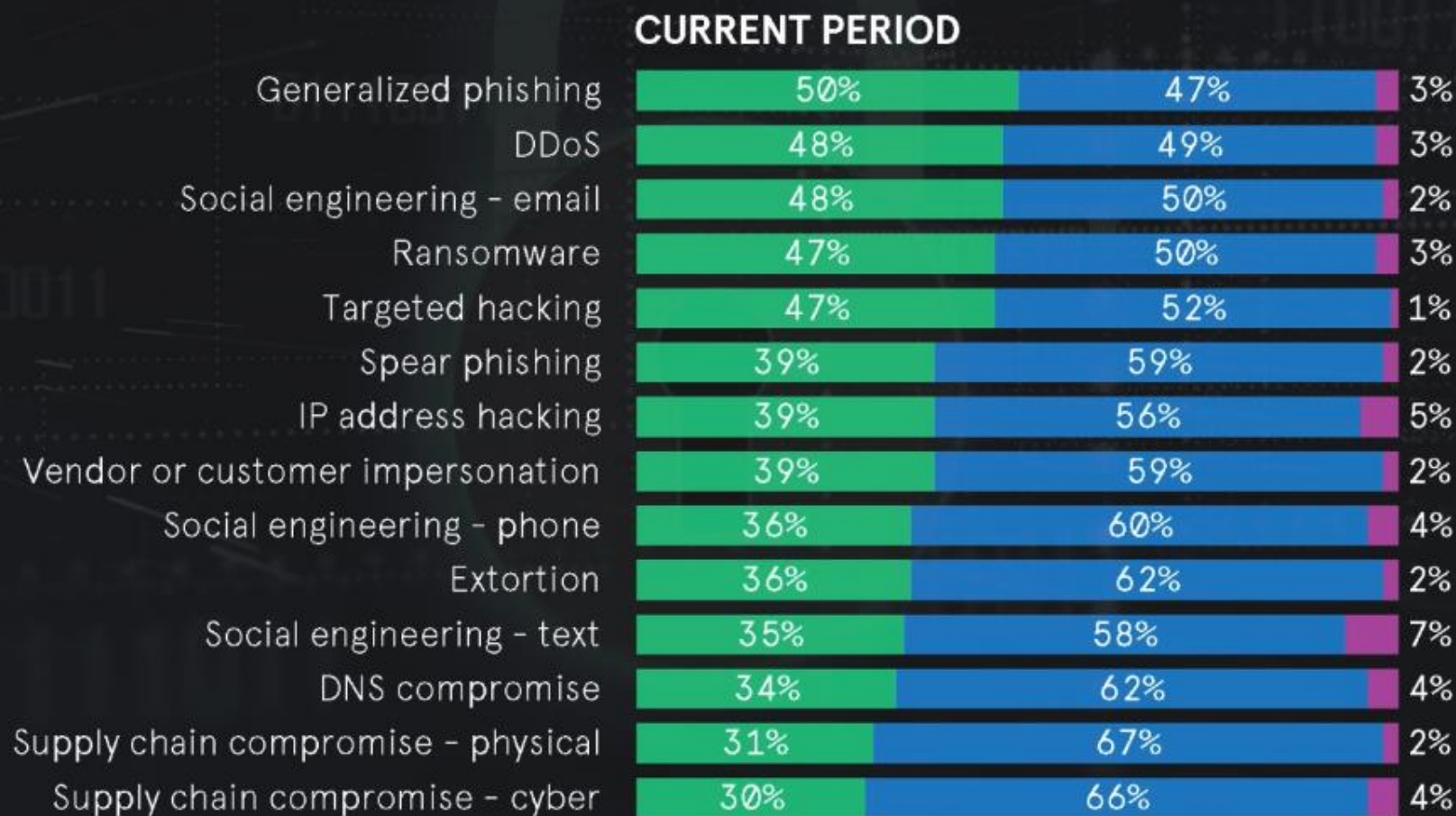
■ Highest threat (1) ■ 2 ■ 3 ■ 4 ■ 5 ■ Lowest threat (6)

