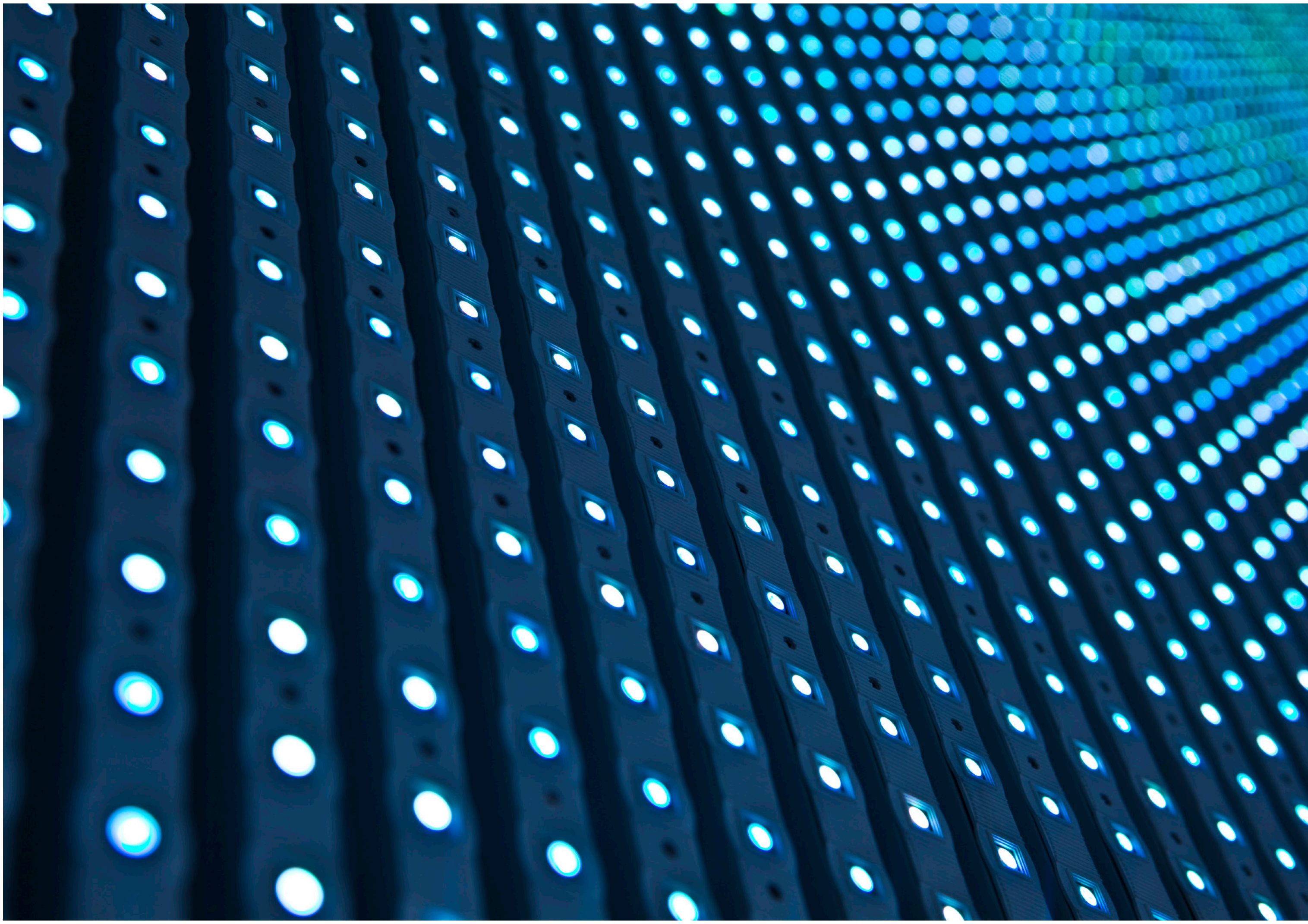
protiviti®

Face the Future with Confidence



Measuring Cyber Risk Quantitatively — Eliminating the Guesswork

The Benefits of Leveraging FAIR

Internal Audit, Risk, Business & Technology Consulting

Introduction

The subjectivity of traditional cyber risk assessment processes can generate scores that are sometimes difficult for business owners and managers to accept. Often, the risk scores are subject to wide interpretation, generating more questions than answers: Is my “medium” someone else’s “high” score? Does a high score accurately reflect a lower risk exposure?

