Security Architecture in a Collaborative De-Perimeterised Environment: Factors of Success

Yulia Cherdantseva[1] · Omer Rana[1] · Jeremy Hilton[2]

[1]Cardiff University
{y.v.cherdantseva | o.f.rana}@cs.cardiff.ac.uk
[2]Cranfield University
j.c.hilton@cranfield.ac.uk

Presentation Outline

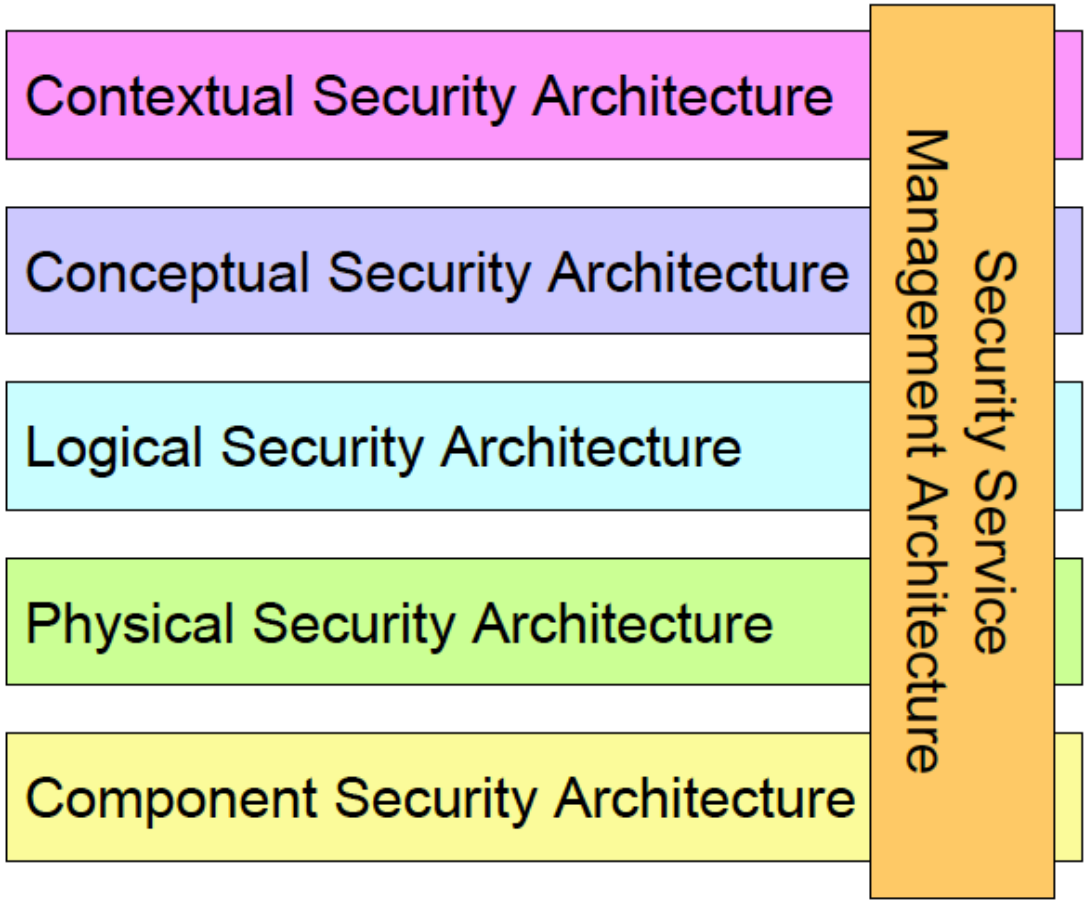
1. Security Architecture
2. Collaborative De-Perimeterised Environment
3. Ten Factors of Success
4. Conclusions
5. Questions and answers

What is a Security Architecture?

Security Architecture is the art and science of designing and supervising the construction of secure business information systems, i.e. systems that are free from danger, damage, reliable and resistant to failures and attacks (Sherwood et al.).

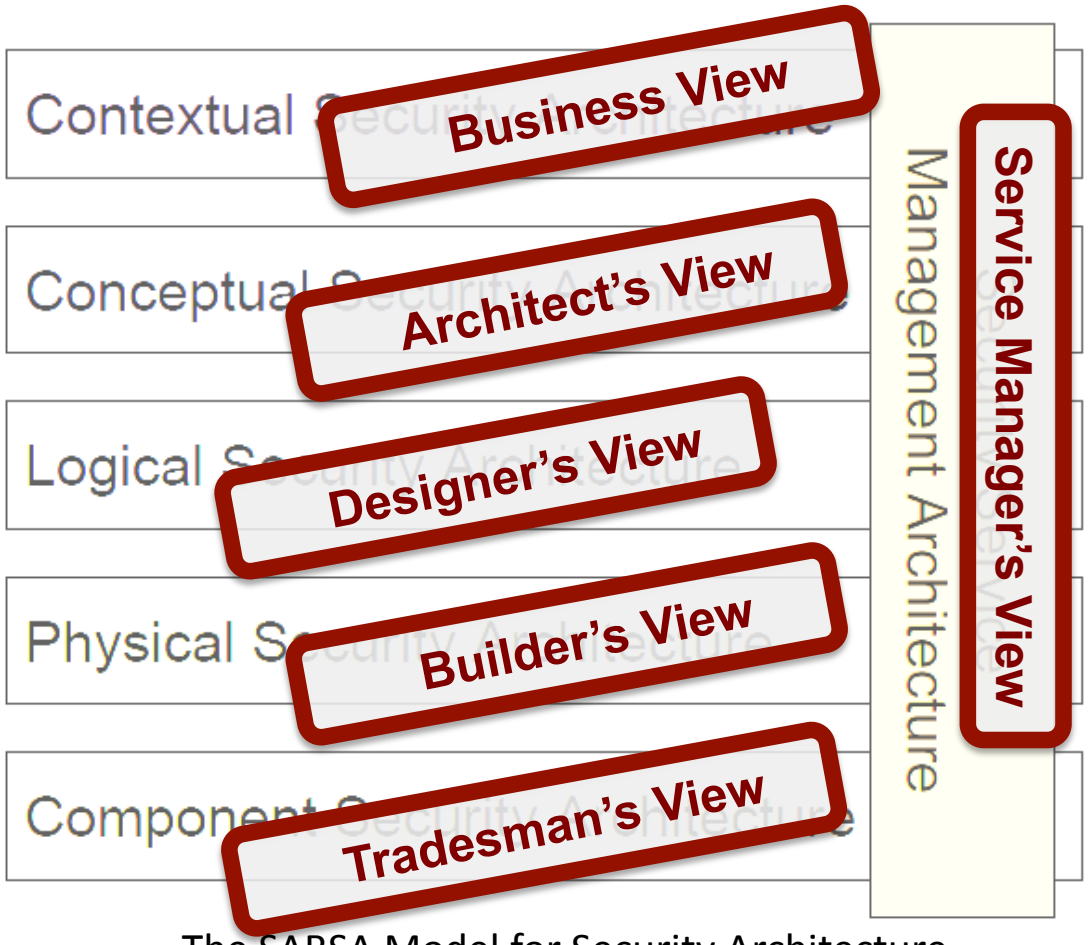
The main goal of a SA is an overall business security.

