RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

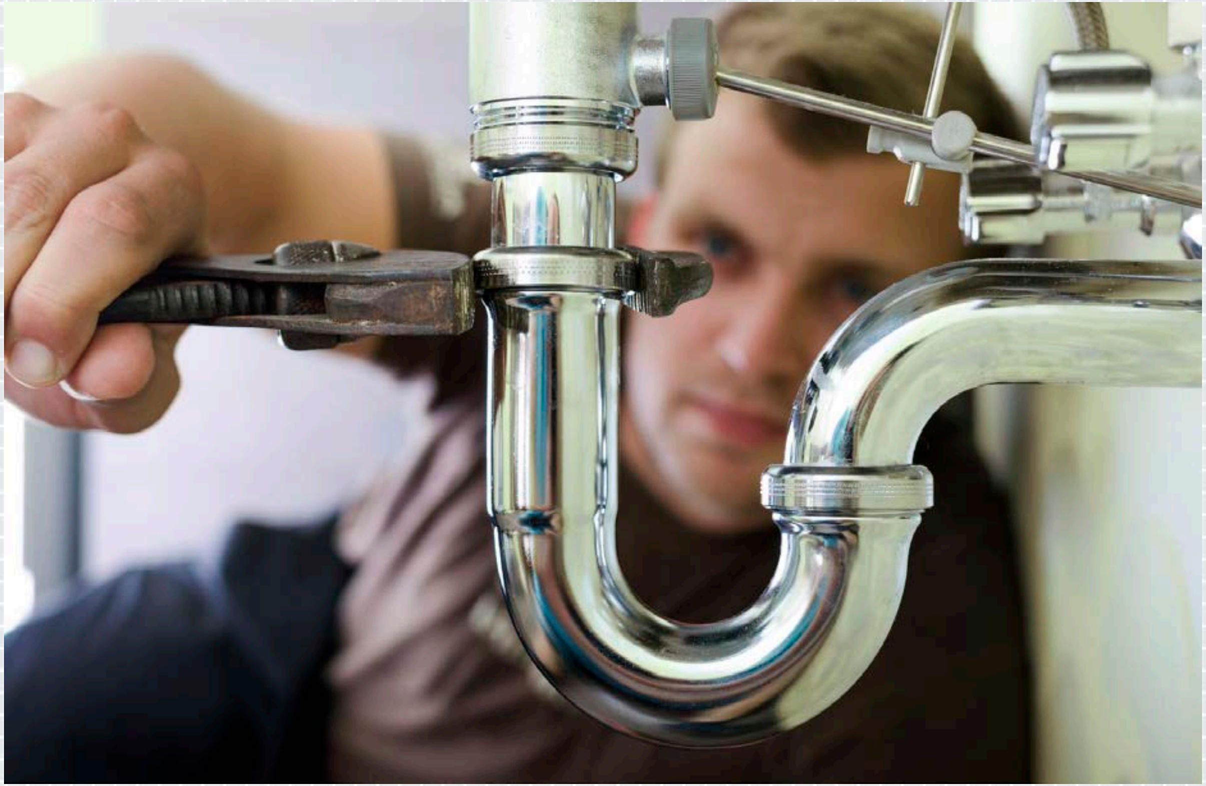
SESSION ID: GRC-F03

Taking a Business Risk Portfolio (BRP) Approach to Information Security

Johna Till Johnson

CEO and Founder
Nemertes Research
@johnatilljohnso - @nemertes

Executive View of InfoSec ca. 2013



Executive View of InfoSec, 2015

Top Trends in 2015

- Cyberattackers are winning
- The universe of threats is growing
- The impact is getting more severe
- Motivations have shifted
- Problems remain unsolved (Inception)

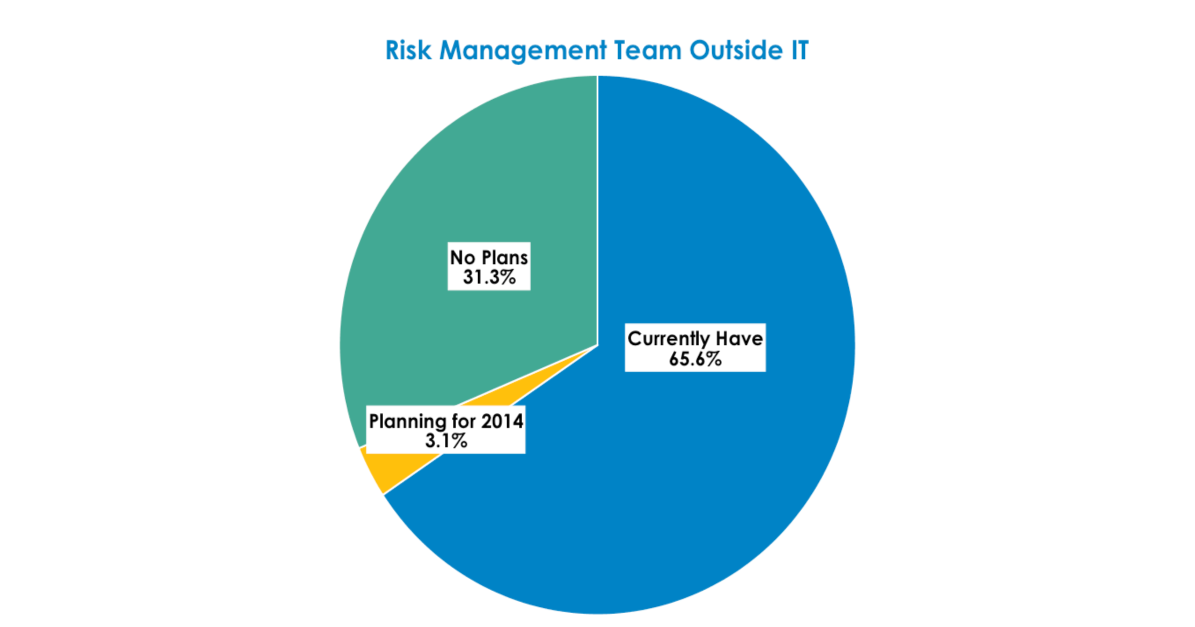
The Regulatory Response (Financial)

Date	Agency	Action
Feb 2014	NIST	Releases cybersecurity risk framework
March 2014	SEC	Holds cybersecurity roundtable and subsequent enterprise assessment, finds 74% to 88% of participants have experienced cyberattack
Feb 3 2015	SEC	Office of Compliance Inspections and Examinations (OCIE) releases Risk Alert addressing cybersecurity for broker-dealers and investment advisers
Feb 3 2015	FINRA	Publishes report on Cybersecurity Practices based on 2014 targeted exam of member firms.

