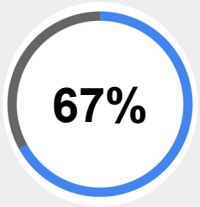
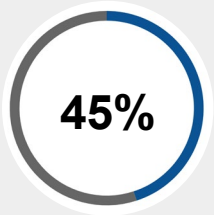

# Building a Better Third-Party Cyber Risk Program

# Current TPRM Environment & Challenges

The global digital ecosystem introduces cybersecurity risks to every organization. Cyber **resilience** and **risk mitigation** are significant challenges.

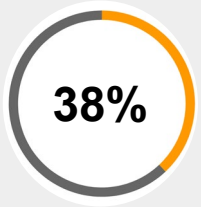



of companies report that third party risk management has **gained visibility among executives and the board, last year.**

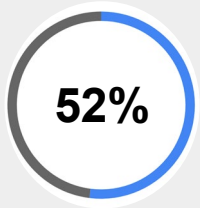



of companies are **still using spreadsheets** to assess their third parties

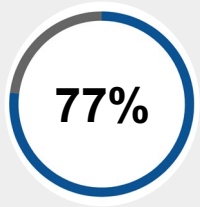
The 2022 Prevalent Third-Party Risk Management Industry Study




of companies have experienced a **significant disruption, monetary loss, or reputational damage** as a result of a third party within the last three years



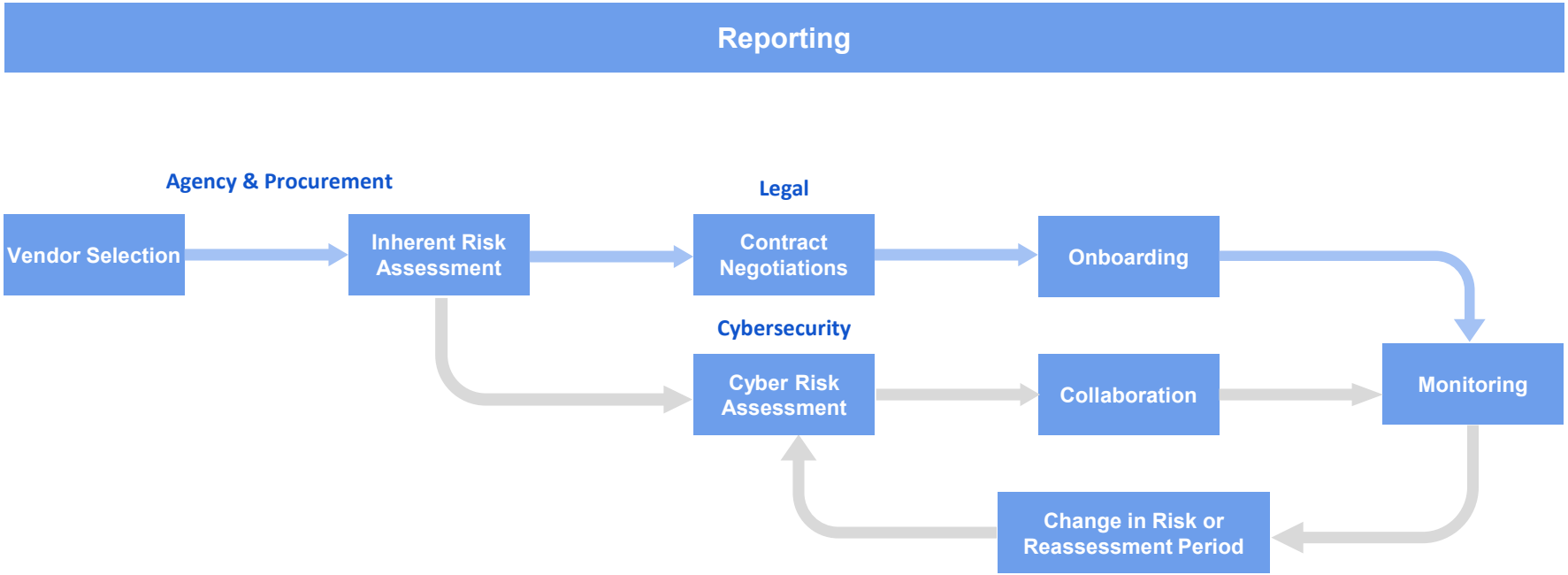

of companies report **not having sufficient capabilities in-house** to manage the third party risks they face




say that the pandemic made it clear it's **time to overhaul** their TPRM operating model

