Internal Audit, Risk, Business & Technology Consulting

Using FAIR to Understand Change in Resilience Risk

August 20, 2020

INNOVATE. TRANSFORM. SUCCEED.

Adapt to the new business reality.

protiviti®

Face the Future with Confidence

FAIR INSTITUTE

INTRODUCTIONS

Vince Dasta
Director
Cyber Risk Quantification
Protiviti

Doug Wilbert
Managing Director
R&C US Operational
Resilience Leader / US
Capital Markets Leader
Protiviti

William Forsell
Associate Director
Risk & Compliance
Protiviti

Operational Resilience

OPERATIONAL RESILIENCE BACKGROUND

Operational resilience continues to be top of mind for industry executives and supervisory authorities around the world.

June 2018
Visa experiences outage due to hardware failure leaving millions of customers unable to pay for goods and services

June 2019
Raphaels Bank fined by UK FCA and PRA for operational resilience failings

October 2019
OCC includes Operational Resilience in 2020 Bank Supervision Operating Plan

November 2019
FFIEC revises the Business Continuity Management Booklet to stress value of Resilience to avoid disruptions to operations

June 2017
Maersk infected with NotPetya causing outages in over 130 countries

July 2018
Bank of England, the PRA and FCA released a joint discussion paper titled Building the UK Financial Sector's Operational Resilience

December 2019
Bank of England, FCA, and PRA released the latest consultation papers on Operational Resilience for UK institutions

Jan 2020
COVID pandemic creates uncertainty globally, forcing stay at home measure, stimulus and massive GDP drop and unemployment

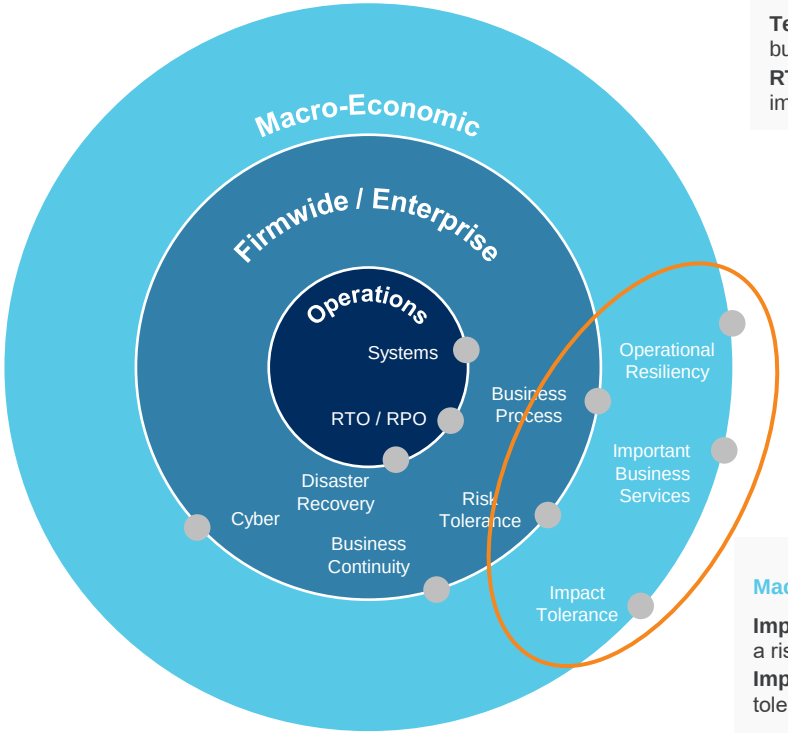
Why is it important?

- Dynamic landscape increases the risk of "extreme but plausible" events
- Impacts the stability of the financial system as well as the viability of firms
- Resilience events can increase risk and threaten growth
- Enhancing a firm's resilience can create long-term competitive advantages and mitigate cost

Who does it impact?

- Large firms whose activity threatens financial stability
- Smaller firms where activity is big enough to threaten the firm's safety and soundness
- Third-party providers of important business or sector-level services

WHAT IS RESILIENCE RISK?



Operations Considerations

Technology: Internal and External Applications, Networks and Data that drive business processes within the firm.

RTO / RPO: System-level metrics on data and recovery time objectives to minimize impact to business activities.

Firmwide Considerations

Business Processes: Defined and clearly understood business processes.

Risk Tolerance: Amount of uncertainty tolerated, specifically with regards to unacceptable outcomes.