CURRENT PERIOD

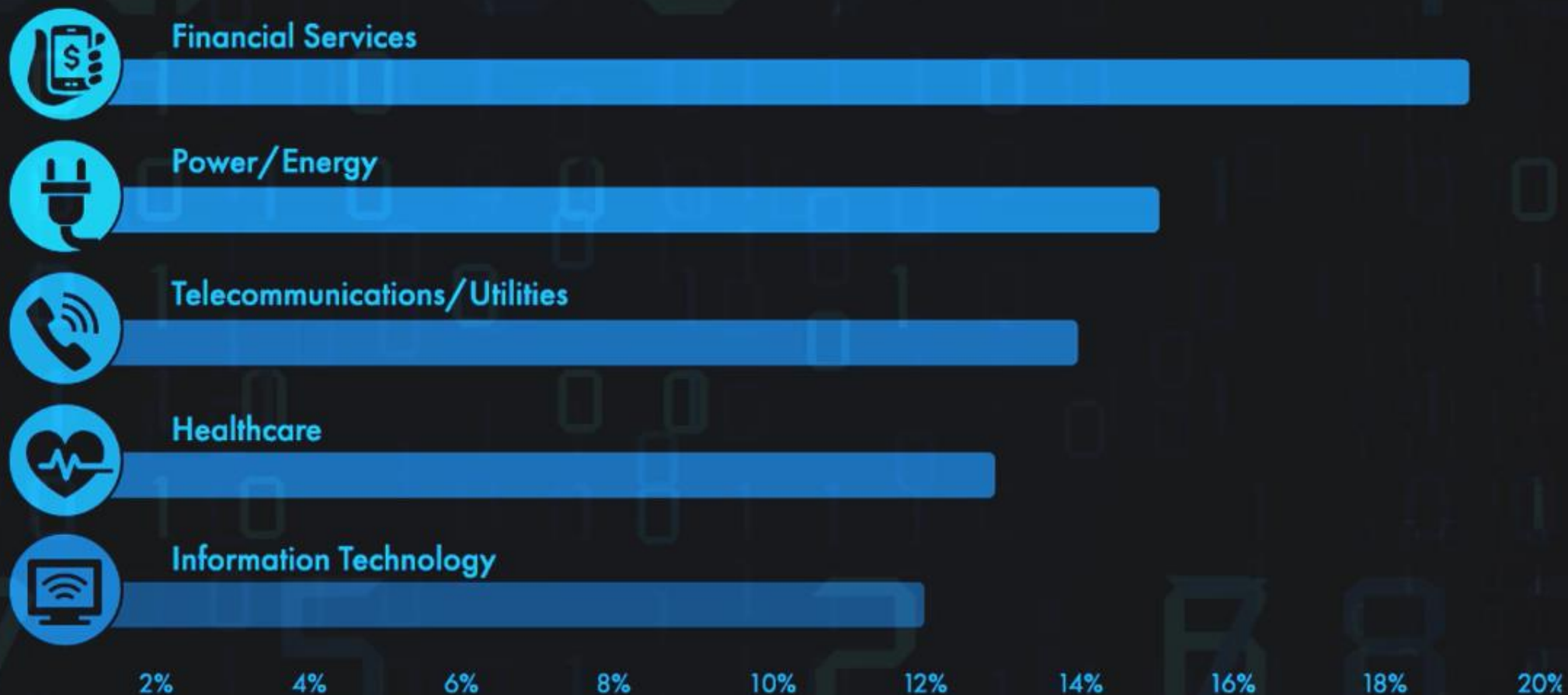


Cyber Security Board Report (II)

Increased Stayed the same Decreased



Global Critical Infrastructure Incident Attack Increases

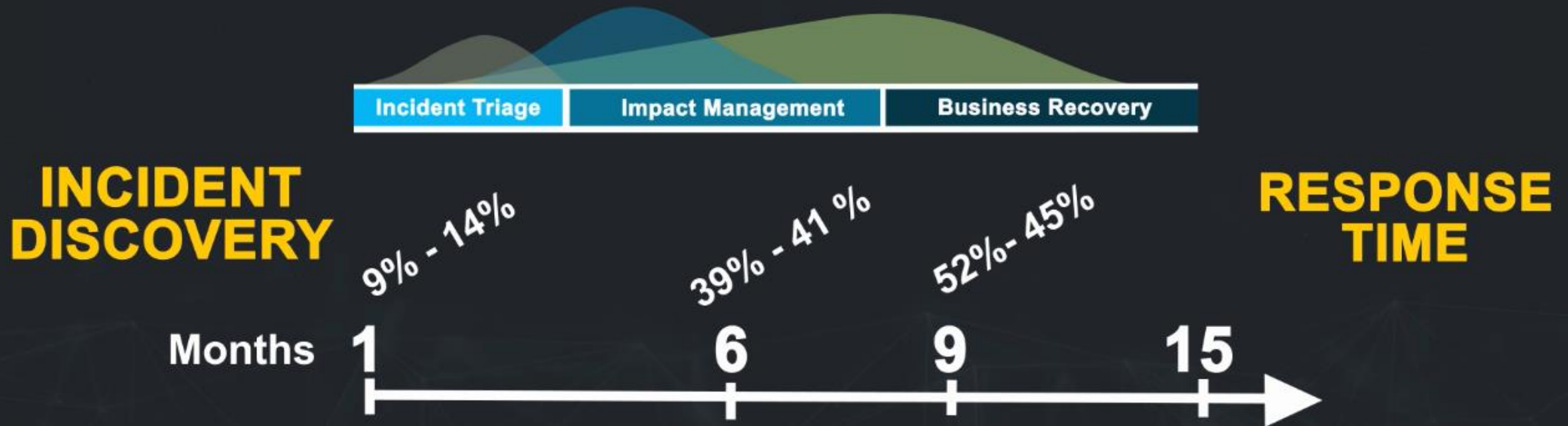


Source



Incident Response Set Up: The Challenge

Events and Impacts of the *Cyber Incident* unfolded



Group Incident Response Matrix

**CRISIS
MANAGEMENT**

**INCIDENT
RESPONSE**

FORENSICS

**RISK
TRANSFER**

Lessons Learnt

COMPROMISE ASSESSMENT



Phase I:
Open Source
Threat
Intelligence



Phase II:
Behavior
Assessment



Phase III:
Monitoring



Phase IV:
Host based
searching
IOCs

Analyze

Risk Circumstances:

Potential impacts, Technical Level, Ramification and Spread, Interruptions, Destruction

Define

Environment, objectives and response

Potential threats, incidents, breaches or scenarios, capabilities, defense strategy and response options.

Risk Transfer and Control

Take actions

be aware of hurdles

- Who needs to be involved in defense?
- What are your fiduciary duties concerning cyber crime and cyber security exposure?
- What are bespoke recovery solutions?
- What are potential pitfalls ?



Thank you