Cyber Risk Case Study: A Scenario-Based Approach to Identifying and Mitigating Key Threats

ERM Symposium
May 2, 2019

Shahryar Shaghaghi
Principal, CohnReznick

Sim Segal
President, SimErgy Consulting

Dave Bartholomew
Director, Gov., Risk & Assurance

Panelists

Shahryar Shaghaghi

Principal, CohnReznick

Sim Segal

President, SimErgy Consulting

Dave Bartholomew

Director, Gov., Risk & Assurance

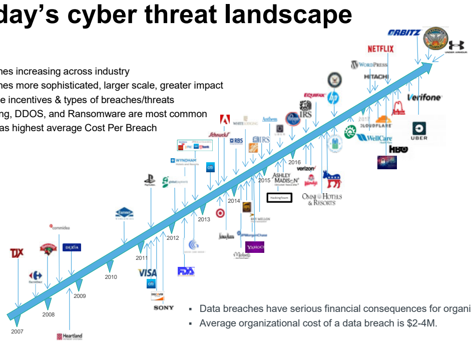
Agenda

- Current state of cybersecurity risks
- Value-based cyber risk management
- Applying value-based cyber risk management: Case study

CURRENT STATE OF CYBERSECURITY

Today’s cyber threat landscape

- Breaches increasing across industry
- Breaches more sophisticated, larger scale, greater impact
- Multiple incentives & types of breaches/threats
- Phishing, DDOS, and Ransomware are most common
- U.S. has highest average Cost Per Breach



- Data breaches have serious financial consequences for organizations
- Average organizational cost of a data breach is $2-4M.

Today’s cyber threat landscape

- Digital transformation will continue and therefore, cybersecurity landscape is constantly evolving.
- Today, we have 20 billion devices attached to the Internet. In 2020, we will have 50 billion devices connected to the Internet.
- Since hackers only need to be right once and those who protect the organization need to be right all the time, your cybersecurity program needs to be constantly evolving.
- In order to evolve, it is vital to understand who is after you, what motivates them, and what they are after.
- Understanding the landscape is a key element in any successful cybersecurity risk management program.

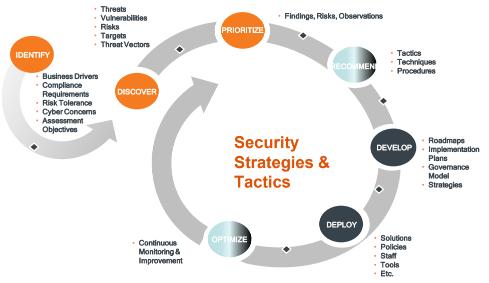
Businesses will be hacked because it’s easy

- Have not fully assessed their cyber risks
- Have not classified their data
- Don’t have latest security controls in place
- Many use social media to market their products and services
- Spend money in siloes
- Challenge to attract and retain internal security talents
- Use encrypted devices and unsecure emails for sensitive data
- Depend on third parties for various functions
- Most concerned about losing their customer data and bank account

What should they do to minimize attack impact?

- Start by assessing your cyber risks: What is core to your business; asset valuation and risk-based.
- Understand motives & drivers.
- Evaluate internal capabilities and outsource as appropriate.
- Incorporate key cybersecurity and privacy programs into your audit plans.
- Treat this as cost of running your business.
- Determine who has access to what.
- Classify and segment your critical data.
- Perform backups and patch management.
- Conduct ongoing security awareness training and social engineering testing.
- Have a tested Incident Response Plan

Cybersecurity lifecycle



IDENTIFY
- Business Drivers
- Compliance Requirements
- Risk Tolerance
- Cyber Concerns
- Assessment Objectives

DISCOVER
- Threats
- Vulnerabilities
- Risks
- Targets
- Threat Vectors

PRIORITIZE
- Findings, Risks, Observations

RECOMMENI
- Tactics
- Techniques
- Procedures

DEVELOP
- Roadmaps
- Implementation Plans
- Governance Model
- Strategies

DEPLOY
- Solutions
- Policies
- Staff
- Tools
- Etc.

