IT Security, Risk, & Enterprise Resiliency Program Updates

Robert Sellers, VP-Chief Technology Officer
Wendy Emanuelson, Director-IT Security & Risk

CITIZENS
PROPERTY INSURANCE CORPORATION

What We Do

Security Operations

- IT Security Operations Communications and Support
- IT Security Network and Systems Event Monitoring
- Threat and Vulnerability Management
- Baseline Compliance Scans
- IT Security Incident Response
- IT Security Awareness and Education
- IT Security Design and Implementation
- Systems Development Life Cycle
- New Software and Firewall Request Analysis
- Subject Matter Expert Support on Citizens' Initiatives
    - Information Security Standards Assessments (ISSA)
- Security Tool Administration
- Citizens Information Security Incident Response Planning

Enterprise Resiliency

- Crisis Management
- Enterprise Business Continuity
- IT Disaster Recovery
    - DR Planning & Exercises
- Claims IT Catastrophe Assurance and Response
- Business Impact Analysis
- Subject Matter Expert Support on Citizens' Initiatives
    - Resiliency Assessments

Governance, Risk, & Compliance (GRC)

- Citizens IT Risk Identification, Management & Remediation
- Risk Assessment of Citizens' Technology Infrastructure and Applications
- Assist and advise on development of Remediation Plans
- Third Party Risk Management
- Citizens' IT Programs and Functions Regulatory Compliance Review
- IT Controls Evaluation and Improvement
- Audit Entities Liaison Support toward Value-added Audit Outcomes.
- Subject Matter Expert Support on Citizens' Initiatives
    - Information Security Standards Assessments (ISSA)

Application Security Architecture

- IT Security Applications Administration
- Liaison with:
    - Application Development,
    - Systems Analysts,
    - Release Managers, and
    - Enterprise Architects
- Identify, design and apply security controls for applications
- Review Secure Code Practices
- Develop Security Champions

Security Solution Architecture

- Provides technical guidance to IT security teams.
- Primary technical point of contact for complex enterprise projects and provides technical security guidance and solutions.
- Works collaboratively with key stakeholders to design, develop, document and implement security integrated solutions.
- Evaluates process improvements through automation, technical process efficiency using new and existing technology and security controls that benefits the entire enterprise.

CONFIDENTIAL

Citizens One-Page Security, Risk, & Enterprise Resiliency Strategic Plan

Mission

Educate, advise, and empower our workforce to make informed cyber-risk decisions and partner with internal and external teams to make Citizens operating environment safe, secure, and resilient.

Strategy Rationale (Why?)

Summary

Security, Risk, and Enterprise Resiliency encompasses all the ways in which we identify, treat and monitor risk while protecting our information assets and digital platforms, thereby safeguarding Citizens' operations, reputation, and brand.

Target Customers

Citizens collects, process and stores information assets from policy holders, agents, adjusters and employees. Their information and their trust are a valuable company asset that we are obligated to protect.

Strategic Drivers

- Protect the confidentiality, integrity and availability of data \ systems
- The Rise and frequency of Attacks (i.e., Ransomware, Malware)
- Advancement of Technology (i.e., Cloud, Artificial Intelligence)
- Strengthen Citizens' Resiliency

Current Challenges

- **Incident and Threat Management:** Expand visibility into our network while reducing noise to allow more efficient and effective response to threats.
- **Access and Data Loss:** Underdeveloped Identity and Access Management (IAM) and Data Leak Protection (DLP) processes and platforms that pose risk.
- **Risk-Based Decision Making:** Opportunity for maturing risk management practices to support decision making.
- **Application Security:** Low visibility of security related vulnerabilities and security logging in our applications.
- **Resiliency:** Influencing a paradigm shift of how Citizens' personnel understand and strategically apply resiliency best practices (to everything they do) to mitigate and minimize the impacts of disruptive events to enterprise business processes and to maintain continuity of operations.

Strategic Objectives (What?)

Strategic Objectives and Focus Areas

Objective 1: To establish a collaborative environment that leverages the expertise and capabilities of both teams to develop a comprehensive program that supports Citizen's overall strategy and enhances its resilience.

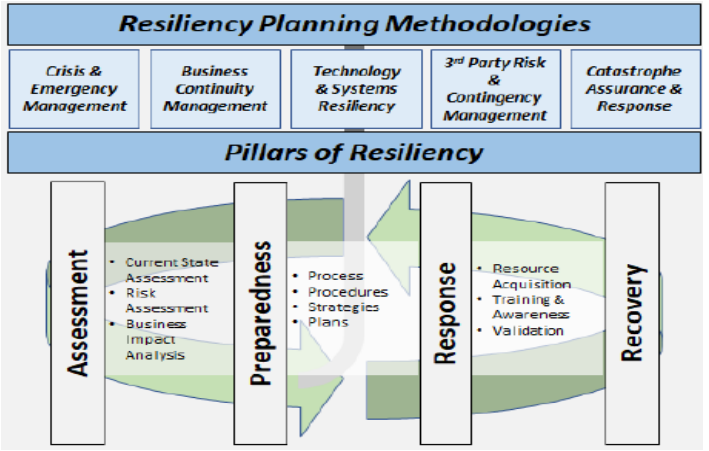
Objective 2: To provide a systematic and proactive approach to identifying, assessing, mitigating, and managing IT risks and threats, while proactively safeguarding Citizens' critical assets and data from potential threats.