Top Regulatory Recommendation

Adopt a risk-management based approach to addressing cybersecurity threats

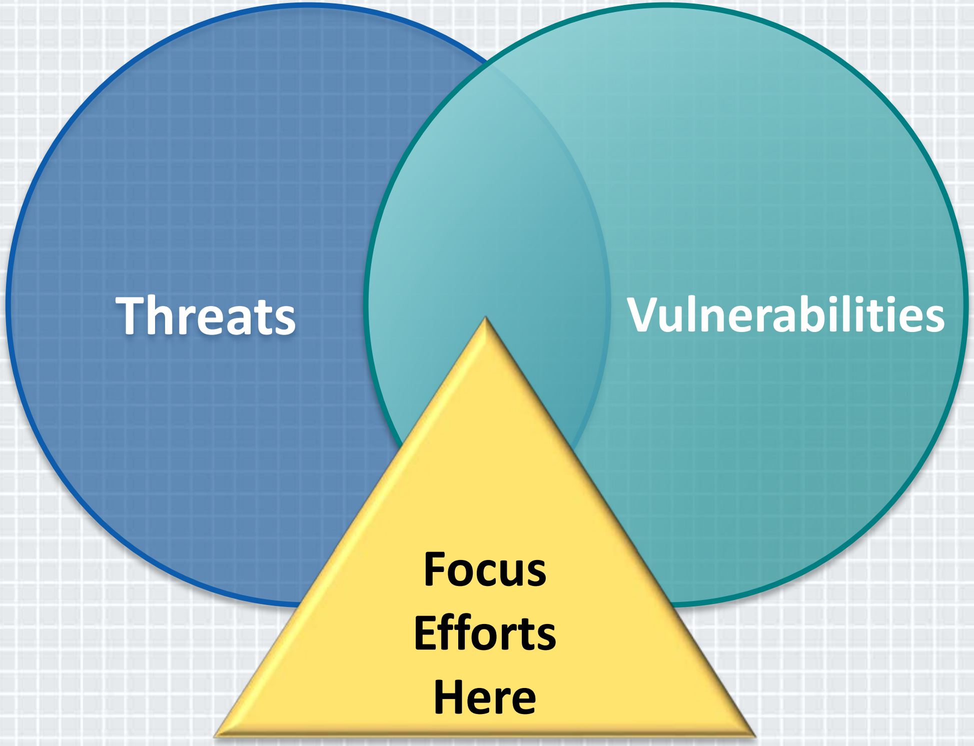
External Risk Management



All (100%) of participants plan to increase budget of external risk management teams in 2015

Source: 2014-2015 Enterprise Security Benchmark, Nemertes Research

Classic InfoSec Worldview



Business Risk Portfolio (BRP) Worldview

Potential Impact

Severe

Minimal

Focus Efforts Here

Unlikely

Highly Probable

Likelihood

Risk Management Definition

Risk management is a systematic process for identifying, evaluating, and addressing potential events that could affect the achievement of business objectives, positively or negatively

Risk Management Definition

Risk management is a systematic process for identifying, evaluating, and addressing potential events that could affect the achievement of business objectives, positively or negatively

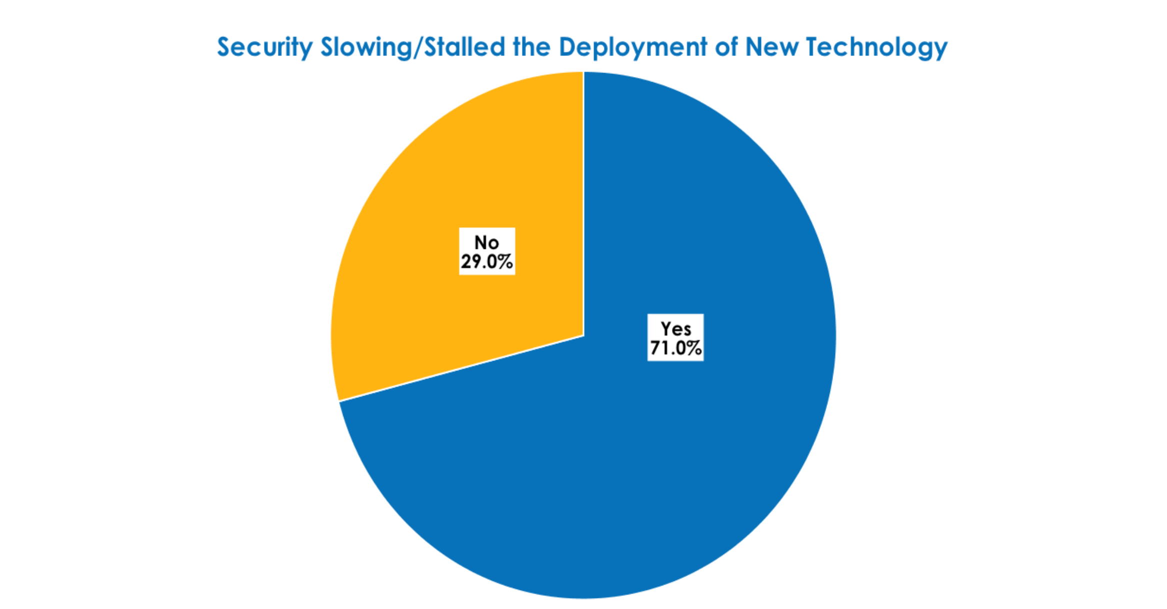
Risk Management Definition

Risk management is a systematic process for identifying, evaluating, and addressing potential events that could affect the achievement of business objectives, positively or negatively

Risk Management Definition

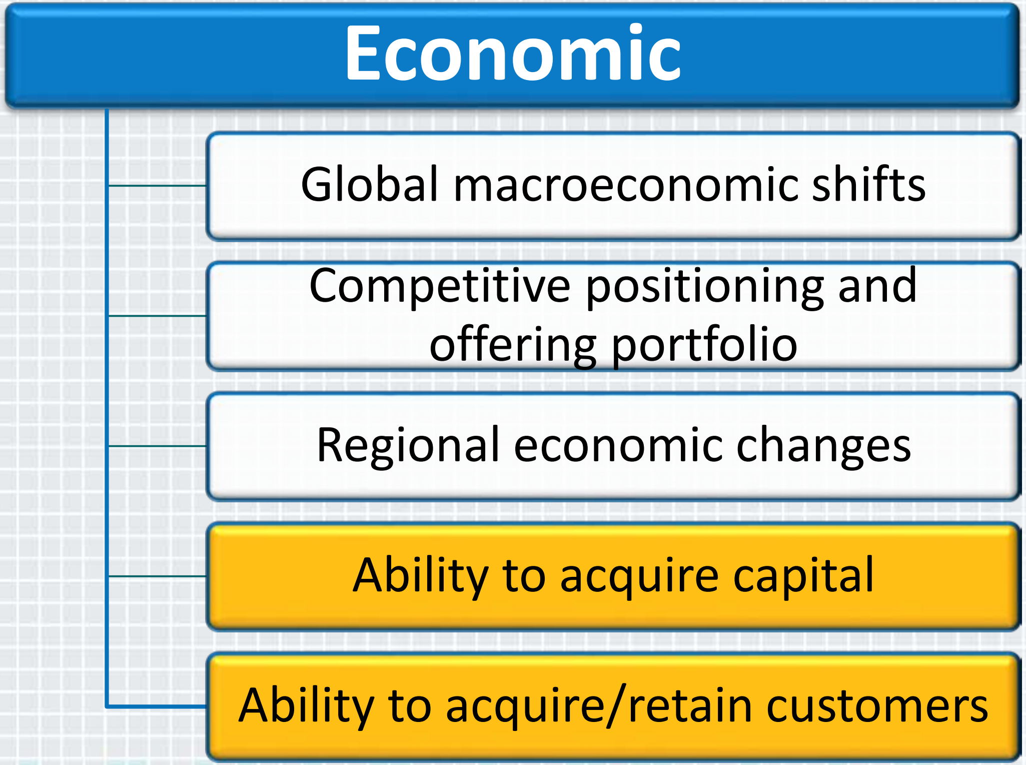
Risk management is a systematic process for identifying, evaluating, and addressing potential events that could affect the achievement of business objectives, positively or negatively