What is a Security Architecture?



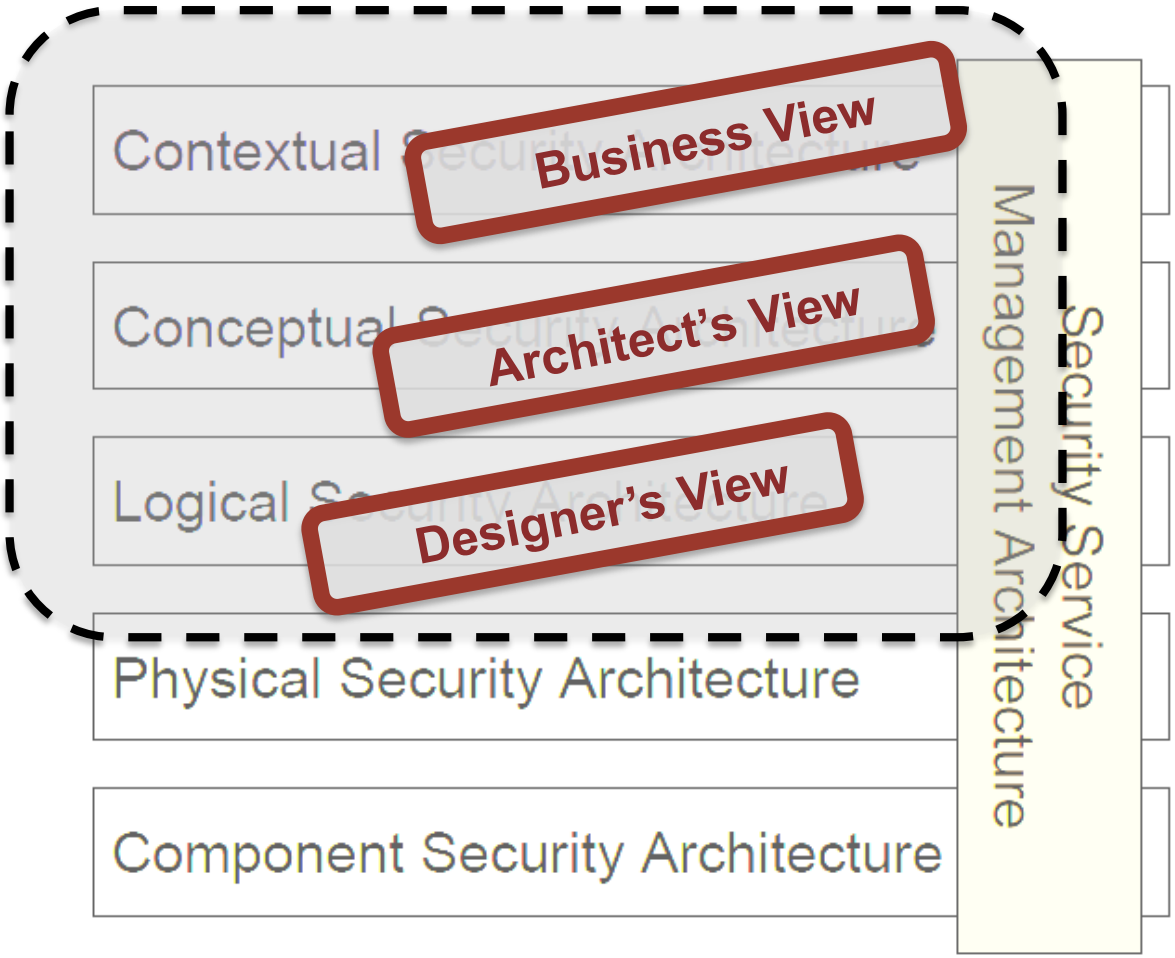
The SABSA Model for Security Architecture

What is a Security Architecture?



The SABSA Model for Security Architecture

What is a Security Architecture?



The SABSA Model for Security Architecture

What affects a Security Architecture?

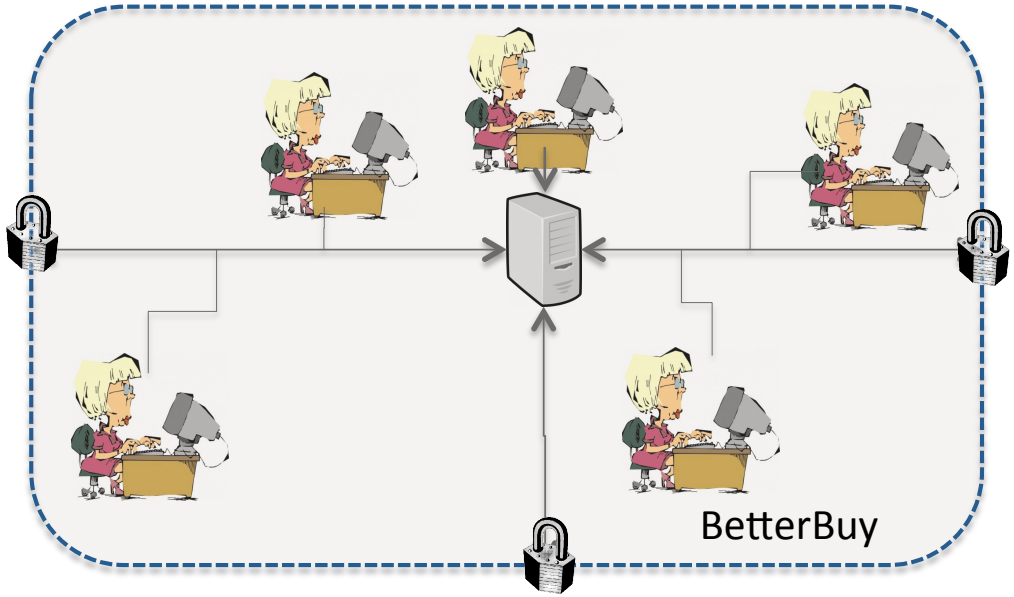
- Business goal
- Technical Capabilities
- The Environment

What is the Collaborative De-perimeterised Environment?