KPMG Third-Party Risk Management Outlook 2022

# TPRM Program Workflow



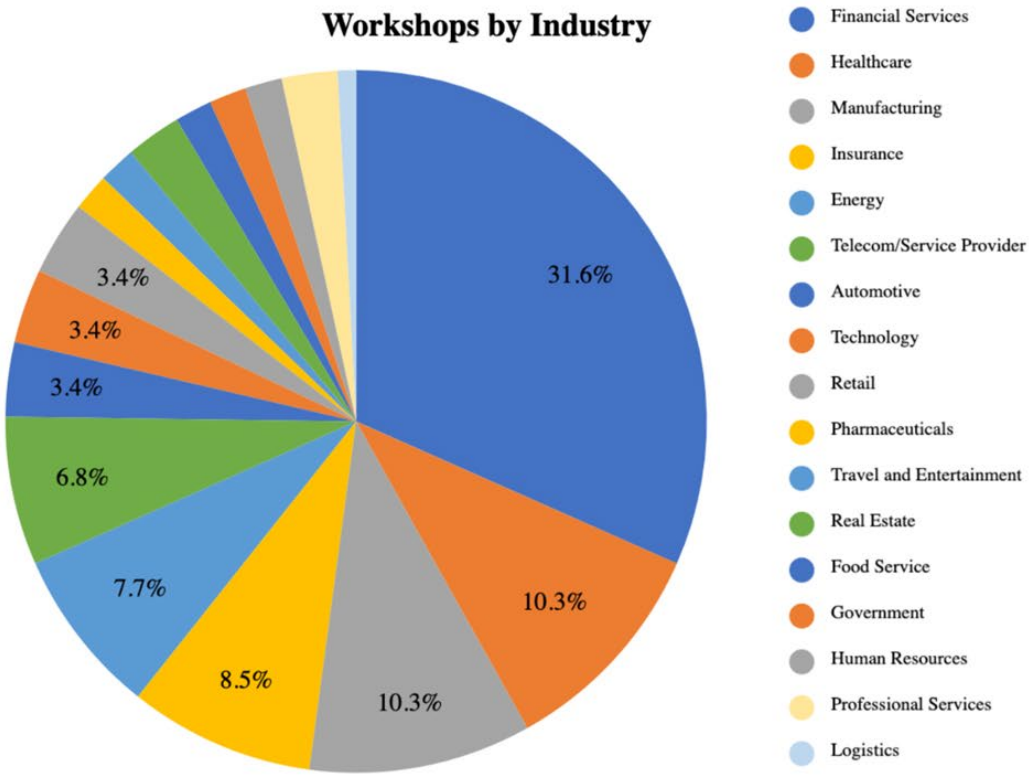
# TPRM Workshop Statistics

**150+**

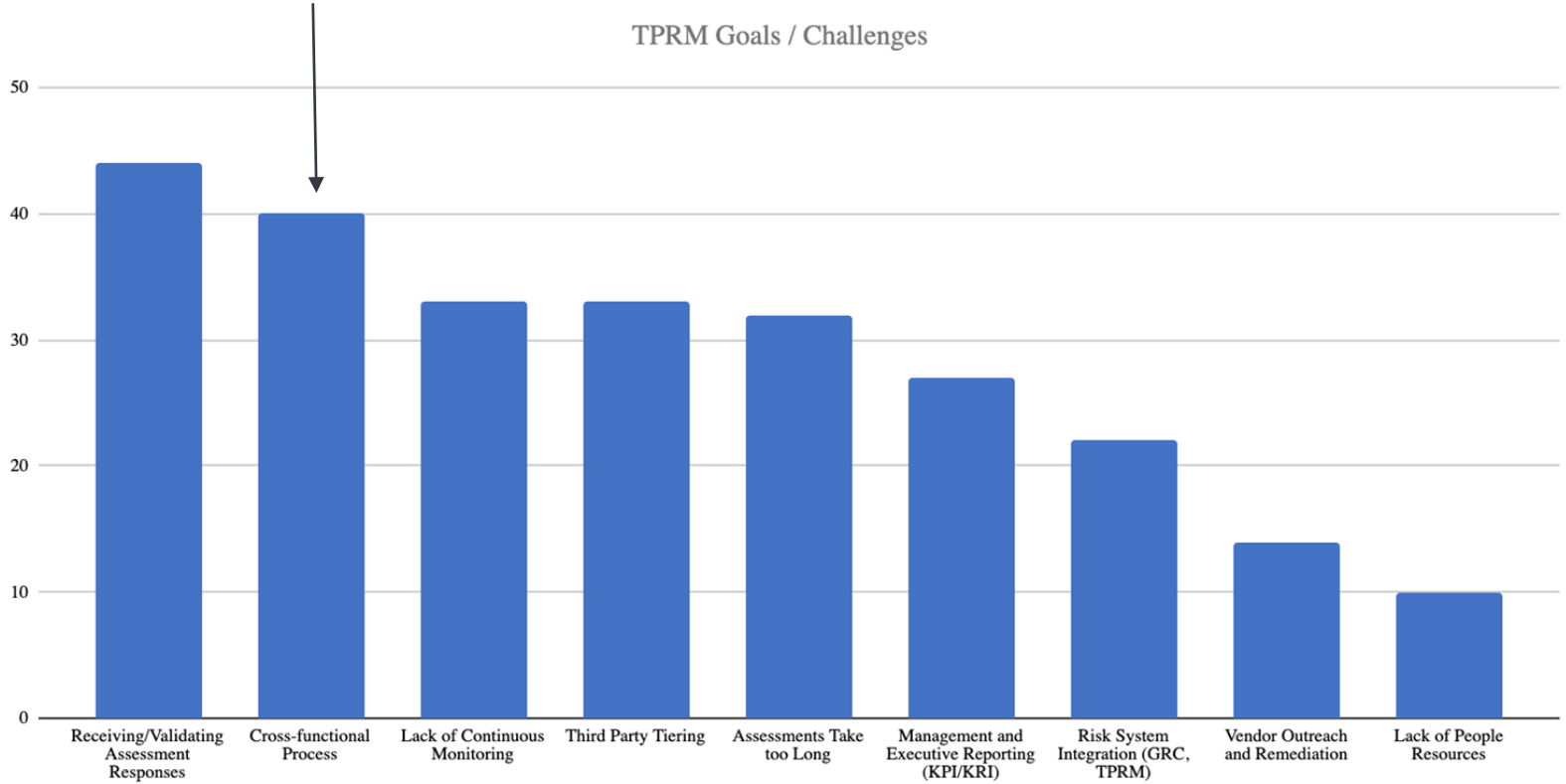
TPRM workshops conducted by BitSight across North America, APAC and EMEA

**17**

industries including Finance, Insurance, Healthcare, Manufacturing and Energy



# TPRM Goals and Challenges



# TPRM Process

**CHALLENGE:**

## Cross-Functional Process

### SYMPTOMS

- Lack of cohesion between Procurement, Legal, Risk and Cyber groups
- No common process across business units, subsidiaries and/or agencies
- Business doesn't follow process, goes around it

