

---

# Contents

|   |           |
|---|-----------|
| <b>Foreword</b>   | <b>5</b>  |
| <b>Executive summary</b>  | <b>6</b>  |
| <b>1. Introduction</b>  | <b>8</b>  |
| 1.1 Increasingly hostile threat landscape   | 9         |
| 1.2 Large and persistent protection gap   | 12        |
| 1.3 Structure of the report   | 13        |
| <b>2. The actuarial challenge in quantifying cyber risks</b>                              | <b>14</b> |
| 2.1 Lack of meaningful historical loss data   | 16        |
| 2.2 Anthropogenic features  | 16        |
| 2.3 Complex interdependencies   | 17        |
| 2.4 'Silent' cyber  | 17        |
| 2.5 Reserve development risks   | 18        |
| <b>3. Key pathways to loss accumulation</b>   | <b>19</b> |
| 3.1 Critical infrastructure failure   | 20        |
| 3.2 Supply chain disruption   | 22        |
| 3.3 Zero-day and open-source software vulnerabilities                                     | 23        |
| 3.4 Mass liability claims   | 25        |
| 3.5 Disaggregating factors – Important caveats  | 25        |
| <b>4. Latest advances in accumulation risk assessment</b>                                 | <b>27</b> |
| 4.1 Innovations in data capture and analytics   | 28        |
| 4.2 Probabilistic models  | 29        |
| 4.3 Deterministic scenarios   | 34        |
| 4.4 Irreducible uncertainty   | 35        |
| <b>5. Towards more optimal risk sharing</b>   | <b>37</b> |
| 5.1 Broader re/insurance participation  | 38        |
| 5.2 Capital markets involvement   | 39        |
| 5.3 Collaboration with critical infrastructure providers and government security agencies | 41        |
| 5.4 Government backstops  | 42        |
| 5.5 Enhanced IT-sector liability  | 43        |
| <b>6. Concluding remarks</b>  | <b>45</b> |
| <b>References</b>   | <b>48</b> |