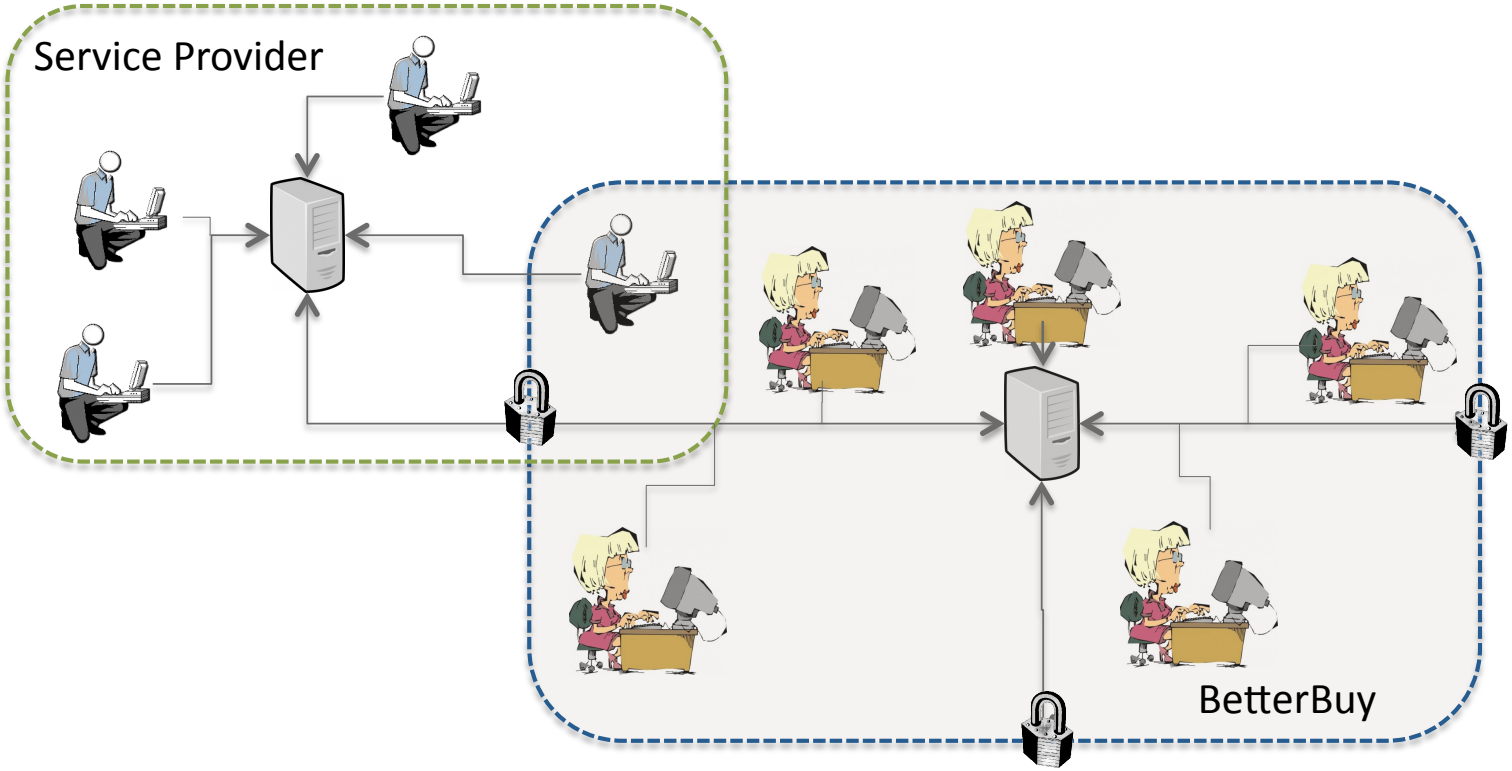
De-perimeterisation is simply the concept of architecting security for the extended business boundary and not an arbitrary IT boundary.

The Jericho Forum

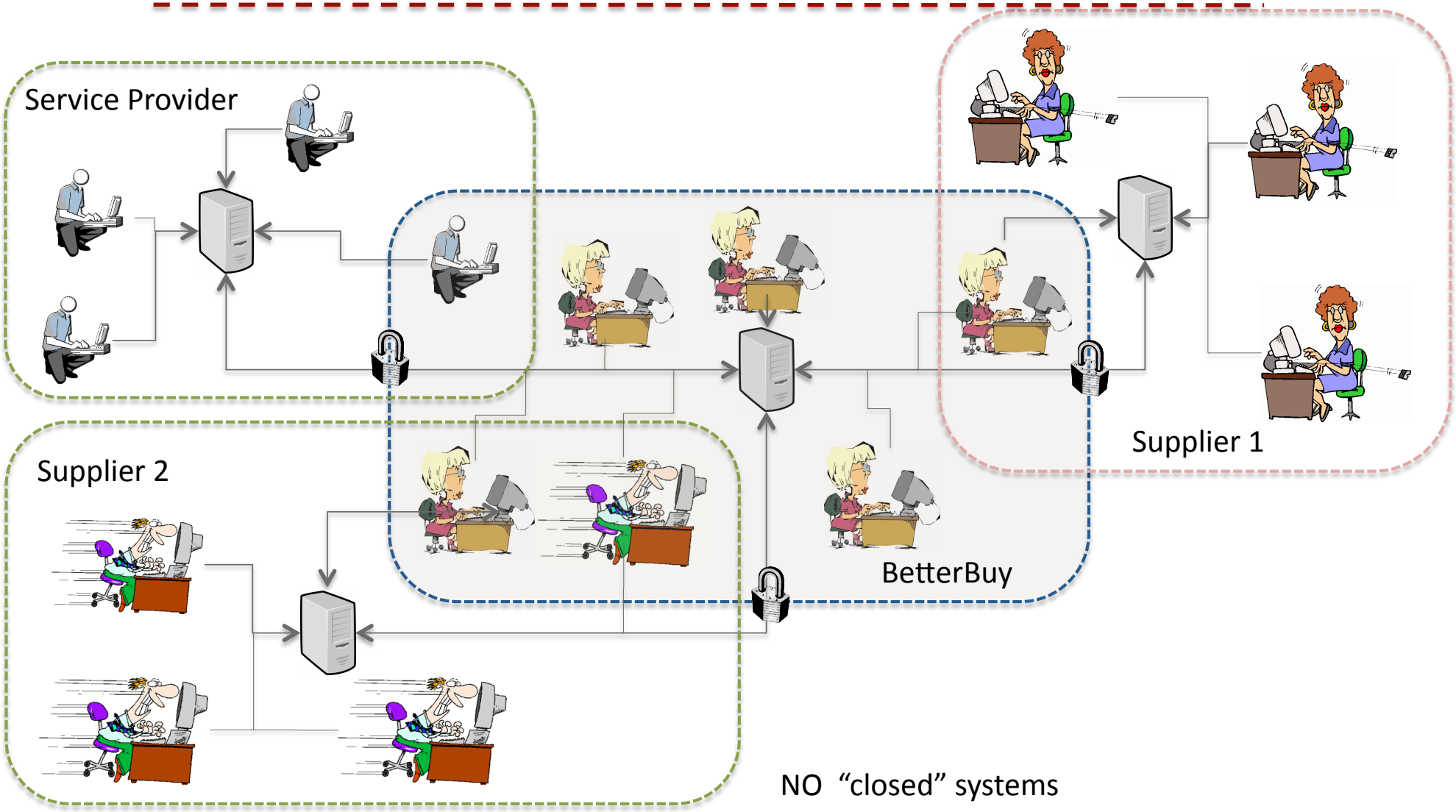
What is the Collaborative De-perimeterised Environment?