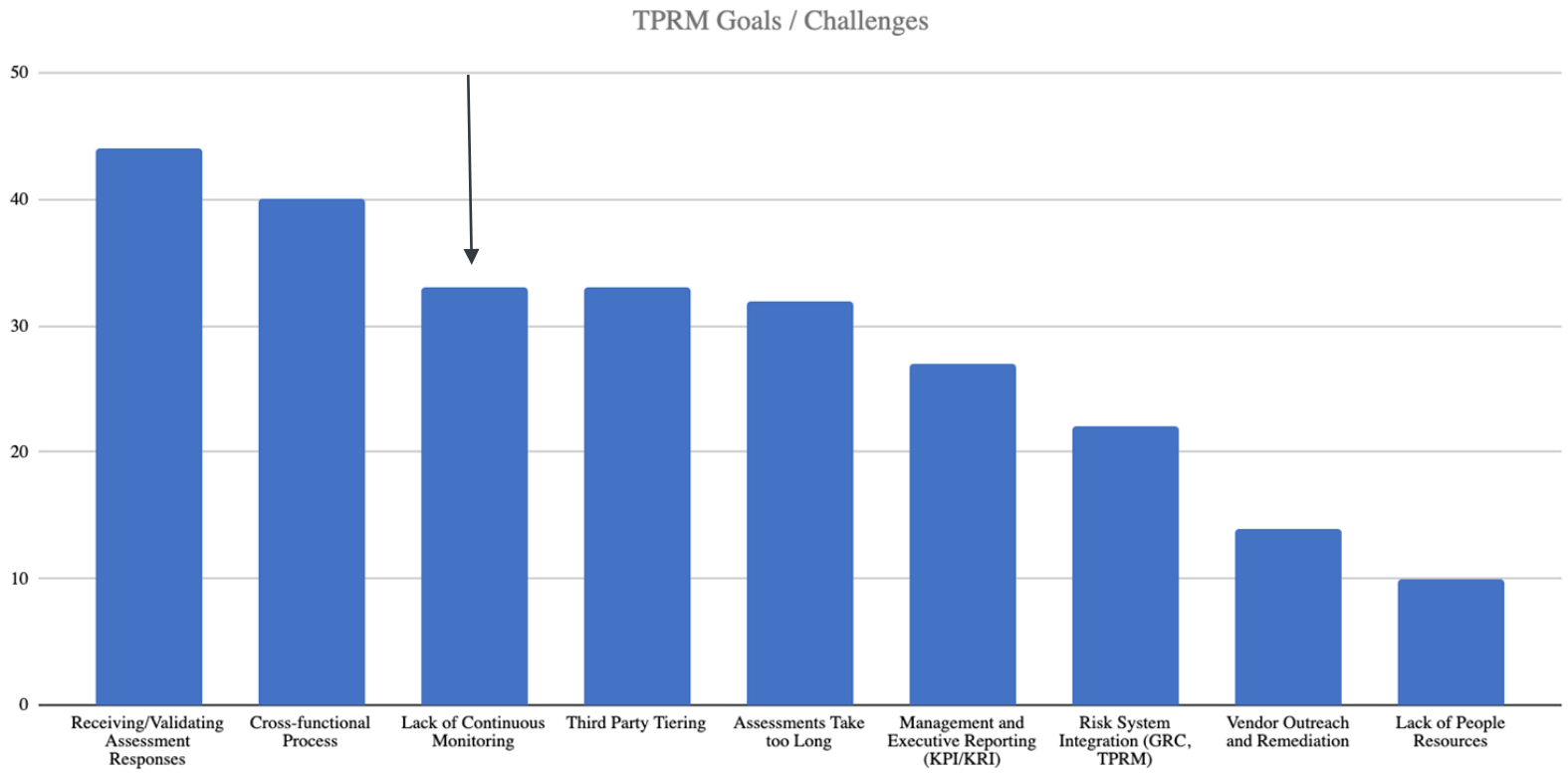
### QUOTES

"Our program is fractured."

"We don't have a standard approach across all of our agencies."

"Sometimes we feel like our role is to get between the business and their vendor before they fall in love and get married."

