Resilience
Cyber Defence
Awareness
Preparedness

OPTIMAL RISK

Be Prepared. For Anything

Cyber Security - Confronting Current & Future Threats

The role of skilled professionals in maintaining cyber resilience

Mike O’Neill – Managing Director   *Graeme McGowan – Associate Director of Cyber Security*

Be Very Worried

OPTIMAL RISK

Be Prepared. For Anything

Timespan of events by % of Web App breaches	Seconds	Minutes	Hours	Days	Weeks	Months	Years
Compromise	19%	42%	12%	23%	0%	5%	1%
Exfiltration	3%	27%	21%	21%	18%	9%	0%
Discovery	0%	3%	11%	17%	16%	41%	11%
Containment	0%	2%	5%	42%	22%	29%	0%

40% of companies experienced a data breach

In 50% of breaches, data is stolen in hours

41% of breaches are not discovered for months

61% of espionage is not discovered for months

34% of companies do not know if/how

51% increase of companies reporting >$10M loss

38% of companies are not capable of resolving an attack

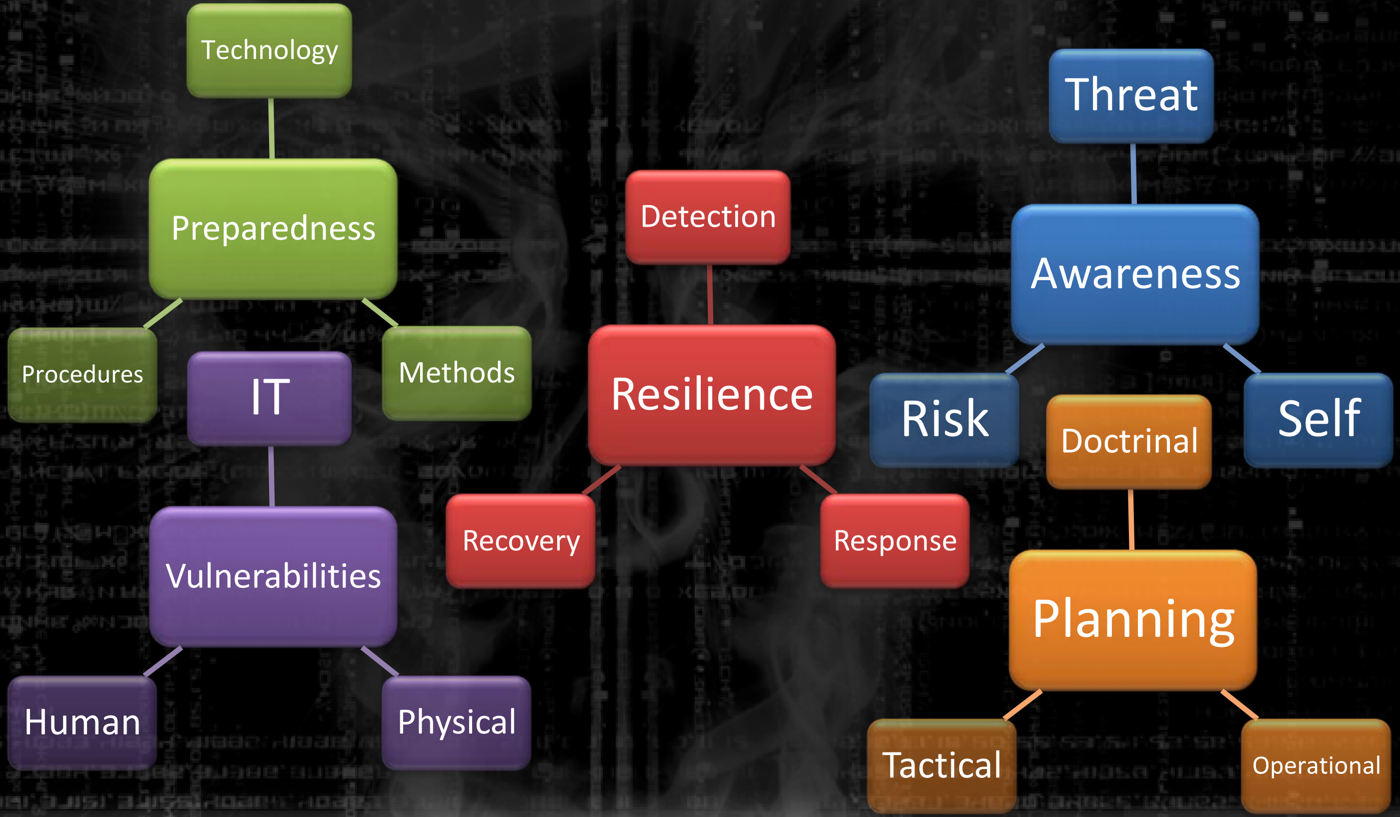
More than 50% of companies do NOT conduct security testing