Objective 3: Continue to improve the organization's resiliency and ability to respond to any unexpected adverse events that may impact the business.

Strategy Execution Approach (How?)

IT Security & Risk Guiding Principles

- **Protect Confidentiality, Integrity and Availability (CIA Triad):** Deliver controls that are designed to progressively mitigate risk and protect data.
- **Enable Risk Based Decisions:** Provide transparency around cyber security risk to educate and enable risk-based decision making.
- **Partner with Stakeholders:** Partner with stakeholders to protect against cybersecurity threats while promoting accountability and risk ownership.
- **Present Options for Risk Treatment:** Recommend options for compensating controls and risk treatment to support organizational priorities.
- **Invest in appropriate resources to balance risk:** Align use of investments and resources with organizational needs to properly manage risk.



Objective 1

Establish a collaborative environment that leverages the expertise and capabilities of both teams to develop a comprehensive program that supports Citizen's overall strategy and enhances its resilience.

Knowledge Sharing

Gaining a **better understanding of the tools and process** as well as the focus of each of the different Swim lanes.

Opportunities for Improvement

Identification of opportunities to streamline work efforts, **minimize overlapping work efforts and automate workflows.**

Build Team Resiliency

Cross Training team members to become T shaped, **building resiliency within the team, the department, and the Organization.**

Value

Focus on Value to Citizens.

Moving from more reactive to proactive approach throughout.

Objective 2: SecOps Optimization Assessment Completed

Current State

SDA's evaluation of the CPIC SecOps Team's tools and practices revealed a **ROBUST SECURITY ARCHITECTURE**, **SKILLED ANALYSTS**, and several **MATURITY INITIATIVES** already underway.

Robust Security Architecture	By investing in a wide set of Microsoft products and complimentary toolsets, CPIC can expect excellent security visibility across their "estate."
Skilled Staff	The small but highly competent team, with advanced domain knowledge, skills and abilities is an organizational asset and force multiplier.
Processes Maturity	Whether processes are informal, partially documented or complete & reviewed regularly, the SecOps Team has invested time in the standardization of processes.
Executive Support	Resources and responsiveness to needs from executive staff demonstrates organizational commitment to cybersecurity.

In Progress

Optimize Tool Set

Establish a **single pane of glass**; Gain up to 94%-time saved, triaging and responding to alerts with automation

In Progress

Improve SecOps Metrics

Define meaningful metrics to evaluate SecOps effectiveness and provide risk visibility to key stakeholders and risk executives.

In Progress

Improve Vulnerability Management

Measure compliance using metrics, assessing risk regularly, and establishing an exception approval process to enforce wider compliance.

Objective 3

Continue to improve the organization's resiliency and ability to respond to any unexpected adverse events that may impact the business.

Program Updates and Activities 2022 - 2023

- Operational Equipment Gap Analysis
  - Completed analysis for operational equipment dependent on technology to minimize risk of SPOFs (Single Point of Failure)
- Enterprise Technology Resiliency/Recovery (DR) Planning & Exercises
  - Annual Plan Maintenance Complete (July 2023)
  - Quarterly Bubble Testing Complete for Winter Haven (DR) and CSX (production) Mission Critical Systems (Quarterly cadence)
  - Annual Failover Exercise – Liferay External (8.31.2022)
  - Annual Failover – Citizens Insurance Suite - Completed August 12, 2023
- Cloud Migration SME support for resiliency strategy and activities
- Organizational Resiliency Capabilities Assessment Tool acquired
- 21 Solicitations provided with Resiliency Consultative SME Services
- 11 Initial Resiliency Assessments completed

Objective 3: CAT Assurance and Response

CAT Preparation and Assurance

- Annual Assurance process completed (155 checklist items)
  - Completed performance load testing for 425K claims event, concurrent with 1.5MM PIF count for 2023 storm season
  - MS Teams Telephone interim implementation and validation for Independent Adjusters
  - Enhanced Independent Adjusters Onboarding process to incorporate telephony changes
- Field Services Readiness
  - Field Service Vehicles, Claims Service Vehicles and Satellite services ready
  - Mock Exercises completed March 31, 2023
  - Claims Services Vehicle 3 acquired in Q2

#	Category/Assurance Item	Category Count	Status Readiness			Percent Ready
			Red	Yellow	Green	
**	Cumulative CAT Prep Assurance Totals/Percentage	155	0	0	155	✓ 100%

As of August 7, 2023

Continuous Improvements in Flight

- Enterprise Identity and Access Management Program
- SIEM/SOAR**
  - Better Alert Tuning
  - Faster Incident Investigation
  - Faster Incident Response
  - Improved Log Querying
  - Increased Automation
- Threat Hunting
- File Integrity Monitoring
- Application Security
- Cloud Security
- Evaluation of MDR** Fit

- Governance, Risk, & Compliance
  - Compliance Assurance Program Enhancements
  - End User Computing
  - Governance Process Documentation Refresh
- Enterprise Resiliency and IT Security and Risk Partnership
- Expansion of the Governance Risk and Compliance tooling:
  - Implementation of Business Continuity add on
  - Automation of Resiliency key workflows
  - Business Impact Analysis
- Organizational Resilience Capabilities Assessment

***SIEM = Security Information and Event Management*
***SOAR = Security Orchestration and Automated Response*
***MDR = Managed Detection and Response*