If you liked it, you should have put security on it

Zoë Rose and Dean Kelshall

24 October 2018

OWASP
Open Web Application
Security Project

Whoami
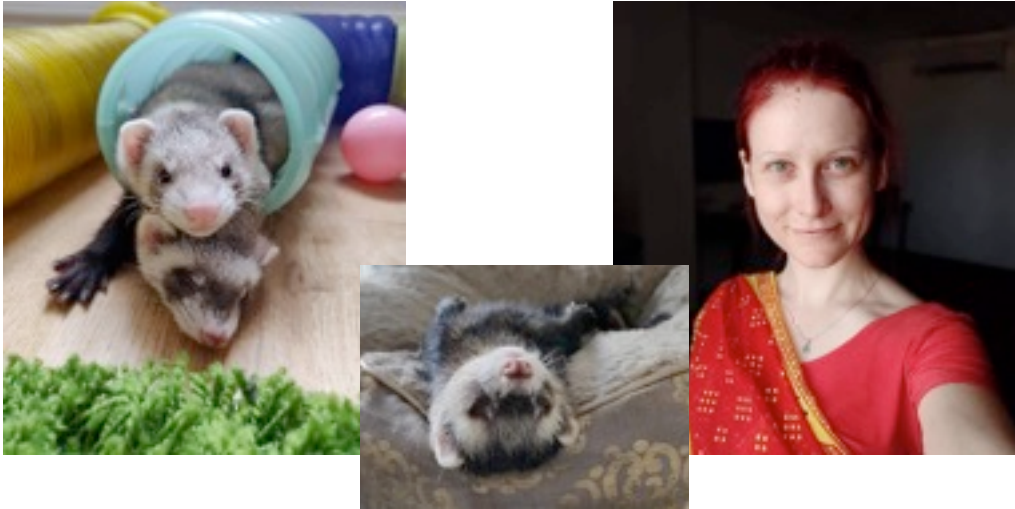
- Ethical hacker

- Certified Splunk Architect and Cisco Champion

- Focused on human behaviour and understanding motivations in regards to cyber security

zoe.rose@Baringa.com

- 5 Years at Baringa as a Consultant

- Cybersecurity, Architecture and Smart Metering

- Passionate about the organisational challenges for cybersecurity

dean.kelshall@Baringa.com

Agenda

Baringa

► How did we get here

► What's going on

► Demystify Hackers

► Lesson 1: Identify the right people

► Lesson 2: Speak the same language

► Lesson 3: Maintain your cyber security programme

► Where to start in our personal and professional lives

zoe.rose@Baringa.com

dean.kelshall@Baringa.com

How did we get here?

Fail by Design

International Access

National Regulations

- ▲ How many people do you talk to in a day?
- ▲ How many apps do you use to connect?
- ▲ Designed to 'just work'
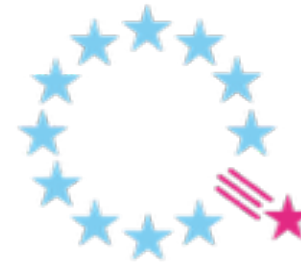- ▲ Inbuilt anonymity, leads to abuse

Inconsistent Boarders

Ease of Use

Limited Reach

zoe.rose@Baringa.com

dean.kelshall@Baringa.com

What is going on in our world?

Designed to Collaborate ◄
Information Sharing ◄
Anonymity ◄
Difficult to Prosecute ◄

Increasing Breaches

Consumer Choice
► Right to be informed
► Right of Access
► Right to Erasure
► Granularity of Controls
► Personal Choice