Source: 2014 Verizon Data Breach Investigations Report

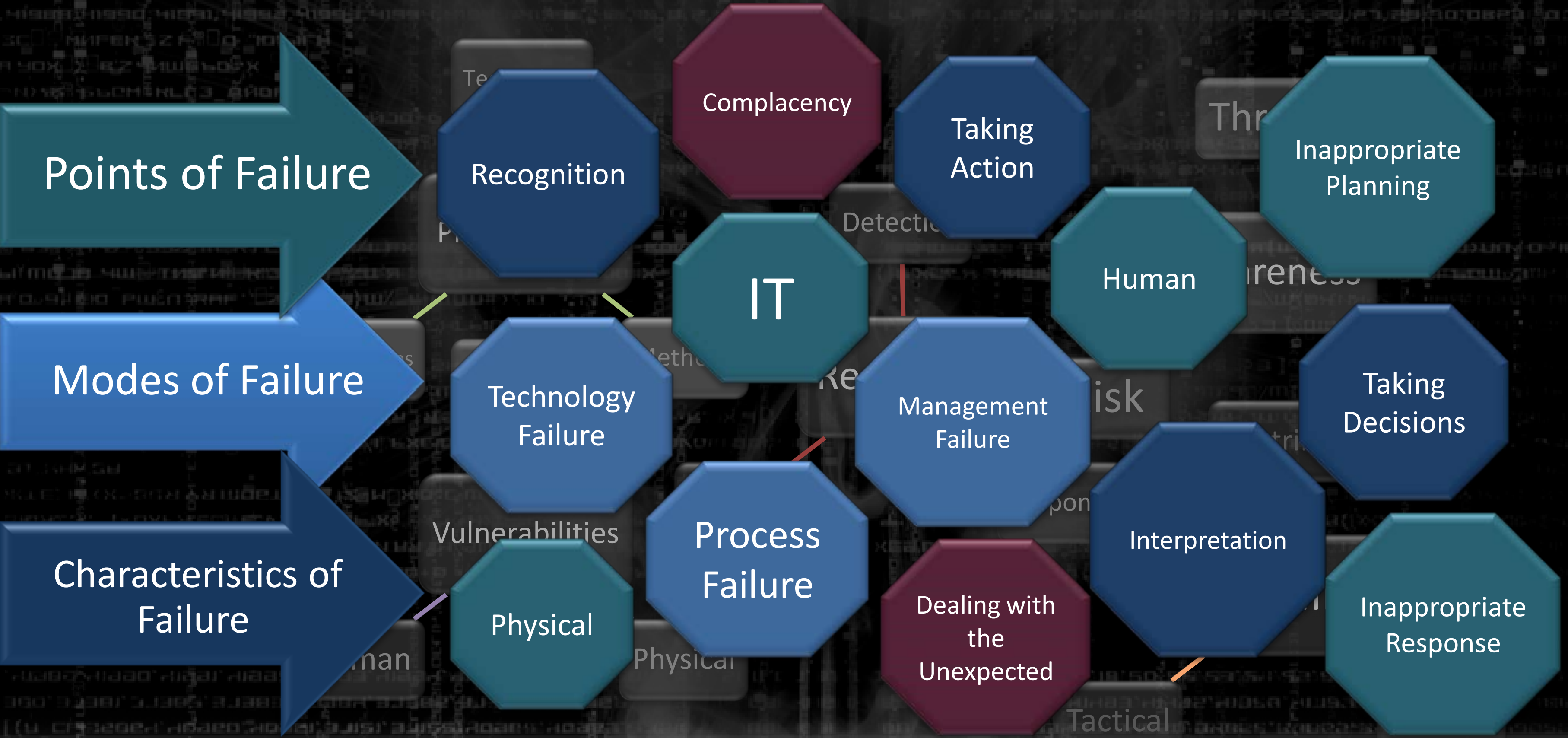
Common Challenges

Optimal Risk

Be Prepared. For Anything



How Resilience Fails



Points of Failure

Modes of Failure

Characteristics of Failure

Recognition

Complacency

Taking Action

Inappropriate Planning

IT

Human

Technology Failure

Management Failure

Taking Decisions