Operational Resiliency

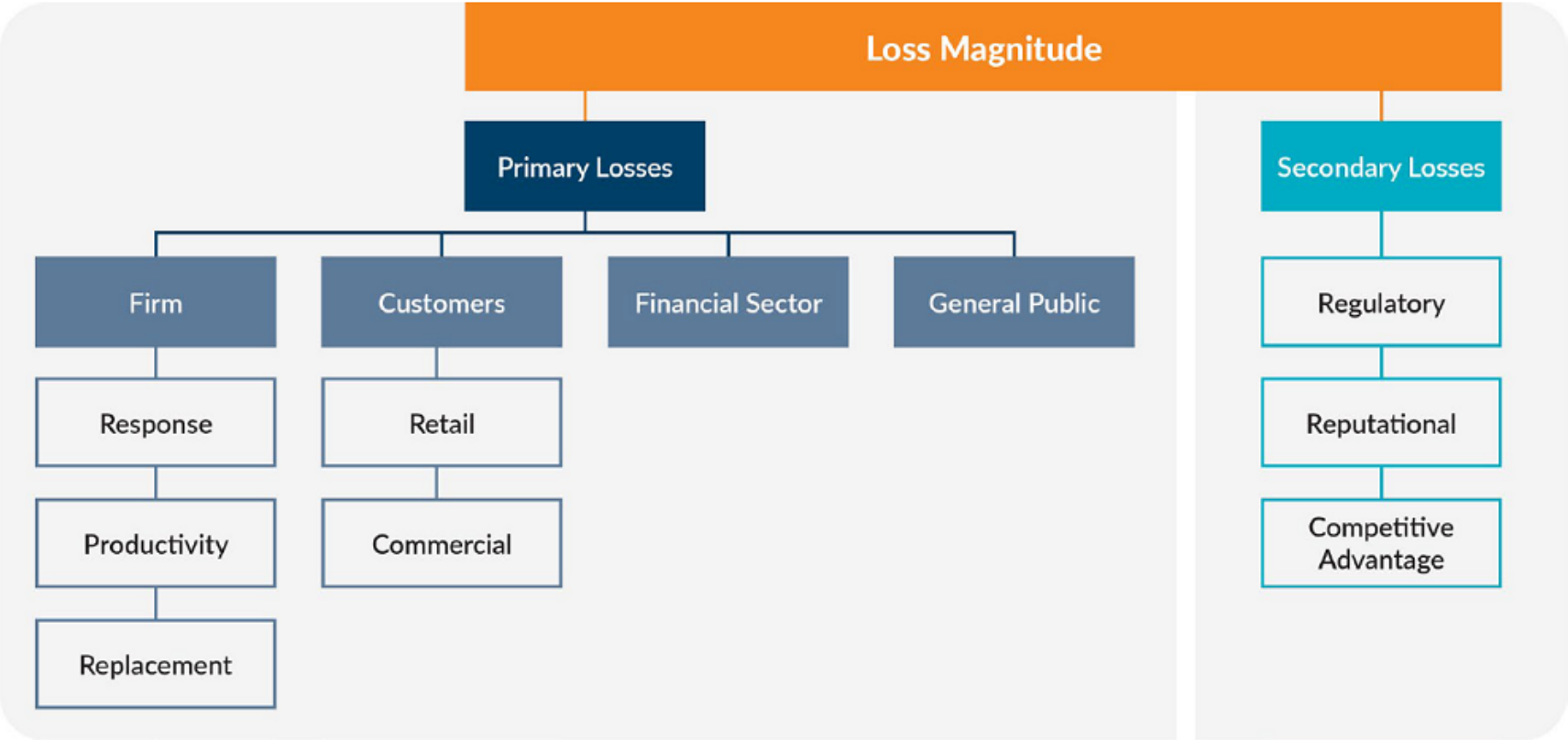
The ability of an organization to withstand adverse changes in its operating environment and continue the delivery of business services and economic functions.

Macro-Economic Considerations

Important Business Services: Business operations to which a disruption poses a risk to an institution's safety and soundness or financial stability

Impact Tolerance: Quantitative measurement to determine 'the maximum tolerable level of disruption to an important business service'.