Security Slowing Down Innovation



Source: 2014-2015 Enterprise Security Benchmark, Nemertes Research

Business Risk Portfolio: Economic



Economic

Global macroeconomic shifts

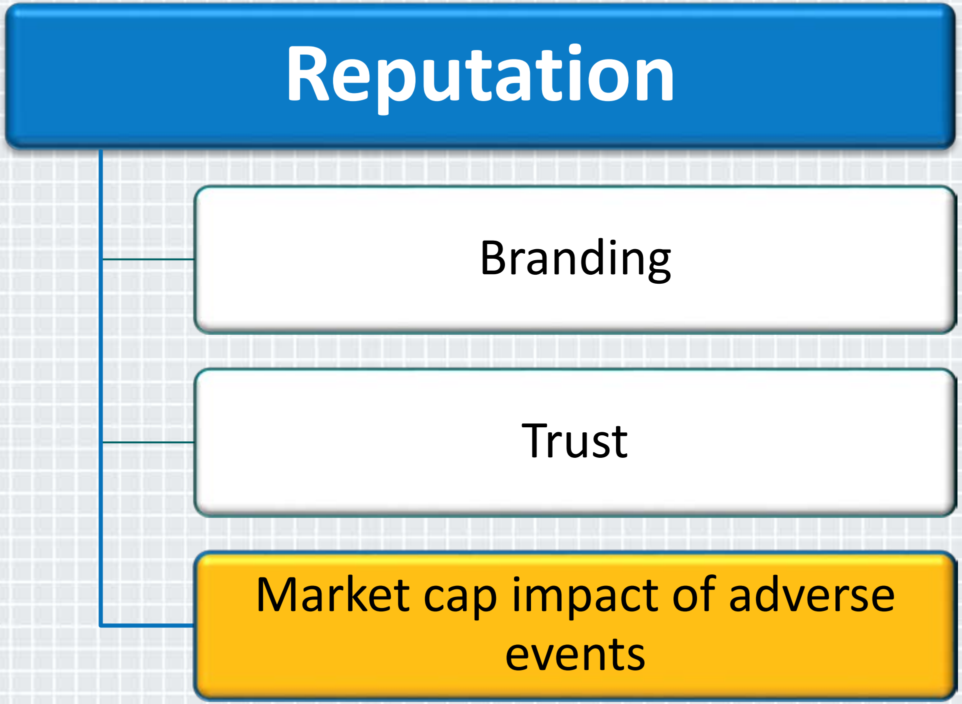
Competitive positioning and offering portfolio