# TPRM Goals and Challenges



# Continuous Monitoring

**CHALLENGE:**

Continuous Monitoring

## SYMPTOMS

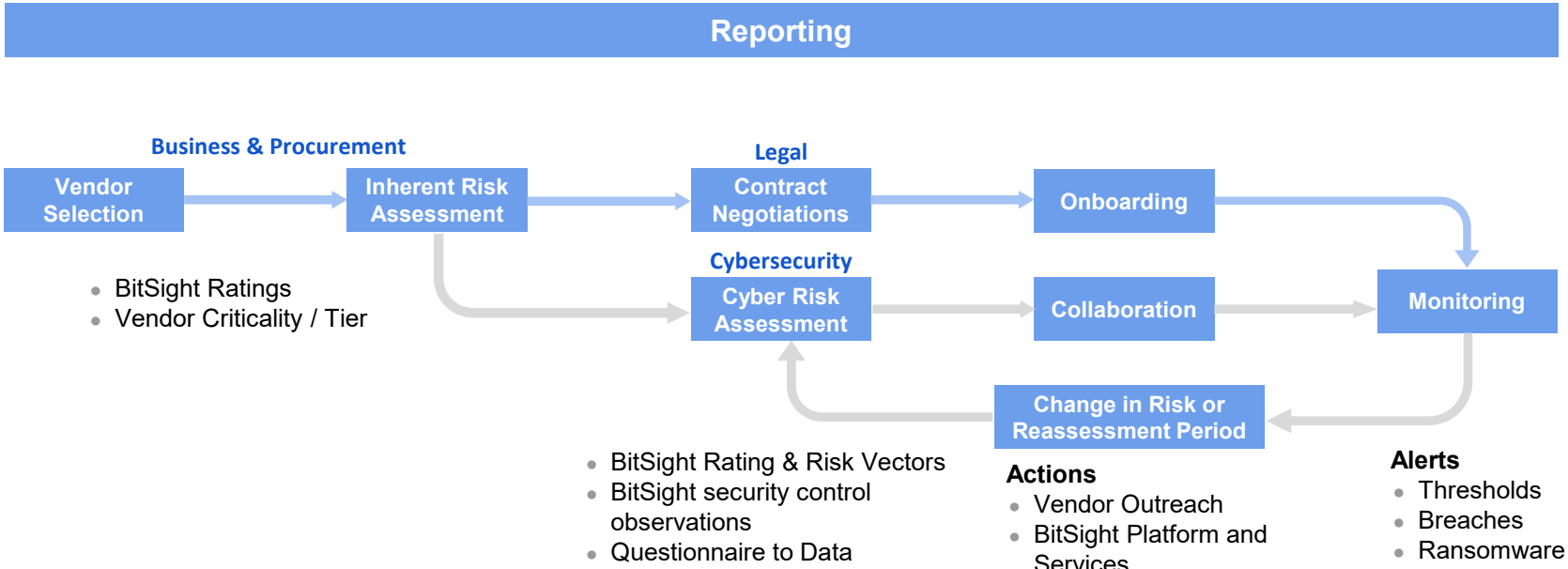
- Reliance on point-in-time assessment data
- Dependence on arbitrary re-assessment cycles
- Lack of knowledge of current state of third party

## QUOTES

"Our continuous monitoring of vendors is really just continually reviewing them at points in time."

"One of our critical software vendors recently experienced a breach (we didn't know about). Vendors are not as transparent as we'd like relative to security incidents."