ADAPTING THE FAIR MODEL TO MEASURE RESILIENCE RISK



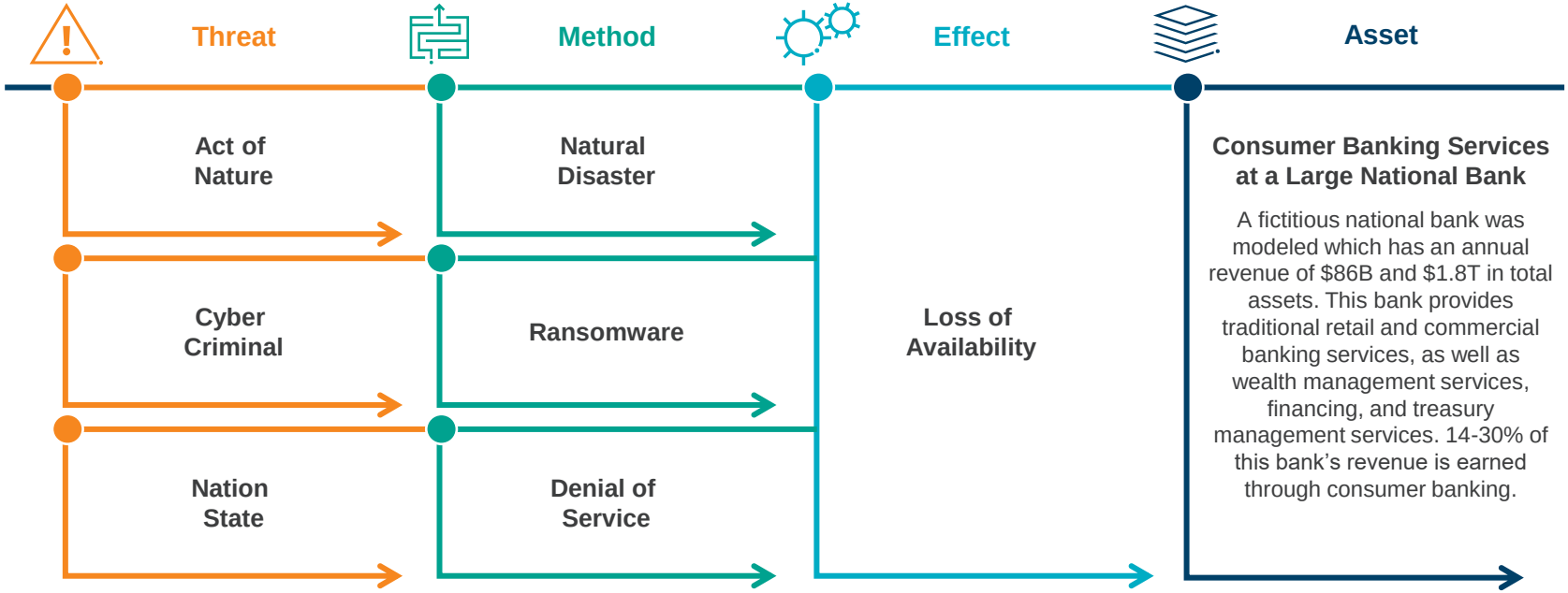
Example Analysis

COMPARATIVE ANALYSIS PROCESS

Conduct baseline analysis → Identify changes from proposed initiative → Adjust model inputs → Compare future state to baseline

ANALYSIS SCOPE

To quantify the risk posed to an asset, the FAIR model requires the definition of a threat, a method used by the threat, and associated effect on an asset. For this analysis, we analyzed the risk associated with **Acts of Nature, Ransomware, and Denial of Service attacks** against consumer banking services.

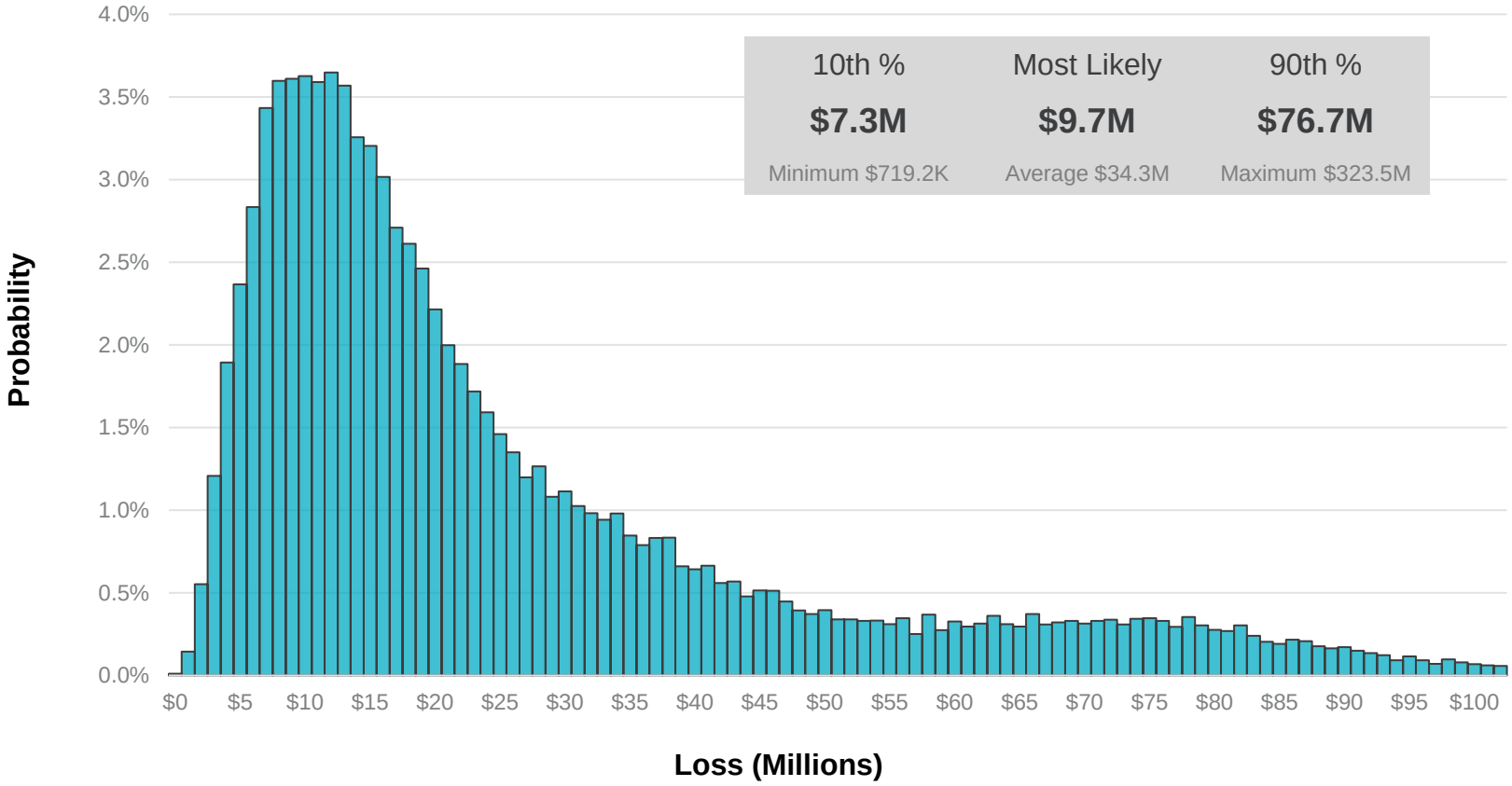


ON PREMISE ANALYSIS

- Based on historical outages at similar financial institutions, we are assuming an outage duration of 1-24 hours, most likely just over 4 hours.
- The number of impacted employees will vary depending on the timing, duration, and nature of the outage. We will use a large distribution of 25-259k impacted employees.
- Based on details from other similar outages we would expect 14-30% of our customers to be negatively impacted from this outage.
- Response will be performed by bank employees

