Ostrich
Cyber-Risk

Use Case: Cyber Risk Management with the Ostrich Cyber-Risk Birdseye Application

Background: A global financial services firm manages sensitive customer information and transactions through various digital platforms. Due to the rising cyber threats and regulatory pressures, the company requires a strong cyber risk management solution to proactively identify, assess, and mitigate cyber risks across its infrastructure and applications.

Objective: Implement the Ostrich Cyber-Risk Birdseye SaaS cyber risk management application to enhance cyber risk management capabilities. This is done using industry loss data to determine the organization's biggest financial risks and mapping those risks to the NIST Cybersecurity Framework (NIST CSF 2.0) within Birdseye. The assessment is further mapped to controls from NIST 800-53 Framework and MITRE ATT&CK Techniques, Tactics, and Procedures (TTPs). These mappings will then be automatically quantified based on the FAIR (Factor Analysis of Information Risk) ontology within the application to show the financial impact of top cyber risks for effective prioritization of remediation efforts.

Use Case Scenario:

1. **Risk Identification:**
   - The company licensed the Ostrich Cyber-Risk - Birdseye application.
   - Company structure was set up via business units (with Ostrich customer experience team).
   - Industry data provided within Birdseye from trusted sources including industry reports such as the Verizon DBIR and aggregated cyber insurance claims data via sources like Advisen.
   - Industry data was filtered by company size, location, and industry to highlight the most frequent and costly risks to the business.

2. **Risk Assessment and Control Mapping:**
   - The company conducted a NIST CSF assessment in the Birdseye application and set three-month target objectives for remediation.
   - The Birdseye application then mapped the assessment results from the NIST CSF sub-categories to NIST 800-53 controls and MITRE ATT&CK TTPs.
   - The Birdseye application then mapped the assessment results to the specific threat data for the company's industry.

3. **Automated Cyber Risk Quantification (CRQ):**
   - Using the FAIR ontology, Birdseye automatically quantified cyber risks in financial terms, considering factors such as threat type, vulnerabilities, and control effectiveness.

4. **Risk Prioritization and Remediation:**
   - Risks were automatically prioritized based on their financial impact and resulted in actionable insights for remediation.
   - The company's cybersecurity team then made informed decisions about resource allocation and prioritized remediation efforts to reduce the most significant financial risks.

5. **Compliance and Reporting:**
   - The company used Birdseye outputs to generate reports that aligned with regulatory requirements and internal governance standards.
   - The CISO took reports to the Board for enhanced quarterly cybersecurity review.

Outcomes:

- **Enhanced Visibility:** The cybersecurity team felt they gained a holistic view of cyber risks across the organization's landscape.

- **Financially Informed Decision Making:** The CISO was able to prioritize cybersecurity investments with limited budget, based on Board approval by understanding the financial consequences of top risks.

- **Compliance and Audit Readiness:** Because Birdseye used trusted industry standard frameworks such as NIST CSF, NIST 800-53, and FAIR, it facilitated smoother audits and regulatory inspections.

- **Ongoing Program Management:** By leveraging the Ostrich Cyber-Risk Birdseye application, the company can effectively manage cyber risks, protect sensitive data, and maintain trust with its customers and stakeholders in the dynamic landscape of cybersecurity threats on an ongoing basis.