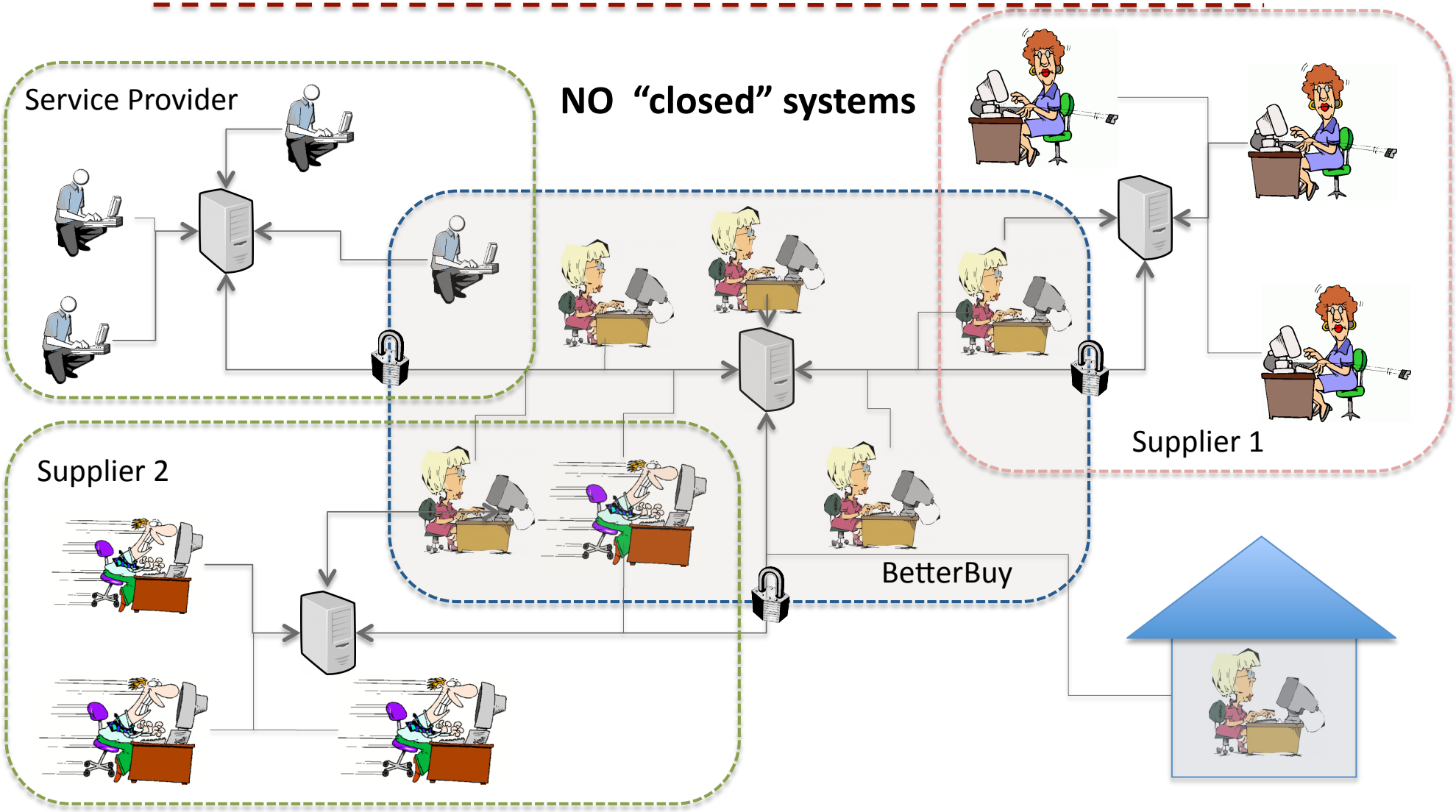
What is the Collaborative De-perimeterised Environment?



What is the Collaborative De-perimeterised Environment?



What is the Collaborative De-perimeterised Environment?



The key message

The specifics of the
Collaborative De-Perimeterised Environement
should be taken into account and addressed
at all layers of a Security Architecture
and from all points of view
including
Business, Architect's and Designer's
viewpoints.