# TPRM Program Workflow with Data



# This could happen to your Third Party…

## Let’s discuss a (quite possible) example, based upon a real story….

Source: The Ransomware Files Podcast - September 15th, 2022 “The Adult Boutique”

# Your vendor is small, and so is their IT department

A ransomware attack occurs in one of your vendors, and you rely on them to provide:

- Specialized Medical Equipment?
- Physical Security Services?
- Manufacturing for a State project

*They are small, because they are somewhat specialized. They also may be in an industry which cannot afford or does not invest in strong cybersecurity…or even a large IT department*

# A ransomware attack


The company accountant has left his desktop open from the Internet with the password set as the street address of the company


The ransomware gang demands a Bitcoin for every computer - CEO scrambles to procure

# A ransomware attack

It is determined that they can afford to save four critical systems


The CEO gets very creative to procure Bitcoin

# A ransomware attack

Ultimately the systems are decrypted, but it has created an existential threat for the company

A short time later, the CEO decides to shutter the business

# All this detail might not matter…

**But what does matter is:**

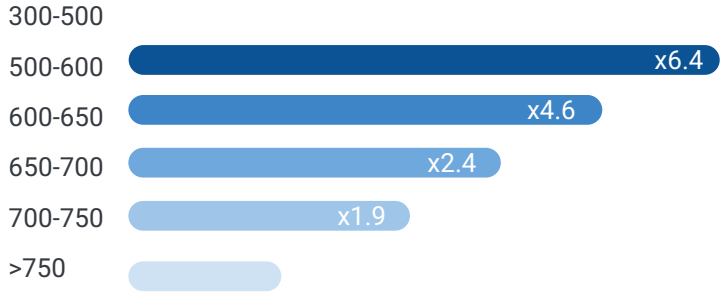
- The business disruption for your third party
- The project for the State of North Carolina has stopped
- The viability of the third party partner is in doubt

# Ransomware Research

## Likelihood of being a ransomware victim

**6.4x**

If the security rating drops below 600 as compared to an organization with a 750 or higher




## Vulnerabilities

| | |
|---|---|
| 1.5x | POODLE (CVE-2014-3466) |
| 1.3x | DROWN (CVE-2016-0800) |
| 1.3x | CVE-2012-6708 |
| 1.8x | CVE-2018-13379 |
| 2.6x | PulseSecure Group |

## Risk Vectors

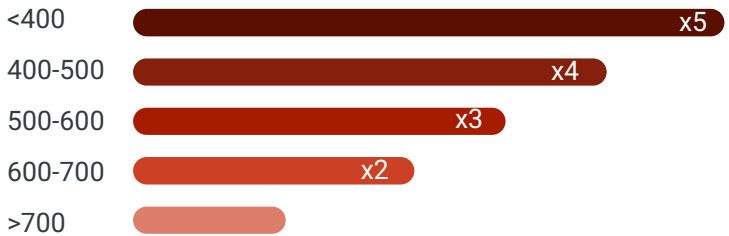
| | |
|---|---|
| 7x | If the Patching Cadence Grade is **C or lower** |
| 4x | If the TLS/SSL Configurations Grade is **C or lower** |
| 3x | If the TLS/SSL Certifications Grade is **C or lower** |

# Breach Correlation and Alert Setting

BitSight provides a **measurable range of risk** and is the only ratings solution with a **third party verified correlation to breaches**.