Process Failure

Physical

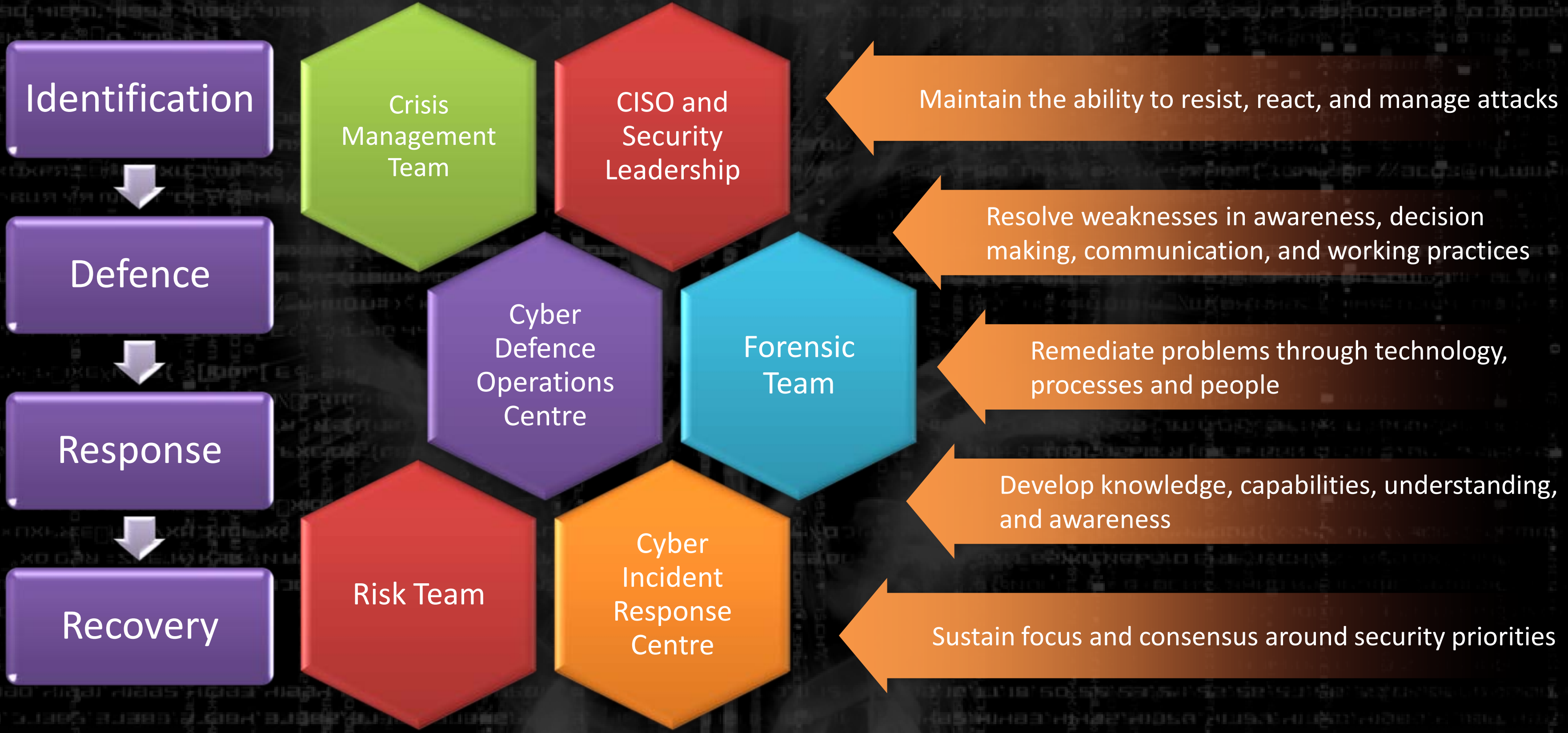
Dealing with the Unexpected

Interpretation

Inappropriate Response

OPTIMAL RISK
Be Prepared. For Anything

Resilience Organisation



Identification

Defence

Response

Recovery

Crisis Management Team

CISO and Security Leadership

Cyber Defence Operations Centre

Forensic Team

Risk Team

Cyber Incident Response Centre