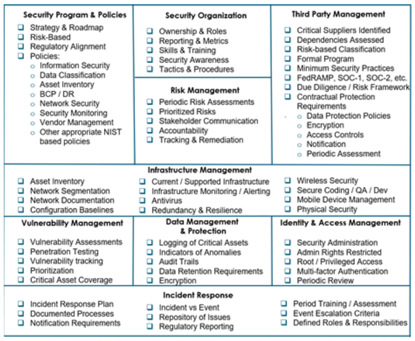
OPTIMIZE
- Continuous Monitoring & Improvement

Security Strategies & Tactics

Areas of cyber risk management

- Awareness & Training
- Policies & Procedures
- Application/ System Inventory
- Security Operations Center
- Software Patching
- Categorize Data
- Business Continuity Planning
- Cyber insurance
- Incident Response
- Third-Party Vendors
- Access Controls and Credential Management
- Configuration
- Spam Filters
- E-mail Detection
- People
- Anti-virus & Malware
- Macro Scripts
- Software Restriction Policies
- App Whitelisting

Components of a cybersecurity framework



Security Program & Policies

□ Strategy & Roadmap
□ Risk-Based
□ Regulatory Alignment
□ Policies:
  ○ Information Security
  ○ Data Classification
  ○ Asset Inventory
  ○ BCP / DR
  ○ Network Security
  ○ Security Monitoring
  ○ Vendor Management
  ○ Other appropriate NIST based policies

Security Organization

□ Ownership & Roles
□ Reporting & Metrics
□ Skills & Training
□ Security Awareness
□ Tactics & Procedures

Risk Management

□ Periodic Risk Assessments
□ Prioritized Risks
□ Stakeholder Communication
□ Accountability
□ Tracking & Remediation

Third Party Management

□ Critical Suppliers Identified
□ Dependencies Assessed
□ Risk-based Classification
□ Formal Program
□ Minimum Security Practices
□ FedRAMP, SOC-1, SOC-2, etc.
□ Due Diligence / Risk Framework
□ Contractual Protection Requirements
  ○ Data Protection Policies
  ○ Encryption
  ○ Access Controls
  ○ Notification
  ○ Periodic Assessment

Infrastructure Management

□ Asset Inventory
□ Network Segmentation
□ Network Documentation
□ Configuration Baselines
□ Current / Supported Infrastructure
□ Infrastructure Monitoring / Alerting
□ Antivirus
□ Redundancy & Resilience
□ Wireless Security
□ Secure Coding / QA / Dev
□ Mobile Device Management
□ Physical Security

Vulnerability Management

□ Vulnerability Assessments
□ Penetration Testing
□ Vulnerability tracking
□ Prioritization
□ Critical Asset Coverage

Data Management & Protection

□ Logging of Critical Assets
□ Indicators of Anomalies
□ Audit Trails
□ Data Retention Requirements
□ Encryption

Identity & Access Management

□ Security Administration
□ Admin Rights Restricted
□ Root / Privileged Access
□ Multi-factor Authentication
□ Periodic Review

Incident Response

□ Incident Response Plan
□ Documented Processes
□ Notification Requirements
□ Incident vs Event
□ Repository of Issues
□ Regulatory Reporting
□ Period Training / Assessment
□ Event Escalation Criteria
□ Defined Roles & Responsibilities

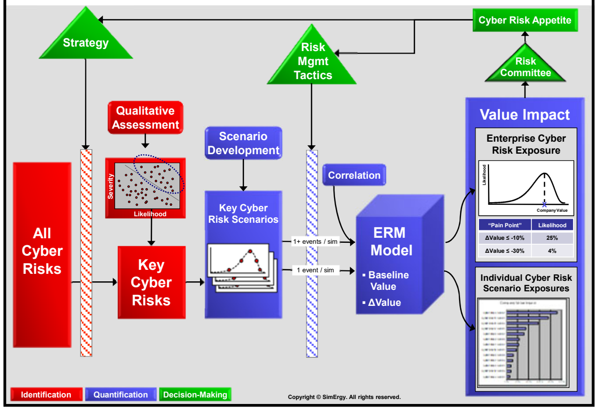
VALUE-BASED CYBER RISK MANAGEMENT

Obstacles in traditional cybersecurity risk management

1) Prioritizing focus amidst myriad cyber risks
2) Making the business case for mitigation decisions
3) Defining cyber risk appetite

Copyright © SimErgy. All rights reserved.

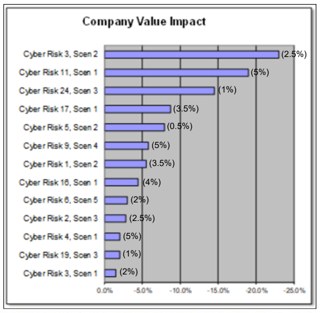
Value-Based Cybersecurity Risk Management



"Pain Point"	Likelihood
ΔValue ≤ -10%	25%
ΔValue ≤ -30%	4%

Copyright © SimErgy. All rights reserved.

