Cybersecurity risks are increasing as a result of the number of ageing or obsolete devices on the network—more than tripling in the last two years. Businesses are neglecting to patch devices due to time and possible service interruptions, but consequences of cybersecurity issues could be far greater.

Many businesses don’t know how exposed their networks are and:

**Key findings uncovered in the Report**

**Vulnerabilities influenced by a device’s lifecycle status**

<table>
<thead>
<tr>
<th>Current</th>
<th>Ageing</th>
<th>Obsolete</th>
</tr>
</thead>
<tbody>
<tr>
<td>19.4 instances per device</td>
<td>26.8 instances per device</td>
<td>42.2 instances per device</td>
</tr>
</tbody>
</table>

Security advisories rise by 38.1% when a device is ‘ageing’ and there’s a 57.5% increase between ‘ageing’ and ‘obsolete’.

Security threats and vulnerabilities

- High severity instances affected by a device’s lifecycle status are much the same:
  - Current devices: 15.9 instances per device
  - Ageing devices: 22.9 instances per device
  - Obsolete devices: 36.6 instances per device

**Your network is the platform for your digital transformation**

A ubiquitous, flexible, robust and secure network lets you adapt easily to business change, while increasing the maturity of your support environment.

**How to reduce your risk**

- A formal, documented security policy
- Enforce strong password usage and centralize device authentication and management
- Identify critical versus non-critical data and applications and invest in areas that will have the biggest impact on their security
- Ensure you have appropriate detection and response mechanisms in place

**Uncover more data-driven insights and find out how NTT can help you to design and address associated risks.**

**Why are businesses not patching?**

- Many vendors are reverting to issuing less-disruptive upgrade mechanisms to minimize service interruptions and encourage operators to perform more frequent updates
- Vulnerabilities influenced by a device’s lifecycle status
  - Many vulnerabilities (42.2) per device as current (19.4)

**Key findings**

- Increasing vulnerabilities: Increasing threats: Increasing gaps
- Number of security vulnerabilities per device category has seen year-on-year increases of between 12.5% and 44.0% since 2016

**Why are businesses not patching?**

- Many vendors are reverting to issuing less-disruptive upgrade mechanisms to minimize service interruptions and encourage operators to perform more frequent updates
- Vulnerabilities influenced by a device’s lifecycle status
  - Many vulnerabilities (42.2) per device as current (19.4)

**Key findings**

- Increasing vulnerabilities: Increasing threats: Increasing gaps
- Number of security vulnerabilities per device category has seen year-on-year increases of between 12.5% and 44.0% since 2016

**Why are businesses not patching?**

- Many vendors are reverting to issuing less-disruptive upgrade mechanisms to minimize service interruptions and encourage operators to perform more frequent updates
- Vulnerabilities influenced by a device’s lifecycle status
  - Many vulnerabilities (42.2) per device as current (19.4)