InfoSec Culture and Awareness

InfoSec Cultural Measurement

Outcomes:

• What is InfoSec security culture measurement and what it is not
• The benefits of measuring InfoSec culture
• How to measure InfoSec culture
• Building a InfoSec culture report
About me

Awards

🎓 • MSc Information Security
   • MSc International Business
   • BSc Sport Science and Management

🏆 • Built an award winning cyber culture capability
   • Multiple Publications

Experience

BAE SYSTEMS

THOMSON REUTERS

PwC
People in every workplace talk about organizational culture, that mysterious word that characterizes the qualities of a work environment.
Why measure security culture?

Identify your cultural blind spots

Build a tailored security culture programme

Demonstrate a return on investment
Common misconceptions

Phishing tests, USB drops, Desk Sweeps etc.

eLearning scores
The problem

How do you measure InfoSec culture in a practical way?
Step 1: Build your measurement framework
Your culture is unique

Security First

A InfoSec culture where InfoSec is embedded in all that we do with employees taking responsibility to safeguard our organization to challenge poor security practices
Step 2: Discovery Exercise via focus groups
Focus groups

Good facilitator

Watch out

Utilise your time
Discovery exercise

A InfoSec culture where InfoSec is embedded in all that we do with employees taking responsibility to safeguard our organization to challenge poor security practices.
Focus group: Security first

Discover

Environmental Factors
### Responses

<table>
<thead>
<tr>
<th>Environmental Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

- I understand the **consequences of clicking on a link** so, I know my **manager would support** my action if I prioritize security.

- If I **saw no visible signs of any damage**, I would carry on working.

- The **leaders** talk about security in the **eLearning** I have done, so I know about the **impact of clicking on a link**.
## SAMPLE grid: Security first

<table>
<thead>
<tr>
<th>Responses</th>
<th>Environmental Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Consequential understanding /Do not understand consequences</td>
</tr>
<tr>
<td>I understand the <strong>consequences of clicking on a link</strong> so, I know my manager would support my action if I prioritize security.</td>
<td></td>
</tr>
<tr>
<td>If I <strong>saw no visible signs of any damage</strong>, I would carry on working.</td>
<td></td>
</tr>
<tr>
<td><strong>The leaders</strong> talk about security in the eLearning I have done, so I know about the <strong>impact of clicking on a link</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

Sensitivity: Public
## SAMPLE grid: Security first

<table>
<thead>
<tr>
<th>Responses</th>
<th>Environmental Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Consequential understanding /Do not understand consequences</td>
</tr>
<tr>
<td>I understand the consequences of clicking on a link so, I know my manager would support my action if I prioritize security.</td>
<td>✔</td>
</tr>
<tr>
<td>If I saw no visible signs of any damage, I would carry on working.</td>
<td></td>
</tr>
<tr>
<td>The leaders talk about security in the eLearning I have done, so I know about the impact of clicking on a link.</td>
<td></td>
</tr>
</tbody>
</table>
## Responses

<table>
<thead>
<tr>
<th>Environmental Factors</th>
<th>Consequential understanding /Do not understand consequences</th>
<th>Tone at the top/Management/Leadership</th>
</tr>
</thead>
<tbody>
<tr>
<td>I understand the <strong>consequences of clicking on</strong> a link so, I know my manager would support my action if I prioritize security.</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>If I <strong>saw no visible signs of any damage</strong>, I would carry on working.</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>The <strong>leaders</strong> talk about security in the <strong>eLearning</strong> I have done, so I know about the impact of clicking on a link.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sensitivity: Public
<table>
<thead>
<tr>
<th>Environmental Factors</th>
<th>Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consequential understanding</td>
<td>Tone at the top/Management/Leadership</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Responses</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>I understand the <strong>consequences of clicking on a link</strong> so, I know my manager would support my action if I prioritize security.</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>If I <strong>saw no visible signs of any damage</strong>, I would carry on working.</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>The <strong>leaders</strong> talk about security in the eLearning I have done, so I know about the <strong>impact of clicking on a link</strong>.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## SAMPLE grid: Security first

<table>
<thead>
<tr>
<th>Responses</th>
<th>Environmental Factors</th>
<th>Training</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Consequential understanding /Do not understand consequences</strong></td>
<td><strong>Tone at the top/Management/Leadership</strong></td>
<td>✔</td>
</tr>
<tr>
<td>I understand the <strong>consequences of clicking on a link</strong> so, I know my <strong>manager would support</strong> my action if I prioritize security.</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>If I <strong>saw no visible signs of any damage</strong>, I would carry on working.</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>The <strong>leaders</strong> talk about security in the <strong>eLearning</strong> I have done, so I know about the <strong>impact of clicking on a link.</strong></td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

