ITAC Cyber Security Technology Summit

John Hewie
National Security Officer
Microsoft Canada

jhewie@microsoft.com
The cybersecurity landscape realities

- Cybercrime is incredibly profitable
- Security skills are in short supply
- Virtually anything can be attacked
Disrupt Attacker ROI
Prioritize investments to maximize impact

Security Return on Investment (SROI)

Defender Return: **Ruin Attacker ROI**
- Deters opportunistic attacks
- Slows or stops determined attacks

Defender Investment:
- Security budget
- Team time/attention

**Attacker Return:**
Successful Monetization
- Rapid detection and response drives down predictability and quantity of return

**Attacker Investment:**
Increase Attack Friction & Cost
- Prioritizing defense can rapidly raise impact attacker cost & friction
**Cost of Attack Examples**

- **Attack techniques observed in your environment**
  - **High likelihood of use**
    - **Low cost**
  - **Low likelihood of use**
    - **$\$$ High cost**

- **Zero day vulnerabilities in common software/protocols**
- **Zero day vulnerabilities in specialized protocols/devices**

**Note:** For-profit attackers generally follow rational economic behavior and favor cheaper/available attacks. Advanced attacks (exceptions) are expected if:

- Low cost attacks are mitigated and criminals value your assets highly
- Advanced nation state actors are targeting you (with their library of advanced techniques)
<table>
<thead>
<tr>
<th>Info Sharing and Collab</th>
<th>Small and Medium Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improve detections and automated response</td>
<td>30%+ of Canadian GDP</td>
</tr>
<tr>
<td>Resource intensive</td>
<td>Most vulnerable population</td>
</tr>
<tr>
<td>Trusted 1:1 relationships</td>
<td>Education – GetCyberSafe</td>
</tr>
<tr>
<td>High data quality with context</td>
<td>Cloud specific guidance</td>
</tr>
<tr>
<td>Derivative info sharing concerns</td>
<td>Cyber Essentials certification</td>
</tr>
<tr>
<td>CCIRC, CCTX, ISACs – need to focus limited resources</td>
<td></td>
</tr>
</tbody>
</table>
Thank you