Increasing Agency

Innovation ◄
Rapid Market Entry ◄

Increasing Vulnerabilities

Increasing Regulation

Increasing Awareness

zoe.rose@Baringa.com

dean.kelshall@Baringa.com

5
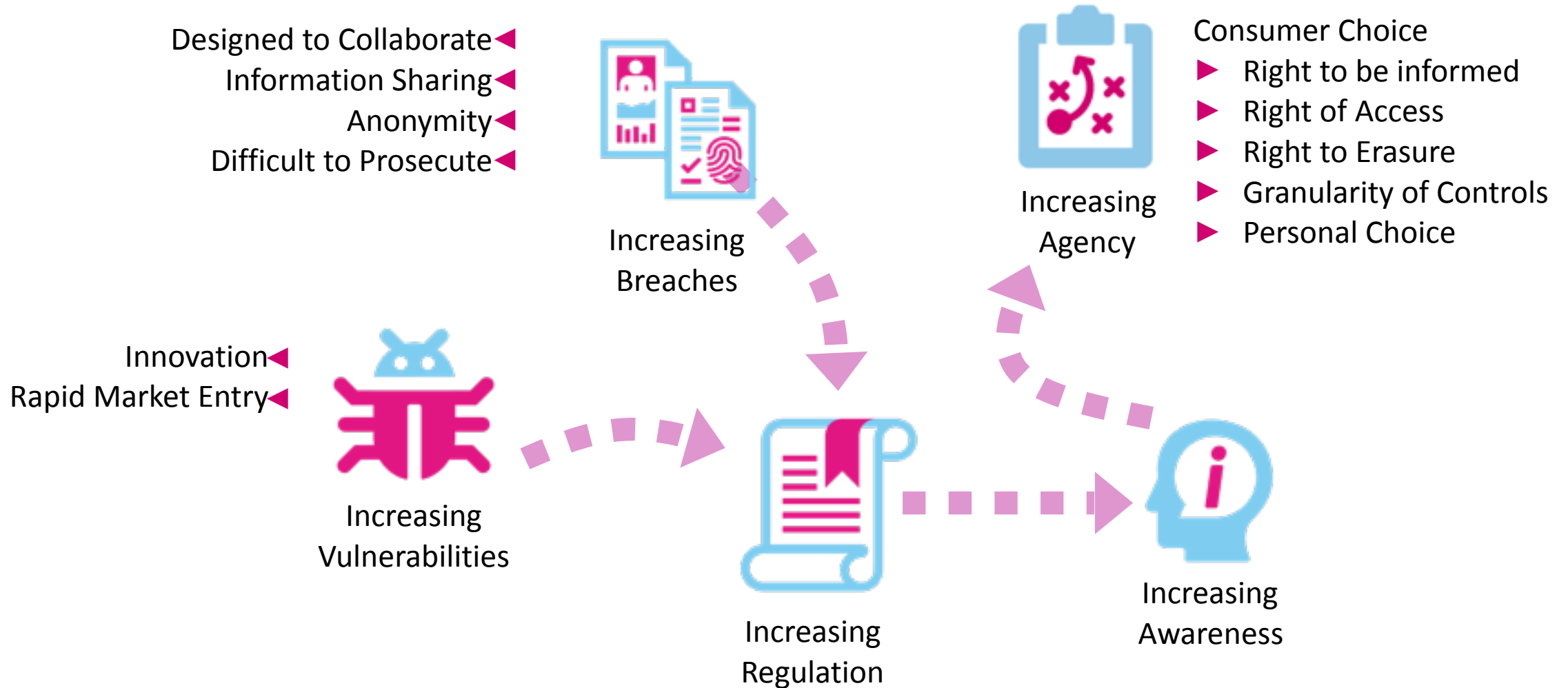
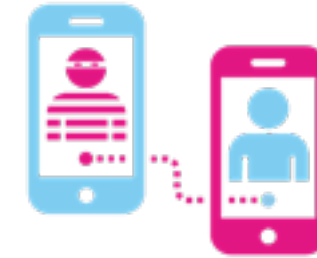# Demystifying Hackers

Black hoodies, Balaclava, Pickaxe

▲ Mind-set

▲ Resourcefulness

▲ Passion

▲ Technical Skills

▲ Toolkits

Resourcefulness

Curiosity

Inherent Trust

zoe.rose@Baringa.com
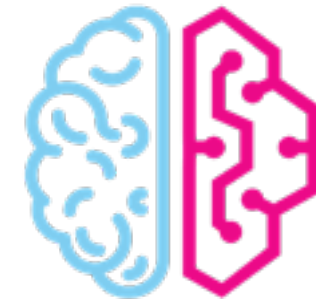
dean.kelshall@Baringa.com

Have the right people

Lesson 1

▲ Stop hiring in your own image
▲ Diversity
▲ Culture
▲ Invest in your talent

Variety of Skills

Intrinsic Motivation

Ways of Working

zoe.rose@Baringa.com

dean.kelshall@Baringa.com

Speak the same language

Lesson 2

Executives

Security Practitioners

Little Time

Complex, Acronym Heavy

Big Picture

Detail Oriented

Business First

Cybersecurity First

Cybersecurity Novice

Low Business Awareness

"Are we secure?"

