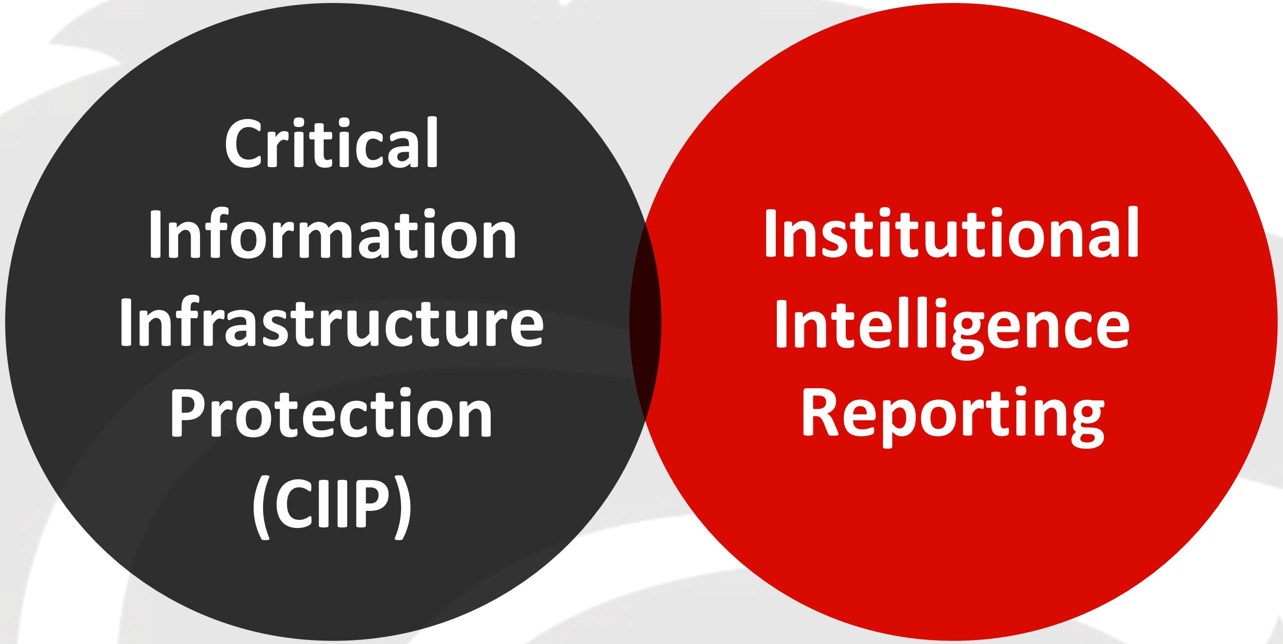
BARNOWL



Critical Information Infrastructure Protection (CIIP)

Institutional Intelligence Reporting

Craig Rosewarne & Jonathan Crisp

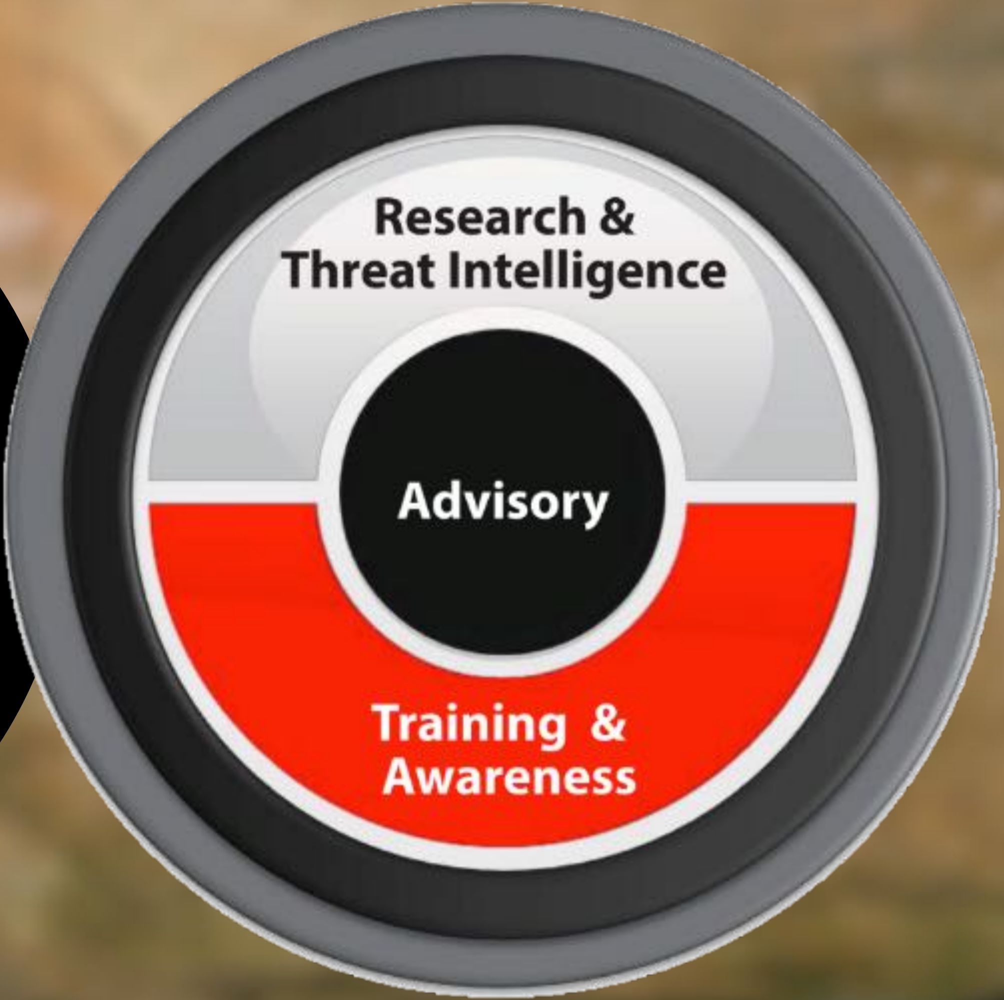
Fast Facts

Wolfpack Information Risk (Pty) Ltd is a proudly South African company established in **2011**