Maintain the ability to resist, react, and manage attacks

Resolve weaknesses in awareness, decision making, communication, and working practices

Remediate problems through technology, processes and people

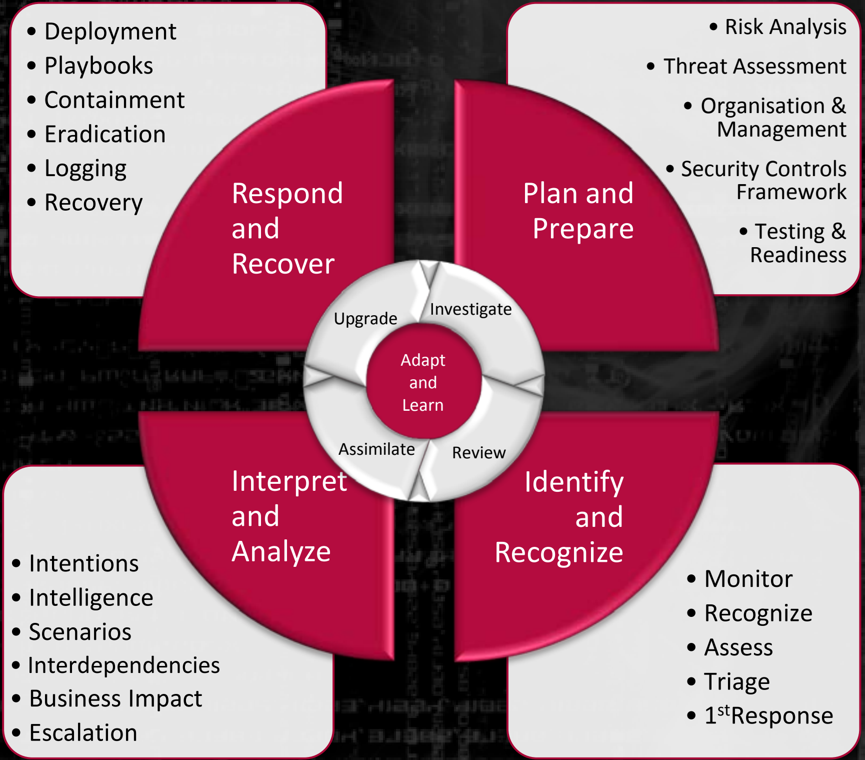
Develop knowledge, capabilities, understanding, and awareness

Sustain focus and consensus around security priorities

Why is it so difficult?