"It's not that simple."

zoe.rose@Baringa.com

dean.kelshall@Baringa.com

Speak the same language

Lesson 2

Executives   **Security Practitioners**

Executives – Learn a little bit about the topic   Practitioners – There are competing priorities

Cybersecurity is not an absolute

Use a common language – Risk
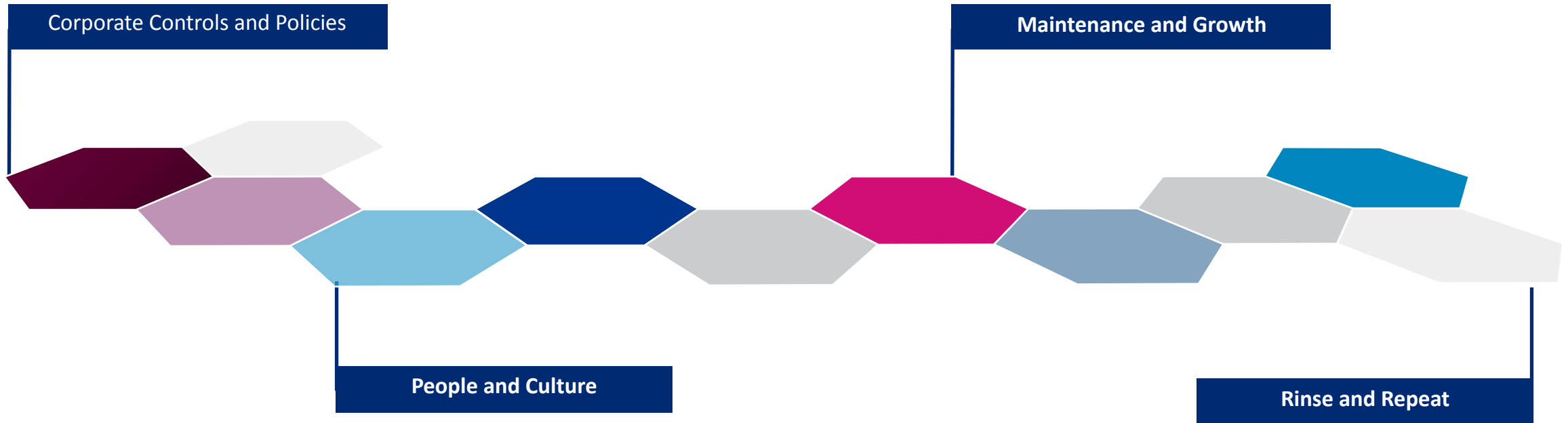
Build Trust – have the evidence to hand

"What's the risk?"   "It's risky."

zoe.rose@Baringa.com   dean.kelshall@Baringa.com
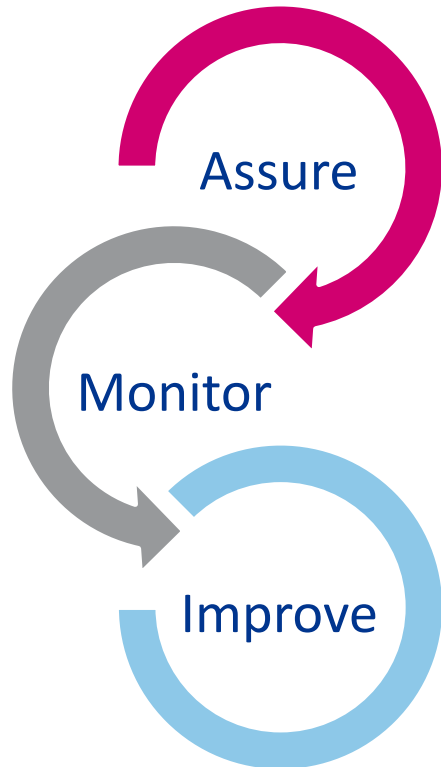
Maintain your cyber security programme