## Likelihood of suffering a data breach

**5x** * If your security rating drops below 400 as compared to an organization with a 700 or higher




**3x** ** If 50% of your computers run outdated Operating System versions

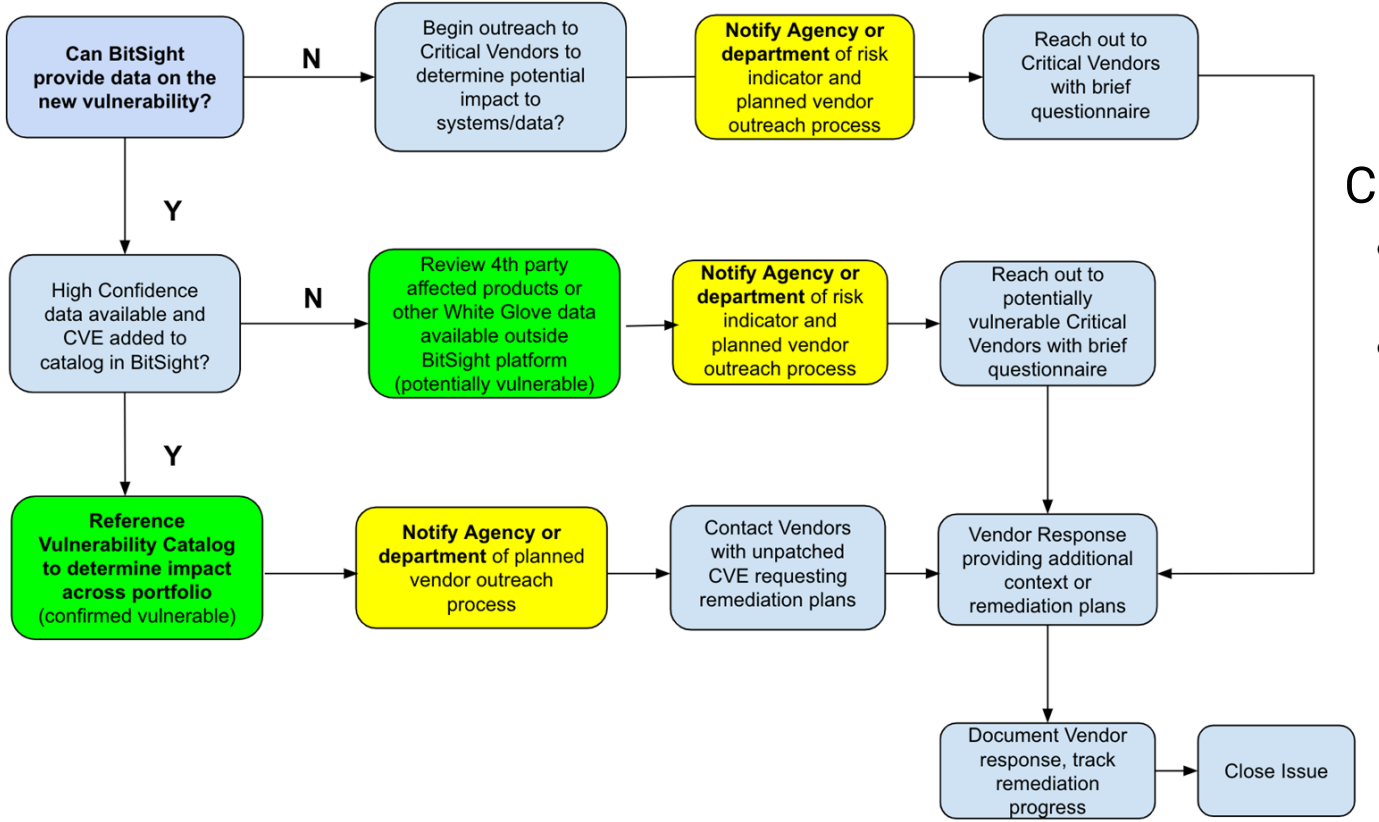
**2x** *** If your Botnet Grade is **B or lower** or the File Sharing grade is **B or lower** or the Open Ports grade is **F**

*AIR Worldwide reviewed and approved our data and analyses

** A Growing Risk Ignored: Critical Updates

*** Beware the Botnets: Botnets correlated to a higher Likelihood of a Significant Breach

# Third Party Vulnerability Process




## Collaboration is critical

- Within the State agencies and departments
- With third parties, vendors, suppliers, and service providers

# Prepare, Identify and Respond

### CONTINUOUSLY MONITOR AND ASSESS THIRD-PARTY RISK

Address third-party performance throughout the vendor lifecycle.

### IDENTIFY VULNERABILITIES AND ACTIVELY HUNT FOR RISK

Quickly find hidden exposures and critical vulnerabilities across your vendor supply chain.

### COLLABORATE WITH VENDORS TO REMEDIATE AND RESOLVE THREATS

Work with your third-parties to proactively improve their security posture and attend to critical issues.

BITSIGHT®
The Standard in SECURITY RATINGS

+

BITSIGHT
The Standard in SECURITY RATINGS

## Questions?