Overview

Diminishing enterprise perimeters have led to a substantial increase in the cyber risk associated with running digital businesses today. A major cybersecurity incident can potentially wipe out millions of dollars in assets and tarnish even the strongest of brands. It is therefore imperative that organizations should proactively measure and manage the financial exposure to cyber risks. By using manual cyber risk management processes organizations are left with disconnected efforts and ineffective controls. Furthermore, due to information silos, security teams not only have incomplete visibility of their security posture to make informed decisions but also have an inaccurate view of their risk exposure.

The need of the hour is a robust Cyber Risk Quantification Solution that can help security teams quantify the cyber risk exposure across people, technology, and processes. Risks need to be identified, prioritized, and remediated at the earliest. Such a solution will enable organizations to identify the appropriate cybersecurity investments to be made, thereby building a more resilient business.

Need for Quantitative Cyber Risk Management

- Structured and unbiased approach to risk quantification
- Comprehensive risk assessment and management
- Justified cyber security investment
- Complete trend analysis of risk over time
- Fair visibility on adequate cyber risk insurance coverage

Infosys Cyber Risk Quantification Service powered by SAFE (Security Assessment Framework for Enterprise)

An enterprise-wide cyber risk quantification view allows an organization to measure and mitigate risks at each level, starting from a single asset or employee to the entire line of businesses, departments and locations. It provides people assessment on both macro and micro level, processes, and policies assessment along with technology – inside out and outside in along with third party risk assessment.
Cyber Risk Quantification Solution & Services

Consulting & Advisory

• Assessing existing cyber risk management practices
• Developing automated, real time and quantitative cyber risk management practice
• Establishing risk management framework aligned with industry standards and regulatory compliance
• Improving cyber risk maturity through effective cyber risk control management

Cyber Risk Quantification (CRQ) Implementation

• Implementing CRQ solution
• Onboarding people, process, policy, technology and third parties to the risk assessment framework
• Integrating CRQ solution with client ecosystem

Continuous Monitoring and Maintenance

• On-boarding and off-boarding assets, assessing policies and running tailored campaigns
• Continuous risk quantification and monitoring, reporting high risk assets, users and vendors
• Providing continuous compliance management
• Providing risk dashboards for improving visibility to internal and external stakeholders

Remediation Governance

• Integrating CRQ solution with ITSM/GRC tools for systematic tracking of remediation activities
• Providing prioritized remediation insights and recommendations
• Providing simulation capability to proactively assess the efficacy of remediation recommendations

Activities

<table>
<thead>
<tr>
<th>DIAGNOSE</th>
<th>DESIGN</th>
<th>DELIVER</th>
<th>DEFEND</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Share prerequisites and onboarding forms</td>
<td>• Provisioning Infrastructure, access &amp; SSL certificate for our CRQ product deployment</td>
<td>• CRQ tool Kick-off Workshop with all stakeholders</td>
<td>• Handover the post migration support activities to BAU team</td>
</tr>
<tr>
<td>• CRQ Server Provisioning &amp; providing privileged access</td>
<td>• Infrastructure team to provide asset inventory inline with pre-requisites</td>
<td>• Installation &amp; commissioning of CRQ solution</td>
<td>• Creating Playbook based on learnings for team for on-boarding any new assets</td>
</tr>
<tr>
<td>• Provisioning of SSL Certificate</td>
<td>• Application team to share latest PT Reports for in-scope applications</td>
<td>• CRQ server hardening as per Client’s security policies</td>
<td>• Supporting in risk prioritization and risk remediation by integrating with ITSM tools.</td>
</tr>
<tr>
<td>• Updating the Asset Onboarding details</td>
<td>• Access to the asset inventory &amp; applications PT report to be on-boarded onto our CRQ product</td>
<td>• User role creation</td>
<td></td>
</tr>
<tr>
<td>• Validate the Asset onboarding details</td>
<td>• Tools configuration to be shared for integration</td>
<td>• Integration of our CRQ solution with Client tools based on the product support available</td>
<td></td>
</tr>
<tr>
<td>• Signoff from Customer team on the assets to be onboarded on our CRQ product</td>
<td></td>
<td>• Provide Phase wise approach for assets on-boarding</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For validation, on-boarding sample unique technology devices to CRQ product asset &amp; applications</td>
<td></td>
</tr>
</tbody>
</table>

Outcome

| • CRQ Solution Requirements | • CRQ solution architecture and design | • CRQ Test Results | • CRQ solution rollout for the business units in scope in a phased manner |
| • Specification Document | • Test plan and approach | • CRQ Operational Runbook | • CRQ solution is monitored on continuous basis |
| • CRQ Governance Model | • CRQ product configured | • Larger rollout plan and user and administrator training needs |
A panoramic view of Enterprise Cyber Risk Quantification solution

**Key Business Benefits**

- **Real-time visibility of the cyber risk posture**
- **Support adherence to regulatory compliance requirements such as NIST CSF, ISO 27001, PCI DSS, HIPAA and SOX**
- **Support cyber insurance policy selection based on actual risk exposure**
- **Clear communication of risk to senior leadership**

To know more, please write to us at cybersecurity@infosys.com

For more information, contact askus@infosys.com