Independent trusted advisors to **government** and **private** sector

Ongoing commitment to **national cyber security community** initiatives

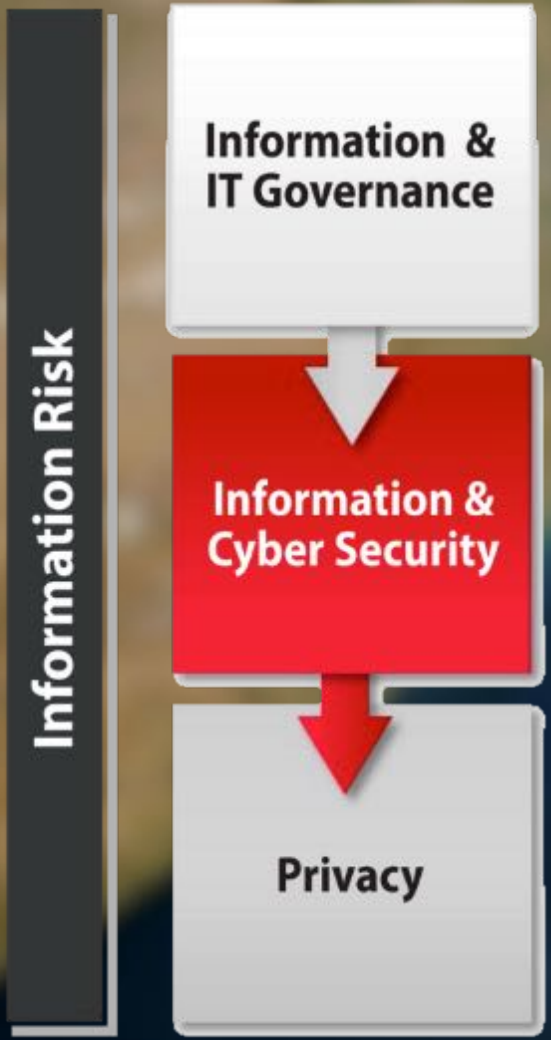
A level **1 BBBEE** contributor



Research & Threat Intelligence

Advisory

Training & Awareness



Information Risk

Information & IT Governance

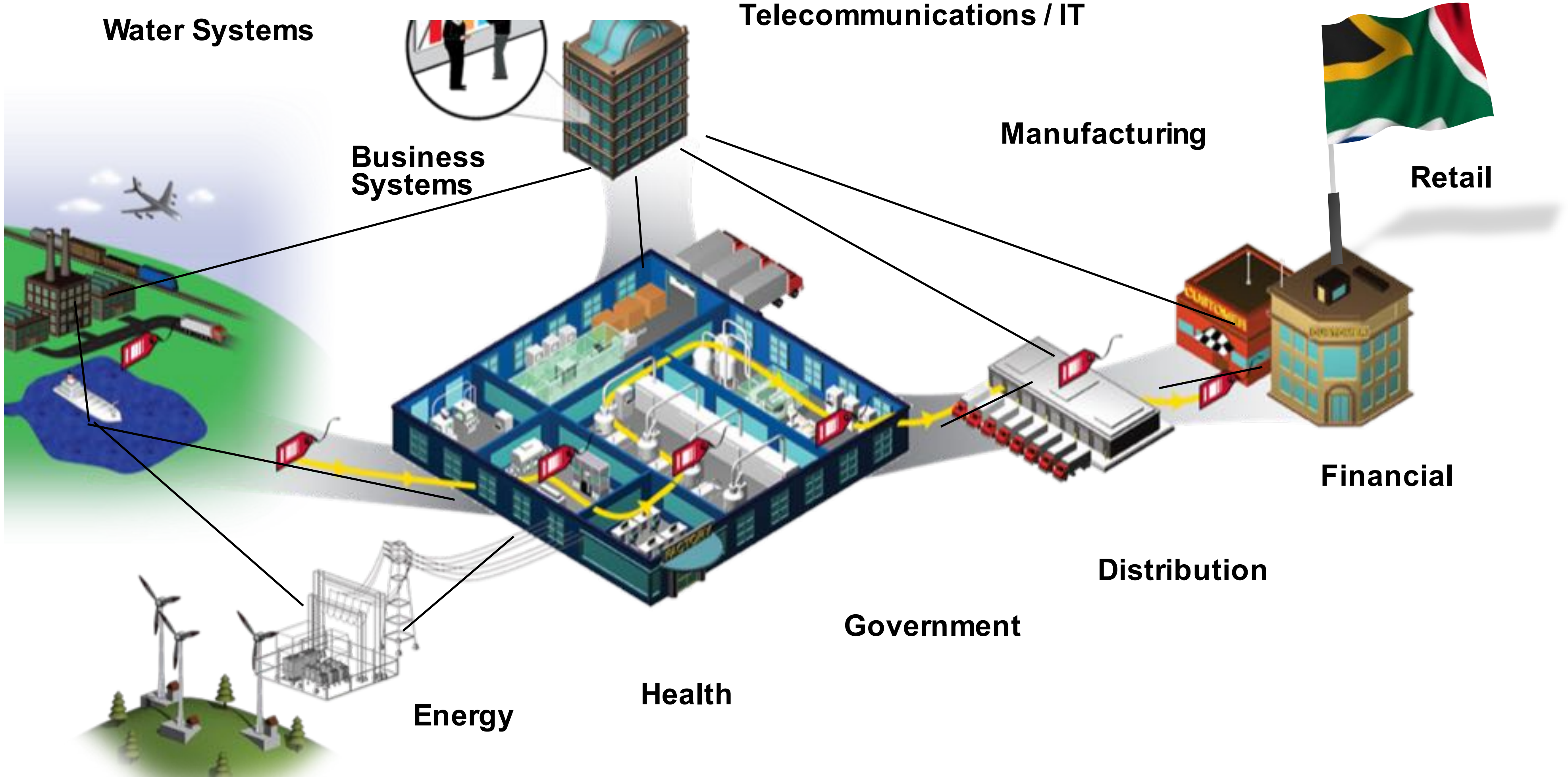
Information & Cyber Security

Privacy

$14.3 BILLION

$3 TRILLION

CRITICAL INFORMATION INFRASTRUCTURE



Water Systems

Telecommunications / IT

Transport

Business Systems

Manufacturing

Retail

Ports

Financial

Distribution

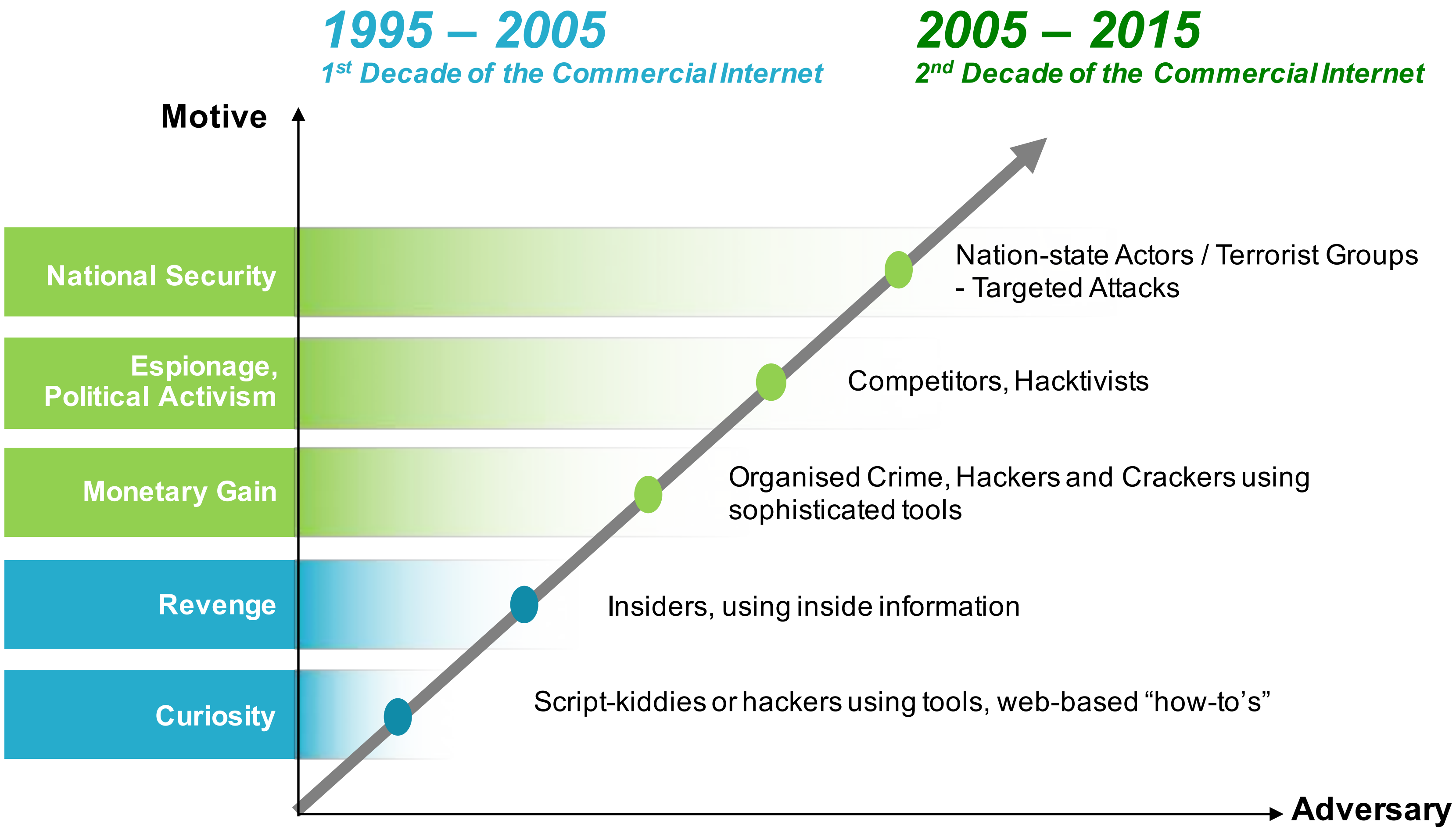
Government

Supply Chain

Health

Energy

THE EVOLVING THREAT

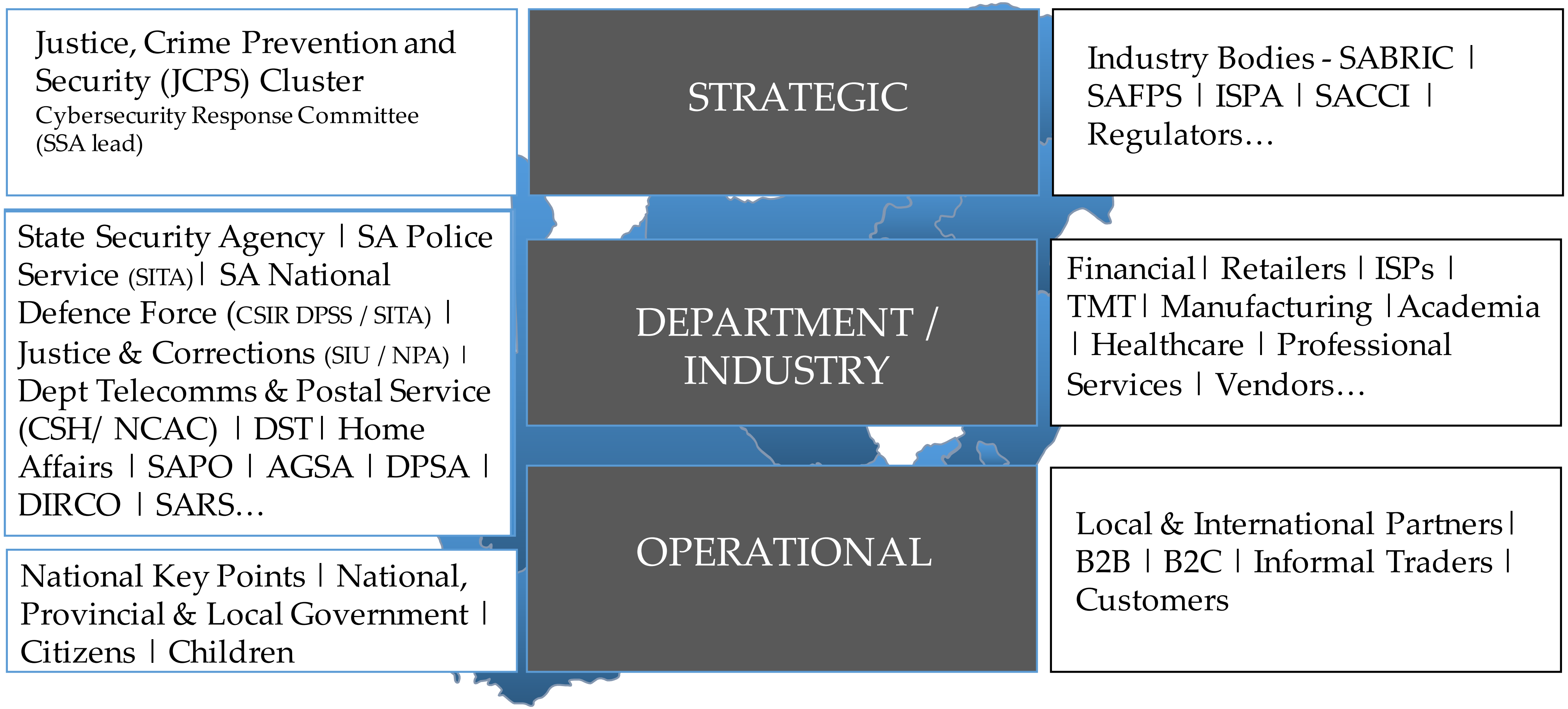

1995 – 2005
1st Decade of the Commercial Internet
2005 – 2015
2nd Decade of the Commercial Internet
Motive
National Security
Espionage, Political Activism
Monetary Gain
Revenge
Curiosity
Nation-state Actors / Terrorist Groups - Targeted Attacks
Competitors, Hacktivists
Organised Crime, Hackers and Crackers using sophisticated tools
Insiders, using inside information
Script-kiddies or hackers using tools, web-based “how-to’s”
Adversary

state security
State Security Agency
REPUBLIC OF SOUTH AFRICA

defence
Department:
Defence
REPUBLIC OF SOUTH AFRICA

SOUTH AFRICAN POLICE SERVICE

SA NATIONAL CYBERSECURITY STAKEHOLDERS



Justice, Crime Prevention and Security (JCPS) Cluster
Cybersecurity Response Committee (SSA lead)

STRATEGIC

Industry Bodies - SABRIC | SAFPS | ISPA | SACCI | Regulators…

State Security Agency | SA Police Service (SITA)| SA National Defence Force (CSIR DPSS / SITA) | Justice & Corrections (SIU / NPA) | Dept Telecomms & Postal Service (CSH/ NCAC) | DST| Home Affairs | SAPO | AGSA | DPSA | DIRCO | SARS…

DEPARTMENT / INDUSTRY

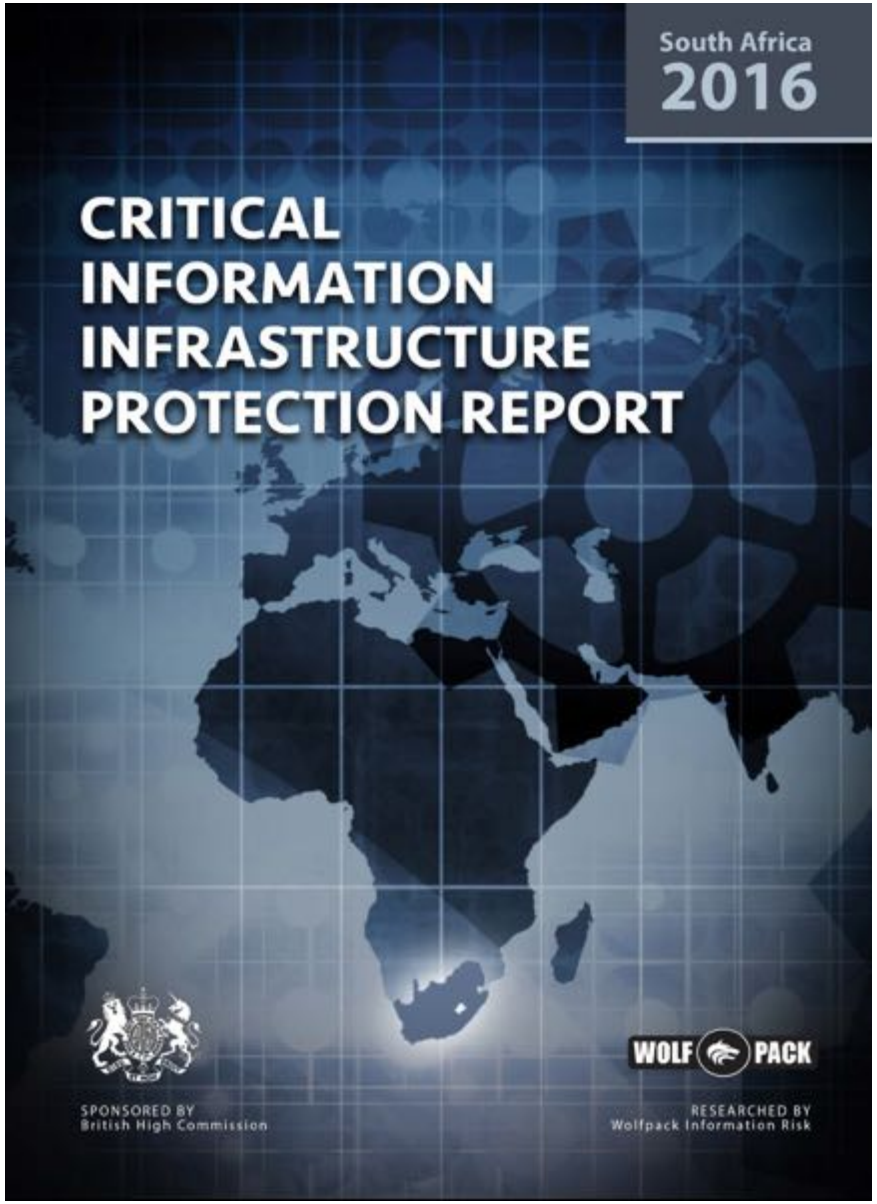
Financial| Retailers | ISPs | TMT| Manufacturing |Academia | Healthcare | Professional Services | Vendors…