Regional economic changes

Ability to acquire capital

Ability to acquire/retain customers

Business Risk Portfolio: Reputation



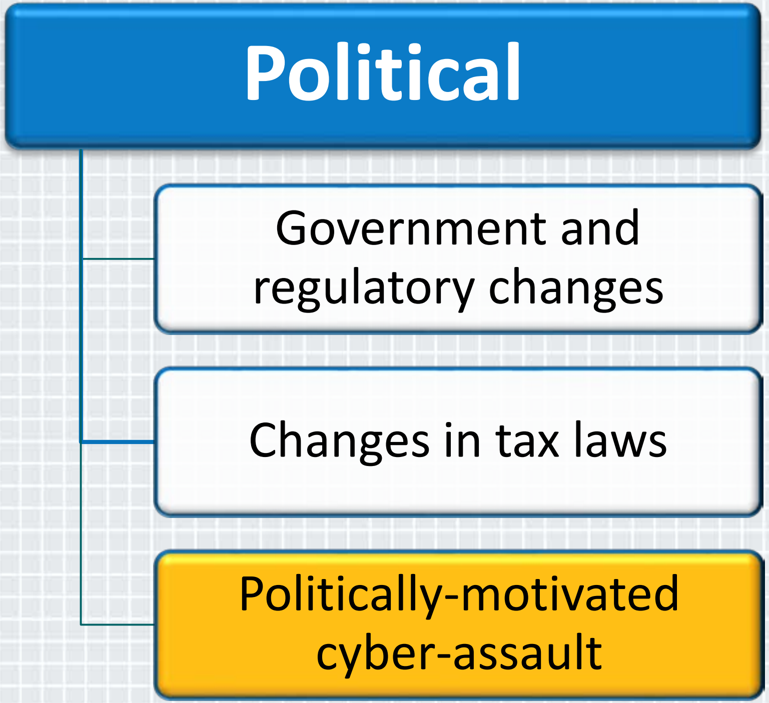
Reputation

Branding

Trust

Market cap impact of adverse events

Business Risk Portfolio: Political



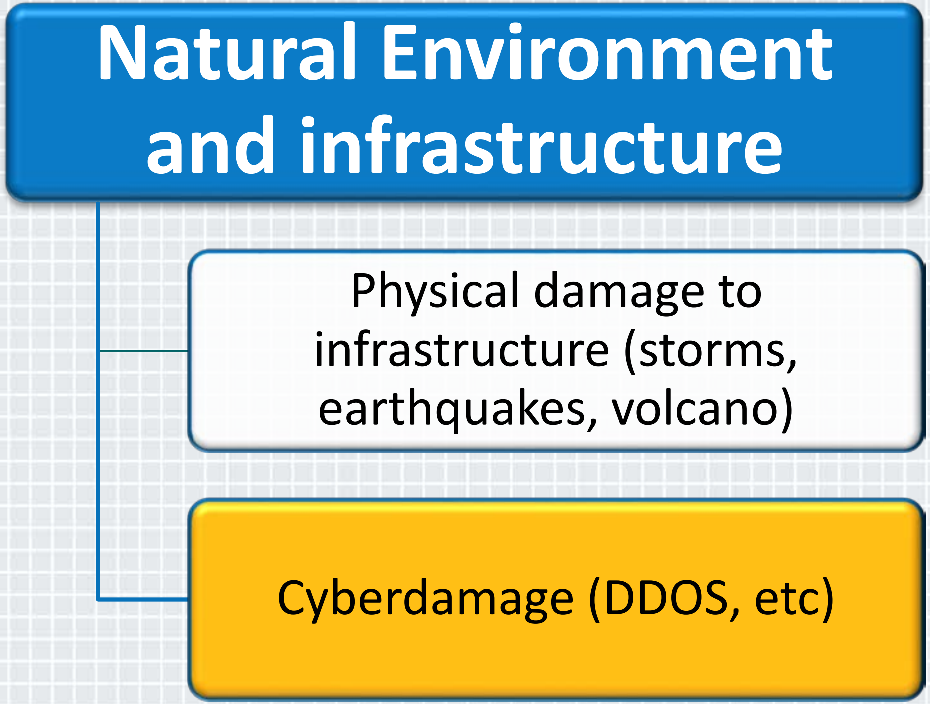
Political

Government and regulatory changes

Changes in tax laws

Politically-motivated cyber-assault

Business Risk Portfolio: Natural Environment

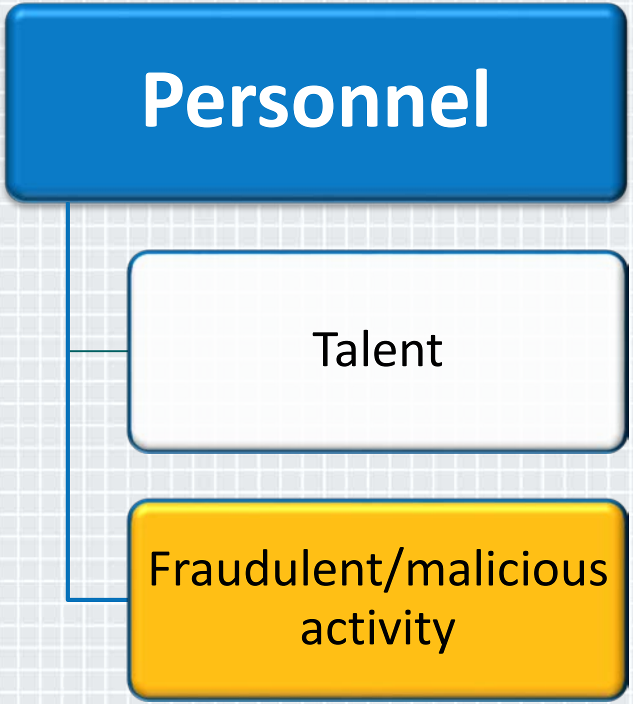


Natural Environment and infrastructure

Physical damage to infrastructure (storms, earthquakes, volcano)

Cyberdamage (DDOS, etc)

Business Risk Portfolio: Personnel

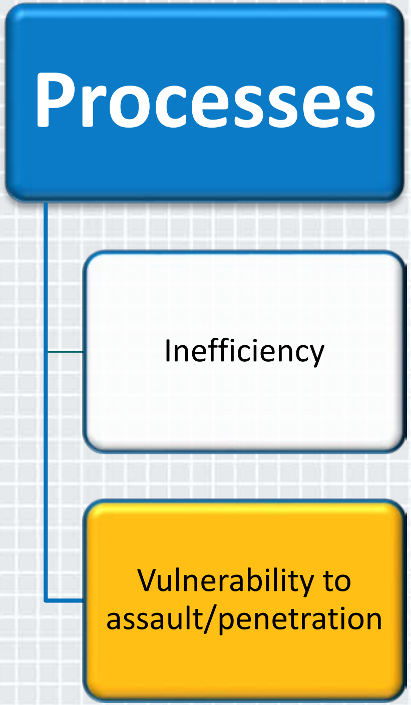


Personnel

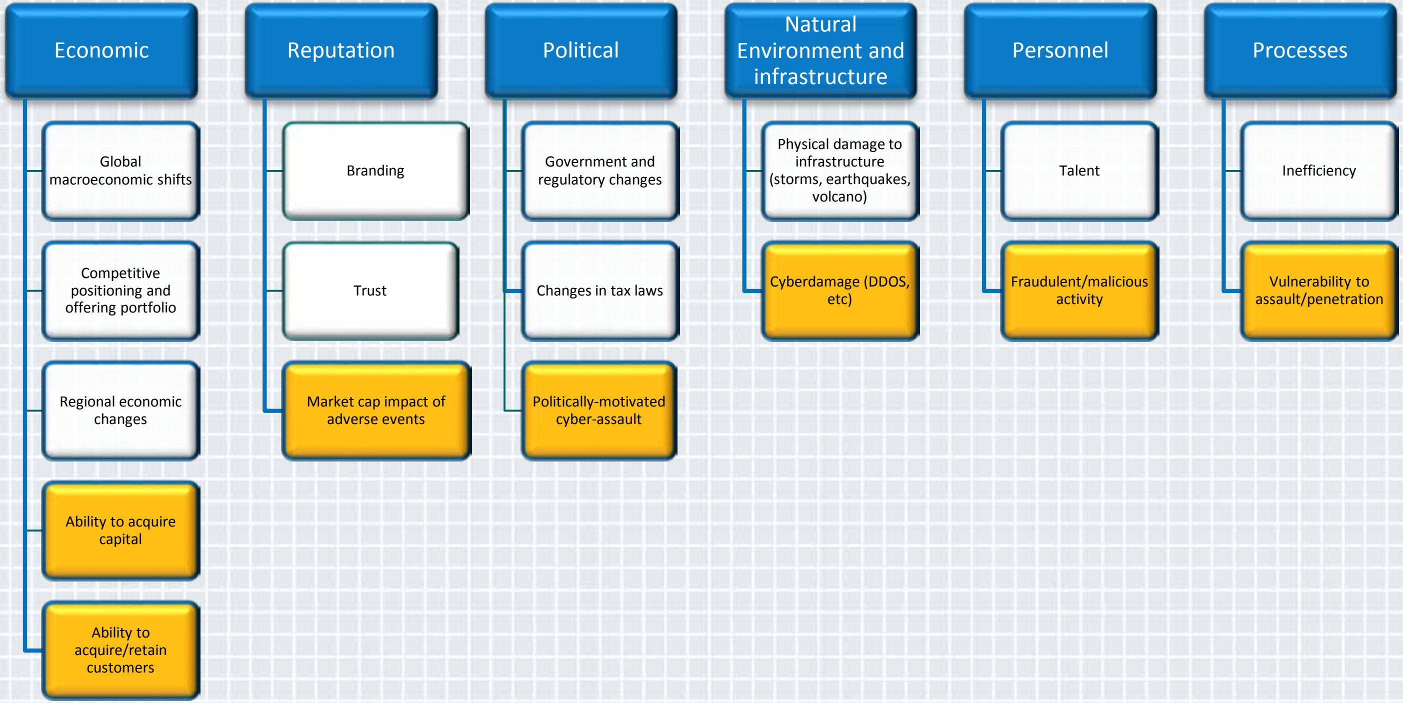
Talent

Fraudulent/malicious activity

Business Risk Portfolio: Processes



Business Risk Portfolio



Economic
- Global macroeconomic shifts
- Competitive positioning and offering portfolio
- Regional economic changes
- Ability to acquire capital
- Ability to acquire/retain customers