10 Factors of Success

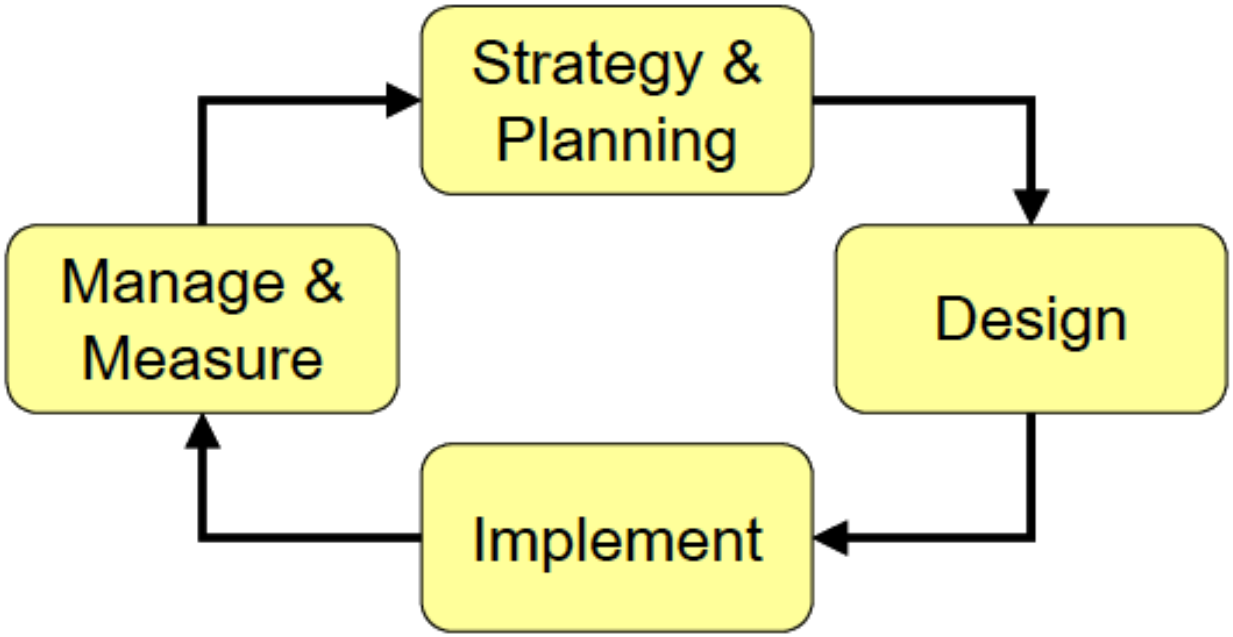
1. Comprehensive and Systematic Approach
2. Adjusted Security Framework
3. Senior Management Role
4. Responsibilities and qualities of InfoSec Personnel
5. Up-to-date Security Policies and Procedures
6. Involvement of Third Parties
7. InfoSec Training and Awareness
8. Approach to Outsourcing
9. Security Return On Investment
10. Business Continuity

Comprehensive and Systematic Approach

Comprehensive protection

exploitation of countermeasures of different layers (people, process and technology)

Systematic protection



The SABSA Lifecycle

2.

Adjusted Security Framework

Issues with existing standards, best practices and frameworks :

1. Bodies that develop security standards/frameworks are not financially or in any other way accountable for the security failures in organisations that follow the standards/frameworks.

2. Do not address changing environment in a timely way

An organisation has to:

1. **Adjust framework to a specific business context**
2. **Fine-tune a framework for the constantly changing environment**

3.

Senior Management Role

Some of the questions to answer:

- Who are the prospective strategic partners?
- To what degree does the company want to share or segregate its information?
- How much does the company trust a partner or a third party?
- What is the liability for information misuse by a partner or a third party?

4. Responsibilities Allocation and Required Qualities of InfoSec Personnel

Some newly emerging responsibilities:

- ✓ Achieve consistency with external parties
- ✓ Develop and implement change-introduction procedures
- ✓ Address security concerns in relationships with customers
- ✓ Co-ordinate all information protection activities

OPEN-MINDEDNESS

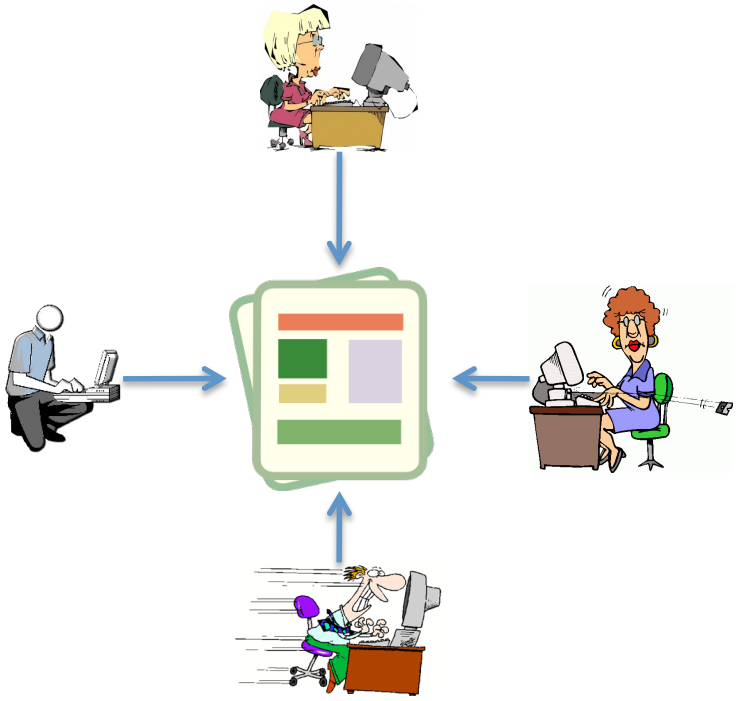
5. Up-to-date Security Policies and Procedures

Should cover continually emerging technologies in a timely manner

- ✓ Mobile Communications
- ✓ Social Networking
- ✓ Social Engineering

Involvement of Interested Parties

1. The scope of the interested parties becomes broader
2. A more in-depth involvement of external parties is required



Example: Parts of an Information Security Policy Document that address protection of information outside of an organisation's perimeter should be developed with the close cooperation of the parties involved.