Complexity: Multiple teams, Complex management & Planning	• Attackers will create and exploit complexity and fault lines
Integration: Technologies with Methodologies with Procedures	• Attacker Perspective: The disjoint offers open doors
Escalation: Scenario understanding, Familiarity, Agility	• Attackers will seek to exploit a lack of ‘depth’
Anticipation: Insight – Foresight - Awareness	• Attackers have the upper-hand and retain the initiative
Interpretation: Intelligence, Analysis, Learning, and its Application	• Attackers are quicker – and will exploit your ‘bias’

Assessing Maturity



- Deployment
- Playbooks
- Containment
- Eradication
- Logging
- Recovery

Respond and Recover

Plan and Prepare

- Risk Analysis
- Threat Assessment
- Organisation & Management
- Security Controls Framework
- Testing & Readiness

Upgrade

Investigate

Adapt and Learn

Assimilate

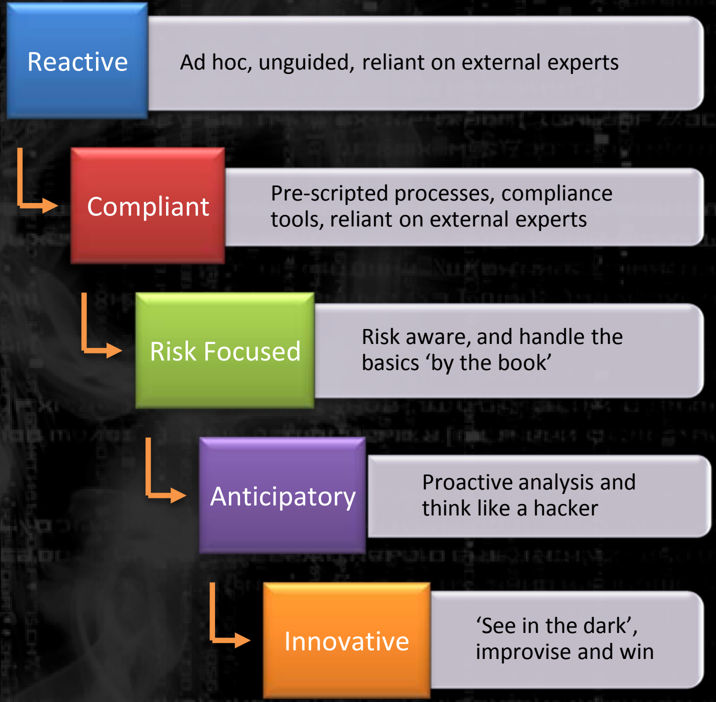
Review

Interpret and Analyze

- Intentions
- Intelligence
- Scenarios
- Interdependencies
- Business Impact
- Escalation

Identify and Recognize

- Monitor
- Recognize
- Assess
- Triage
- 1st Response



Reactive	Ad hoc, unguided, reliant on external experts
Compliant	Pre-scripted processes, compliance tools, reliant on external experts
Risk Focused	Risk aware, and handle the basics ‘by the book’
Anticipatory	Proactive analysis and think like a hacker
Innovative	‘See in the dark’, improvise and win

Why Resilience Fails

Outdated Assumptions

Competing Priorities

Assessing Probabilities

Silos

Converged Threat Awareness

Misaligned Strategy

Reactive approach

Risk

Vulnerability Scanning

Cultural Myopia

Leadership

Perspectives on ‘Cold War’