Reputation
- Branding
- Trust
- Market cap impact of adverse events

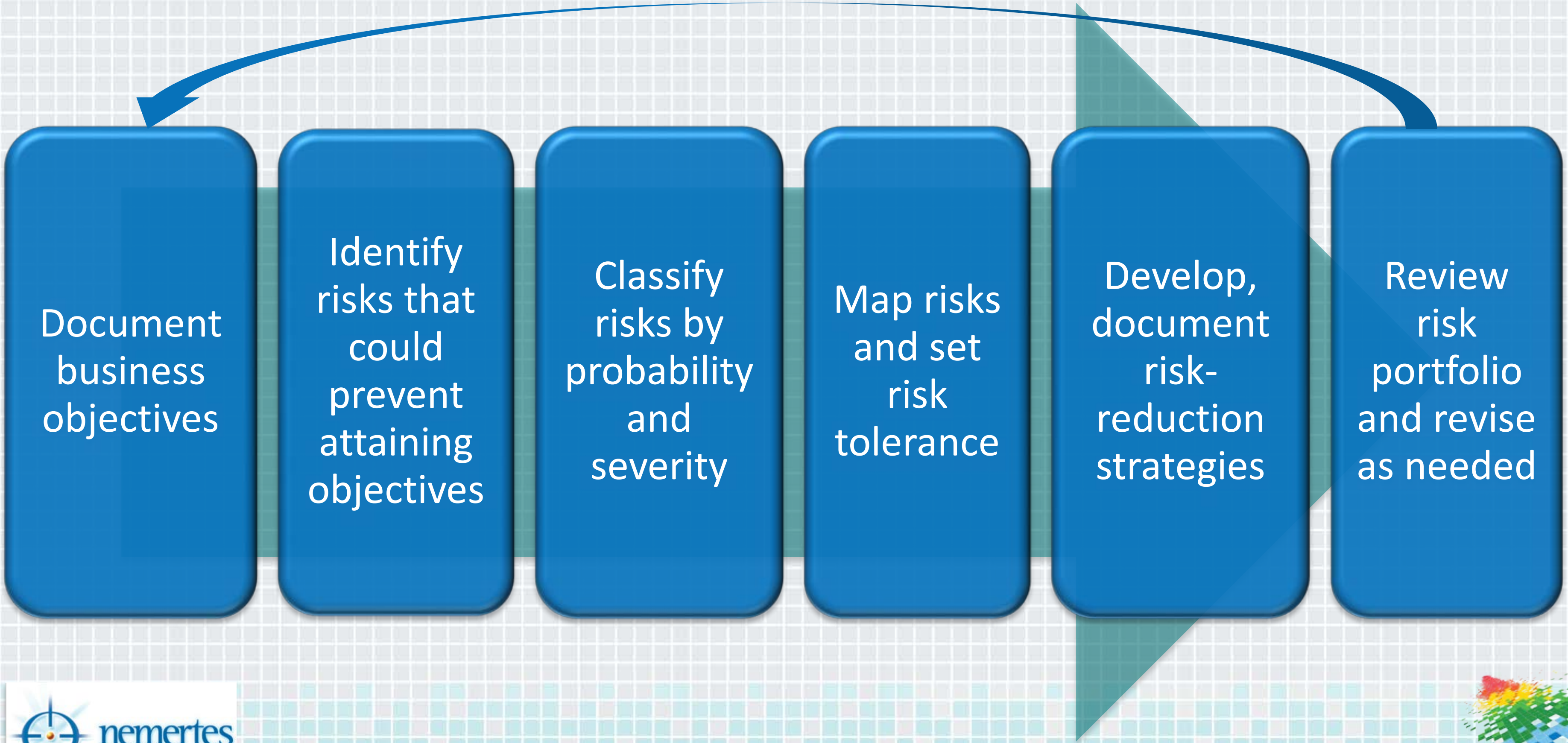
Political
- Government and regulatory changes
- Changes in tax laws
- Politically-motivated cyber-assault

Natural Environment and infrastructure
- Physical damage to infrastructure (storms, earthquakes, volcano)
- Cyberdamage (DDOS, etc)

Personnel
- Talent
- Fraudulent/malicious activity

Processes
- Inefficiency
- Vulnerability to assault/penetration

Building A Business Risk Portfolio

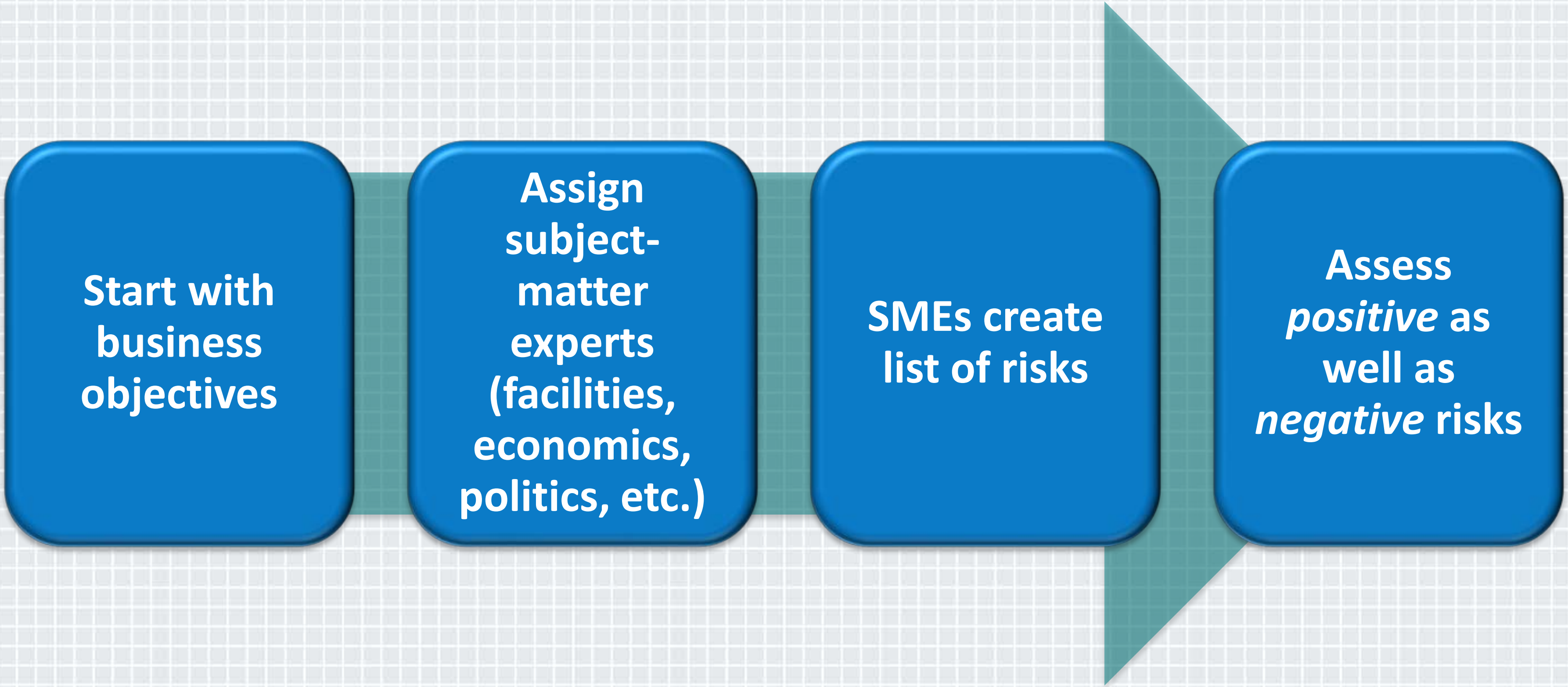


- Document business objectives
- Identify risks that could prevent attaining objectives
- Classify risks by probability and severity
- Map risks and set risk tolerance
- Develop, document risk-reduction strategies
- Review risk portfolio and revise as needed

Document Business Objectives

- Increase market share by offering cutting-edge services
- Increase revenue by expanding globally
- Maintain sterling reputation
- Increase margins by greater efficiency

Identify Risks



Start with business objectives

Assign subject-matter experts (facilities, economics, politics, etc.)