Form of Loss	Minimum	Most Likely	Maximum
Primary Productivity	$70K	$5M	$319M
Primary Response	$31.4K	$894K	$2.2M
Per Customer Harm	$500	$147K	$3.6M
Secondary Response	$1.3K	$3.8M	$18.2M

SINGLE LOSS EVENT MAGNITUDE – ON PREMISE



CLOUD VERSUS ON PREMISE – WHAT CHANGES?

The FAIR Model was utilized to quantify the risks / resilience of a hypothetical company whose applications and data were all on premises versus the same company whose applications and data were all on the cloud.

Key Assumptions

- Technology investment, uptime metrics, process and abilities for Cloud Providers are derived from publicly available sources
- Aggregation of publicly available data and client experiences were utilized to derive hypothetical institutional characteristics
- CSP can more effectively address certain technology concerns than FSIs:
  - Evergreen (always patched) databases and underlying infrastructure
  - Deep and comprehensive logging
  - Threat Analysis deployed with a click
  - Access to multiple geographic regions for resource deployment
  - Best of the Best Technical Resources

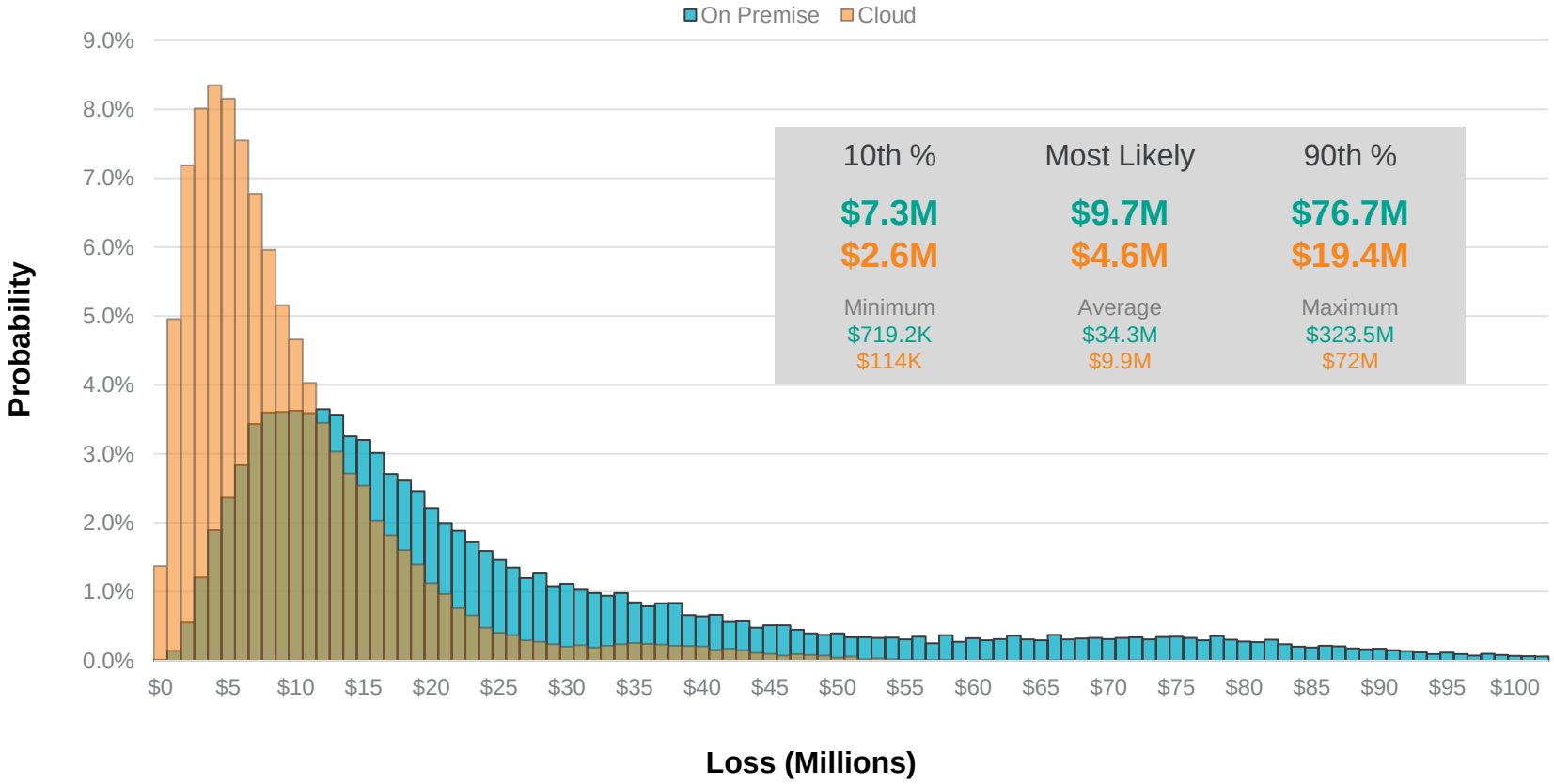
Risk Mitigation Characteristic	Cloud Provider	FSI 'Standard' Approach
Architecture	Anticipates failure of hardware and software building in automated resilience	Aversion to failure. Focus on resilience through traditional disaster recovery sites. Redundancy requires human intervention to bring online
Security Controls	Comprehensive Defense-in-Depth and Highly Automated	Some Defense-in-Depth and limited automation
Change Management	Automated testing with extensive coverage and Continuous Integration/Continuous Delivery	Semi-automated, human-process intensive change management with limited testing coverage
Service Delivery Model	All service requests exclusively via application programmable interfaces (APIs)	Service requests via human workflow
Operability	Programmatic and automated operations requires fewer human operators as demand increases	Human-intensive operations, grows linearly with demand
Culture	Focus on IT user (CSP client) experience Small, accountable teams Hyper-scale ambition	Limited focus on IT user experience Large, semi-accountable teams Limited application-defined ambition