National Key Points | National, Provincial & Local Government | Citizens | Children

OPERATIONAL

Local & International Partners| B2B | B2C | Informal Traders | Customers

SA 2016 CIIP REPORT



South Africa
2016

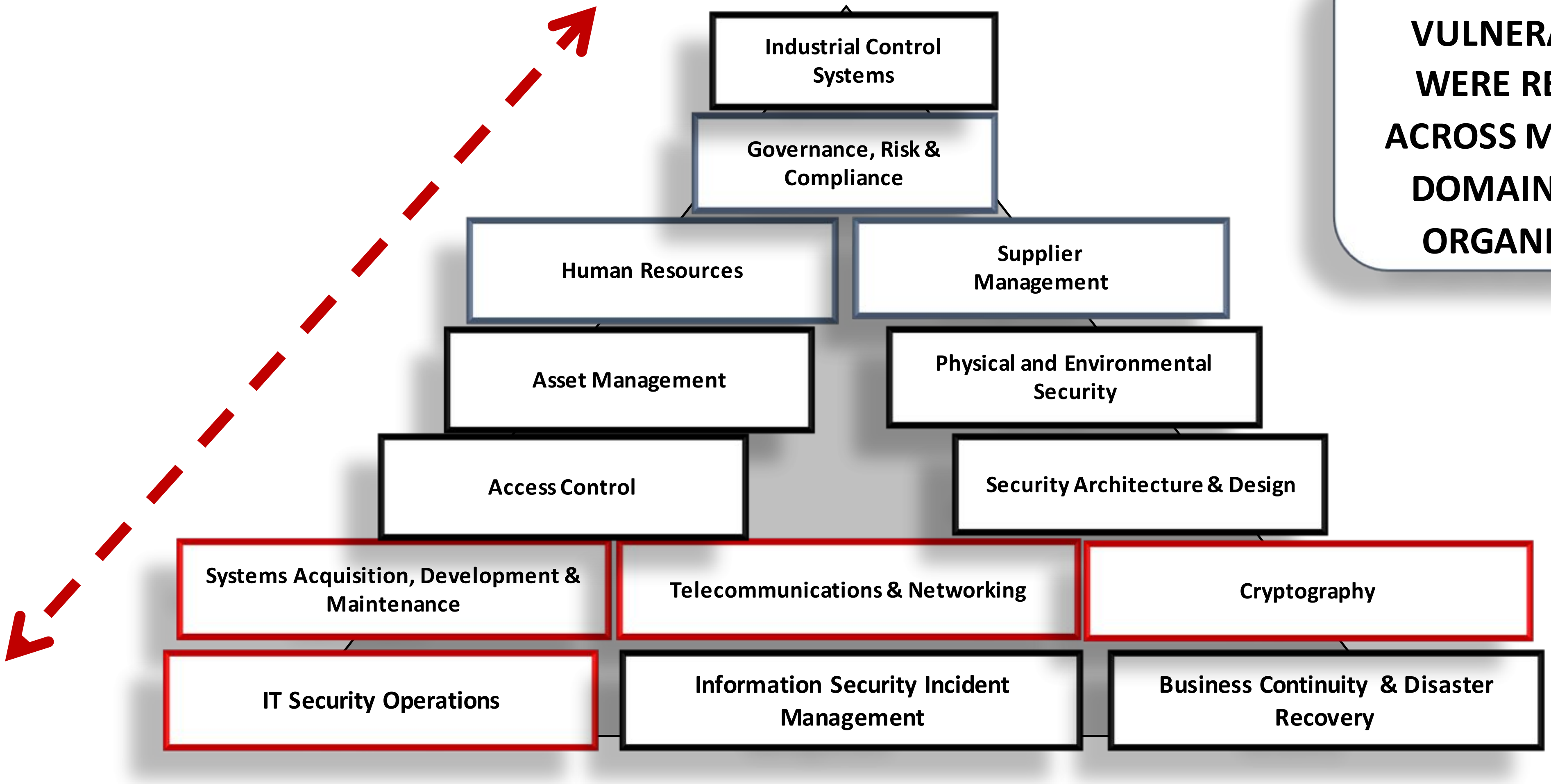
CRITICAL INFORMATION INFRASTRUCTURE PROTECTION REPORT

WOLF PACK

SPONSORED BY
British High Commission

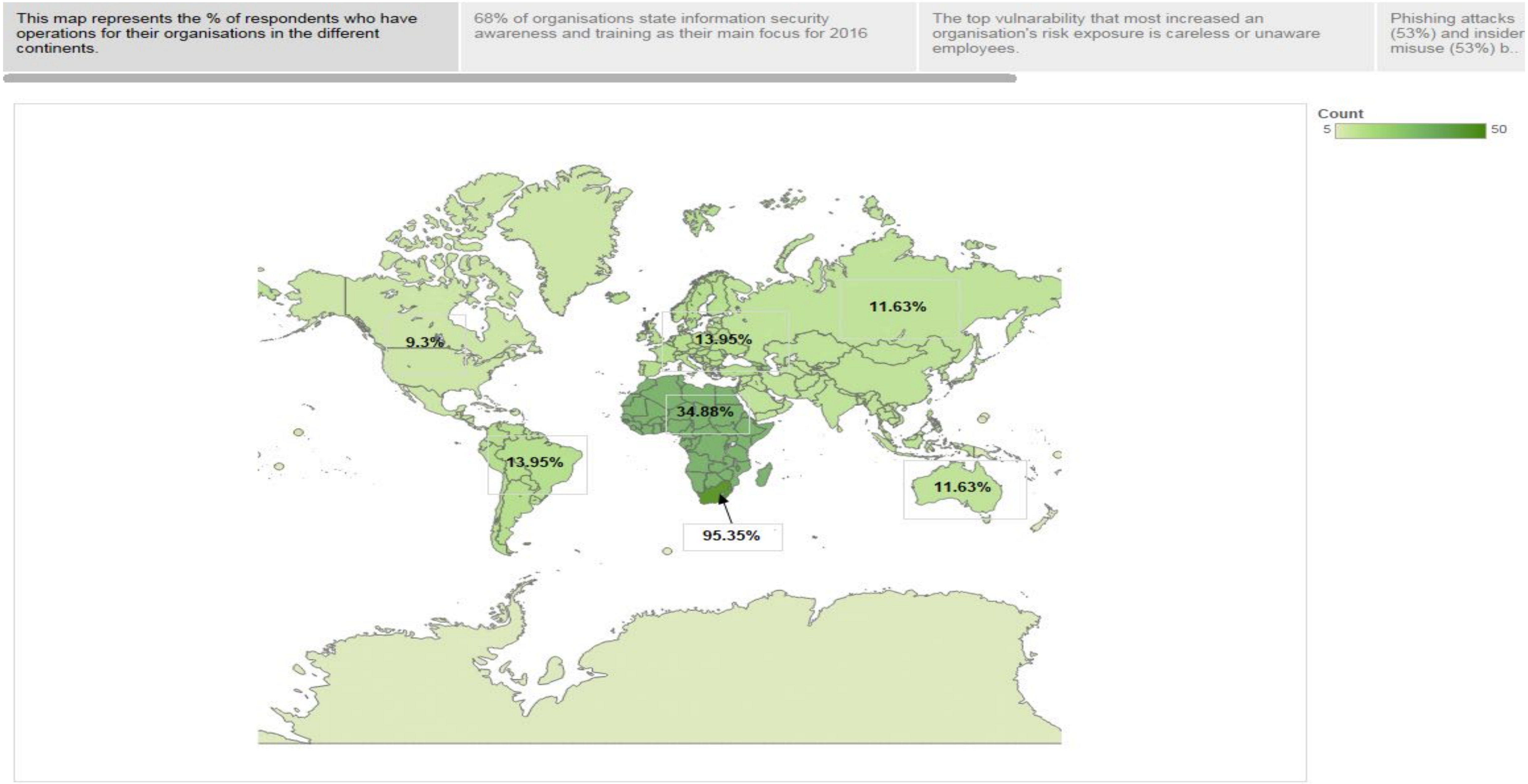
RESEARCHED BY
Wolfpack Information Risk

INFORMATION RISK ASSESSMENT


Industrial Control Systems
Governance, Risk & Compliance
Human Resources
Supplier Management
Asset Management
Physical and Environmental Security
Access Control
Security Architecture & Design
Systems Acquisition, Development & Maintenance
Telecommunications & Networking
Cryptography
IT Security Operations
Information Security Incident Management
Business Continuity & Disaster Recovery

160 POSSIBLE VULNERABILITIES WERE REVIEWED ACROSS MAJOR RISK DOMAINS OF THE ORGANISATION.

INSTITUTIONAL INTELLIGENCE REPORTING



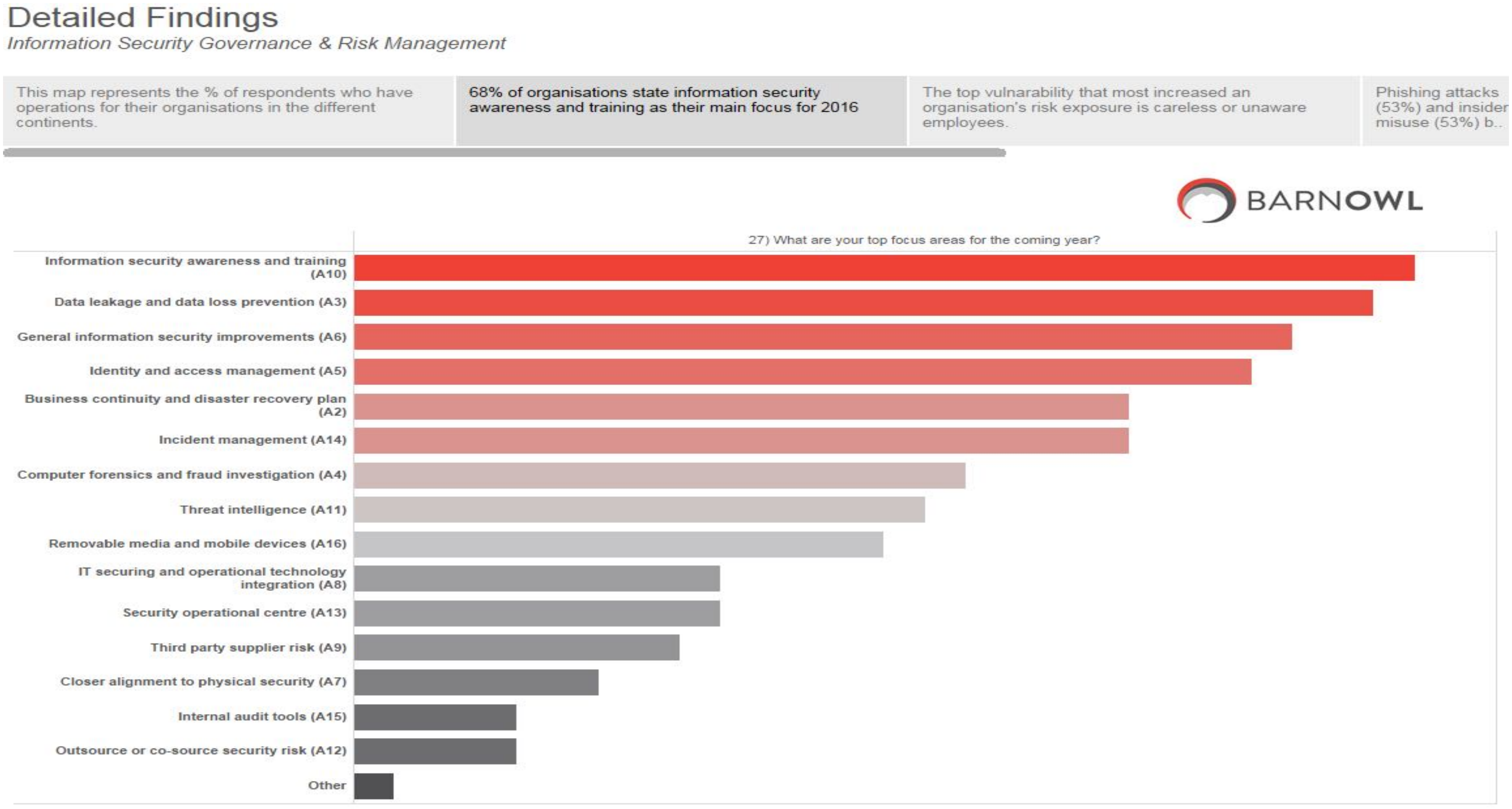
This map represents the % of respondents who have operations for their organisations in the different continents.