SMEs create list of risks

Assess *positive* as well as *negative* risks

Classify Risks By Probability and Impact

Probability

- **Unlikely:** Less than 1% chance of occurring within timeframe
- **Likely:** 1% to 10% chance of occurring within timeframe
- **Highly likely**: 10% or more chance of occurring within timeframe

Classify Risks By Probability and Impact

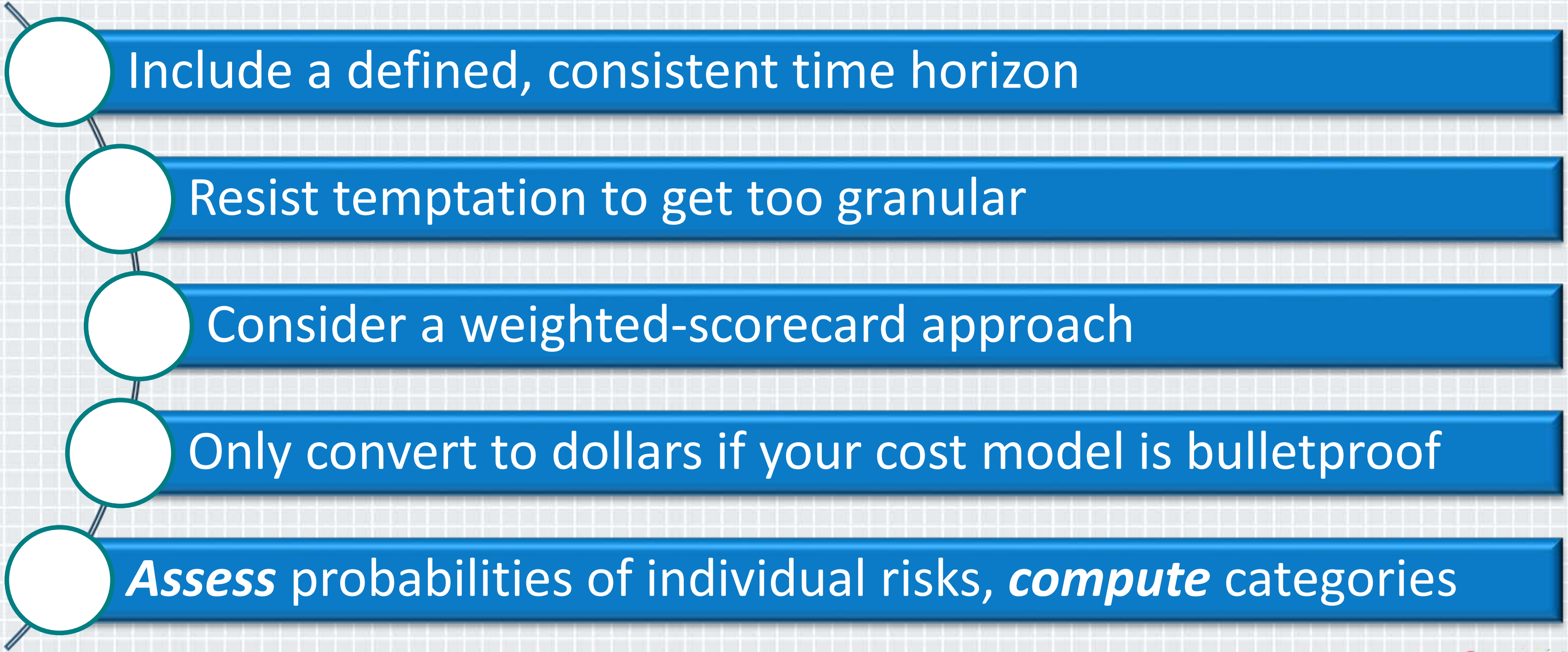
Probability

- **Unlikely:** Less than 1% chance of occurring within timeframe
- **Likely:** 1% to 10% chance of occurring within timeframe
- **Highly likely**: 10% or more chance of occurring within timeframe

Impact

- **Level 1:** Not severe; minimal impact
- **Level 2:** Moderately severe; upsets operations
- **Level 3**: Severe, significantly disruptive
- **Level 4**: Extremely severe, threatens existence of organization
- **Level 5**: Catastrophic, will destroy organization

Classification Best Practices



- Include a defined, consistent time horizon
- Resist temptation to get too granular
- Consider a weighted-scorecard approach
- Only convert to dollars if your cost model is bulletproof
- ***Assess*** probabilities of individual risks, ***compute*** categories

Classification Best Practices

- ✓ Include a defined, consistent time horizon
- ○ Resist temptation to get too granular
- ○ Consider a weighted-scorecard approach
- ○ Only convert to dollars if your cost model is bulletproof
- ○ ***Assess*** probabilities of individual risks, ***compute*** categories

Classification Best Practices

- ✔ Include a defined, consistent time horizon
- ✔ Resist temptation to get too granular
- ○ Consider a weighted-scorecard approach
- ○ Only convert to dollars if your cost model is bulletproof
- ○ ***Assess*** probabilities of individual risks, ***compute*** categories

Classification Best Practices

- ✓ Include a defined, consistent time horizon
- ✓ Resist temptation to get too granular
- ✓ Consider a weighted-scorecard approach
- ○ Only convert to dollars if your cost model is bulletproof
- ○ ***Assess*** probabilities of individual risks, ***compute*** categories