CLOUD ANALYSIS

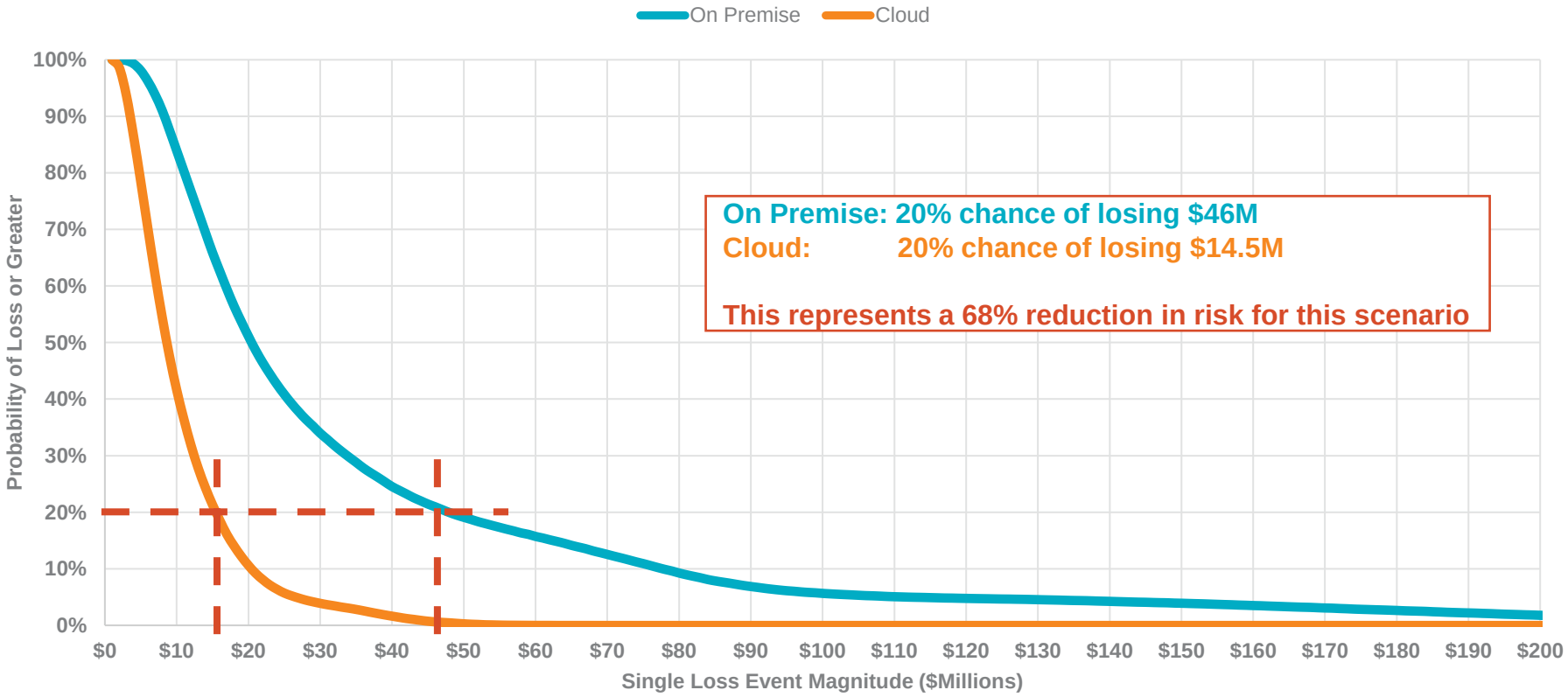
- Based on historical outages at similar financial institutions, we are assuming an outage duration of 0.1 to 4 hours most likely 1 hour.
- The number of impacted employees will vary depending on the timing, duration, and nature of the outage. The magnitude of impact will be less due to the shorter duration of an outage.
- Based on details from other similar outages we would expect 14-30% of our customers to be negatively impacted from this outage however the magnitude of harm would be less.
- Primary response will be performed by cloud provider with involvement from bank employees

Form of Loss	Minimum	Most Likely	Maximum
Primary Productivity	$7K	$635K	$67.6M
Primary Response	$8.7K	$145K	$351K
Per Customer Harm	$500	$55K	$386K
Secondary Response	$1K	$3.7M	$18.2M