7. Information Security Training and Awareness

- ✓ Should be up-to-date
- ✓ Should make reasoning clear to overcome rote compliance

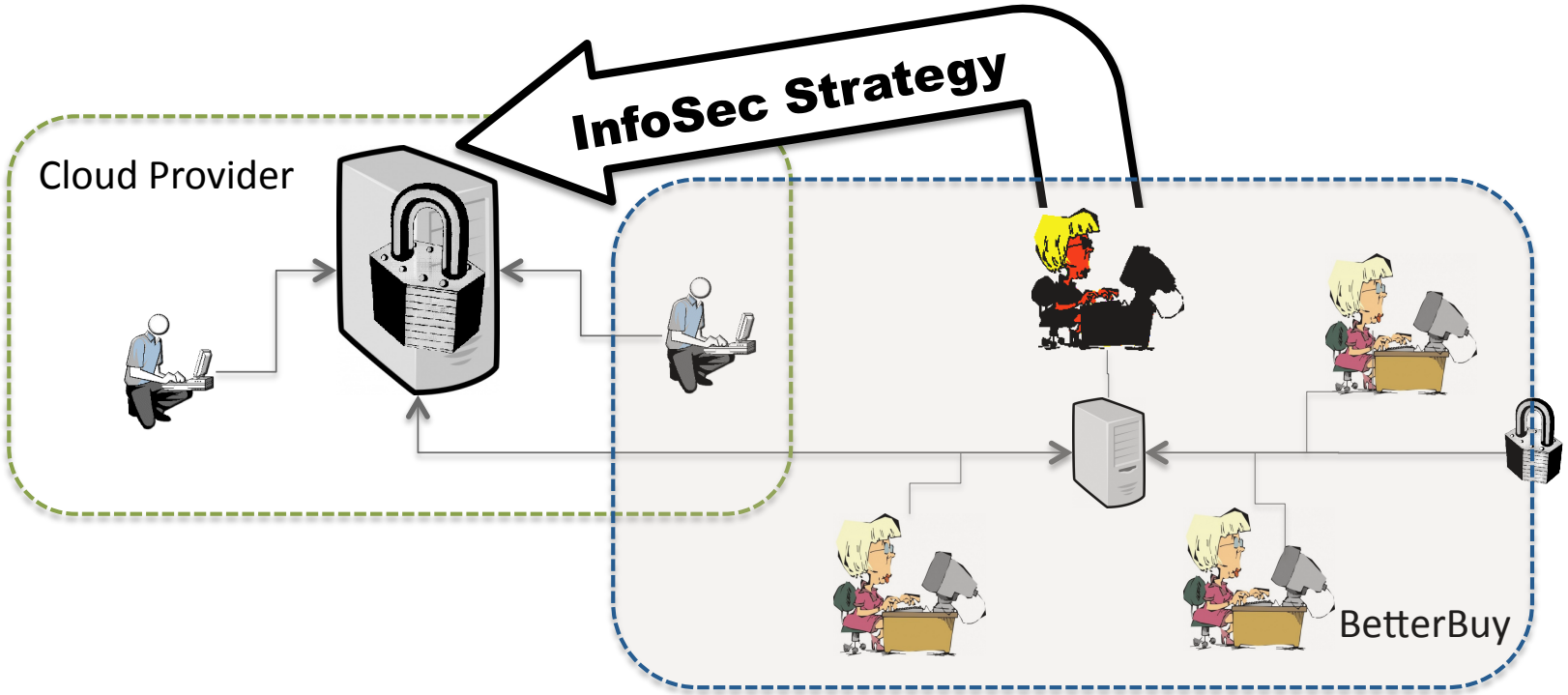
Two main tasks – to teach users:

1. To exploit common sense when using progressive technologies or working in unforeseen circumstances.

2. To perceive information security as everyone's personal responsibility

Approach to Outsourcing

- ✓ Differentiate Service Outsourcing and InfoSec Outsourcing
- ✓ Information Security is not a feature provided by default
- ✓ In-house Security Strategy Making is preferred
- ✓ SA should be adjusted to a preferred way of operation



