

**BinaryMist<sup>®</sup>**  
Limited

**Does Your Cloud Solution  
Look Like a Mushroom?**



1: Asset Identification

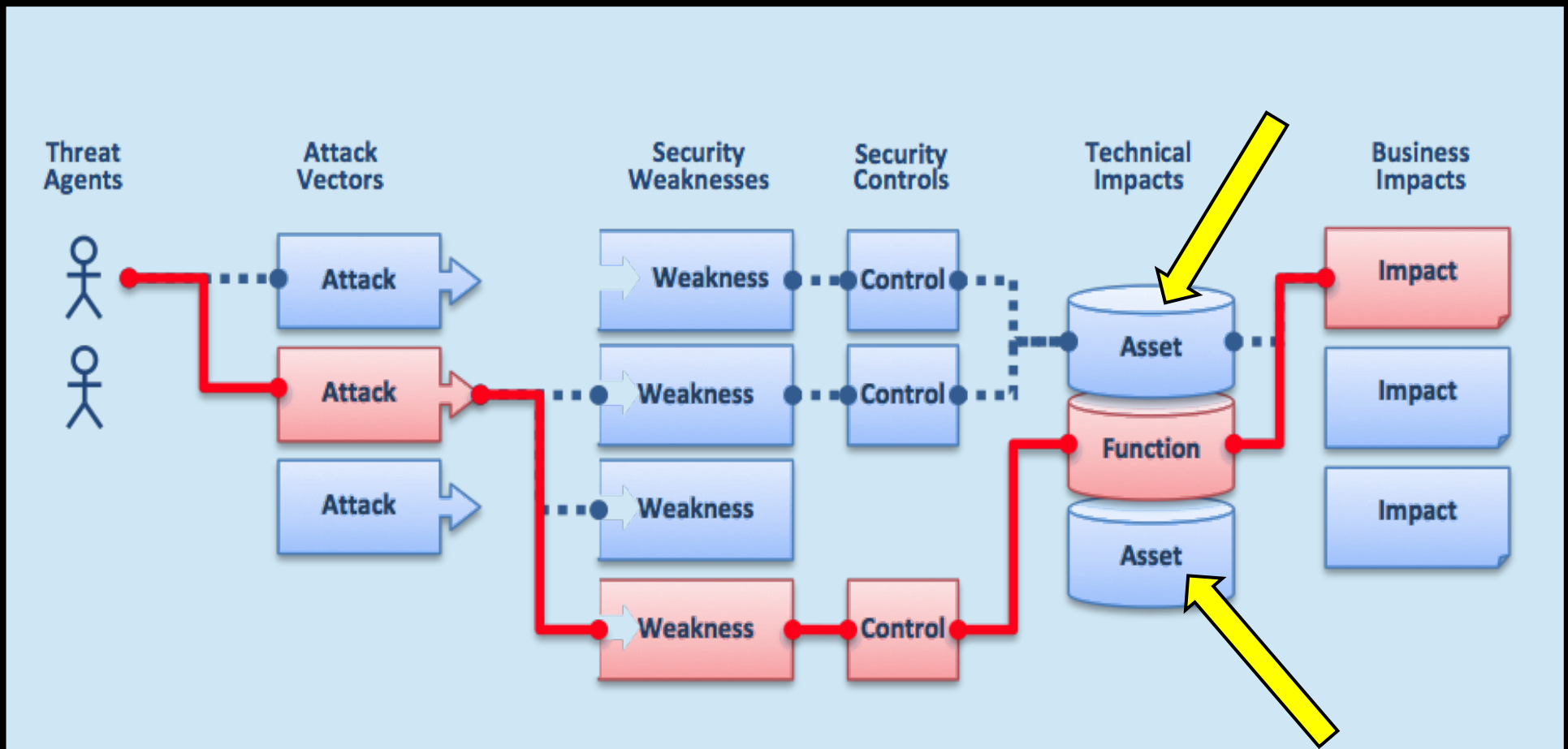
2: Identify Risks

3: Countermeasures

4: What risks does solution cause?