SINGLE LOSS EVENT MAGNITUDE - COMPARISON



LOSS EXCEEDANCE CURVE - COMPARISON



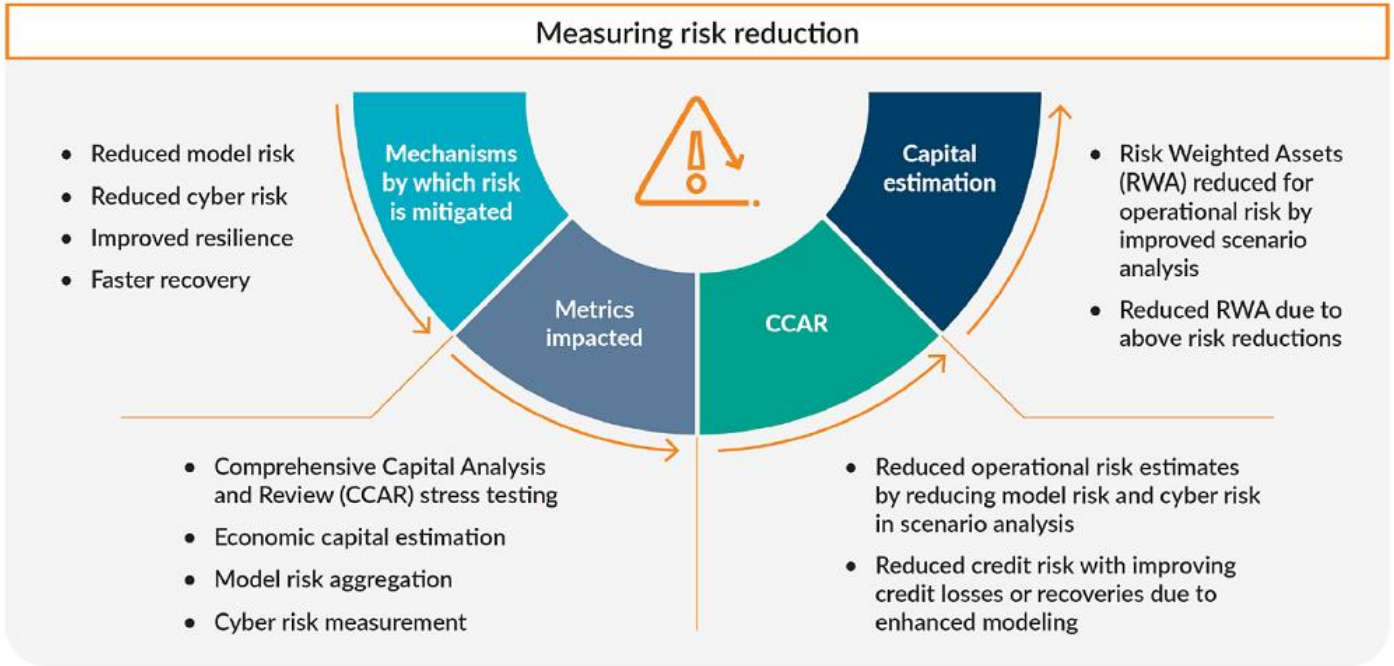
The Real Financial Impact

BANK CAPITAL CHARGES FOR OPERATIONAL RISK

- Banks are required to hold capital for operational risk under regulatory capital rules and Comprehensive Capital Analysis and Review (CCAR) stress tests
  - Regulatory capital requirements are based on risk-weighted asset (RWA) calculations for operational risk for "advanced approaches" banks
  - Operational risk loss projections are included in required stress capital buffers based on the Federal Reserve's CCAR scenarios
- Large U.S. banks hold several hundred billion dollars of common equity capital for operational risk including regulatory capital minimums and stress loss estimates
  - Regulators have relied primarily on the industry's historical operational loss experience in setting ops risk capital requirements
  - Banks have been challenged to translate reductions in operational risk into reductions in capital charges on a timely basis
- Robust analytical techniques like FAIR can be incorporated in stress test scenarios to quantify reductions in operational risk and associated capital needs
- Expected future changes in the U.S. regulatory capital regime provide an opportunity to incorporate a more structured and transparent approach to operational risk capital measurement

QUANTIFYING RISK REDUCTION FROM MOVING TO THE CLOUD

Comprehensive Capital Analysis and Review (CCAR) stress testing and Risk Weighted Assets are ways that financial services companies measure risk. Below we demonstrate how these metrics can be impacted by moving data and processes to the cloud.



MEASURING RISK MITIGATION FROM REDUCTION IN CYBER RISK

Below is a sample with estimated values to demonstrate the potential risk mitigation and the impact of moving to the cloud on Comprehensive Capital Analysis and Review (CCAR) stress testing loss estimates and RWA for capital. This is only for the Operational Risk impact of Cyber Risk aspect and these are conceptual numbers only.

Based on these two calculations, the capital savings for a $250B bank could be $600M.