Quantifying individual cyber risk scenarios



Copyright © SimErgy. All rights reserved.

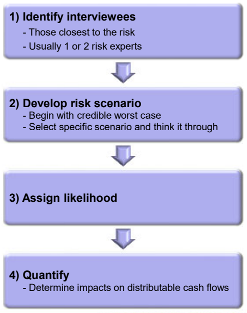
1) Prioritizing focus amidst myriad cyber risks

Traditional Approach		Value-based Approach
Method 1: Qualitative	Cannot support decision-making	Quantifies impact to value / supports decision-making
Method 2: Industry data	Often unavailable, inappropriate, static	Available, company/situation-specific, dynamic
Method 3: Risk capital	Arbitrary / often directionally incorrect	Risk-based

Copyright © SimErgy. All rights reserved.

ILLUSTRATIVE EXAMPLE

Developing risk scenarios: FMEA

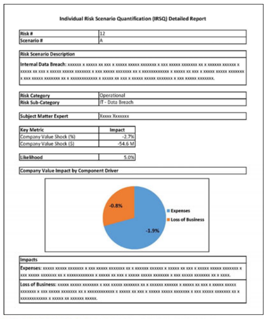


1) Identify interviewees
- Those closest to the risk
- Usually 1 or 2 risk experts

2) Develop risk scenario
- Begin with credible worst case
- Select specific scenario and think it through

3) Assign likelihood

4) Quantify
- Determine impacts on distributable cash flows



Individual Risk Scenario Quantification (IRSQ) Detailed Report

Risk #	12
Scenario #	A

Risk Scenario Description

Internal Data Breach: xxxxxx x xxxxx xx xxx x xxxxx xxxxx xxxxxxx x xxx xxxxx xxxxxxx xx x xxxxxx xxxxxx x xxxxx xx xxx x xxxxx xxxxx xxxxxxx x xxx xxxxx xxxxxxx xx x xxxxxxxxxxxx x xxxxx xx xxx x xxxxx xxxxx xxxxxxx x xxx xxxxx xxxxxxx xx x xxxxxxxxxxxx x xxxxx xx xxx x xxxxx xxxxx xxxxxxx x xxx xxxxx xxxxxxx.

Risk Category	Operational
Risk Sub-Category	IT - Data Breach

Subject Matter Expert	Xxxxx Xxxxxxx

Key Metric	Impact
Company Value Shock (%)	-2.7%
Company Value Shock ($)	-54.6 M

Likelihood	5.0%

Company Value Impact by Component Driver

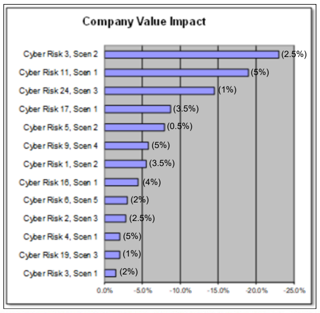
Impacts

Expenses: xxxxx xxxxx xxxxxxx x xxx xxxxx xxxxxxx xx x xxxxxx xxxxxx x xxxxx xx xxx x xxxxx xxxxx xxxxxxx x xxx xxxxx xxxxxxx xx x xxxxxxxxxxxx x xxxxx xx xxx x xxxxx xxxxx xxxxxxx x xxx xxxxx xxxxxxx xx x xxxx.

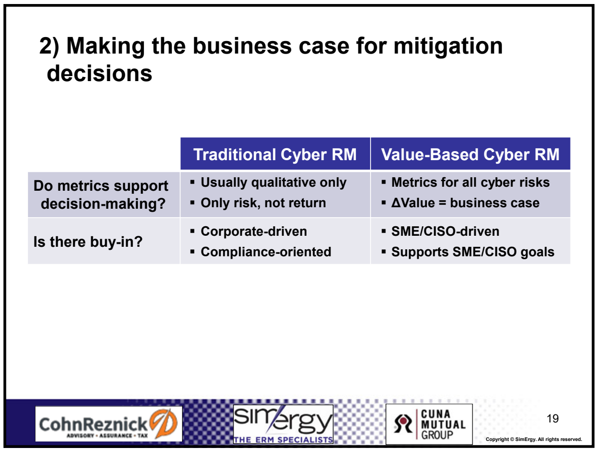
Loss of Business: xxxxx xxxxx xxxxxxx x xxx xxxxx xxxxxxx xx x xxxxxx xxxxxx x xxxxx xx xxx x xxxxx xxxxx xxxxxxx x xxx xxxxx xxxxxxx xx x xxxxxxxxxxxx x xxxxx xx xxx x xxxxx xxxxx xxxxxxx x xxx xxxxx xxxxxxx xx x xxxxxxxxxxxx x xxxxx xx xxxxxx xxxxx.