68% of organisations state information security awareness and training as their main focus for 2016

The top vulnarability that most increased an organisation's risk exposure is careless or unaware employees.

Phishing attacks (53%) and insider misuse (53%) b..

INSTITUTIONAL INTELLIGENCE REPORTING



Detailed Findings

Information Security Governance & Risk Management

This map represents the % of respondents who have operations for their organisations in the different continents.

68% of organisations state information security awareness and training as their main focus for 2016

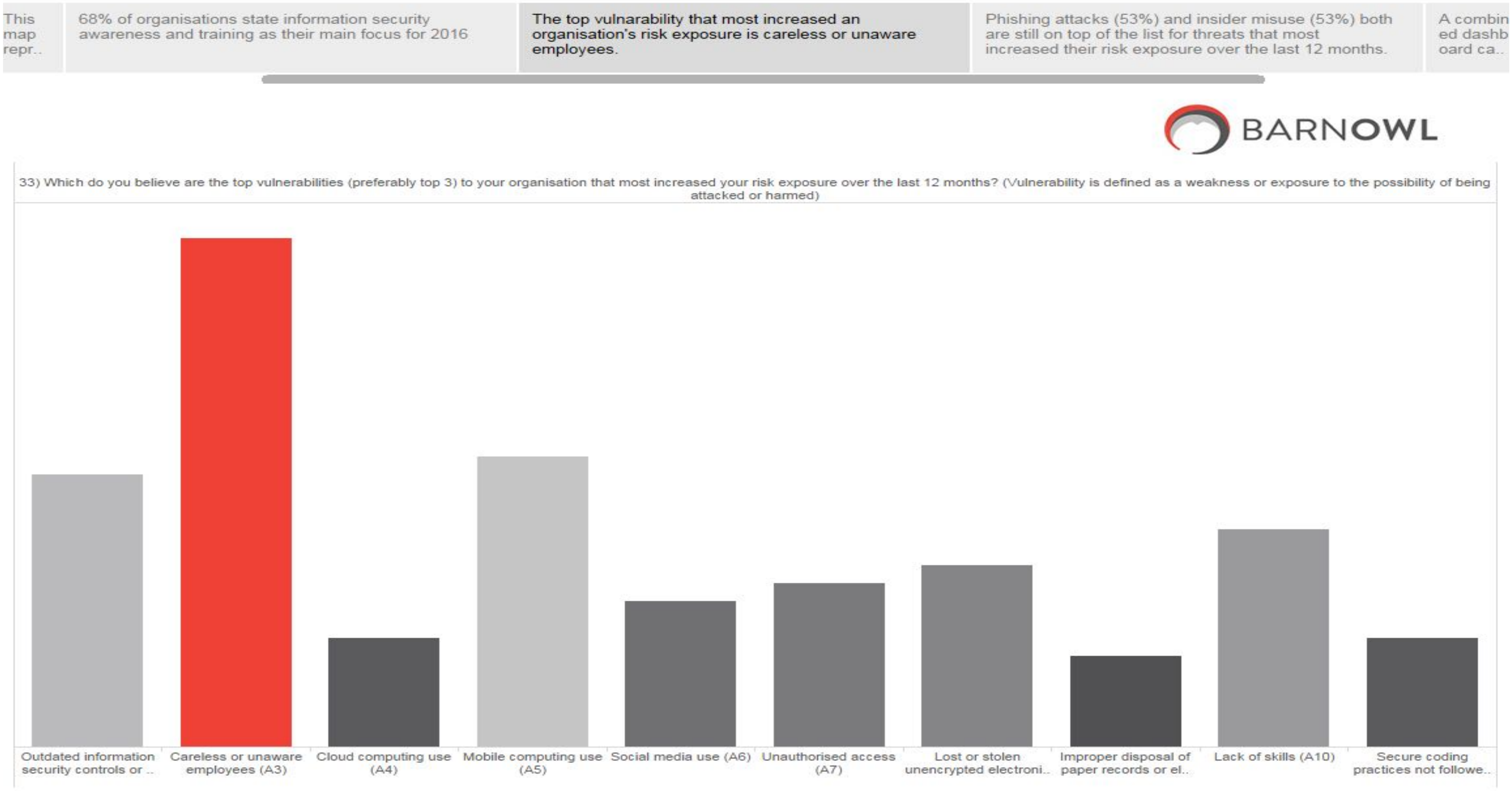
The top vulnarability that most increased an organisation's risk exposure is careless or unaware employees.

Phishing attacks (53%) and insider misuse (53%) b..

BARNOWL

27) What are your top focus areas for the coming year?
Information security awareness and training (A10)
Data leakage and data loss prevention (A3)
General information security improvements (A6)
Identity and access management (A5)
Business continuity and disaster recovery plan (A2)
Incident management (A14)
Computer forensics and fraud investigation (A4)
Threat intelligence (A11)
Removable media and mobile devices (A16)
IT securing and operational technology integration (A8)
Security operational centre (A13)
Third party supplier risk (A9)
Closer alignment to physical security (A7)
Internal audit tools (A15)
Outsource or co-source security risk (A12)
Other

INSTITUTIONAL INTELLIGENCE REPORTING



This map repr..

68% of organisations state information security awareness and training as their main focus for 2016

The top vulnarability that most increased an organisation's risk exposure is careless or unaware employees.

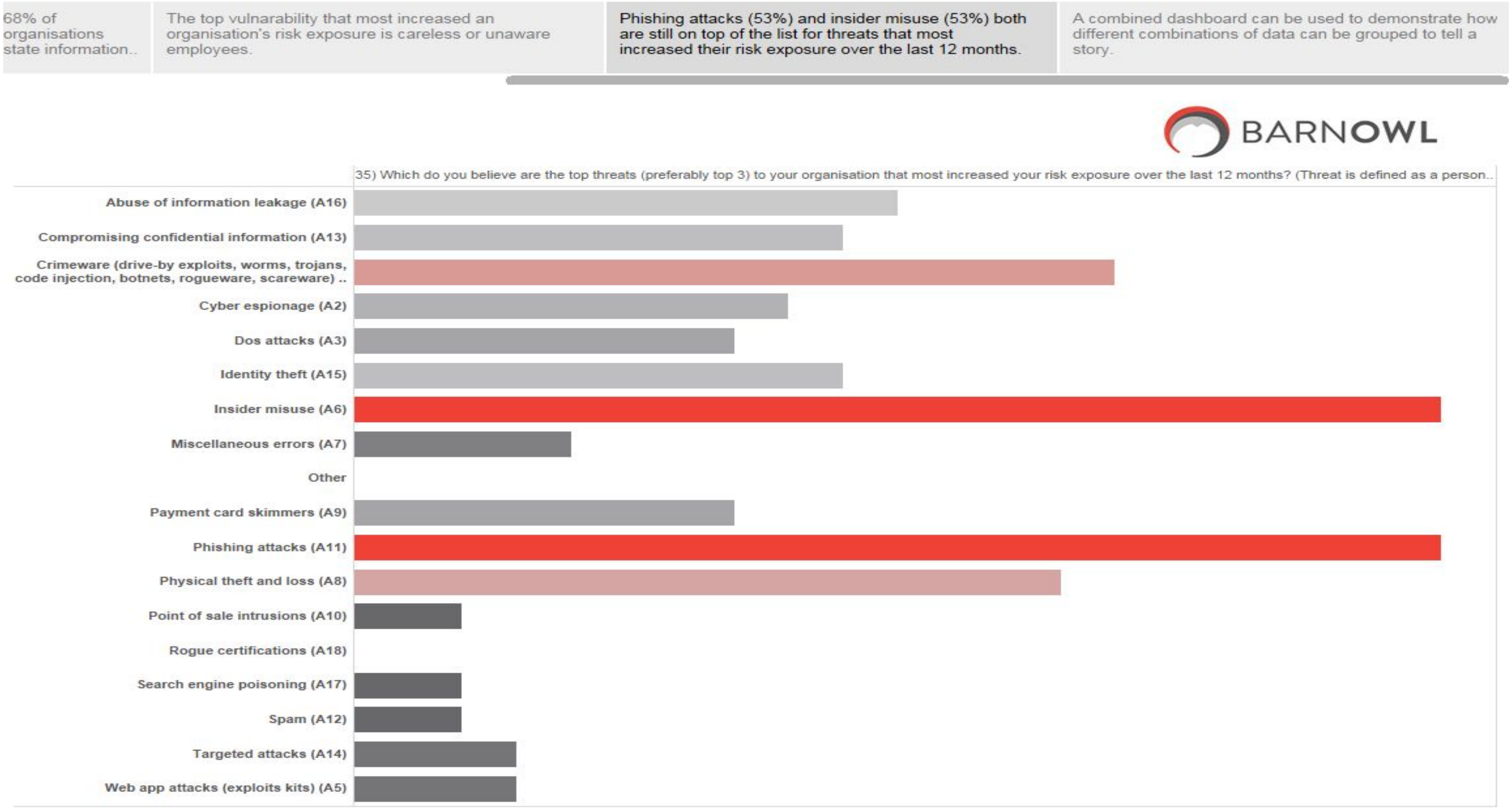
Phishing attacks (53%) and insider misuse (53%) both are still on top of the list for threats that most increased their risk exposure over the last 12 months.

A combined dashboard ca..

33) Which do you believe are the top vulnerabilities (preferably top 3) to your organisation that most increased your risk exposure over the last 12 months? (Vulnerability is defined as a weakness or exposure to the possibility of being attacked or harmed)

BARNOWL
Outdated information security controls or ..
Careless or unaware employees (A3)
Cloud computing use (A4)
Mobile computing use (A5)
Social media use (A6)
Unauthorised access (A7)
Lost or stolen unencrypted electroni..
Improper disposal of paper records or el..
Lack of skills (A10)
Secure coding practices not followe..

INSTITUTIONAL INTELLIGENCE REPORTING



68% of organisations state information..

The top vulnarability that most increased an organisation's risk exposure is careless or unaware employees.

Phishing attacks (53%) and insider misuse (53%) both are still on top of the list for threats that most increased their risk exposure over the last 12 months.