Sensitivity: Public
## SAMPLE grid: Security first

<table>
<thead>
<tr>
<th>Responses</th>
<th>Consequential understanding /Do not understand consequences</th>
<th>Environmental Factors</th>
<th>Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>I understand the <strong>consequences</strong> of clicking on a link so, I know my manager would support my action if I prioritize security.</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>If I <strong>saw no visible signs of any damage</strong>, I would carry on working.</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The leaders <strong>talk about security</strong> in the eLearning I have done, so I know about the <strong>impact of clicking on a link</strong>.</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sensitivity: Public
Results of the discovery exercise

- Environmental Factors
- Tone from the top
- Consequential understanding
- Security First
- Responsibility
- Challenge

A InfoSec culture where InfoSec is embedded in all that we do with employees taking responsibility to safeguard our organization to challenge poor security practices.
Step 3: Measure your environmental factors via surveys
Surveys

- Likert scales
- Build confidence
- Measure smart
Measure Smart

Challenge

Environmental Factors

Environmental Factors

Environmental Factors

Tone from the top

Consequential understanding

Security First

Responsibility

A InfoSec culture where InfoSec is embedded in all that we do with employees taking responsibility to safeguard our organization to challenge poor security practices
SAMPLE questions: Security first

Tone from the top

**Sample Question:** Executive Committee (ExCo) regularly communicates the importance on good info sec behaviours

Consequential understanding

**Sample Question:** I believe my colleagues feel that the consequences are made clear to them about the impact of poor information security behaviours

<table>
<thead>
<tr>
<th>Options</th>
<th>Strongly Disagree</th>
<th>Disagree</th>
<th>Somewhat Disagree</th>
<th>Somewhat agree</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Score</td>
<td>0</td>
<td>20</td>
<td>40</td>
<td>60</td>
<td>80</td>
<td>100</td>
</tr>
</tbody>
</table>
Security first: Company score

Tone from the top

Q1: 42
Q2: 55
Q3: 58
Q4: 65

Consequential Understanding

Company Score

Avg: 55
Overall culture score: Company score

Overall, we are rated as an amber risk.
Step 4: Reporting
Exec summary: Our security culture

Key Findings

Security First: Lorem ipsum dolor sit amet, ei eam pericula elaboraret deterruisset. Cu eam quot dicit utroque. Eu his homero perfecto intellegat, elit senserit rationibus id per..

Challenge: Lorem ipsum dolor sit amet, ei eam pericula elaboraret deterruisset. Cu eam quot dicit utroque. Eu his homero perfecto intellegat, elit senserit rationibus id per..

Responsibility: Lorem ipsum dolor sit amet, ei eam pericula elaboraret deterruisset. Cu eam quot dicit utroque. Eu his homero perfecto intellegat, elit senserit rationibus id per.

Evidence

<table>
<thead>
<tr>
<th>Factor</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Factor 1</td>
<td>55%</td>
</tr>
<tr>
<td>Factor 2</td>
<td>60%</td>
</tr>
<tr>
<td>Factor 3</td>
<td>70%</td>
</tr>
</tbody>
</table>

Total InfoSec Culture Score: 62%

Lorem ipsum dolor sit amet, ei eam pericula elaboraret deterruisset. Cu eam quot dicit utroque. Eu his homero perfecto intellegat, elit senserit rationibus id per.
Value: Security First

Key findings

- Lorem ipsum dolor sit amet, ei eam pericula elaboraret deterruisset. Cu eam quot dicit utroque. Eu his homero perfecto intellegat, elit senseri t rationibus id per.

- Lorem ipsum dolor sit amet, ei eam pericula elaboraret deterruisset. Cu eam quot dicit utroque. Eu his homero perfecto intellegat, elit senseri t rationibus id per.

- Lorem ipsum dolor sit amet, ei eam pericula elaboraret deterruisset. Cu eam

Evidence

- 32%

...Lorem ipsum dolor sit amet, ei eam pericula elaboraret deterruisset. Cu eam

Lorem ipsum dolor sit amet, ei eam pericula elaboraret deterruisset. Cu eam

Lorem ipsum dolor sit amet, ei eam pericula elaboraret deterruisset. Cu eam

‘Lorem ipsum dolor sit amet.’

Lorem ipsum dolor sit amet, ei eam pericula elaboraret deterruisset. Cu eam

Consequential Understanding

Tone from the top
Environmental Factor: Tone from the top

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weakness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opportunity</td>
<td>Threats</td>
</tr>
<tr>
<td>(Indicative solutions)</td>
<td>(So what?!)</td>
</tr>
</tbody>
</table>

Key statistics

- 60%: Lorem ipsum dolor sit amet, sea stet
- 45%: Lorem ipsum dolor sit amet, sea stet
- 67%: Lorem ipsum dolor sit amet, sea stet
Step 5: Using your report
Insert roadmap here
Summary
Next steps

1. Agree with your executive committee your ‘InfoSec cultural statement’ and ‘values’

2. Discover your environmental factors through a discovery exercise using focus groups

3. Measure your InfoSec culture by creating a tailored survey based on your environmental factors

4. Analyse and report your security culture
Questions? Feel free to contact:

✉️ Lushin.Premji@tr.com
LinkedIn Lushin Premji