Copyright © SimErgy. All rights reserved.

Prioritizing focus through quantification



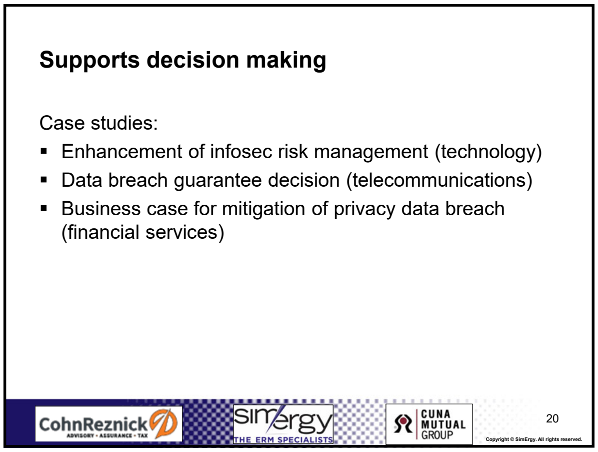
Copyright © SimErgy. All rights reserved.



2) Making the business case for mitigation decisions

	Traditional Cyber RM	Value-Based Cyber RM
Do metrics support decision-making?	▪ Usually qualitative only ▪ Only risk, not return	▪ Metrics for all cyber risks ▪ ΔValue = business case
Is there buy-in?	▪ Corporate-driven ▪ Compliance-oriented	▪ SME/CISO-driven ▪ Supports SME/CISO goals

Copyright © SimErgy. All rights reserved.

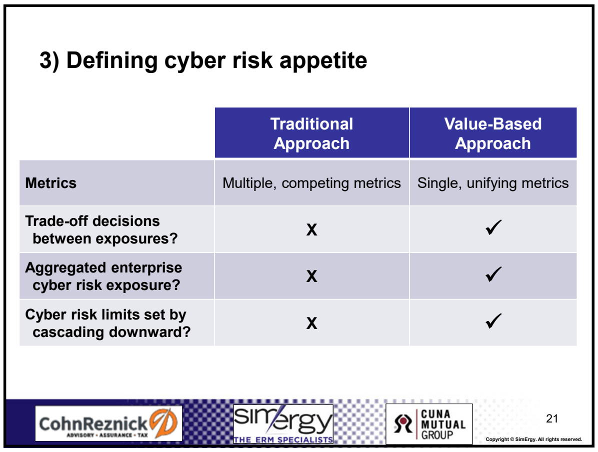


Supports decision making

Case studies:

- Enhancement of infosec risk management (technology)
- Data breach guarantee decision (telecommunications)
- Business case for mitigation of privacy data breach (financial services)

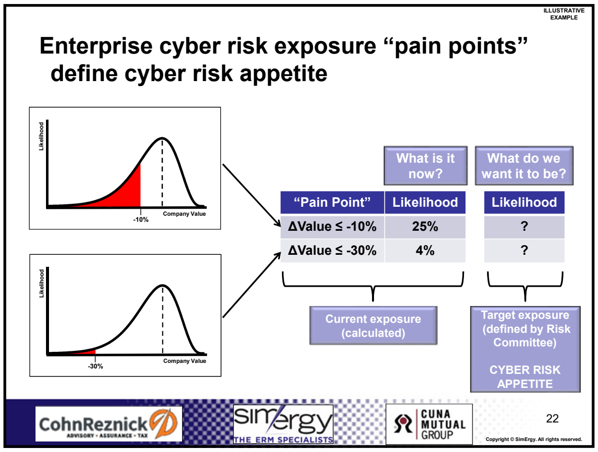
Copyright © SimErgy. All rights reserved.



3) Defining cyber risk appetite

	Traditional Approach	Value-Based Approach
Metrics	Multiple, competing metrics	Single, unifying metrics
Trade-off decisions between exposures?	X	✓
Aggregated enterprise cyber risk exposure?	X	✓
Cyber risk limits set by cascading downward?	X	✓

Copyright © SimErgy. All rights reserved.



