# The greenCore IT Security Incident Taxonomy Model*

| | | |
|---|---|---|
| An **ATTACKER** | • Hackers<br>• Vandals<br>• Voyeurs<br>• Spies/Terrorists<br>• Corporate Rivals<br>• Professional Thieves | **NO** Business control |
| uses a **TOOL/ MECHANISM** | • Physical<br>• Logical<br>• Active(performs action)/Passive (watches/listens) | **NO** Business control |
| to exploit a **VULNERABILITY** | • Hardware (e.g. Remote Management)<br>• Software (e.g. Bug)<br>• Process (e.g. Password Reset)<br>• People (e.g. Insider)<br>• Policy (e.g. Firewall misconfiguraion) | **SIGNIFICANT** Business control |
| to perform an **AN ACTION** | • Read<br>• Copy/Steal<br>• Modify/Delete<br>• Probe/Scan<br>• Flood<br>• Bypass<br>• Spoof/Decieve | **MODERATE** Business control (once breach occurred) |
| on a **TARGET** | • Data<br>• Network<br>• Account<br>• Process<br>• Application/Platform | **LIMITED** Business control (once breach occurred) |
| resulting in a **CONSEQUENCE** | • Increased Access<br>• Disclosure of information<br>• Corruption/Deletion of Information<br>• Misrepresentation of information/reputation<br>• Denial of Service<br>• Theft of resources | **LIMITED** Business control (once breach occurred) |
| for the purposes of an **OBJECTIVE** | • Malicious damage<br>• Challenge/Thrill<br>• Status<br>• Political gain<br>• Financial gain<br>• Personal gain | **NO** Business control (once breach occurred) |

* Adaption of the TERENA Incident Taxonomy

©

greenCore IT SOLUTIONS

A: Level 3, 480 Collins Street Melbourne, VIC, 3000
W: www.greencore.com.au
E: contact@greencore.com.au
T: (03) 8610 6380 80