Often, the risk scores generated from a traditional cyber risk assessment process is subject to wide intepretation. Analysts typically develop scores using a risk assessment template with predefined risk factors. This one-size-fits-all approach can produce inconsistent results.

Even when the underlying assessment is performed correctly, a low score may not sit well with a business owner or manager who is uneasy with the assessment process. This is especially true with the traditional approach, where analysts develop scores using a risk assessment template with predefined risk factors. This one-size-fits-all approach can produce inconsistent results.

There is a more effective, informative method for analyzing cyber risk that exposes specific actionable information about measuring and mitigating risk. Factor Analysis of Information Risk (FAIR) is a sophisticated, sensitive and substantive approach to analyzing risk.[1] The end result of FAIR is not a score of high, medium or low but rather a quantifiable measure of the financial effects of unknown cyber risk over time. FAIR can then be used to weigh any cyber risk against an organization’s risk profile or the variance between its risk appetite and the degree of risk that can be tolerated.[2]

The FAIR approach also considers the impact on additional parties or stakeholders. For example, when used to analyze a cyber breach, FAIR will access not only the direct impact to an organization but also the trickle-down effect from regulatory fines and potential loss of business due to customer defections. This model aligns with the recent focus on understanding the broader impact of operational disruptions or outages on financial institutions — a concept financial sector regulators have referred to as “impact tolerance.”

Protiviti is engaged in high-level conversations with numerous organizations about using FAIR to better assess impact tolerance.[3] In this paper, we discuss the use of FAIR for cyber risk analysis. However, FAIR can also be applied to operational and conduct risk analysis. In future papers, we will focus on the use of FAIR in those specific areas.

[1] www.fairinstitute.org/what-is-fair

[2] www.fairinstitute.org/blog/risk-appetite-vs.-risk-tolerance.-whats-the-difference

[3] www.protiviti.com/US-en/fair

What is FAIR?

FAIR applies the Monte Carlo statistical analysis method to help businesses measure and manage information risk[4]. The Monte Carlo simulation can respond to questions such as, “How long can the business survive this risk event?” and “If we take a particular risk reduction measure, what risk reduction can we actually achieve?” It is used to analyze highly uncertain data and to understand the impact of risk in a variety of contexts, including financial risk, project risk and others.

The FAIR method of analyzing risk has been tested in organizations since 2001[5]. It can be used in conjunction with other risk frameworks such as ISO 31000, COSO, COBIT, and NIST CSF[6]. The Open Group, a global consortium that enables achievement of business objectives through vendor-neutral technology standards[7], has chosen FAIR as the international standard information risk management model for understanding, analyzing and quantifying information risk in financial terms.[8]

	FAIR	Traditional Risk Assessment
Depth	Analysis	Assessment
Focus	Business services	Information systems
Basis	Quantifiable information	Subjective ratings
Orientation	Business risk	Controls
Output	Cost and time information	High/medium/low ratings
Considers Event Timing and Duration	Yes	No

[4] www.fairinstitute.org/blog/is-fair-a-value-at-risk-model; http://news.mit.edu/2010/exp-monte-carlo-0517

[5] www.fairinstitute.org/blog/how-was-fair-started

[6] www.fairinstitute.org/blog/standards-groups-and-regulators-recognize-fair

[7] www.opengroup.org/about-us

[8] www.fairinstitute.org/what-is-fair

The following is a summary of the gaps in traditional cyber risk assessments and why a growing community of risk professionals continue to support adoption of FAIR:

- Many traditional methods prescribe the need to quantify risk but mostly leave it up to practitioners to figure it out. FAIR allows organizations to quantify the cost of service unavailability in probabilistic terms.
- In the traditional approach, the likelihood and severity of risks are subjectively rated, resulting in loss of actionable information. With FAIR, specific threat scenarios against individual assets, like a malware attack orchestrated by a nation-state intelligence service that results in the theft of customer financial information, can be measured.
- Traditional cyber risk scoring can create hazards of its own by implying certainty where no certainty exists, and by miscategorizing threats. The consistent and logical terms and definitions that make up FAIR's ontology can significantly improve the quality of risk-related communication within an organization and between organizations.
- FAIR is complementary to other risk assessment models or frameworks and can be used to improve the quality of other traditional model results.

Based on FAIR, organizations can take certain business decisions or actions, such as:

- Quantify the organization's resilience for various business services.
- Select the most effective risk management initiatives based on projections of cyber resilience project outcomes.
- Validate and demonstrate the effectiveness of cyber resilience measures based on FAIR's cyberrisk analyses conducted over time.
- Improve board reporting[9] by quantifying the return on cyber resilience investment.[10]

[9] www.isaca.org/Journal/archives/2017/Volume-1/Pages/evolving-cyberrisk-practices-to-meet-board-level-reporting-needs.aspx?utm_referrer=

[10] www.fairinstitute.org/blog/faircon-2018-wrap-tips-on-board-reporting-cyber-insurance-buying-ciso-cro-relating

Deeper Analysis Drives Confidence

When an organization employs FAIR to quantify cyber risk, there is less room for misinterpretation. As previously mentioned, decision-makers and analysts understand one another better by using probabilistic language and a common taxonomy of risk. Any risk management decision can be challenged and defended in this common language. By decomposing risk into its factors, FAIR provides information to support decisions, and the organization develops an understanding of how cyber risk management efforts and investments impact its overall risk profile.

Also, with FAIR, an organization is better positioned to evaluate a variety of possible threats and to calculate the effects of operational resilience measures with greater confidence. For instance, once the organization uses FAIR to establish its risk tolerance window, it can also use FAIR to evaluate the return on investment for various operational resilience procedures and subsequently prioritize its corrective actions accordingly.

Furthermore, because FAIR involves deeper analysis encompassing more diverse stakeholders, organizations can evaluate loss impacts to a stakeholder group or consider all stakeholders in aggregate to comprehend the total cost of an event. These evaluations help identify stakeholders with the least ability to withstand an event, which enables the organization to set impact tolerance thresholds with the most vulnerable stakeholders in mind.

Finally, the calculations undertaken in a FAIR cyber risk analysis also support a variety of data visualization techniques, which can be refined and customized to address an organization's reporting needs. Charts that show costs over time help leaders visualize the potential outcomes of their decisions.

Decision-makers and analysts understand one another better by using probabilistic language and a common taxonomy of risk. Any risk management decision can be challenged and defended in this common language. FAIR provides information to support decisions, and allows organization to develop a better understanding of how cyber risk management efforts and investments impact its overall risk profile.

Sophisticated and Sensitive Cyber Resilience Decisions — A Case Study

A multinational consumer financial services firm wanted to improve its understanding of cyber risks and gain greater insight into how effectively certain mitigations and controls being considered would contribute strengthen cyber resilience.