PROJECT STRESS TESTING

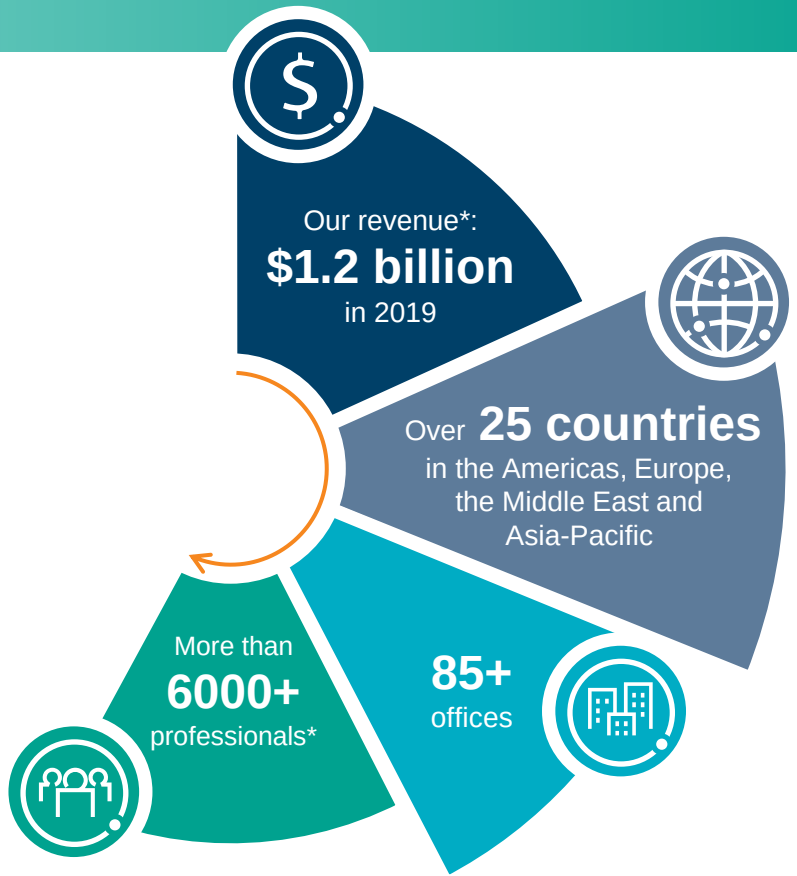
- Most banking organizations are challenged to measure a technology project's reduction of resilience risk
- FAIR can be used to stress test technology projects, both in the planning stage and after completion, allowing for a more comprehensive view of:
  - Project selection
  - Project outcome
  - Return on investment
- Project stress tests allow management to update the board on trends in the organization's resilience risk
- Risk can be measured in several dimensions including time, dollars, and potential capital savings

About Protiviti

WHO WE ARE

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 85 offices in over 25 countries.

We have served more than 60 percent of Fortune 1000® and 35 percent of Fortune Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

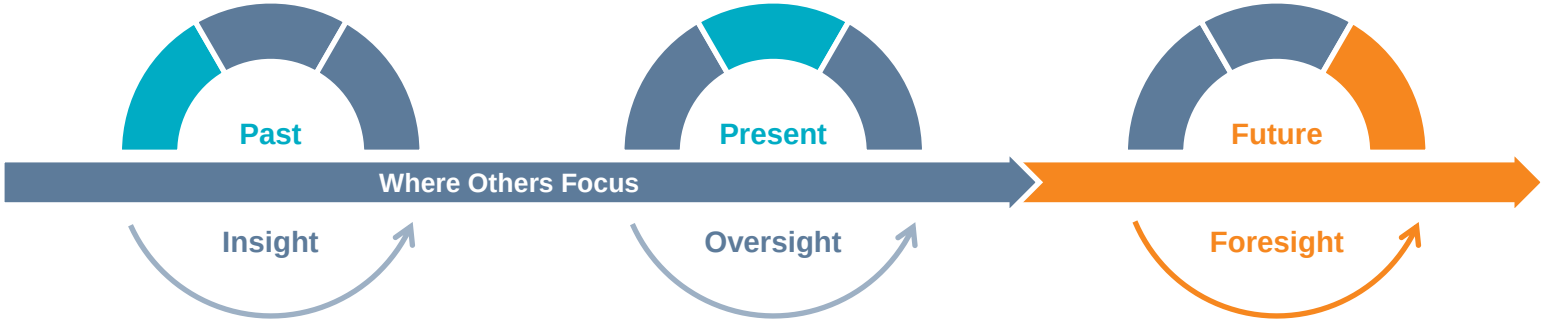


*Inclusive of Protiviti's Member Firm network

THE PROTIVITI ADVANTAGE

Risk Intuition

We help leaders make better decisions by managing the risks they face today, as well as illuminating the risks and unforeseen consequences inherent in their strategies for growth and opportunity in the future.



- How do we better manage risks we have faced in the past?

- How well are we controlling known risks?
- Are we identify and managing new risks effectively?
- Are we in compliance?

- What risks are embedded in our plans for growth or acquisitions?
- What risks inhibit our ability to innovate and perform?

GLOBAL PRESENCE

The Americas

1. UNITED STATES
Alexandria, VA
Atlanta, GA
Baltimore, MD
Boston, MA
Charlotte, NC
Chicago, IL
Cincinnati, OH
Cleveland, OH
Dallas, TX
Denver, CO
Ft. Lauderdale, FL
Houston, TX
Kansas City, KS
Los Angeles, CA
Milwaukee, WI
Minneapolis, MN
New York, NY
Orlando, FL
Philadelphia, PA
Phoenix, AZ
Pittsburgh, PA
Portland, OR
Richmond, VA
Sacramento, CA
Salt Lake City, UT
San Francisco, CA
San Jose, CA
Seattle, WA
Stamford, CT
St. Louis, MO
Tampa, FL
Washington, D.C.
Winchester, VA
Woodbridge, NJ