5: Costs and Trade-offs

# 1: Asset Identification





# 1: Asset Identification



# 1: Asset Identification





# 1: Asset Identification

Bank	Online Banking URL	Header?
ASB	<a href="https://fnc.asbbank.co.nz/1/User/LogOn">https://fnc.asbbank.co.nz/1/User/LogOn</a>	YES!
ANZ	<a href="https://secure.anz.co.nz/IBCS/pgLogin">https://secure.anz.co.nz/IBCS/pgLogin</a>	no
BankDirect	<a href="https://vault.bankdirect.co.nz/default.asp">https://vault.bankdirect.co.nz/default.asp</a>	no
BNZ	<a href="https://www.bnz.co.nz/ib/app/login">https://www.bnz.co.nz/ib/app/login</a>	no
HSBC	<a href="https://www.hsbc.co.nz/1/2/HUB_IDV2/IDV_EPP...">https://www.hsbc.co.nz/1/2/HUB_IDV2/IDV_EPP...</a>	no
Kiwibank	<a href="https://www.ib.kiwibank.co.nz/">https://www.ib.kiwibank.co.nz/</a>	no
Rabobank	<a href="https://secure1.rabodirect.co.nz/exp/authenticationDGPEN.jsp">https://secure1.rabodirect.co.nz/exp/authenticationDGPEN.jsp</a>	no
SBS	<a href="https://sbsbanking.sbs.net.nz/secure/">https://sbsbanking.sbs.net.nz/secure/</a>	no
TSB	<a href="https://homebank.tsbbank.co.nz/online/">https://homebank.tsbbank.co.nz/online/</a>	no
Westpac	<a href="https://sec.westpac.co.nz/IOLB/Login.jsp">https://sec.westpac.co.nz/IOLB/Login.jsp</a>	no

Python Script by François Marier

# 1: Asset Identification

Bank	Online Banking URL	Header?
ANZ	<a href="https://www.anz.com/INETBANK/bankmain.asp">https://www.anz.com/INETBANK/bankmain.asp</a>	no
Bank of China	<a href="https://ebs.boc.cn/BocnetClient/LoginFrameAbroad.do?_locale=en_US">https://ebs.boc.cn/BocnetClient/LoginFrameAbroad.do?_locale=en_US</a>	no
Bank of Melbourne	<a href="https://ibanking.bankofmelbourne.com.au/ibank/loginPage.action">https://ibanking.bankofmelbourne.com.au/ibank/loginPage.action</a>	no
Bankwest	<a href="https://ibs.bankwest.com.au/BWLogin/rib.aspx">https://ibs.bankwest.com.au/BWLogin/rib.aspx</a>	no
Bendigobank	<a href="https://www.bendigobank.com.au/banking/BBLIBanking/">https://www.bendigobank.com.au/banking/BBLIBanking/</a>	no
Bank of Queensland	<a href="https://www.ib.boq.com.au/boqbl">https://www.ib.boq.com.au/boqbl</a>	no
Citibank	<a href="https://www.citibank.com.au/AUGCB/JSO/signon/DisplayUsernameSignon.do">https://www.citibank.com.au/AUGCB/JSO/signon/DisplayUsernameSignon.do</a>	no
Commonwealth Bank	<a href="https://www.my.commbank.com.au/netbank/Logon/Logon.aspx">https://www.my.commbank.com.au/netbank/Logon/Logon.aspx</a>	no
Heritage Bank	<a href="https://online.hbs.net.au/hbsv47/ntv471.asp?wci=entry">https://online.hbs.net.au/hbsv47/ntv471.asp?wci=entry</a>	no
HSBC	<a href="https://www.hsbc.com.au/1/2/HUB_IDV2/IDV_EPP...">https://www.hsbc.com.au/1/2/HUB_IDV2/IDV_EPP...</a>	no
Mebank	<a href="https://ib.mebank.com.au/ME">https://ib.mebank.com.au/ME</a>	no
NAB	<a href="https://ib.nab.com.au/nabib/index.jsp">https://ib.nab.com.au/nabib/index.jsp</a>	no
Rabobank	<a href="https://secure.rabodirect.com.au/exp/policyenforcer/pages/loginB2CDGPEN.jsf?login">https://secure.rabodirect.com.au/exp/policyenforcer/pages/loginB2CDGPEN.jsf?login</a>	no
St. George	<a href="https://ibanking.stgeorge.com.au/ibank/loginPage.action">https://ibanking.stgeorge.com.au/ibank/loginPage.action</a>	no
Suncorp Bank	<a href="https://internetbanking.suncorpbank.com.au/">https://internetbanking.suncorpbank.com.au/</a>	no
Westpac	<a href="https://online.westpac.com.au/esis/Login/SrvPage">https://online.westpac.com.au/esis/Login/SrvPage</a>	no

1: Asset Identification

2: Identify Risks

3: Countermeasures

4: What risks does solution cause?