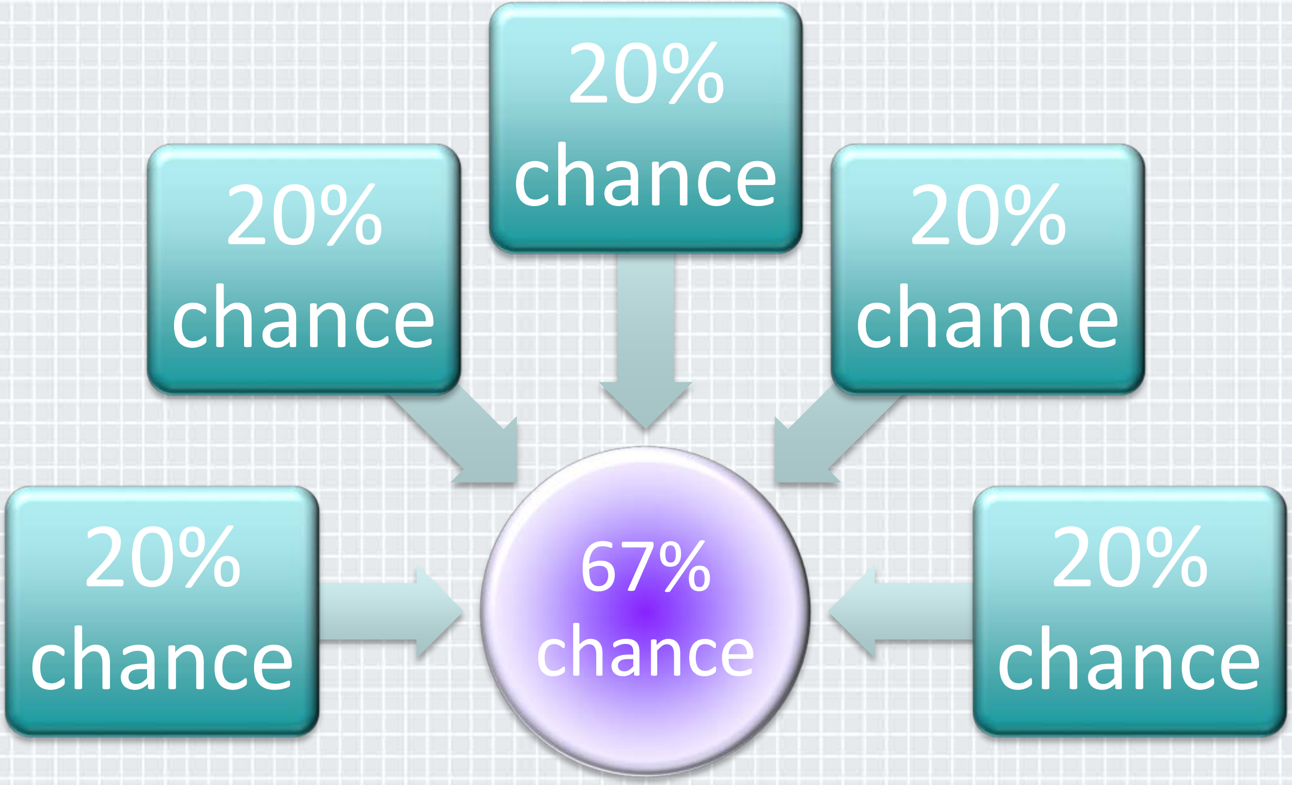
Classification Best Practices

- ✓ Include a defined, consistent time horizon
- ✓ Resist temptation to get too granular
- ✓ Consider a weighted-scorecard approach
- ✓ Only convert to dollars if your cost model is bulletproof
- ○ ***Assess*** probabilities of individual risks, ***compute*** categories

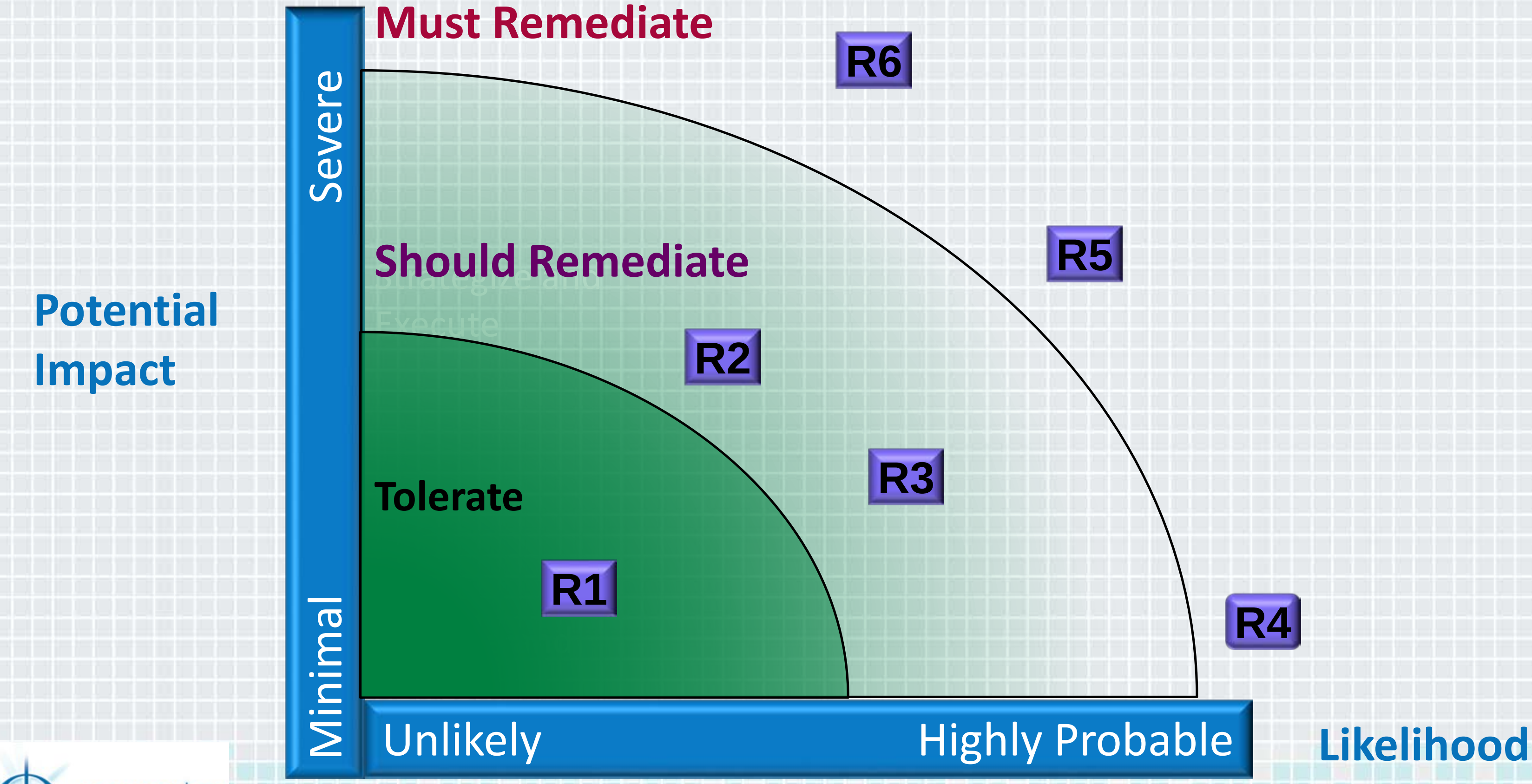
Classification Best Practices

- ✓ Include a defined, consistent time horizon
- ✓ Resist temptation to get too granular
- ✓ Consider a weighted-scorecard approach
- ✓ Only convert to dollars if your cost model is bulletproof
- ✓ ***Assess*** probabilities of individual risks, ***compute*** categories