A combined dashboard can be used to demonstrate how different combinations of data can be grouped to tell a story.

35) Which do you believe are the top threats (preferably top 3) to your organisation that most increased your risk exposure over the last 12 months? (Threat is defined as a person..

BARNOWL
Abuse of information leakage (A16)
Compromising confidential information (A13)
Crimeware (drive-by exploits, worms, trojans, code injection, botnets, rogueware, scareware) ..
Cyber espionage (A2)
Dos attacks (A3)
Identity theft (A15)
Insider misuse (A6)
Miscellaneous errors (A7)
Other
Payment card skimmers (A9)
Phishing attacks (A11)
Physical theft and loss (A8)
Point of sale intrusions (A10)
Rogue certifications (A18)
Search engine poisoning (A17)
Spam (A12)
Targeted attacks (A14)
Web app attacks (exploits kits) (A5)

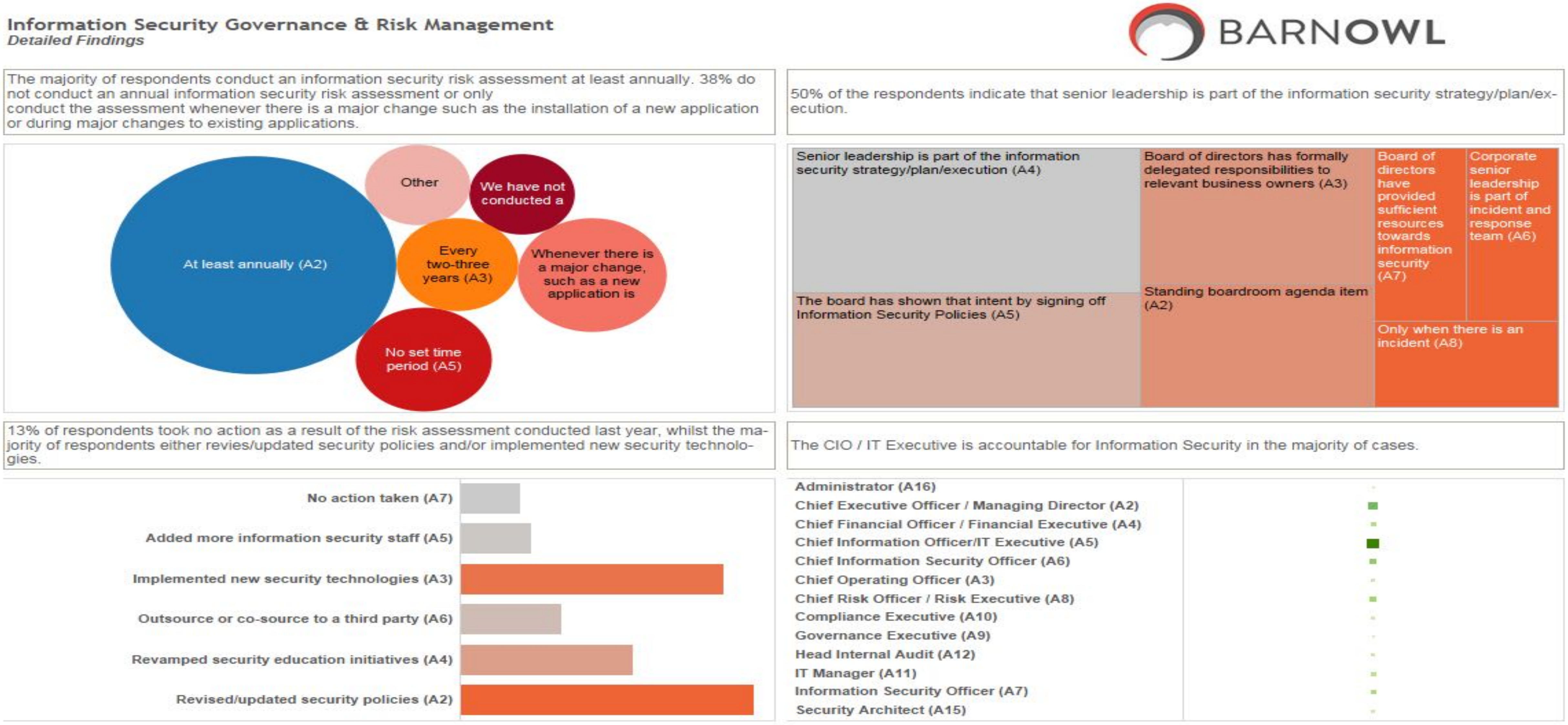
INSTITUTIONAL INTELLIGENCE REPORTING

68% of organisations state information..

The top vulnarability that most increased an organisation's risk exposure is careless or unaware employees.

Phishing attacks (53%) and insider misuse (53%) both are still on top of the list for threats that most increased their risk exposure over the last 12 months.

A combined dashboard can be used to demonstrate how different combinations of data can be grouped to tell a story.



Information Security Governance & Risk Management

Detailed Findings

BARNOWL

The majority of respondents conduct an information security risk assessment at least annually. 38% do not conduct an annual information security risk assessment or only conduct the assessment whenever there is a major change such as the installation of a new application or during major changes to existing applications.

At least annually (A2)
Other
We have not conducted a
Every two-three years (A3)
Whenever there is a major change, such as a new application is
No set time period (A5)

50% of the respondents indicate that senior leadership is part of the information security strategy/plan/execution.

Senior leadership is part of the information security strategy/plan/execution (A4)
The board has shown that intent by signing off Information Security Policies (A5)
Board of directors has formally delegated responsibilities to relevant business owners (A3)
Standing boardroom agenda item (A2)
Board of directors have provided sufficient resources towards information security (A7)
Corporate senior leadership is part of incident and response team (A6)
Only when there is an incident (A8)

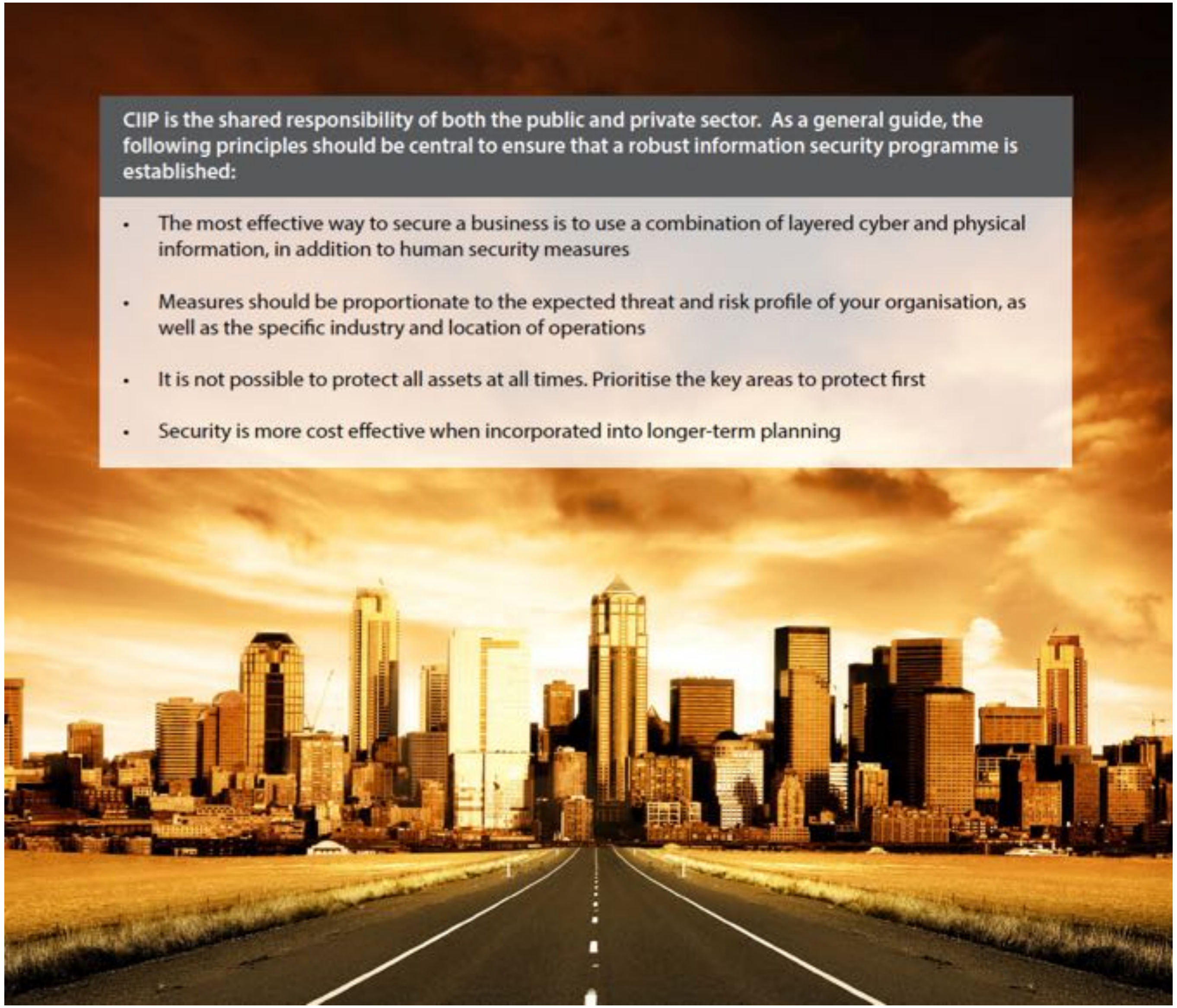
13% of respondents took no action as a result of the risk assessment conducted last year, whilst the majority of respondents either revies/updated security policies and/or implemented new security technologies.

No action taken (A7)
Added more information security staff (A5)
Implemented new security technologies (A3)
Outsource or co-source to a third party (A6)
Revamped security education initiatives (A4)
Revised/updated security policies (A2)

The CIO / IT Executive is accountable for Information Security in the majority of cases.