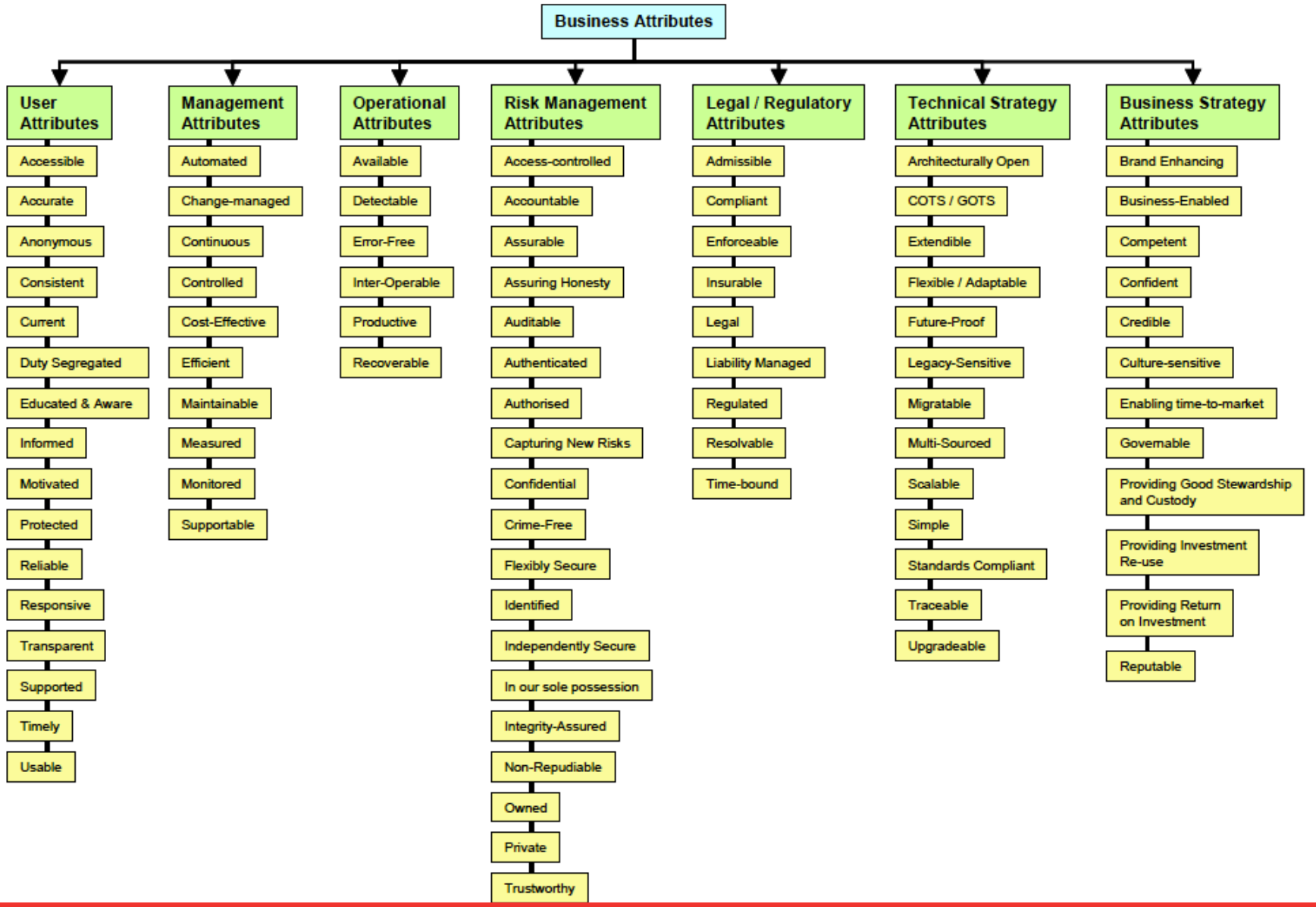
9. Security Return On Investment

Translate security concerns through probability arithmetic into monetary terms

Sherwood et al. propose security ROI calculations based on a set of 85 attributes

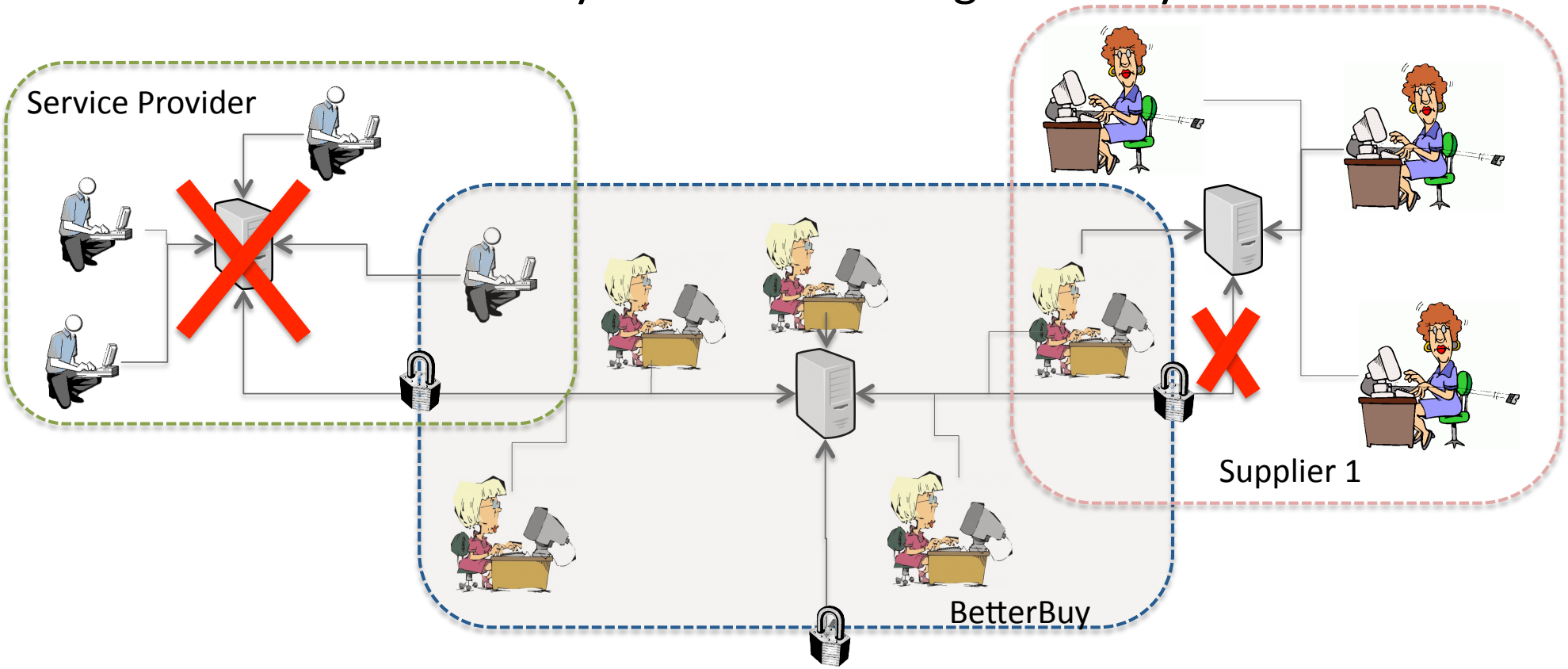
Attribute	Metric Type	Measurement Approach	Performance Target
Informed	Hard	Awareness Program	Adherence to awareness plan
	Soft	Focus groups or satisfaction surveys	Monthly report on all customer feedback relating to level of awareness Report from customer and non-customer groups