Computing vs. Assessing



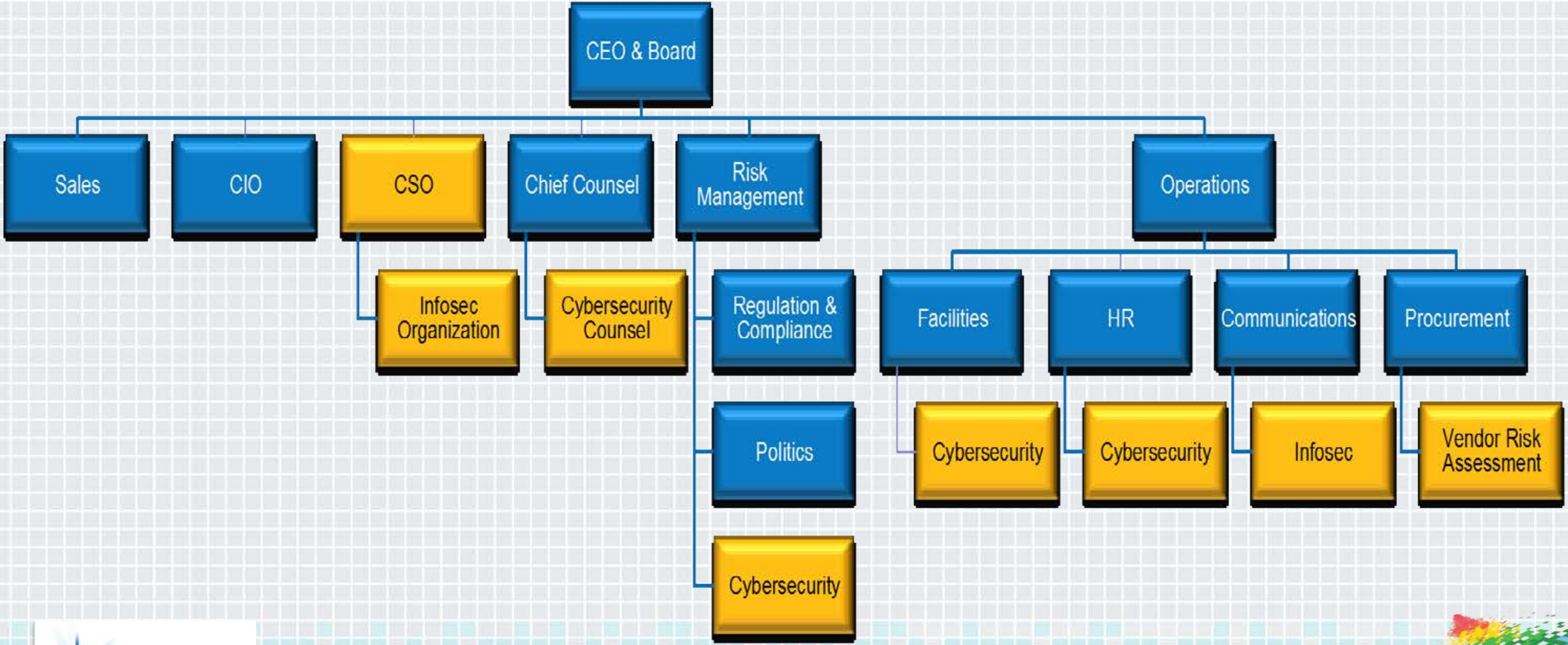
Map Risks And Set Tolerance



Develop and Document Remediation Strategies

R2	Insurance
R3	Process and Training
R4	New Technology
R5	Revise Business Processes
R6	Technology, Process, Insurance

Security Across the Organization



Key New Roles and Responsibilities

- Cybersecurity Counsel
- Cybersecurity Risk Manager
- HR and/or Communications Infosec Specialist
- Third Party Risk Assessor

Revamp Operations: Best Practices

- Engage emerging roles (Cybersecurity Counsel, Risk Management, etc.)
- War-game regularly
- Extend security/risk management measures to partners and customers
- Engage strategic customers
- Third party security credentials and testing
- Automate vendor certification and risk management
- Include cloud and mobile security

Revamp Operations: Best Practices

- ✔ Engage emerging roles (Cybersecurity Counsel, Risk Management, etc.)
- ○ War-game regularly
- ○ Extend security/risk management measures to partners and customers
- ○ Engage strategic customers
- ○ Third party security credentials and testing
- ○ Automate vendor certification and risk management
- ○ Include cloud and mobile security

Revamp Operations: Best Practices

- ✔ Engage emerging roles (Cybersecurity Counsel, Risk Management, etc.)
- ✔ War-game regularly
- ○ Extend security/risk management measures to partners and customers
- ○ Engage strategic customers
- ○ Third party security credentials and testing
- ○ Automate vendor certification and risk management
- ○ Include cloud and mobile security

Revamp Operations: Best Practices

- ✔ Engage emerging roles (Cybersecurity Counsel, Risk Management, etc.)
- ✔ War-game regularly
- ✔ Extend security/risk management measures to partners and customers
- ○ Engage strategic customers
- ○ Third party security credentials and testing
- ○ Automate vendor certification and risk management
- ○ Include cloud and mobile security

Revamp Operations: Best Practices

- ✓ Engage emerging roles (Cybersecurity Counsel, Risk Management, etc.)
- ✓ War-game regularly
- ✓ Extend security/risk management measures to partners and customers
- ✓ Engage strategic customers
- Third party security credentials and testing
- Automate vendor certification and risk management
- Include cloud and mobile security

Revamp Operations: Best Practices

- ✓ Engage emerging roles (Cybersecurity Counsel, Risk Management, etc.)
- ✓ War-game regularly
- ✓ Extend security/risk management measures to partners and customers
- ✓ Engage strategic customers
- ✓ Third party security credentials and testing
- ○ Automate vendor certification and risk management
- ○ Include cloud and mobile security

Revamp Operations: Best Practices

- ✔ Engage emerging roles (Cybersecurity Counsel, Risk Management, etc.)
- ✔ War-game regularly
- ✔ Extend security/risk management measures to partners and customers
- ✔ Engage strategic customers
- ✔ Third party security credentials and testing
- ✔ Automate vendor certification and risk management
- ○ Include cloud and mobile security

Revamp Operations: Best Practices

- ✔ Engage emerging roles (Cybersecurity Counsel, Risk Management, etc.)
- ✔ War-game regularly
- ✔ Extend security/risk management measures to partners and customers
- ✔ Engage strategic customers
- ✔ Third party security credentials and testing
- ✔ Automate vendor certification and risk management
- ✔ Include cloud and mobile security

Risk-Based Budgeting

Old:

- Infosec spend as a percentage of IT budget
- IT budget of $100 M
- Infosec budget of $6 M

Risk-Based Budgeting

Old:

- Infosec spend as a percentage of IT budget
- IT budget of $100 M
- Infosec budget of $6 M

New:

- Infosec spend based on estimated impact to organization
- 10% probability of market cap reduction of $1 B
- Spend to reduce risk: $10 M

Apply Slide: Putting It All Together

- **Next week**:
  - Identify risk-management teams at your organization
  - Engage and gain consensus for proceeding with risk-based approach
  - Familiarize yourself with existing risk management framework
- **Next month:**
  - Begin infosec risk assessment
  - Identify new roles and responsibilities outside infosec/IT
  - Designate liaisons and begin engagement process
- **Next quarter:**
  - Brief executive stakeholders
  - Revise analysis as needed
  - Make risk-based budget requests

Questions?

johna@nemertes.com