ILLUSTRATIVE EXAMPLE

Enterprise cyber risk exposure "pain points" define cyber risk appetite

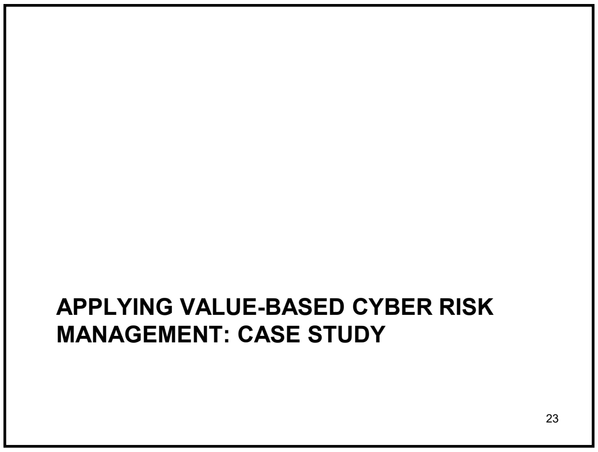
	What is it now?	What do we want it to be?
"Pain Point"	Likelihood	Likelihood
ΔValue ≤ -10%	25%	?
ΔValue ≤ -30%	4%	?

Current exposure (calculated)

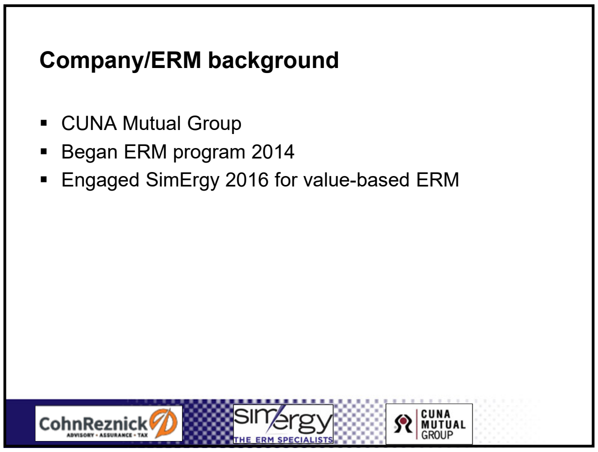
Target exposure (defined by Risk Committee)

CYBER RISK APPETITE

Copyright © SimErgy. All rights reserved.

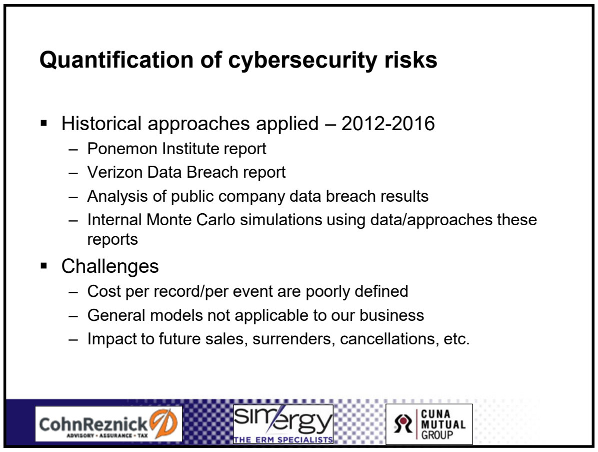


APPLYING VALUE-BASED CYBER RISK MANAGEMENT: CASE STUDY



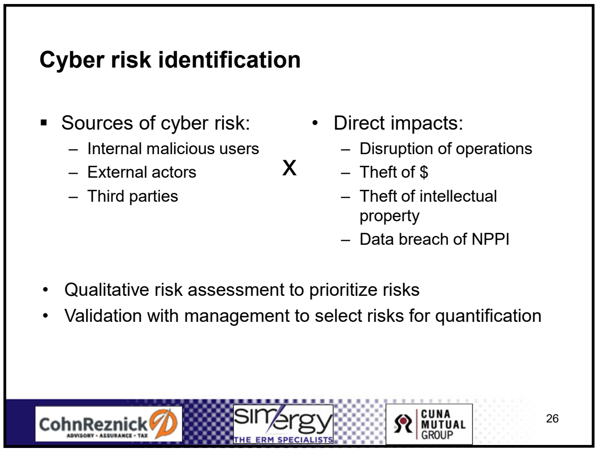
Company/ERM background

- CUNA Mutual Group
- Began ERM program 2014
- Engaged SimErgy 2016 for value-based ERM



Quantification of cybersecurity risks

- Historical approaches applied – 2012-2016
  - Ponemon Institute report
  - Verizon Data Breach report
  - Analysis of public company data breach results
  - Internal Monte Carlo simulations using data/approaches these reports
- Challenges
  - Cost per record/per event are poorly defined
  - General models not applicable to our business
  - Impact to future sales, surrenders, cancellations, etc.