5: Costs and Trade-offs



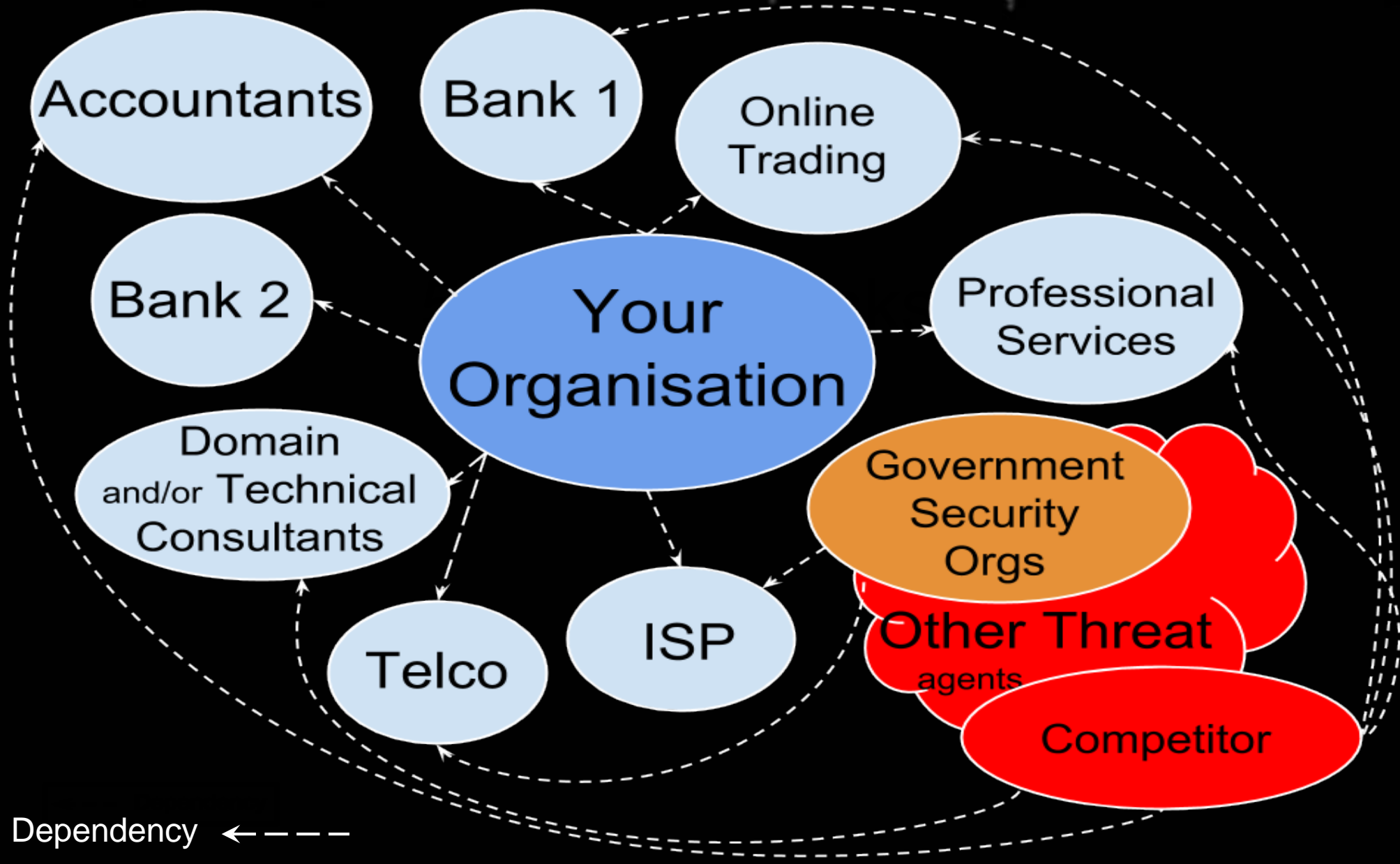
## 2: Identify Risks



## 2: Identify Risks

$\text{Risk} = \text{Likelihood} * \text{Impact}$

## 2: Identify Risks





## 2: Identify Risks

### Likelihood

### Threat Agent Factors

- Skill level
- Motive
- Opportunity
- Size

## 2: Identify Risks

### Likelihood

### Vulnerability Factors

- Ease of discovery
- Ease of exploit
- Awareness
- Intrusion detection

## 2: Identify Risks

### Impact

#### Technical Factors

- Loss of confidentiality
- Loss of integrity
- Loss of availability
- Loss of accountability



## 2: Identify Risks



### Impact

#### Business Factors

- Financial damage
- Reputation damage
- Non-compliance
- Privacy violation



## 2: Identify Risks

### The Cloud vs In-House Security Comparisons

The Cloud 	In-House 
Secrets not safe	Potential for greater security
Have to trust others	Trust yourself and your experts
Only some risks can be mitigated	Control over what to fix when
Lack of empathy	You control amount of empathy
Coerced, forced to give up secrets	Your decision. A lot less likely

## 2: Identify Risks

### The Cloud vs In-House Security Comparisons

The Cloud 	In-House 
Out of business	Visibility. Strategies.
Inherent lack of security	Your decision
Out-sourcing their out-sourced	You decide what goes where
Physical location unknown	Can see your rack
Physical security <b>uncertainty</b>	Physical security certainty

We also use third party software (such as customer relationship management and accounting software) that holds your information, sometimes overseas.



## 2: Identify Risks

### The Cloud vs In-House Security Comparisons

The Cloud 	In-House 
No knowledge of your domain	Domain expert

## 2: Identify Risks

### Control Lost

Duffy said that because it was a bulk request, Trade Me could have notified members whose details had been released.

Trade Me considered "at length" whether to do so, but "eventually made the decision not to inform members directly so as not to create undue panic or distress members unnecessarily

Senior lawyers and the Privacy Commissioner have told the *Herald* of concerns over the practice which sees the companies voluntarily give the information to police.

Instead of seeking a legal order, police have asked companies to hand over the information to assist with the "maintenance of the law", threatened them with prosecution if they tell the person about whom they are interested and accept data with no record keeping to show how often requests are made.

The request from police carries no legal force at all yet is regularly complied with.

## 2: Identify Risks





1: Asset Identification

2: Identify Risks

3: Countermeasures

4: What risks does solution cause?