Budgets

Risk-Informed

Accepting Mediocrity

Analytical Bias

Dealing with Complexity

Outdated methods

Information Assurance

Cost

Analytical Failure

Silver Bullets

Board-level Consensus

Tackling Uncertainty

Formalised Policy & Planning

Symptoms of Delusion

Insurance

Inertia

Ignorance

Complacency

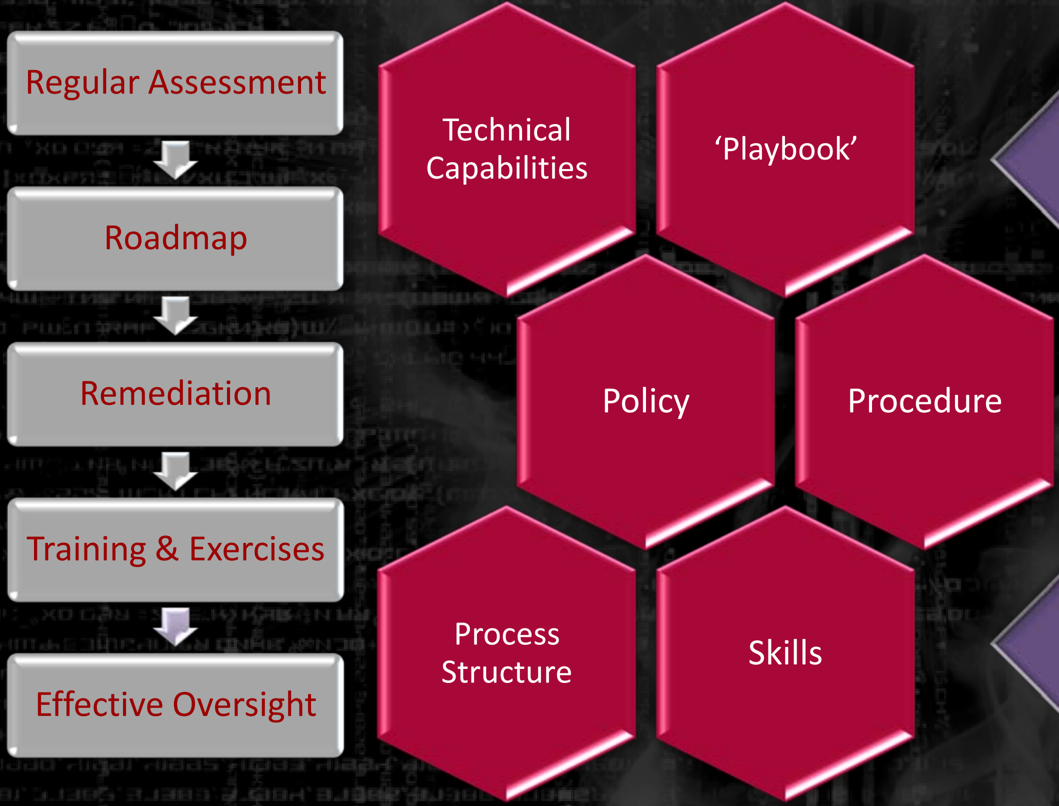
Compliance

Intelligence

Ineffective Capability

Forewarning

What Does it Take?



Regular Assessment → Roadmap → Remediation → Training & Exercises → Effective Oversight

Technical Capabilities

‘Playbook’

Policy

Procedure

Process Structure

Skills

Establish MONITORING processes to test adoption of initiatives, controls and measures to build confidence in security and a high state of readiness.

Establish CONTINUOUS IMPROVEMENT program for measurement, development and learning processes.

Establish MANAGEMENT program organisational processes, and infrastructure, that will provide governance & direction towards objectives.

Assurance Program Set-up

OPTIMAL RISK

Be Prepared. For Anything

Objectives

Monitoring

- Program Objectives
- Desired End State View
- Embed Evaluative Processes
- Regular Testing
- Assessment Schedule
- Current State of Readiness
- Ongoing Gap Analysis
- Operational Priorities

Capabilities
Playbook
Policy
Procedures
Skills

- **Investigate**:
  the degree to which organizational readiness is appropriate, complete and effective.
- **Evaluate**:
  IR planning, capabilities, and procedures are, and under which conditions they are more likely to fail.

Practise! Practise! Practise!