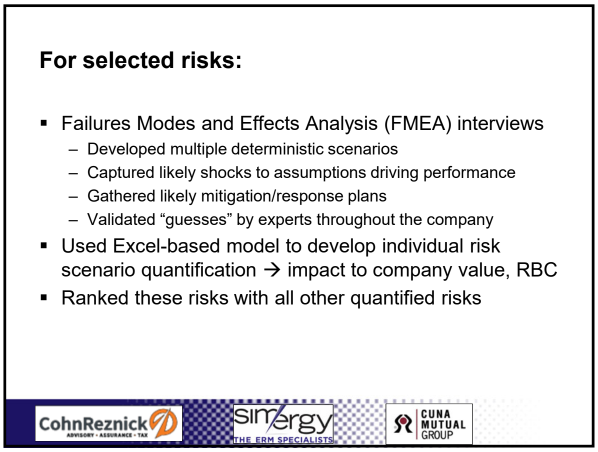
Cyber risk identification

- Sources of cyber risk:
  - Internal malicious users
  - External actors
  - Third parties

X

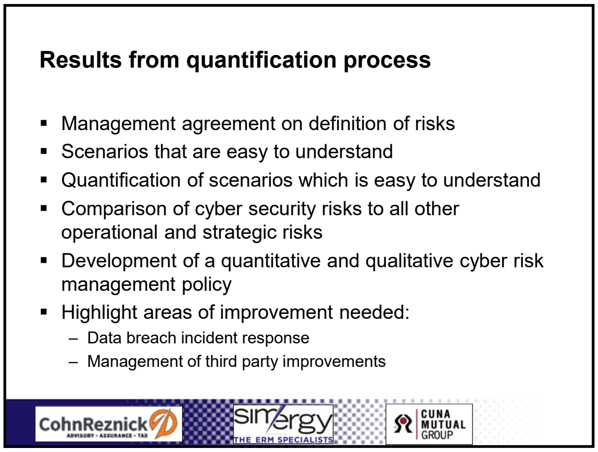
- Direct impacts:
  - Disruption of operations
  - Theft of $
  - Theft of intellectual property
  - Data breach of NPPI

- Qualitative risk assessment to prioritize risks
- Validation with management to select risks for quantification



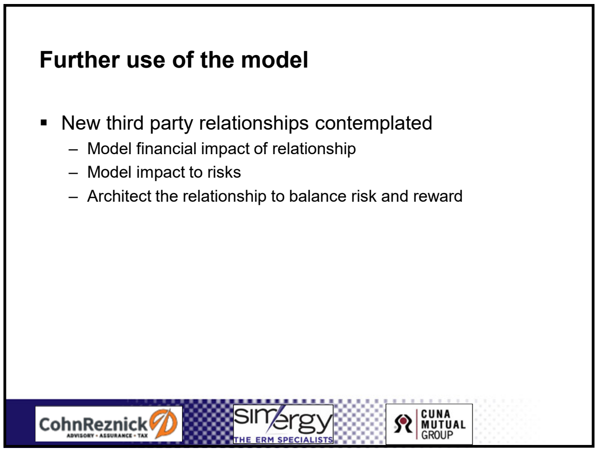
For selected risks:

- Failures Modes and Effects Analysis (FMEA) interviews
  - Developed multiple deterministic scenarios
  - Captured likely shocks to assumptions driving performance
  - Gathered likely mitigation/response plans
  - Validated “guesses” by experts throughout the company
- Used Excel-based model to develop individual risk scenario quantification → impact to company value, RBC
- Ranked these risks with all other quantified risks



Results from quantification process

- Management agreement on definition of risks
- Scenarios that are easy to understand
- Quantification of scenarios which is easy to understand
- Comparison of cyber security risks to all other operational and strategic risks
- Development of a quantitative and qualitative cyber risk management policy
- Highlight areas of improvement needed:
  - Data breach incident response
  - Management of third party improvements



Further use of the model

- New third party relationships contemplated
  - Model financial impact of relationship
  - Model impact to risks
  - Architect the relationship to balance risk and reward

Contact information

Shahryar Shaghaghi	Sim Segal	Dave Bartholomew
Principal, CohnReznick	President, SimErgy Consulting	Director, Gov., Risk & Assurance
Shahryar.Shaghaghi@CohnReznick.com	sim@simergy.com	db3184@columbia.edu