5: Costs and Trade-offs

### 3: Countermeasures

The Cloud



On top only

In-House



Full control



OWASP AppSensor

IMPLEMENT REAL-TIME  
INTRUSION DETECTION  
WITHIN YOUR SOFTWARE

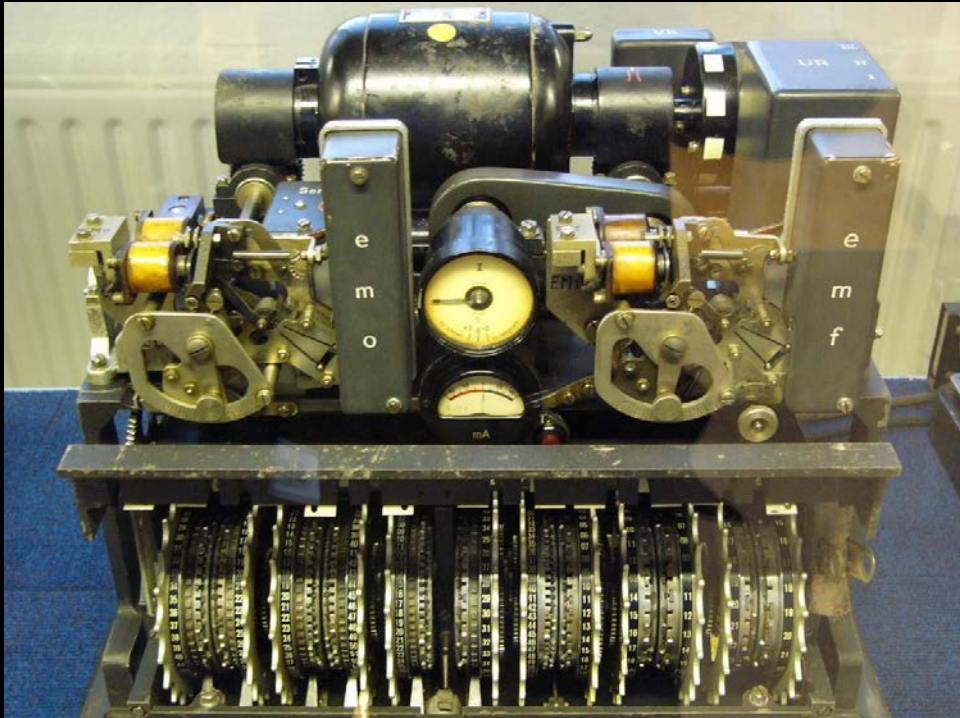
# ATTACK DETECTION

# RESPOND AUTOMATICALLY

Free, open source, DevOps friendly and cloud compatible



### 3: Countermeasures



- Avoid Commercial
- Use Public-Domain

# 3: Countermeasures



## 3: Countermeasures

### Hardening VPS's

- Create Multiple Partitions
- Review Password Strategies
- Disable Remote Root Logins
- Harden SSH





### 3: Countermeasures

#### Hardening VPS's

- Disable or Remove Services
- Schedule Backups
- Keep Systems Up to date
- Logging to Off-site



## 3: Countermeasures

### Hardening VPS's



## 3: Countermeasures

### Hardening VPS's





## 3: Countermeasures

### Hardening VPS's





**Software Engineering Institute**  
Carnegie Mellon.

# New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CSIRTs)

Robin Ruefle  
Ken van Wyk  
Lana Tasic

May 2013

New Zealand National Cyber Security Centre  
Government Communication Security Bureau

Developed in cooperation with the CERT<sup>®</sup> Division of the Software Engineering  
Institute at Carnegie Mellon University

# 3: Countermeasures

Break Your System





1: Asset Identification

2: Identify Risks

3: Countermeasures

4: Risks that solution causes

5: Costs and Trade-offs

# 4: Risks that solution causes

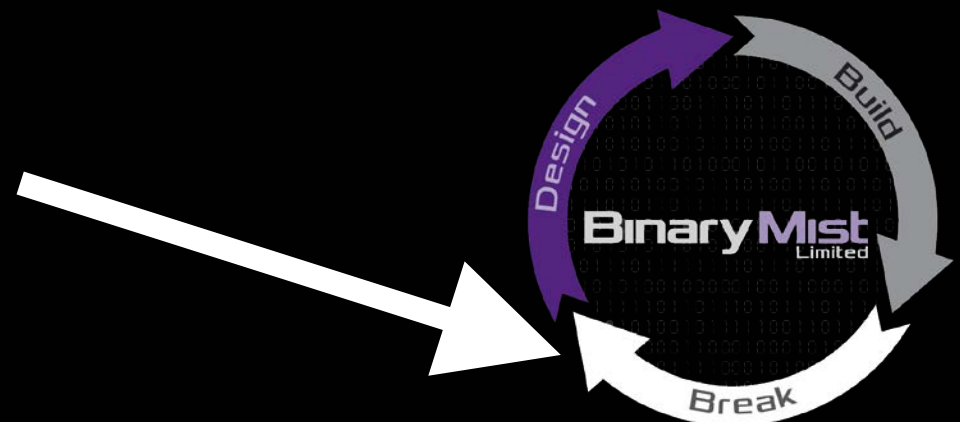
## New Risks

<p>The Cloud</p> 	<p>In-House</p> 
<p>Hack CSP -&gt; Prosecution</p>	<p>Hack Yourself -&gt; Find Holes -&gt; Harden</p>

# 4: Risks that solution causes

## New Risks

<p>The Cloud</p> 	<p>In-House</p> 
<p>Hack CSP -&gt; Prosecution</p>	<p>Hack Yourself -&gt; Find Holes -&gt; Harden</p>