① How your security organisation enacts ‘playbook’ responses to cyber incidents

② How security professionals work with technology, methods, and procedures

③ How security leadership adapts plans and responses to unexpected aspects

④ How different teams work together on complex challenges

If you identified a breach could you resolve it?

If you had a breach could you detect it?

Could you accurately & quickly assess impact?

Have you prepared for worst case scenario?

The early stages are designed to test the teams’ abilities:

- To detect & analyse malware
- To identify loss of command & control
- To assimilate threat intelligence
- To ‘triage’ technical attacks.

Subsequent evolutions examine:

- The management of ‘triage’ under different conditions
- The organisational & procedural aspects of coordinating a multi-faceted response.
- The management of ‘crises’ in the face of a targeted cyber attack

Targeted by Advanced Attackers

Be Prepared. For Anything

A coordinated attack in an attempt to cripple the client has caused widespread damage.

Sensitive data has been leaked and the client's website has been defaced.

Information about the attack itself leaks and goes viral on social media, with reference to a cyber 9/11, and causes severe reputational consequences.

Growing fears about the state of the client's well-being leads to pressure from the client's customers, and eventually…….. the regulator.

This pressure is intensified by continued cyber-attacks that affect customer data.

Triage Basics?

1. Who should be part of the response team:
   - Who should call on the response team?
   - Who should manage such an event?
   - Does he know who should be attended in each type of event?
   - Does it work in reality?
   - Clear triggers for initiating a forensic investigation (post-mortem and in-action)?

2. Who initiates an in-action forensic investigation?
   - Do they have the proper means?
   - Can the team cover the needed scope?
   - Do they have sufficient training?
   - Do they have sufficient experience and practice?
   - What is the scope of each team? (incident response and forensic team)

3. Does the forensic team know what they can get from each of the available security systems at their disposal?
4. Is there a documented process for assessing the infected system and its implications?
5. How is it determined that a threat has been completely eliminated?

