**Ransomware Updates to Consider**

**Section 1-3: Letter A: General Information Technology Review**

*Proposing new sub-section which covers ransomware concepts and cyber hygiene at a high level.*

**Ransomware**

Ransomware is one of the more common manifestations of a cybersecurity risk. Ransomware attacks pose a significant risk to confidentiality and availability on company data. It is difficult to predict when and where a ransomware attack will strike, so it is important for a company to maintain strong cyber hygiene habits to stay ready for ransomware attacks. At a minimum, insurers with good cyber hygiene do the following:

* Patch their systems/networks regularly, timely, and in accordance with application updates
* Require strong passwords and multi-factor authentication
* Have email filtering and anti-phishing training for employees
* Monitor and react to suspicious activity on their network
* Have system backups that are stored in an air gapped, offline environment that is inaccessible from the internet; this backup can be quickly deployed in the event the production environment is infected. Companies should test backup deployment regularly.
* Have firewalls within the network so someone with unauthorized access cannot move laterally
* Limit user access rights to the minimum necessary to perform their job
* Have and test a robust incident response plan

**Exhibit C – Part 2 Narrative guidance – Instructional Notes**

*Adding areas of focus in the Exhibit C table in a similar format as the procedures related to cybersecurity.*

**INSTRUCTION NOTE 3:** Examiners may determine that cybersecurity risks are significant for the insurer under examination. This may be based on responses provided to the ITPQ, results of planning and examiner’s judgment. To ensure that the examination procedures performed include an adequate response to the insurer’s cybersecurity risk, which can affect multiple facets of the IT environment, examiners may consider performing procedures in relation to risk statements APO 1, APO 10, APO 12, DSS 02 and DSS 05. Note these risk statements and associated procedures may or may not explicitly mention the threat of cybersecurity in the language presented, but examiners should customize the procedures provided to respond to this risk as appropriate. DSS 04 covers the protection of system backups in the event of a ransomware attack. Examiners may determine that additional risks are relevant when considering cybersecurity and ransomware exposure, and should tailor their work program based on information available on the exam. Additional considerations for cybersecurity concerns are located in Section 1-III (A) of the Examination Handbook guidance, entitled “General Information Technology Review.”

**Exhibit C – Part 2 Table**

*Proposing new test procedures to the Exhibit C table.*

DSS 04 Risk Statement -Inadequate continuity management may result in the inability to ensure critical business functions.

**DSS 04.07**:

|  |  |  |
| --- | --- | --- |
| **Common Controls** | **Preliminary Information Request** | **Possible Test Procedures** |
| All critical backup media, documentation and other IT resources necessary for IT recovery and continuity plans are stored off-site in a secure location. | Provide a copy of policies and procedures relating to the backup of systems and data, including copies of recovery procedures for off-site backups and information about off-site backup locations and/or service providers. | Inquire and verify that data is protected and secured when taken off-site and while in transit to the storage location.  Inquire and verify that the backup facilities are not subject to the same risks as the primary site.  Inquire and verify that there is an air gap between the company’s production environment and backup systems. The air gap should be designed in a manner that if a ransomware attack infects the company’s main production systems, the offline backups could be deployed to replace the infected systems. |

**DSS 04.08:**

|  |  |  |
| --- | --- | --- |
| The company has procedures in place for backup and restoration of systems, applications, data and documentation that are consistent with its business requirements and continuity plan. The backup environment should be isolated, air gapped, and inaccessible from the internet so that information cannot be accessed remotely. | Provide evidence that backup and storage requirements for critical systems, applications, data and related documents are periodically reviewed and aligned with risks and the continuity plan.  Provide evidence that backup and storage environments are properly isolated and inaccessible remotely. | Verify that critical systems, applications, data and related documents that affect business operations are periodically reviewed for alignment with the risk management model and IT service continuity plan.  Verify that adequate policies and procedures for backup of systems, applications, data and documentation exist and consider factors including: 1) Frequency and age of backups. Older backups can be used in the event a newer backup copy is infected. 2) Type of backups (e.g., disk mirroring, external media, full, incremental, air gapped offline copy, etc.). 3) Automated online backups. 4) Data types (e.g., voice, optical). 5) Creation of logs. 6) Critical end-user computing data (e.g., spreadsheets). 7) Physical and logical location of data sources. 8) Security and access rights. 9) Encryption. |