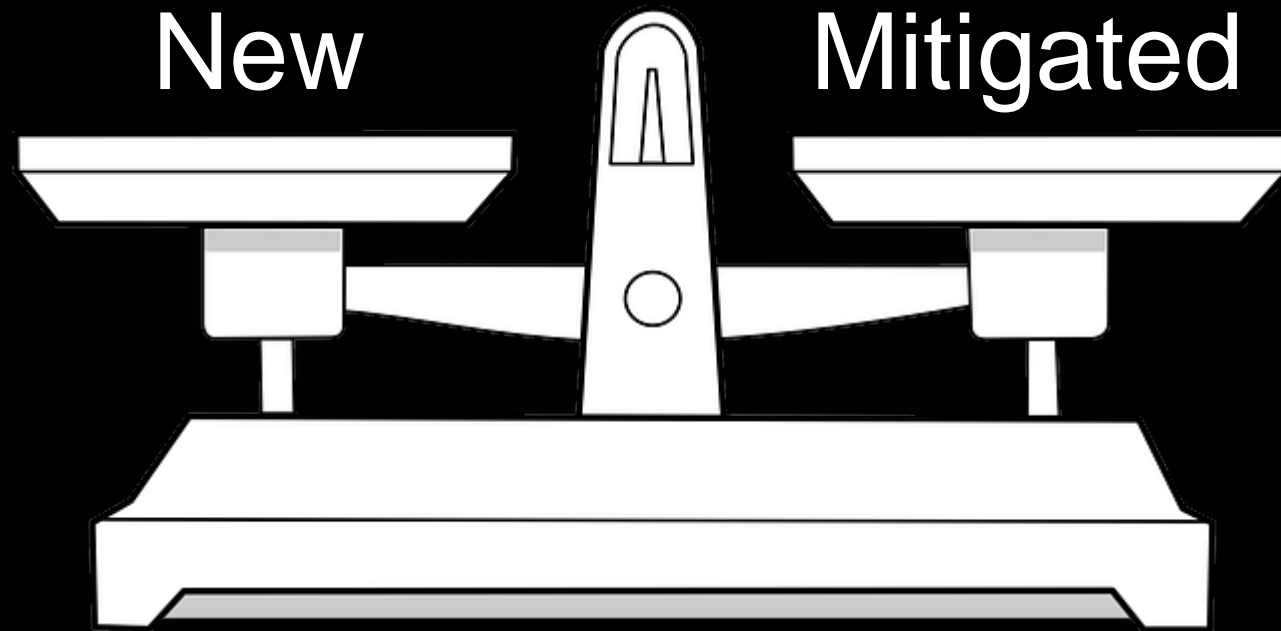


## 4: Risks that solution causes

New Risks



## 4: Risks that solution causes



1: Asset Identification

2: Identify Risks

3: Countermeasures

4: Risks that solution causes

**5: Costs and Trade-offs**



## 5: Costs and Trade-offs

Establish Value

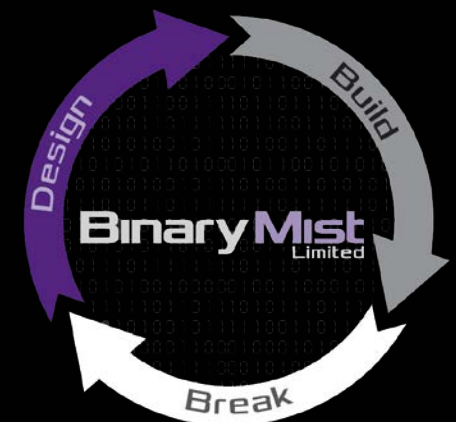


Loss of Convenience



## 5: Costs and Trade-offs

Staying on Top



# Resource Compilation

- Cloud Security Assessment
- Automation
- Security Focused Facility
- In-house Cloud Planning





The background of the entire image is a dark field filled with a dense, vertical stream of white and light blue binary code (0s and 1s), reminiscent of the 'Matrix' effect. The code appears to be falling from the top of the frame. In the center, the company name 'BinaryMist' is written in a large, bold, sans-serif font. 'Binary' is in white, and 'Mist' is in a light blue color. A registered trademark symbol (®) is located at the top right of the word 'Mist'. Below 'BinaryMist', the word 'Limited' is written in a smaller, white, sans-serif font.

# BinaryMist®

Limited

**Where Passion, Quality and Technical Expertise meet**