So Now What?
Using risk assessments to inform security behaviours

Alison Crockford
Sociotechnical Security Specialist
So now what?

You’ve got your senior management’s attention.

What practical steps can you take to move your organisation towards security awareness maturity?

This is one example of such a journey.
Who am I?

Enthusiastic amateur geek
Who am I?

Risk assessor
Who am I? Enthusiastic risk taker
Who am I?

I explain things
Example Takeaways...

Understand business requirements

Align your messaging to those requirements

Get your board on board
But how?
Risk Management and Security behaviours
Established security structure

Information Security function since 2013

Security Awareness campaigns

ISO 27001

Security Operations Centre

Governance and Risk

Network Security teams
65 Behaviours
Be careful what you disclose outside the walls

Lock devices when not in use

Do not use personal device for Bank business

Use file links rather than sending attachments

No Bank equipment to high cyber threat environments

Complete all vetting forms as required

Understand the risks of phishing

Only open links from trusted sources

Do not install unauthorised software

Escort your visitors

Shred papers when you are finished with them

Secure sensitive information in locked storage

Minimise printing

Turn on two factor authentication whenever possible

Leave your desk clear when you finish at the end of the day

Challenge and accept challenge gracefully

Keep your laptop and tokens apart

Keep your devices and papers with you when travelling

Shut down your laptop when leaving the building

Engage with Travel Security when travelling away from the Bank

Take care of your online presence

Always carry IT equipment in hand

65 Behaviours
Campaigns
Map behaviours to risks
## Risk Taxonomy

<table>
<thead>
<tr>
<th>Category</th>
<th>Cyber</th>
<th>People</th>
<th>Physical</th>
<th>Information Security (Human)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Lack of availability</td>
<td>Insider: theft or leak</td>
<td>Destruction</td>
<td>Mishandling of sensitive information</td>
</tr>
<tr>
<td></td>
<td>System/Network compromise</td>
<td>Social engineering and coercion</td>
<td>Disruption</td>
<td>Offsite Compromise</td>
</tr>
<tr>
<td></td>
<td>Process Failure</td>
<td>Recklessness or negligence</td>
<td>Destruction</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Disruption</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Theft of physical assets</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Misclassification</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Paper loss</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Email mistakes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Credential sharing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Espionage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Disclosure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Terrorism</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Blockade</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Unauthorised access</td>
</tr>
</tbody>
</table>

- **Cyber**
  - Lack of availability
  - System/Network compromise
  - Process Failure

- **People**
  - Insider: theft or leak
  - Social engineering and coercion
  - Recklessness or negligence

- **Physical**
  - Destruction
  - Disruption
  - Theft of physical assets

- **Information Security (Human)**
  - Mishandling of sensitive information
  - Offsite Compromise

- **Miscellaneous**
  - Password attack
  - Phishing
  - Man in the middle
  - Misclassification
  - Paper loss
  - Email mistakes
  - Credential sharing
  - Espionage
  - Disclosure
  - Terrorism
  - Blockade
  - Unauthorised access
## Behaviours to risks

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>12 Cyber</strong></td>
<td>Lack of availability, System/Network compromise, Process Failure</td>
<td>Phishing testing, Strong passwords, Only use Bank equipment, 2FA</td>
</tr>
<tr>
<td><strong>33 Information Security (Human)</strong></td>
<td>Mishandling of sensitive information, Offsite Compromise</td>
<td>Report any worries, Classify documents, No photography, Clear workspaces</td>
</tr>
<tr>
<td><strong>14 People</strong></td>
<td>Insider: theft, leak or exfiltration, Social engineering and coercion, Recklessness or negligence</td>
<td>Changes in circumstances, Visitor management, Social media presence</td>
</tr>
<tr>
<td><strong>6 Physical</strong></td>
<td>Destruction, Disruption, Theft of physical assets</td>
<td>Keep your devices safe, Wear your pass, Report any losses</td>
</tr>
</tbody>
</table>
Review incidents against risk taxonomy
## Risk Taxonomy

<table>
<thead>
<tr>
<th>Category</th>
<th>Risk Types</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cyber</strong></td>
<td>Lack of availability, System/Network compromise, Process Failure</td>
</tr>
<tr>
<td><strong>Information Security (Human)</strong></td>
<td>Mishandling of sensitive information, Offsite Compromise</td>
</tr>
<tr>
<td><strong>People</strong></td>
<td>Insider: theft or leak, Social engineering and coercion, Recklessness or negligence</td>
</tr>
<tr>
<td><strong>Physical</strong></td>
<td>Destruction, Disruption, Theft of physical assets</td>
</tr>
</tbody>
</table>
Risk Taxonomy: most incidents logged

- **Cyber**
  - Lack of availability
  - System/Network compromise
  - Process Failure

- **Information Security (Human)**
  - Mishandling of sensitive information
  - Offsite Compromise

- **People**
  - Insider: theft or leak
  - Social engineering and coercion
  - Recklessness or negligence

- **Physical**
  - Destruction
  - Disruption
  - Theft of physical assets
<table>
<thead>
<tr>
<th>Relevant behaviours</th>
<th>Compliance behaviours</th>
<th>Mature behaviours</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cyber</strong></td>
<td>Lack of availability</td>
<td>Never reuse or share passwords</td>
</tr>
<tr>
<td></td>
<td>System/Network compromise</td>
<td>Use 2FA</td>
</tr>
<tr>
<td></td>
<td>Process Failure</td>
<td>Use passphrases</td>
</tr>
<tr>
<td><strong>Information Security</strong></td>
<td>Mishandling of sensitive information</td>
<td>Classify correctly</td>
</tr>
<tr>
<td><strong>(Human)</strong></td>
<td>Offsite Compromise</td>
<td>Clear workspaces</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Minimise printing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Digital skills</td>
</tr>
<tr>
<td><strong>People</strong></td>
<td>Insider: theft or leak</td>
<td>No photography in the Bank</td>
</tr>
<tr>
<td></td>
<td>Social engineering and coercion</td>
<td>Problem spotting for managers</td>
</tr>
<tr>
<td></td>
<td>Recklessness or negligence</td>
<td></td>
</tr>
</tbody>
</table>
Campaign mapping: Drumbeat + focus

Q1: Cyber
Passwords matter

Q2: Information
Document classification

Q3: People
Photo policy

Q4: Information
Clear workspace

Explaining 2FA
Greener Bank
Problem spotting

+ Induction + E-learning + Dashboards + ...
Make sure you consider...

Organisational culture
Security maturity
Risk maturity
Incident reporting
Technology structure
Future business direction
Check your thinking and accept ideas
So now what?

Consider the evidence
Find the knowledge and analyse it, even if it’s anecdotal.

Listen and include
What worries people? What does the business feel about the idea?

Keep the conversation going
Report back on campaigns and measurable outcomes.
Engage senior leaders in your continuous improvement process.