9. Security Return On Investment



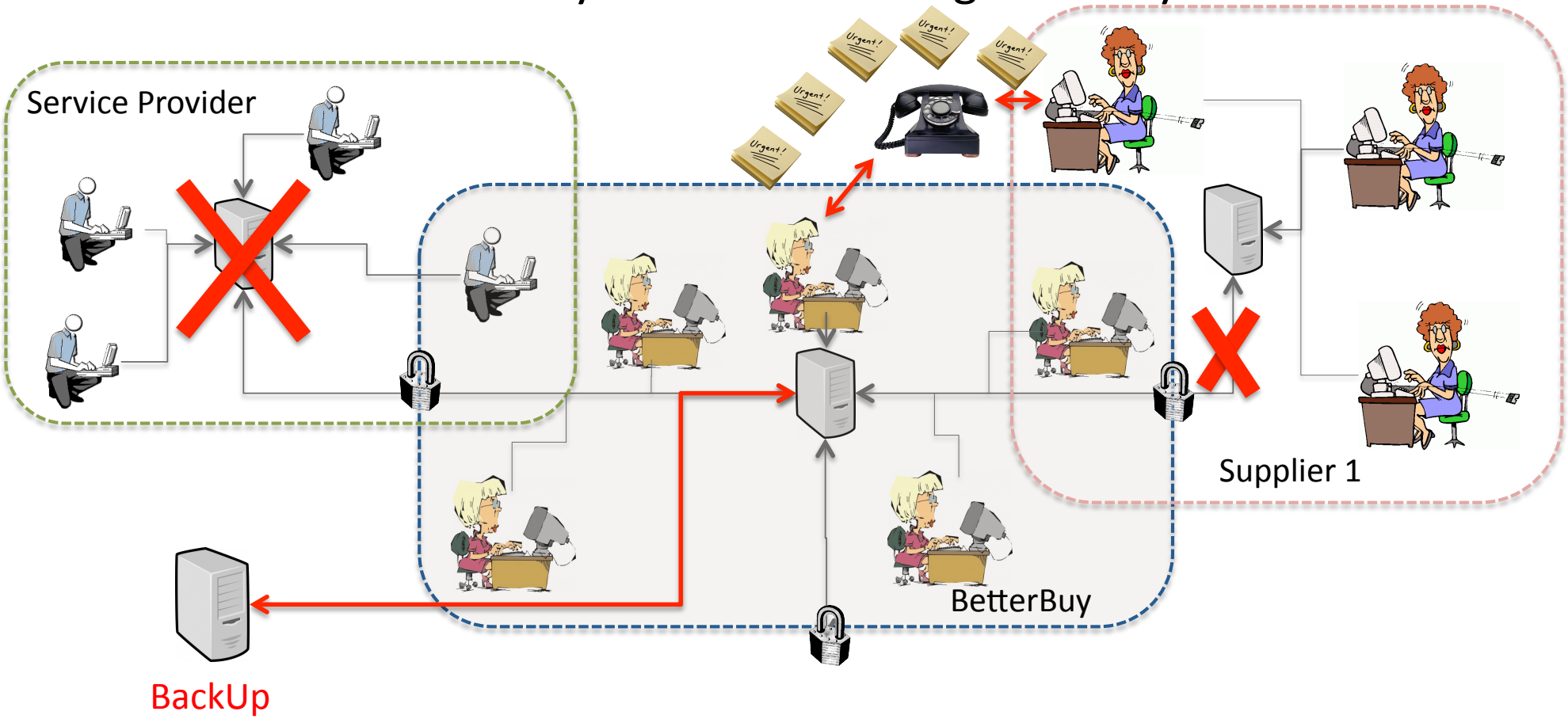
Business Continuity

allows a system to fail in a “good” way



Business Continuity

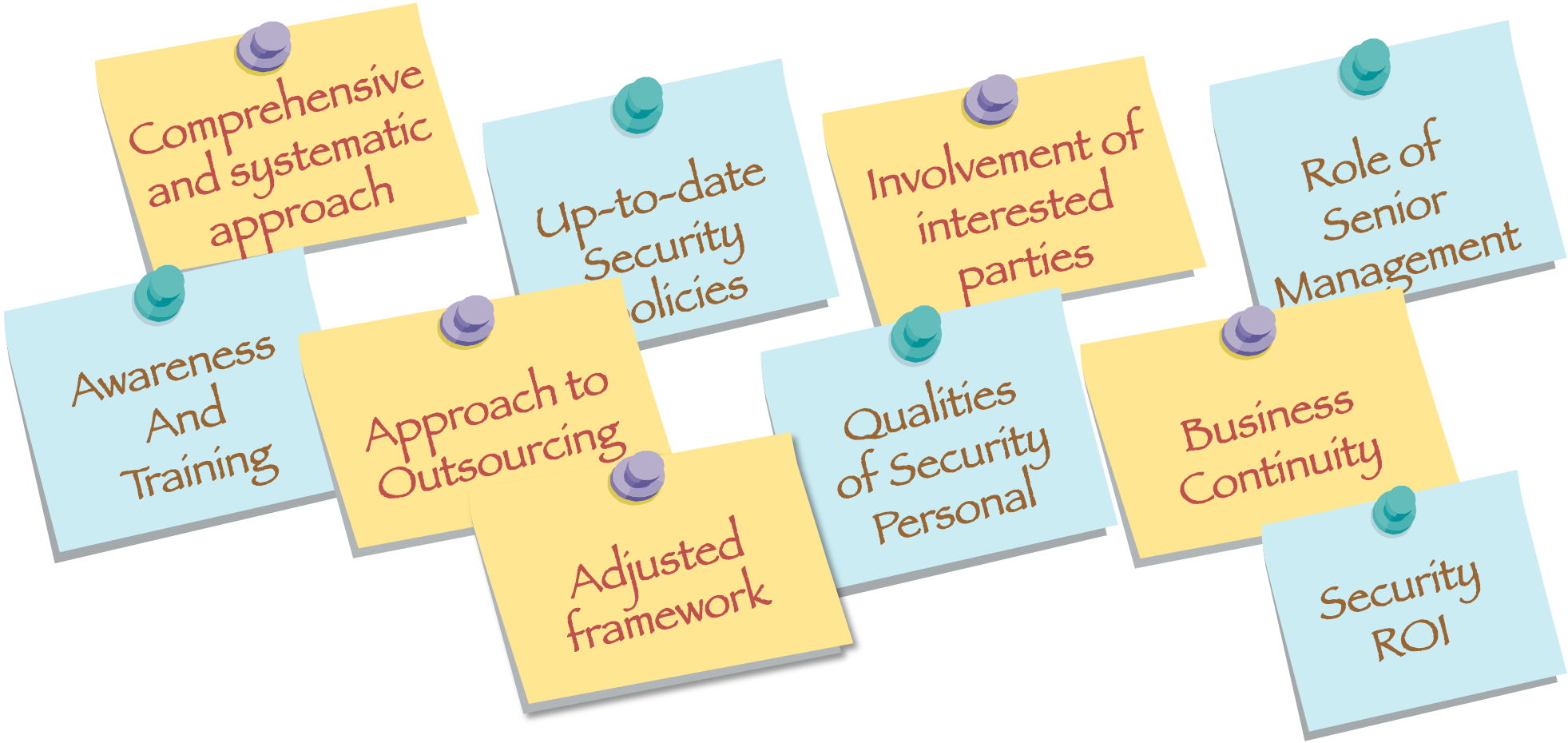
allows a system to fail in a “good” way



A SA should be built to avoid the complete dependence on external parties

Conclusions

The specifics of de-perimeterised environment are underestimated at the level of business, system and security architects



Thank you

The paper and presentation was prepared by
Yulia Cherdantseva[1] · Omer Rana[1] · Jeremy Hilton[2]

[1]Cardiff University
{y.v.cherdantseva | o.f.rana}@cs.cardiff.ac.uk
[2]Cranfield University
j.c.hilton@cranfield.ac.uk