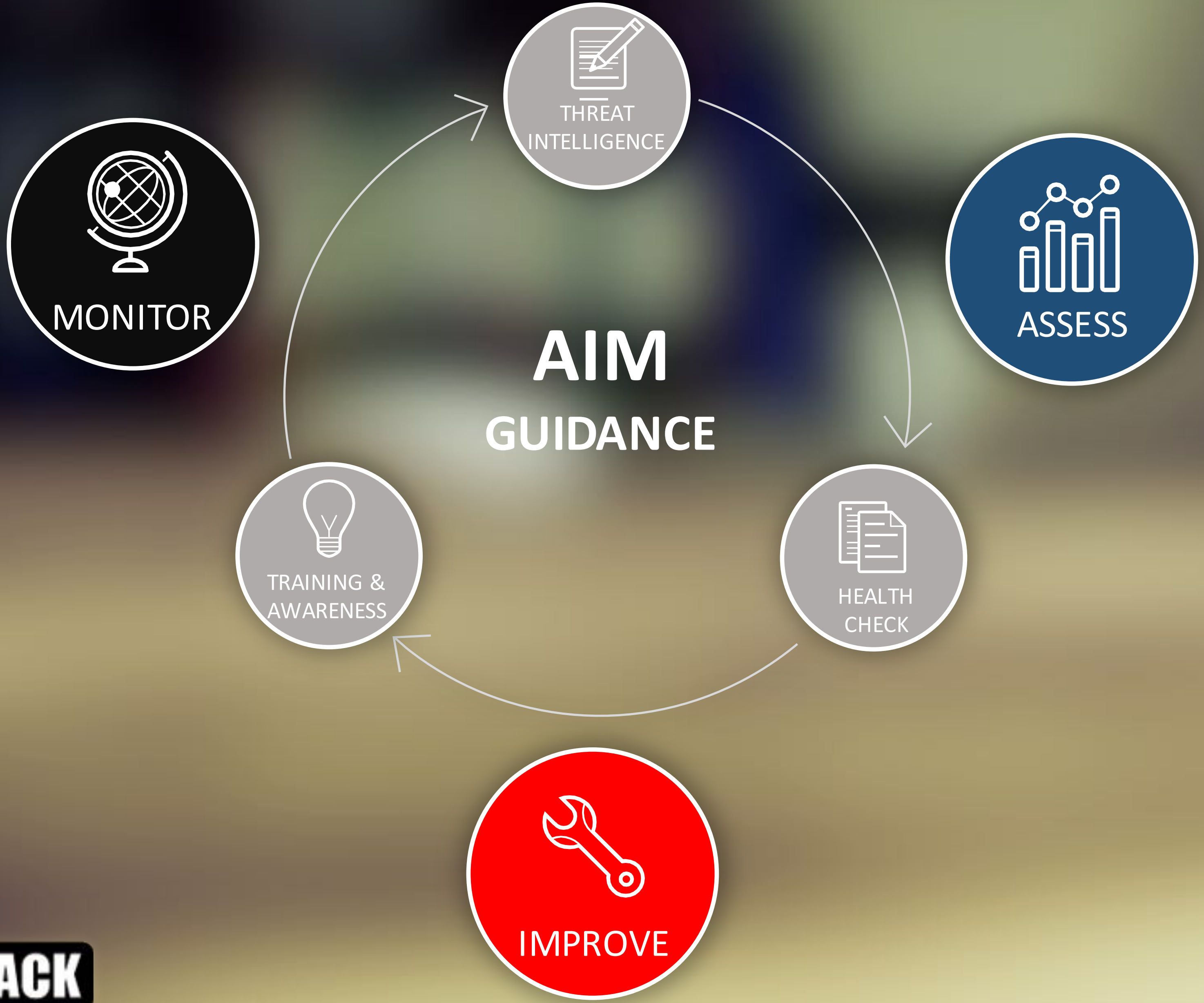
Administrator (A16)
Chief Executive Officer / Managing Director (A2)
Chief Financial Officer / Financial Executive (A4)
Chief Information Officer/IT Executive (A5)
Chief Information Security Officer (A6)
Chief Operating Officer (A3)
Chief Risk Officer / Risk Executive (A8)
Compliance Executive (A10)
Governance Executive (A9)
Head Internal Audit (A12)
IT Manager (A11)
Information Security Officer (A7)
Security Architect (A15)

SA 2016 – THE ROAD AHEAD



CIIP is the shared responsibility of both the public and private sector. As a general guide, the following principles should be central to ensure that a robust information security programme is established:

- The most effective way to secure a business is to use a combination of layered cyber and physical information, in addition to human security measures
- Measures should be proportionate to the expected threat and risk profile of your organisation, as well as the specific industry and location of operations
- It is not possible to protect all assets at all times. Prioritise the key areas to protect first
- Security is more cost effective when incorporated into longer-term planning



AIM
GUIDANCE

MONITOR

THREAT INTELLIGENCE

ASSESS

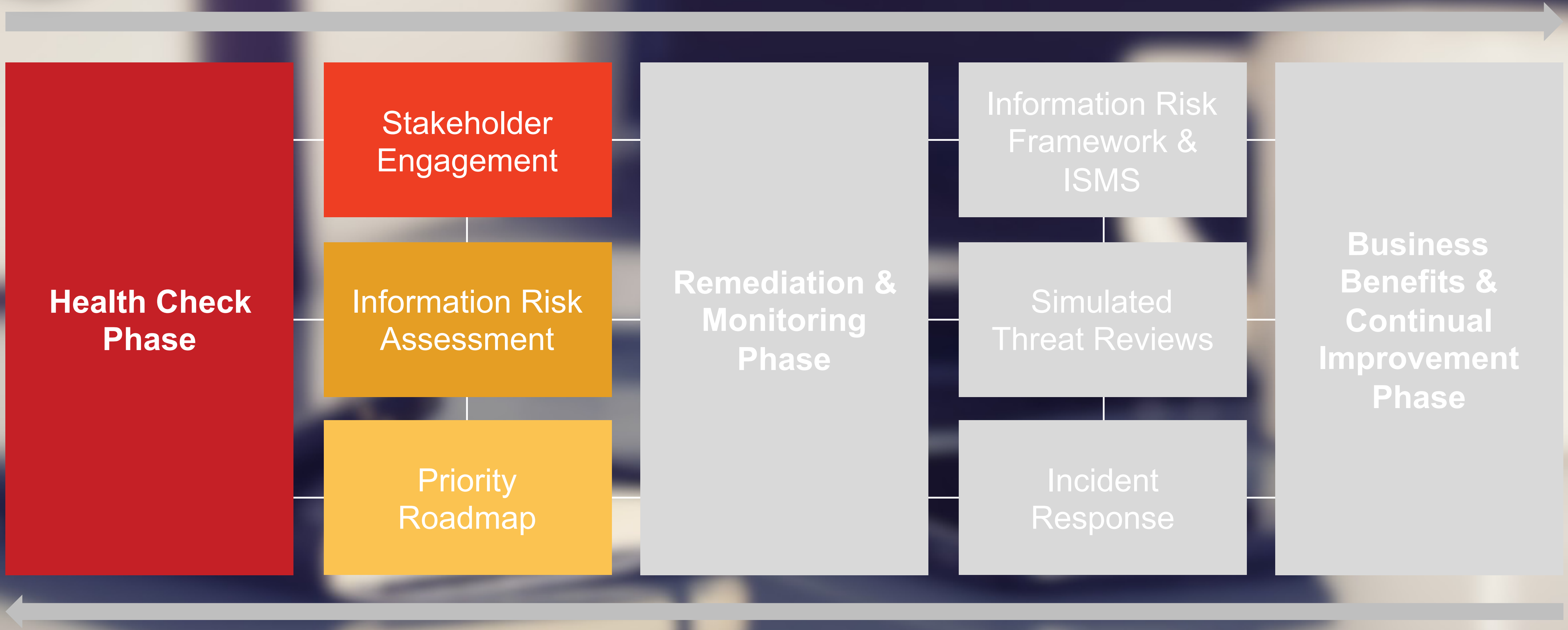
HEALTH CHECK

TRAINING & AWARENESS

IMPROVE

WOLF PACK

ASSESS



Health Check Phase

Stakeholder Engagement

Information Risk Assessment

Priority Roadmap

Remediation & Monitoring Phase

Information Risk Framework & ISMS

Simulated Threat Reviews

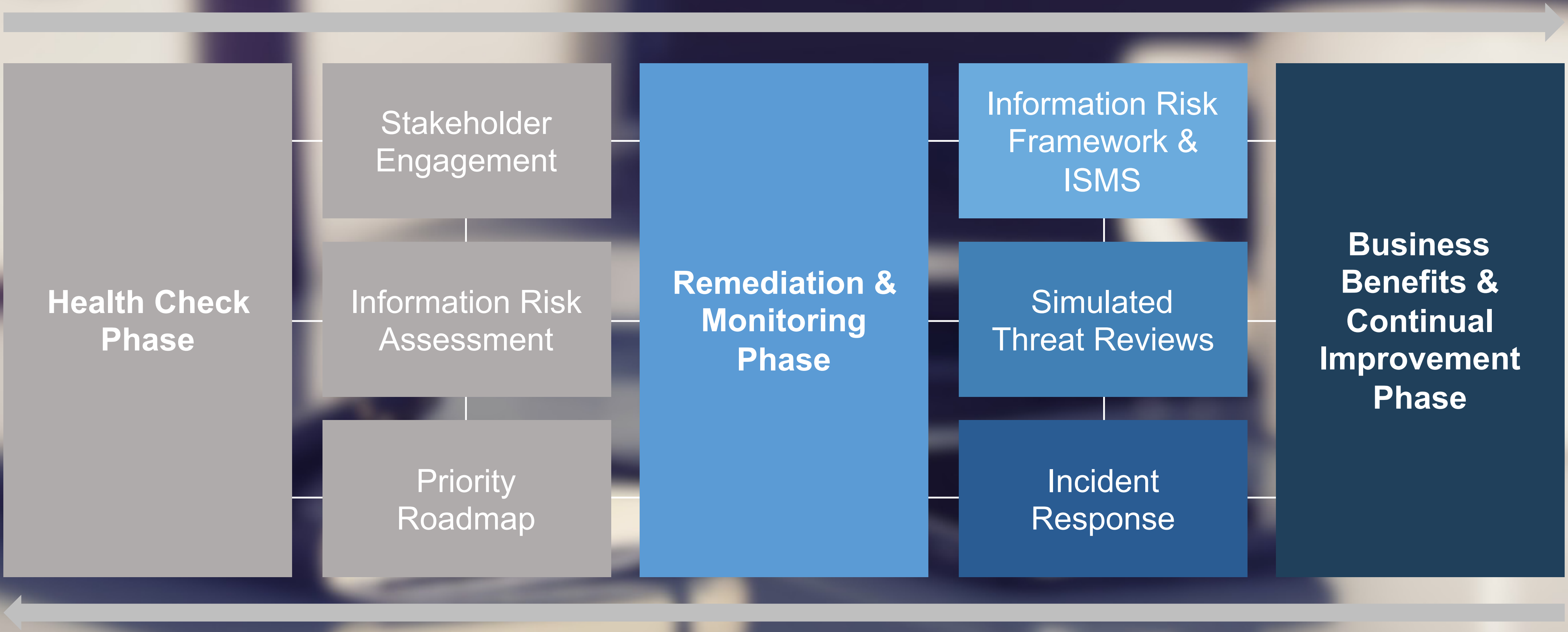
Incident Response

Business Benefits & Continual Improvement Phase

WOLF PACK

IMPROVE

REMEDIATION



Health Check Phase

Stakeholder Engagement

Information Risk Assessment

Priority Roadmap

Remediation & Monitoring Phase

Information Risk Framework & ISMS

Simulated Threat Reviews

Incident Response

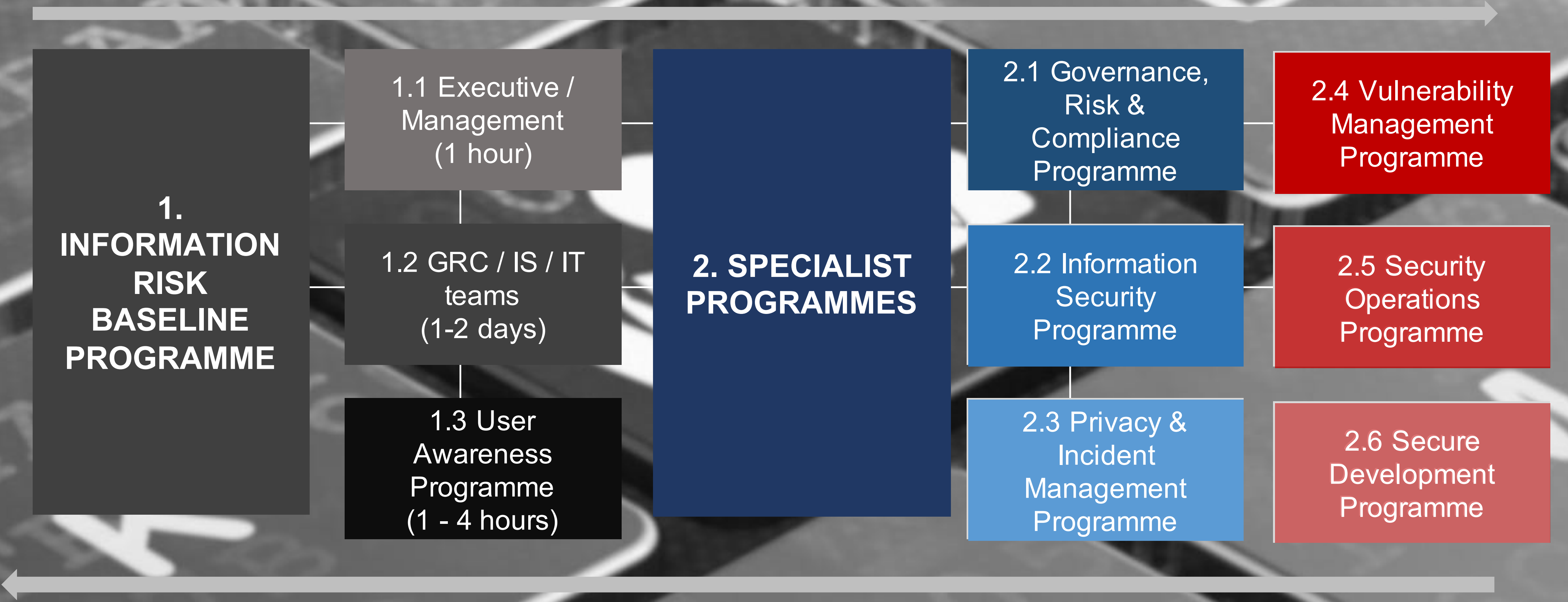
Business Benefits & Continual Improvement Phase

