

# Quick Assessment

This quick assessment might give you some insight into your current state of readiness. We've provided a list of very common issues. Score yourself based on your knowledge. If you don't know for certain that something is in place to prevent an issue, you have to score its impact as high.

**IMPACT** - If this happened, what would be the impact? A score of 0 would mean there was no impact at all. 1 to 2 means it's inconvenient. 3 to 4 means a business interruption that is noticeable to customers. 5 means there is a significant impact that prevents work or creates a real issue for the business.

**PROBABILITY** - A score of 0 means it absolutely couldn't happen. A score of 5 means it will definitely happen. Hint – we haven't chosen anything that we haven't seen in most businesses. Second hint - every business gets hacked.

Type of threat	A. Impact <i>0 (low) to 5 (highest)</i>	B. Probability <i>0 (low) to 5 (highest)</i>	Score (A X B)
<b>Human Factors</b>			
<ul style="list-style-type: none"> <li>Accidental deletion or destruction of key data</li> </ul>			
<ul style="list-style-type: none"> <li>Inadequate security awareness (creates opportunities for hackers and malware)</li> </ul>			
<ul style="list-style-type: none"> <li>Disregard for security policies (creates security weaknesses)</li> </ul>			
<ul style="list-style-type: none"> <li>Weak passwords (easy to guess or hack)</li> </ul>			
<ul style="list-style-type: none"> <li>Dishonesty or disgruntled employees able to steal information</li> </ul>			

<b>Type of threat</b>	<b>A. Impact</b> <i>0 (low) to 5 (highest)</i>	<b>B. Probability</b> <i>0 (low) to 5 (highest)</i>	<b>Score</b> (A X B)
<b>Policies</b>			
<ul style="list-style-type: none"> <li>No policies</li> </ul>			
<ul style="list-style-type: none"> <li>Policies not enforced</li> </ul>			
<ul style="list-style-type: none"> <li>Policies not up to date (e.g. new federal regulations as of Nov 2018)</li> </ul>			
<b>General</b>			
<ul style="list-style-type: none"> <li>Equipment not secured</li> </ul>			
<ul style="list-style-type: none"> <li>Unauthorized software or hardware connected to network</li> </ul>			
<b>Business Resumption/Recovery</b>			
<ul style="list-style-type: none"> <li>No formal business resumption plan</li> </ul>			
<ul style="list-style-type: none"> <li>Plan exists but hasn't been tested</li> </ul>			
<ul style="list-style-type: none"> <li>Backups not enforced rigorously</li> </ul>			
<ul style="list-style-type: none"> <li>Backups not tested</li> </ul>			
<b>Legal</b>			
<ul style="list-style-type: none"> <li>No privacy policy or privacy officer</li> </ul>			
<ul style="list-style-type: none"> <li>Little or no understanding of regulations and legislation</li> </ul>			
<b>Technical</b>			
<ul style="list-style-type: none"> <li>Software not kept up to date</li> </ul>			
<ul style="list-style-type: none"> <li>Cloud software requirements not understood</li> </ul>			

<b>Type of threat</b>	<b>A. Impact</b> <i>0 (low) to 5 (highest)</i>	<b>B. Probability</b> <i>0 (low) to 5 (highest)</i>	<b>Score</b> <b>(A X B)</b>
Technical (cont'd)			
<ul style="list-style-type: none"> <li>• Anti-virus software not updated consistently</li> </ul>			
<ul style="list-style-type: none"> <li>• Administrative accounts not managed (too widely used, weak passwords, shared accounts etc.)</li> </ul>			
<ul style="list-style-type: none"> <li>• Software not thoroughly tested before implementing</li> </ul>			
<b>TOTAL SCORE</b>			

**TOTAL SCORE** – Every company is different, and everyone may score differently, but we suggest the following guidelines. Any score above 120 should have warning lights going of. You have significant exposure. A score between 50 to 120 should still be cause for concern. With a score of 50 you can focus on the key issues where you are vulnerable.

**OVERALL ASSESSMENT**

This is an abbreviated and simplified version of the threat assessment that we would do for a business. Our full threat assessment is more rigorous and is based on ISO standards, best practices and current legislation/regulation. Hopefully after this quick self-assessment you can see how valuable a full assessment would be. But even this quick assessment should give you some good information about what you need to do to protect your business.