## PwC’s Board Cybersecurity Governance Framework

We’ve designed the following framework and questions to help Boards and senior executives build effective cybersecurity governance.

<table>
<thead>
<tr>
<th>Cybersecurity strategy</th>
<th>Cybersecurity controls</th>
<th>Third party relationships</th>
<th>Cybersecurity governance</th>
<th>Vulnerability management</th>
<th>Security monitoring</th>
<th>Critical data and assets</th>
<th>Compliance, assurance and risk</th>
<th>Breach response</th>
<th>Awareness and training</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q: Does management have a cybersecurity strategy that links to business priorities and objectives?</td>
<td>Q: Does management have adequate technical and process controls in place for the company?</td>
<td>Q: Does management have visibility on its third party cybersecurity risks (e.g. contractors, suppliers and partners)?</td>
<td>Q: Does management have a cybersecurity policy and breach response procedure in place?</td>
<td>Q: Does management know where the company’s vulnerabilities are in the corporate IT and operational technology environments? Is it conducting threat, vulnerability and breach assessments and penetration testing?</td>
<td>Q: What processes and tools are in place to alert management when the company has been breached?</td>
<td>Q: Has management defined and located the most valuable assets ‘Crown Jewels’ that could be threatened by a cybersecurity attack (e.g. critical data and IT and operational technology systems)?</td>
<td>Q: Does management understand its cybersecurity and privacy compliance obligations across all company jurisdictions?</td>
<td>Q: Does management have the correct plans and people in place to respond swiftly to a breach?</td>
<td>Q: Have employees been adequately trained to understand their risks, obligations and roles when it comes to cybersecurity?</td>
</tr>
<tr>
<td>Q: Does management’s cybersecurity strategy consider the range of impacts that cyber threats may have on the company?</td>
<td>Q: Does management continue to understand the details of these controls as the networks evolve?</td>
<td>Q: How confident is management that these third parties manage their cybersecurity risks adequately on management’s behalf?</td>
<td>Q: Does management sufficiently oversee, monitor and report on cybersecurity governance?</td>
<td>Q: How well and how often does management assess and report on its security posture across the business?</td>
<td>Q: Does management effectively monitor what’s coming into and leaving the corporate IT systems and networks? And does management monitor internal network and end user activities in corporate and operational environments?</td>
<td>Q: Does management know who has remote or direct access to these assets and how and when they can access them?</td>
<td>Q: Does management effectively use Internal Audit and third parties to maintain compliance?</td>
<td>Q: Do board, executive and internal teams understand their roles and the breach communications plan?</td>
<td>Q: Does management have a good cybersecurity culture in the head office and other operational locations?</td>
</tr>
</tbody>
</table>
**Context for cybersecurity**

**Three cybersecurity and privacy areas**

Cyber protection has become complex and needs to cover the following:
- your corporate IT network and partner networks
- systems that monitor and control your operations
- personal and mobile devices that may be connected to either or both of the above

**Cybersecurity attackers**

The profile of the traditional hacker has changed. We’re now facing attacks from highly disciplined teams employed by foreign nation-states, organized crime groups, activist groups and data brokers. And over 50% of breaches involve current or past employees.

**Cybersecurity business impacts**

Impacts from cybersecurity and privacy breaches are broader than they may initially appear. They may include the following:
- financial
- reputational
- operational
- legal
- environmental
- regulatory
- health and safety
- competitive
- customer retention
- investor confidence

**We view cybersecurity differently**

Establishing sound cybersecurity and privacy capabilities will increase the likelihood that your organization will perform as planned. This isn’t about technology—it’s about understanding and managing the continuity of your data, business availability, safety and reputation. You must demonstrate the link between cybersecurity threats and your desired business performance.

**Four cybersecurity actions**

<table>
<thead>
<tr>
<th>1. Strategy and transformation</th>
<th>3. Privacy and consumer protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Build a strategic cyber governance operating model</td>
<td>• Know your privacy regulatory requirements</td>
</tr>
<tr>
<td>• Identify your key data</td>
<td>• Test your systems continuously</td>
</tr>
<tr>
<td>• Establish policies, standards and processes to execute and sustain your security program</td>
<td>• Assess and report on your security risks and controls</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2. Implementation and operations</th>
<th>4. Incident response, threat intelligence and information sharing</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Invest in people with the right skills</td>
<td>• Have a plan to respond when breaches occur</td>
</tr>
<tr>
<td>• Acquire security systems to create a strong perimeter and monitor 24/7</td>
<td>• Define roles, responsibilities and communications from the Board to technical remediation levels</td>
</tr>
<tr>
<td>• Procure specialized cybersecurity services</td>
<td></td>
</tr>
</tbody>
</table>

**Contact our team to discuss a plan for your organization**

- **Richard Wilson**  
  Partner, Cybersecurity & Privacy  
  416 941 8374 | richard.m.wilson@pwc.com

- **Sajith (Saj) Nair**  
  Partner, Cybersecurity & Privacy  
  416 815 5185 | s.nair@pwc.com

- **David Craig**  
  Partner, Cybersecurity & Privacy  
  416 814 5812 | david.craig@pwc.com