WOLF PACK

IMPROVE

TRAINING & AWARENESS

TRAINING



1. INFORMATION RISK BASELINE PROGRAMME

1.1 Executive / Management (1 hour)

1.2 GRC / IS / IT teams (1-2 days)

1.3 User Awareness Programme (1 - 4 hours)

2. SPECIALIST PROGRAMMES

2.1 Governance, Risk & Compliance Programme

2.2 Information Security Programme

2.3 Privacy & Incident Management Programme

2.4 Vulnerability Management Programme

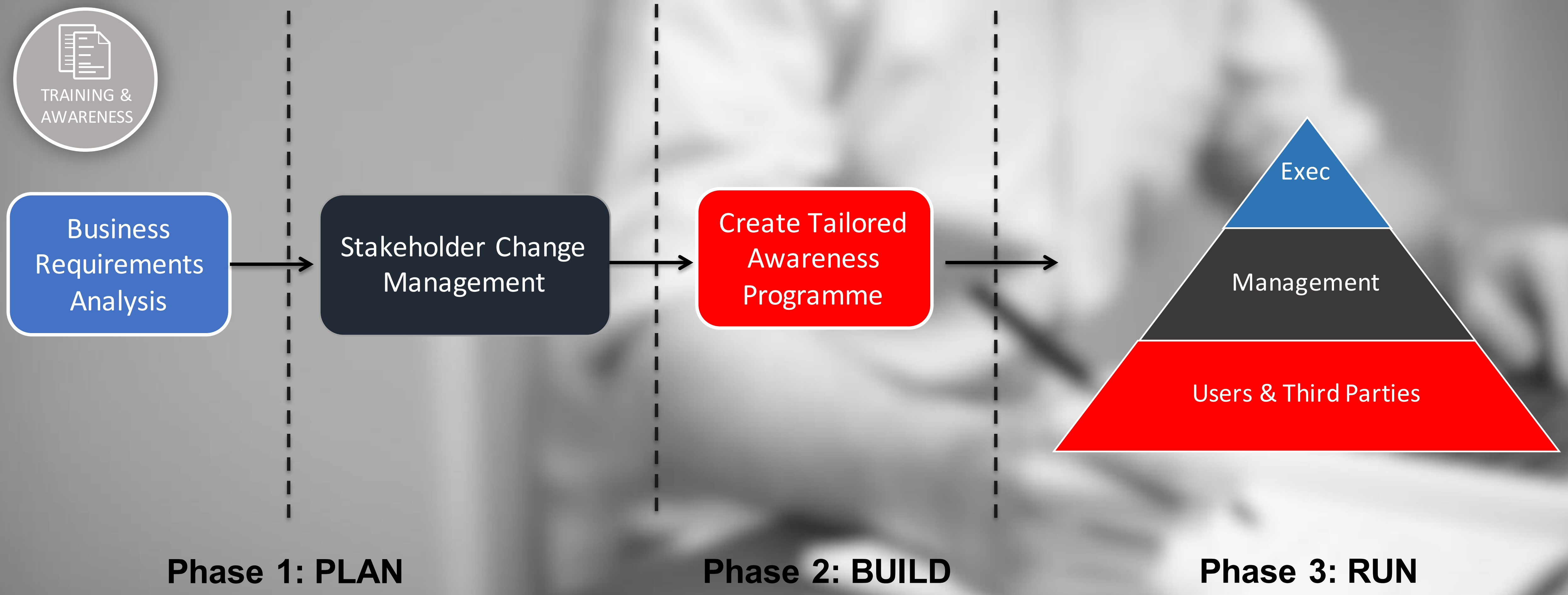
2.5 Security Operations Programme

2.6 Secure Development Programme

IMPROVE

TRAINING & AWARENESS

AWARENESS


Business Requirements Analysis

Stakeholder Change Management

Create Tailored Awareness Programme

Phase 1: PLAN

Phase 2: BUILD

Phase 3: RUN

WOLF PACK

HUMAN VULNERABILITY TESTING

COVERT CALLING

WOLF PACK

MONITOR

Threat Intelligence

- ✓ Global & local threat feeds

Asset Discovery

- ✓ Know your assets

Continuous Monitoring

- ✓ Identify suspicious behaviour

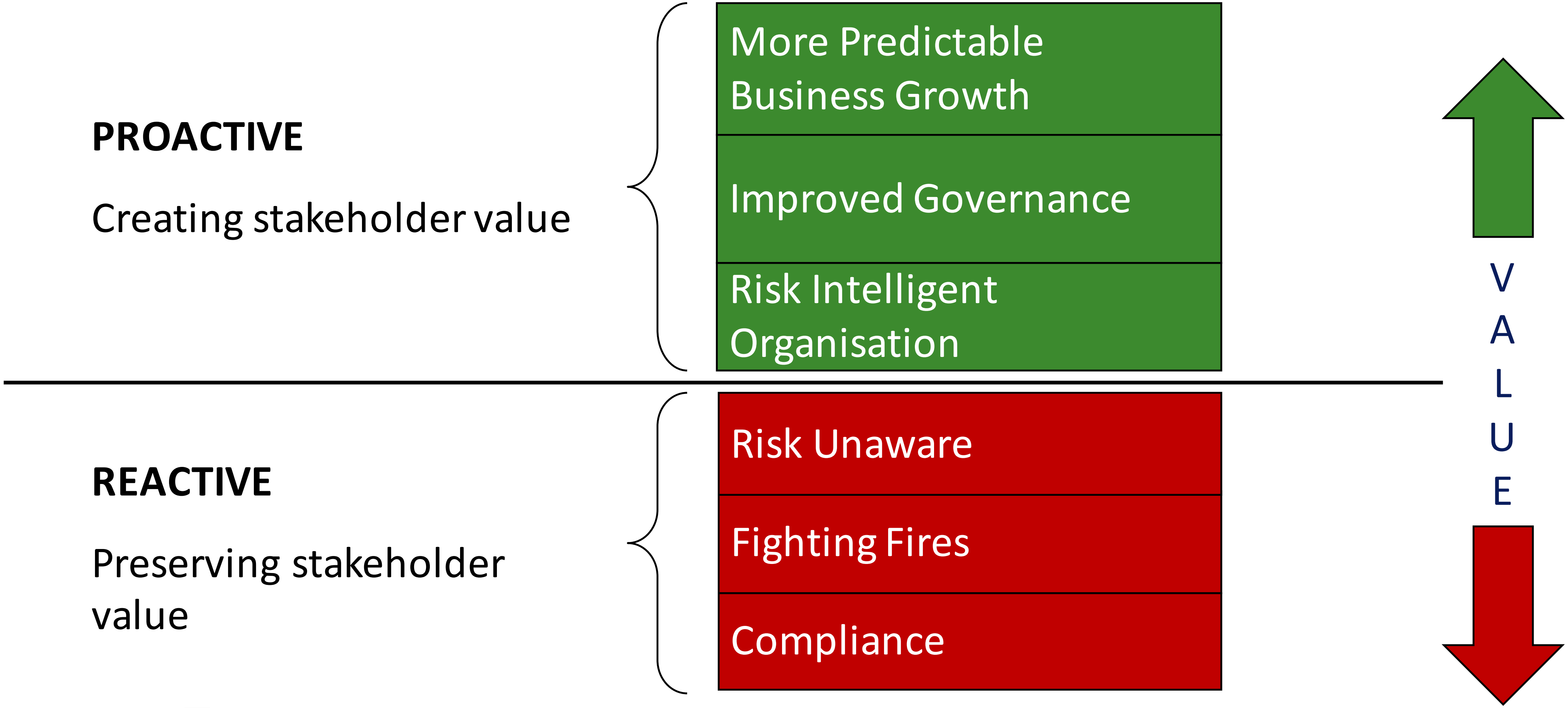
Vulnerability Assessments

- ✓ Effectively identify vulnerabilities

Threat Management

- ✓ Determine threat to your organisation

BALANCING RISK & REWARD



PROACTIVE

Creating stakeholder value

More Predictable Business Growth

Improved Governance

Risk Intelligent Organisation

REACTIVE

Preserving stakeholder value

Risk Unaware

Fighting Fires

Compliance

VALUE

Wolfpack Information Risk (Pty) Ltd

Protection in the pack

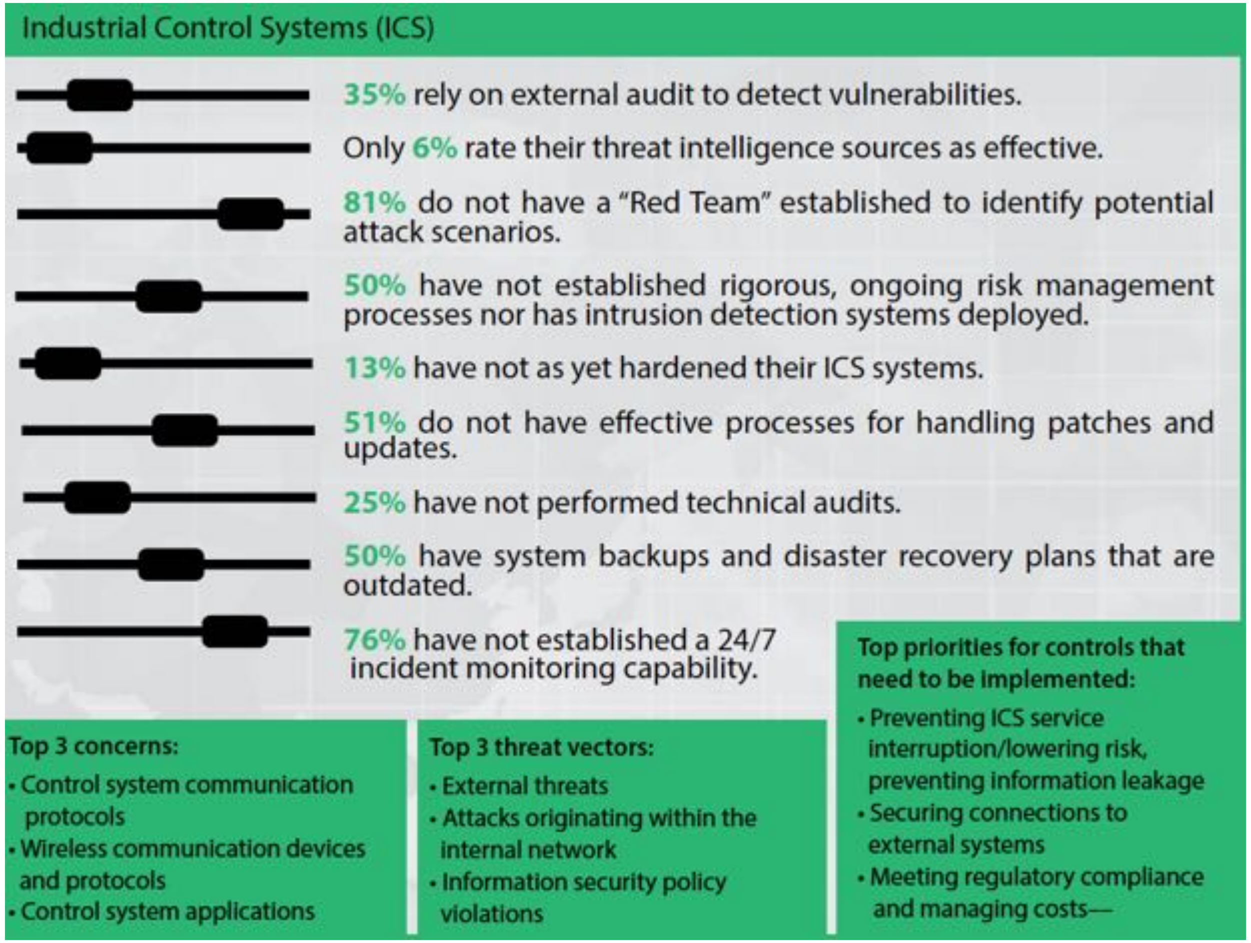
info@wolfpackrisk.com
www.wolfpackrisk.com

Threat Intelligence| Advisory | Training | Awareness

BARNOWL

FULLY INTEGRATED GOVERNANCE, RISK MANAGEMENT, COMPLIANCE
AND AUDIT SOFTWARE
www.barnowl.co.za

REPORT – HIGHLIGHTS



Industrial Control Systems (ICS)

35% rely on external audit to detect vulnerabilities.