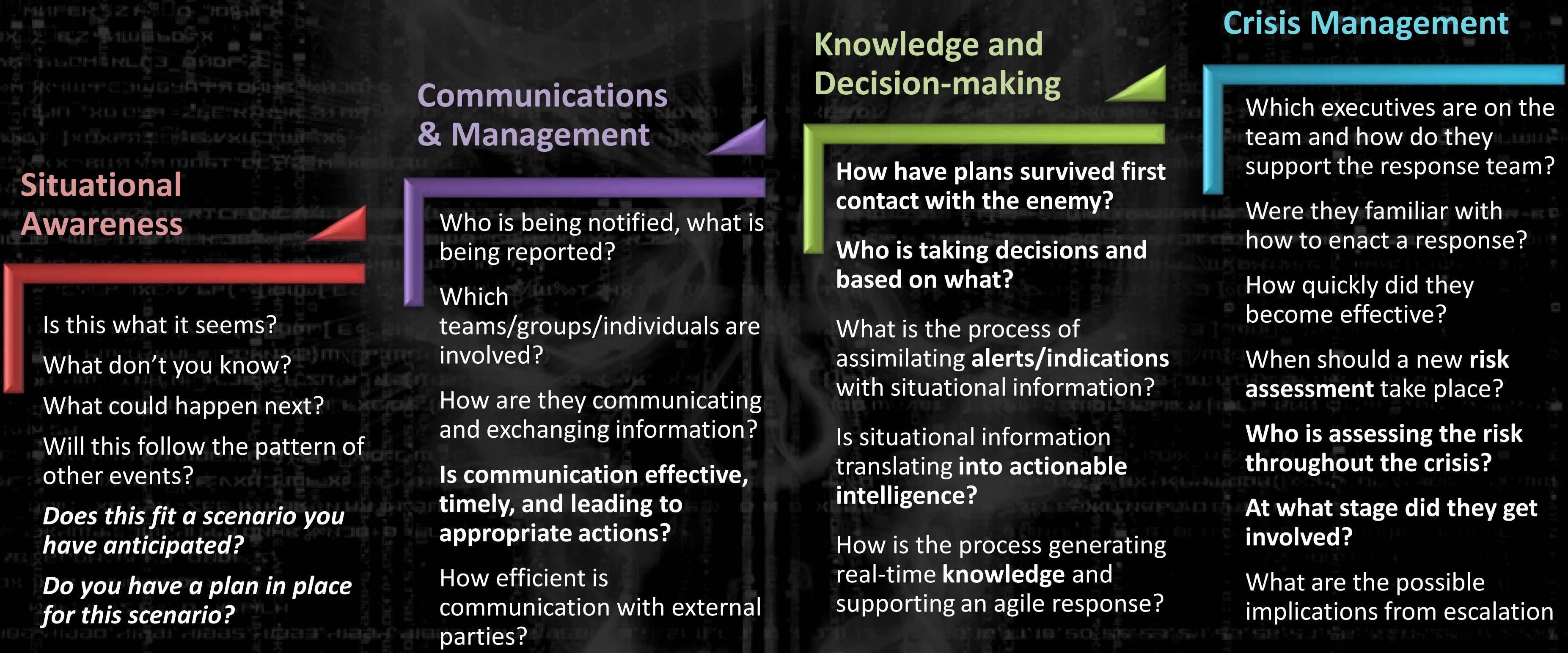
Incident Management

- How well do security principals manage and lead a cyber-attack crisis?
- How well does the security organization responds to a cyber-attack?
- How consistently and how efficient is reporting to upper management?
- Is there a documented and familiar policy regarding when and how to switch between incident response and crisis management?
- Can the immediate threats be detected? Can the risks that stem from them be understood and neutralized?
- Can the participants understand the attacker’s intentions and way of thinking in order to proactively neutralize them?

Managerial Processes & Capabilities

OPTIMAL RISK

Be Prepared. For Anything



Situational Awareness

Is this what it seems?

What don't you know?

What could happen next?

Will this follow the pattern of other events?

Does this fit a scenario you have anticipated?

Do you have a plan in place for this scenario?

Communications & Management

Who is being notified, what is being reported?

Which teams/groups/individuals are involved?

How are they communicating and exchanging information?

Is communication effective, timely, and leading to appropriate actions?

How efficient is communication with external parties?

Knowledge and Decision-making

How have plans survived first contact with the enemy?

Who is taking decisions and based on what?

What is the process of assimilating **alerts/indications** with situational information?

Is situational information translating **into actionable intelligence?**

How is the process generating real-time **knowledge** and supporting an agile response?

Crisis Management

Which executives are on the team and how do they support the response team?

Were they familiar with how to enact a response?

How quickly did they become effective?

When should a new **risk assessment** take place?

Who is assessing the risk throughout the crisis?

At what stage did they get involved?

What are the possible implications from escalation

The more common problems?

- Lack of Intelligence
- Too many signals or noise
- Early Warning?
- Pinning Hopes on Technology
- Coping with the familiar
- Analytical Bias
- Obsession with ‘The Probable’
- Lack of Options

Concerns

- Skills and Experience
- Lack of ‘Maturity’
- Security Testing Only?
- Desk-top ‘exercise’
- Proper ‘expert’ scrutiny?
- Lack of Familiarity!
- Lack of Options!

Be Prepared

- ✓ *uncertainty is the essence of war, surprise its rule*
- ✓ Embrace the attackers view
- ✓ Accelerate your Maturity
- ✓ Practice makes Perfect
- ✓ Develop a Preoccupation with Causes of Failure
- ✓ A Commitment to Proactive Defence

Optimal Risk

Be Prepared. For Anything

Optimal Risk

Dan Solomon
Director, Cyber Risk & Resilience Services

Email: **dan.solomon@optimalrisk.com**

Advanced Cyber Defence Services

Resilience
Cyber Defence
Preparedness
Awareness