2. ARGENTINA*
Buenos Aires

3. BRAZIL*
Rio de Janeiro
São Paulo

4. CANADA
Kitchener-Waterloo
Toronto

5. CHILE*
Santiago

6. COLOMBIA*
Bogota

7. MEXICO*
Mexico City

8. PERU*
Lima

9. VENEZUELA*
Caracas

**Protiviti Member Firm*

Europe/Middle East

10 FRANCE
Paris

11. GERMANY
Frankfurt
Munich

12. ITALY
Milan
Rome
Turin

13. THE NETHERLANDS
Amsterdam

14. UNITED KINGDOM
Birmingham
Bristol
Leeds
London
Manchester
Milton Keynes
Swindon

15. BAHRAIN*
Manama

16. KUWAIT*
Kuwait City

17. OMAN*
Muscat

18. QATAR*
Doha

19. UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

20. SAUDI ARABIA*
Riyadh

21. EGYPT*
Cairo

22. SOUTH AFRICA*
Durban
Johannesburg

Asia-Pacific

23. AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

24. CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

25. INDIA*
Bengaluru
Chennai
Hyderabad
Kolkata
Mumbai
New Delhi

26. JAPAN
Osaka
Tokyo

27. SINGAPORE
Singapore

**Protiviti Member Firm*

CYBER RISK QUANTIFICATION: HOW PROTIVITI CAN HELP

Define the Risk Taxonomy

Clearly defining a risk vocabulary and establishing a risk taxonomy to allow practitioners and the business to take a threats based approach to cybersecurity risk and provide consistent risk register statements.

Quantitative Cyber Risk Assessment

Assessing cyber threats facing your organization using open quantitative risk measurement methods such as Applied Information Economics (AIE) and Factor Analysis of Information Risk (FAIR)

Program Design & Implementation

Designing and implementing the programs and processes required to shift from a controls orientation of cybersecurity to a business risk orientation and optimizing compliance frameworks based on risks.

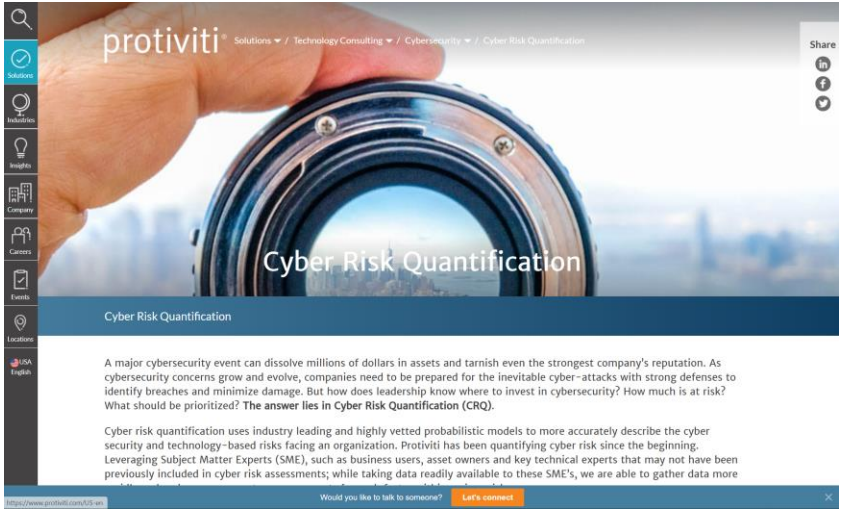
Metrics & Data

Building cybersecurity datamarts to collect, process, and store relevant metrics for analysis and reporting including customized interactive reports and dashboards to replace legacy PowerPoint decks and spreadsheets

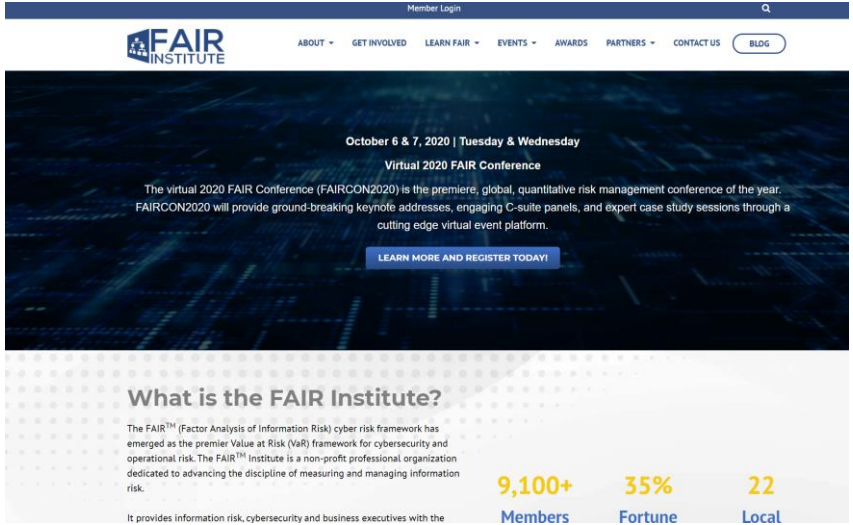
Training & Change Management

Conducting training and organizational change management to help your organization embrace a culture of data driven informed decision making

ADDITIONAL RESOURCES



Protiviti.com/FAIR



fairinstitute.org

Founding Advisory Partner

Questions?

Face the Future with Confidence

protiviti®