Every day, due to data hacks or breaches, another company is in the news. IBM (2014) indicate that after a information security breach a company will lose about $145 per record.
- Target’s 2013 breach cost $191M
- Home Depot’s 2014 cost $62M
72% of all security incidents result from:
- Miscellaneous errors by employees
- Insider and privilege misuse

Organizations need employees that are motivated to follow IT policies. Organizations such as the IT Governance Institute and ISACA recommend governance structures to prevent security incidents from happening.

Literature from Chen, Deci et al., Payne et al., and Verizon discuss the importance of ITSG and general methods to develop.

**Data Collection**
- Participants included 116 University of Minnesota TC faculty and staff.
- Participants completed a 15 minute online survey.
- Surveys included three reward scenarios and one post scenario questionnaire.
- Post scenario questionnaire included adapted questions from the Intrinsic Motivation Inventory (IMI) Survey tool (Ryan 1982).

**Data Analysis**
- Dependent variable: the level of motivation
- Independent variables: types of reward (oral, written, no reward)
- One tailed two sample t-test
- Interest/enjoyment is the largest predictor of intrinsic motivation and was used as the leading indicator of intrinsic motivation in this study.

**Hypothesis**
Non-contingent oral reward will have a stronger positive effect on ITSG conformance than non-contingent written reward.

**Results**

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Oral</th>
<th>Written</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean</td>
<td>3.542</td>
<td>3.781</td>
<td></td>
</tr>
<tr>
<td>Standard Deviation</td>
<td>1.168</td>
<td>1.305</td>
<td></td>
</tr>
<tr>
<td>P-Value</td>
<td>0.072</td>
<td></td>
<td>Reject null at : Level of Significance</td>
</tr>
</tbody>
</table>

Written reward has a higher impact on intrinsic motivation to follow IT security policies than does oral reward.

**Hypothesis Evaluation**
The hypothesis was not supported. The results for the interest/enjoyment for oral and written reward are as follows:

**Participant Demographics**
39% Have average security policy experience
50% Under age 30
71% Female
73% Identified as Asian, Hispanic or Latino, and other
27% Identified as Caucasian

**T-test results for all scenarios**

<table>
<thead>
<tr>
<th></th>
<th>Interest/Enjoyment</th>
<th>Perceived Choice</th>
<th>Perceived competence</th>
<th>Pressure/Tension</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oral &gt; Written</td>
<td>0.072</td>
<td>0.234</td>
<td>0.500</td>
<td>0.424</td>
</tr>
<tr>
<td>Oral &gt; Control</td>
<td>0.448</td>
<td>0.418</td>
<td>0.422</td>
<td>0.323</td>
</tr>
<tr>
<td>Written &gt; Control</td>
<td>0.085</td>
<td>0.187</td>
<td>0.428</td>
<td>0.255</td>
</tr>
</tbody>
</table>

**Discussion**
The effect of oral reward was not significantly different than no reward. Management Message:
In the context of IT security policies they should utilize a written reward, such as a certificate, to enhance intrinsic motivation of employees.

Intrinsic motivation predictor showed significance, but not perceived motivation.

Management Message:
Although it may appear that employees do not react differently among different reward styles, internally employees’ intrinsic motivation will be increased when given a written reward in the context of IT security policies.

Managers should not be discouraged if it appears employees do not become any more motivated after receiving a written reward.

**Application & Future**
The most important implication of this study is that it allows organizations to better understand how they can motivate employees in the context of IT security.

This study suggest that organizations should use written rewards instead of oral reward to improve ITSG conformance. Improving employee intrinsic motivation to follow IT security policies will help secure the organization’s information and prevent future financial and reputation losses.

This study can be built on by conducting a physical experiment where participants perform a set of activities and interact with the scenarios prior to completing the survey.

**Acknowledgements**
Author expresses gratitude to Corrinne Fiedler for her advice and guidance, and the University of Minnesota’s Undergraduate Research Opportunity’s Program (UROP) for providing funds for this project.