Lesson 3

Corporate Controls and Policies

Maintenance and Growth

People and Culture

Rinse and Repeat

zoe.rose@Baringa.com

dean.kelshall@Baringa.com

Maintain your cyber security programme

Lesson 3

Baringa

Assure

Monitor

Improve

1

Seek Assurance
- Validate what has been done, has been done correctly

2

Monitor Performance
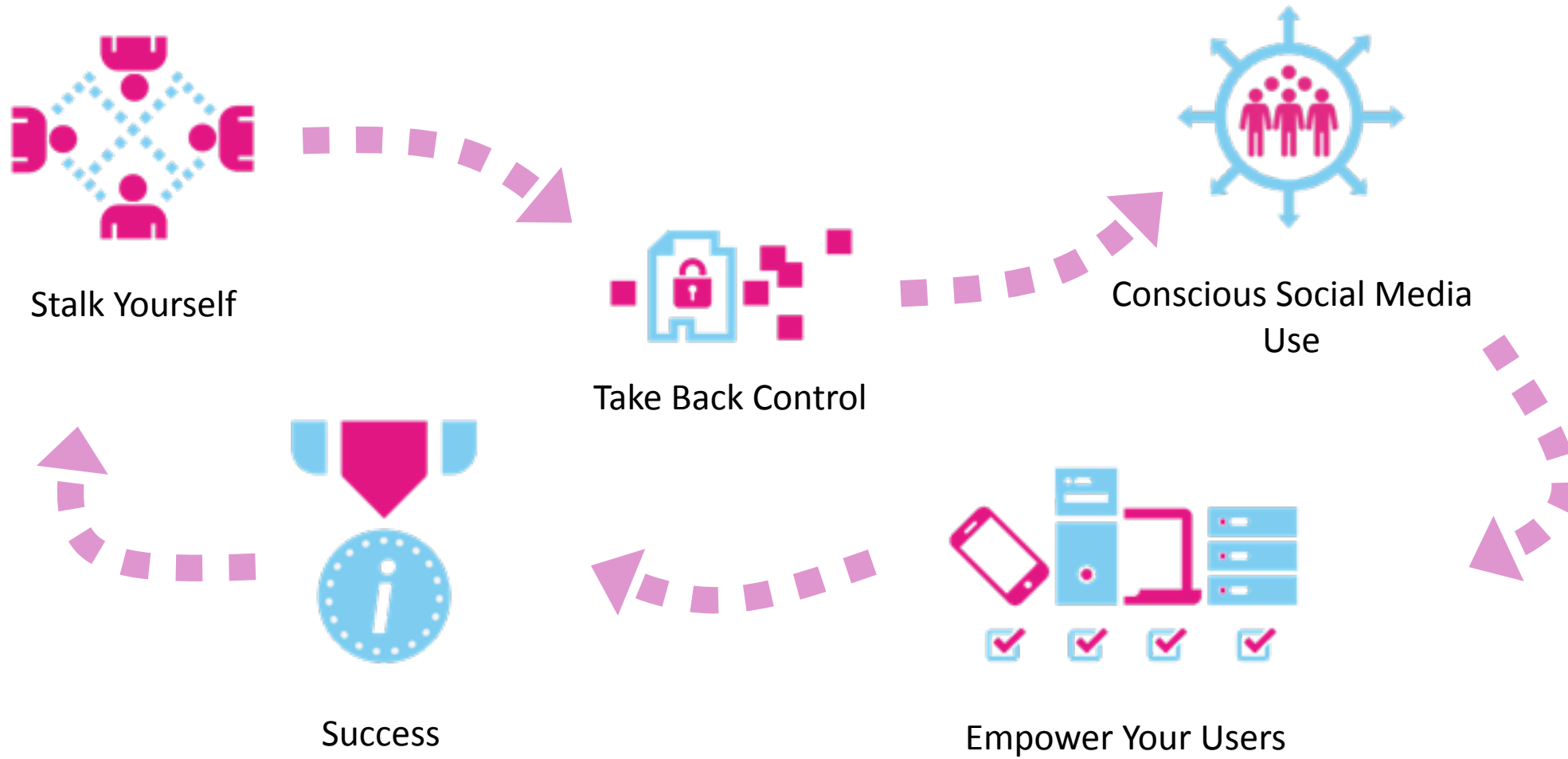- Govern and review your security
- Use reports, dashboards, KPIs

3

Continuous Improvement
- It's never perfect so always improve
- Get 1% better every day

zoe.rose@Baringa.com

dean.kelshall@Baringa.com

Where to start in our personal and professional lives

Security vs Usability

Stalk Yourself

Take Back Control

Conscious Social Media Use

Success

Empower Your Users

zoe.rose@Baringa.com

dean.kelshall@Baringa.com

Questions?

@5683Monkey

Baringa

zoe.rose@Baringa.com

dean.kelshall@Baringa.com

13