Only 6% rate their threat intelligence sources as effective.

81% do not have a “Red Team” established to identify potential attack scenarios.

50% have not established rigorous, ongoing risk management processes nor has intrusion detection systems deployed.

13% have not as yet hardened their ICS systems.

51% do not have effective processes for handling patches and updates.

25% have not performed technical audits.

50% have system backups and disaster recovery plans that are outdated.

76% have not established a 24/7 incident monitoring capability.

Top 3 concerns:

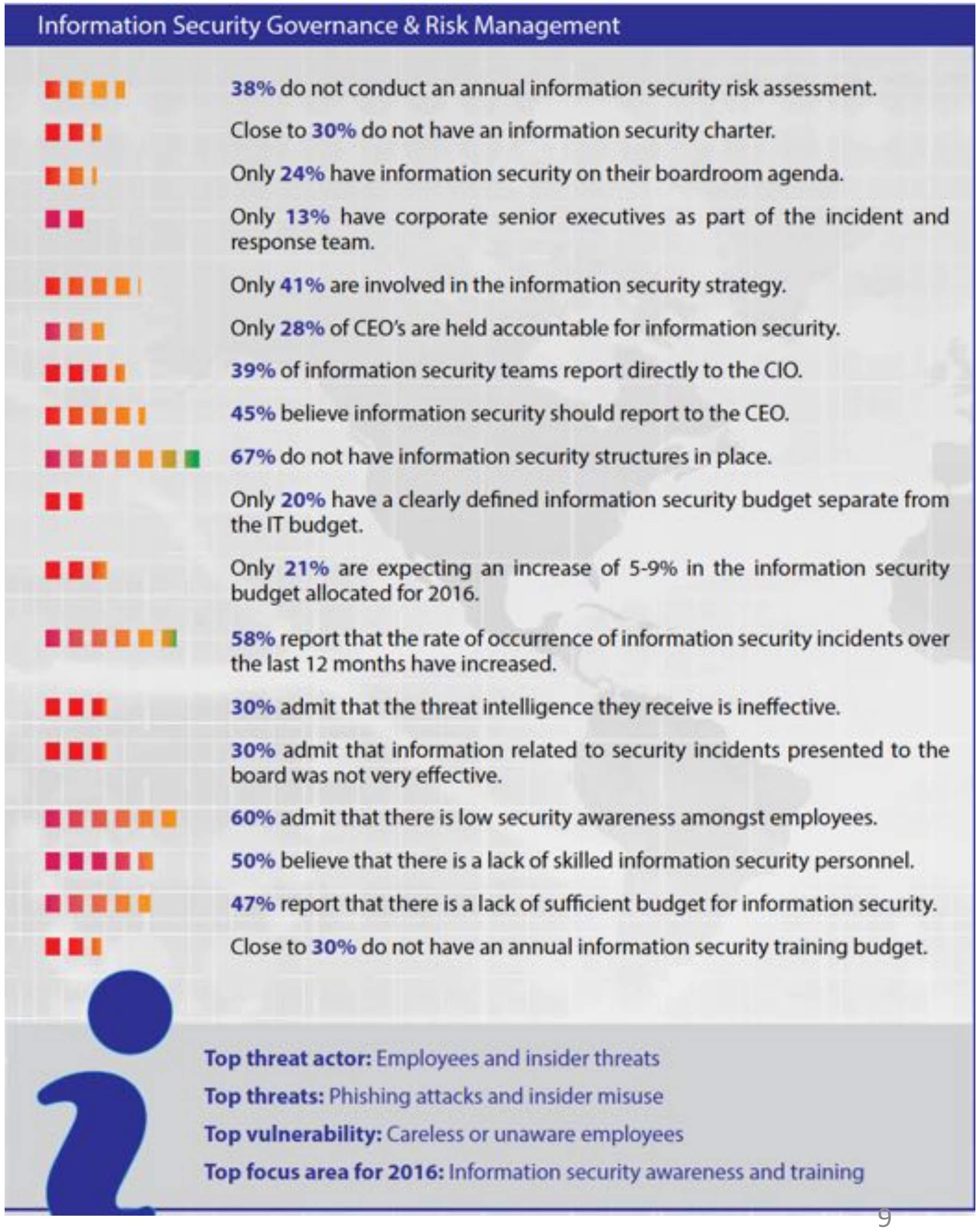
- Control system communication protocols
- Wireless communication devices and protocols
- Control system applications

Top 3 threat vectors:

- External threats
- Attacks originating within the internal network
- Information security policy violations

Top priorities for controls that need to be implemented:

- Preventing ICS service interruption/lowering risk, preventing information leakage
- Securing connections to external systems
- Meeting regulatory compliance and managing costs—



Information Security Governance & Risk Management

38% do not conduct an annual information security risk assessment.

Close to 30% do not have an information security charter.

Only 24% have information security on their boardroom agenda.

Only 13% have corporate senior executives as part of the incident and response team.

Only 41% are involved in the information security strategy.

Only 28% of CEO's are held accountable for information security.

39% of information security teams report directly to the CIO.

45% believe information security should report to the CEO.

67% do not have information security structures in place.

Only 20% have a clearly defined information security budget separate from the IT budget.

Only 21% are expecting an increase of 5-9% in the information security budget allocated for 2016.

58% report that the rate of occurrence of information security incidents over the last 12 months have increased.

30% admit that the threat intelligence they receive is ineffective.

30% admit that information related to security incidents presented to the board was not very effective.

60% admit that there is low security awareness amongst employees.

50% believe that there is a lack of skilled information security personnel.

47% report that there is a lack of sufficient budget for information security.

Close to 30% do not have an annual information security training budget.

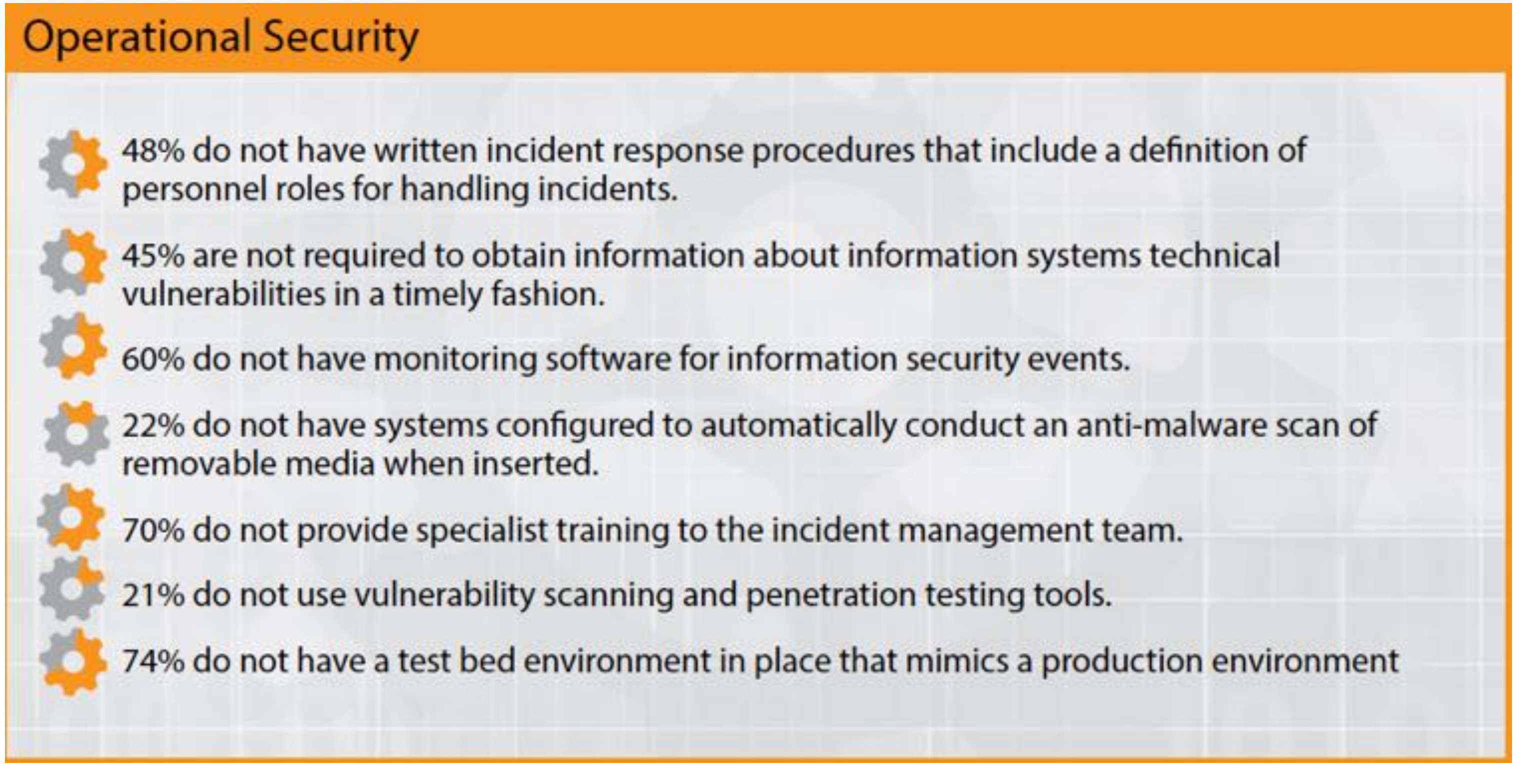
Top threat actor: Employees and insider threats

Top threats: Phishing attacks and insider misuse

Top vulnerability: Careless or unaware employees

Top focus area for 2016: Information security awareness and training

SA 2016 CIIP REPORT – HIGHLIGHTS



Operational Security

- 48% do not have written incident response procedures that include a definition of personnel roles for handling incidents.
- 45% are not required to obtain information about information systems technical vulnerabilities in a timely fashion.
- 60% do not have monitoring software for information security events.
- 22% do not have systems configured to automatically conduct an anti-malware scan of removable media when inserted.
- 70% do not provide specialist training to the incident management team.
- 21% do not use vulnerability scanning and penetration testing tools.
- 74% do not have a test bed environment in place that mimics a production environment