brinqa

Syed Abdur
Director, Product Management

# Risk-Centric Cybersecurity Management

## Goals, critical capabilities and use-cases from the real world

# AGENDA

Explore a real-world use case for risk-focused cybersecurity management

Identify the key goals for a cyber security risk management program

Create the blue-print for risk-focused cybersecurity management program

# GOALS

Communicate the benefits of a risk-focused approach to cybersecurity management

Identify the capabilities required to implement a risk-based cybersecurity program

Understand how to grow your cybersecurity risk management programs

Cybersecurity Risk Management

Vs.

Risk-based Cybersecurity Management

# Application

# Vs.

# Program

# Cybersecurity Risk Management Use Case

## Vulnerability Management

Basic Requirements

Limitations

Risk-based Approach

# 3 Questions of Vulnerability Management Risk

Which vulnerabilities, if exploited, pose the greatest risk of disrupting critical business functions?

Which vulnerabilities, if exploited, pose the greatest risk of exposing vital or confidential data?

Which vulnerabilities stand the greatest risk of being exploited?

# Which vulnerabilities, if exploited, pose the greatest risk of disrupting critical business functions?

Business Context

**CMDB**

Compliance Flags (PCI)

Operational Status (Production)

Internal / External / DMZ

**Business Hierarchy**

Location

Department

Business Line

**Business Functions**

Services

Processes

Applications

## Which vulnerabilities, if exploited, pose the greatest risk of exposing vital or confidential data?

Data Context

Data Management & Protection Systems

DLP

Data Segmentation

Network Segmentation

Business Continuity / Disaster Recovery (BC/DR)

Data Lifecycle Management (DLM)

# Which vulnerabilities stand the greatest risk of being exploited?

**Threat Intelligence**

Zero-day Threats

Advanced Persistent Threats

Exploits

# Cybersecurity Risk Management Goals

Integrate all relevant data sources seamlessly

Allow practitioners to focus their efforts on the most critical problems

Facilitate the implementation of solutions

Improve communication within and between teams, departments and stake holders

Do this automatically and continuously

# Manual Remediation Management

## ITSM Integration

Automatic Ticket Creation

Vulnerability Consolidation

Ownership Assignment

SLA Enforcement

# Automated Remediation Management

Orchestration

Server Automation

Endpoint Management

Patch Deployment

Patch Intelligence

# Risk Communication

## Metrics & Reporting

Security professionals - focus on actionable, imminent risks

InfoSec managers - program effectiveness and performance

InfoSec leaders - board and C-level metrics

Business users - assumed technology risks, remediation cost and effort

# Risk-based Cybersecurity Management Program Blue-print

1. Identify all technology assets (and their sources) in scope for this program
2. Identify all security monitoring and assessment systems in scope for this program
3. Identify all relevant business, technology, environmental contexts (and their sources) in scope for this program
4. Automatically integrate & correlate data from 1, 2, 3
5. Evaluate pre-defined algorithms for risk evaluation and insights

# Risk-based Cybersecurity Management Program Blue-print

6. Identify all processes, systems and users that can be leveraged for risk remediation

7. Implement play-books and strategies for manual remediation efforts

8. Orchestrate automatic risk remediation

9. Inform and engage ALL relevant stakeholders

# Beyond Network Vulnerabilities

Application Security

Penetration Testing

IDS / IPS

Network Flow

Change & Configuration Management

Policy Compliance

# Parting Thoughts

Better security management is possible

Get started today!

Build it forward

Own your security

Empower your SMEs

Beware of 'Secret Sauce'

# Q & A