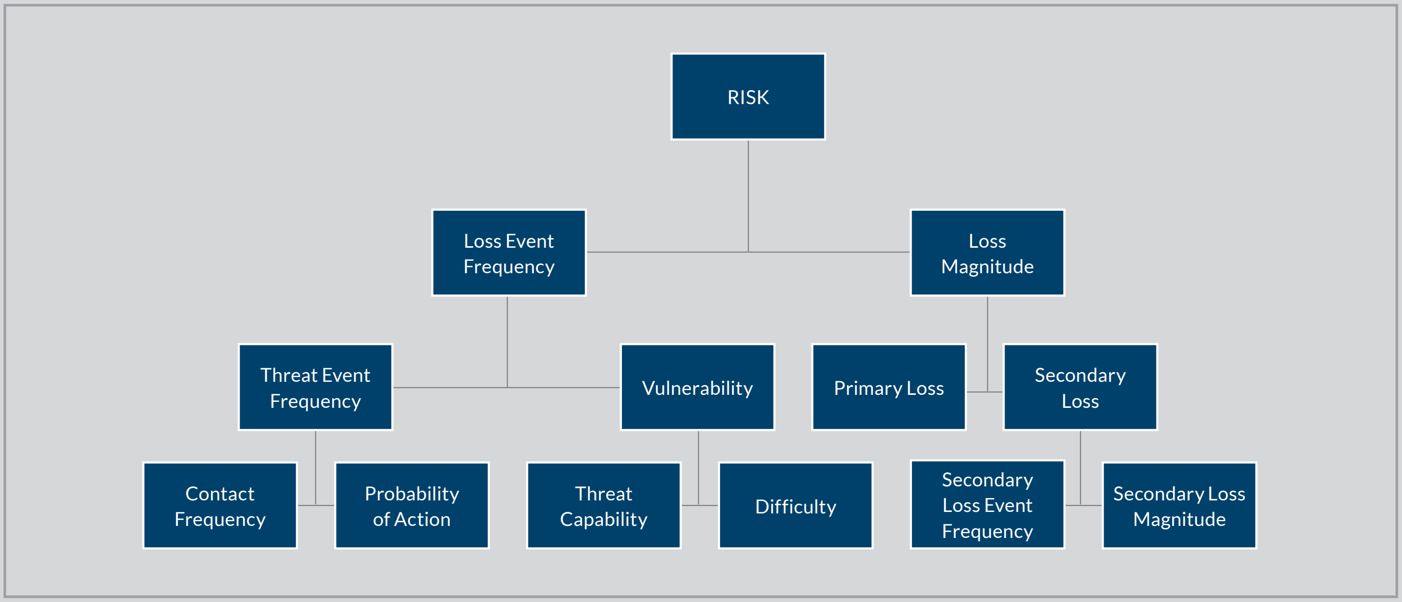
The firm's management started by socializing FAIR concepts among the cybersecurity functions and other internal groups to establish a FAIR team. To support its adoption of FAIR, the organization provided workshops and training for the core team and presentations for other stakeholders.

The FAIR team then held a workshop to assess threats to the organization's critical business services. Rather than viewing this exercise system by system, the team broadly examined each business service, carefully weighing impacts to different stakeholder groups, including the system administrator who handled the initial trouble call to the end consumer who was unable to use her debit card. This exercise produced an inventory of threats to analyze. Their scope included systems and services already in place as well as all proposed and in-flight initiatives.

The team then identified all the FAIR loss event scenarios. In FAIR terminology, loss event scenarios are threats against assets of business value, not just IT assets, that could result in losses. Loss-event scenarios could include any event that might interrupt or compromise business services, like natural disasters, cyberattacks, data breaches, and ransomware, among others. The loss event scenarios identified can be used to conduct a deeper analysis.

Next, the team analyzed each loss event scenario in greater detail. Decomposing each loss event scenario enabled the team to see how it would impact stakeholders. The FAIR approach to analyzing cyber risk provides a standard taxonomy and ontology for risk, which shows relationships between concepts in a branch structure.

The FAIR Risk Ontology — A model of how risk works by describing the factors that make up risk and their relationships to one another. These relationships can then be described mathematically, which allows us to calculate risk from measurements and estimates of those risk factors.



Sophisticated and Sensitive Cyber Resilience Decisions — A Case Study *(continued)*

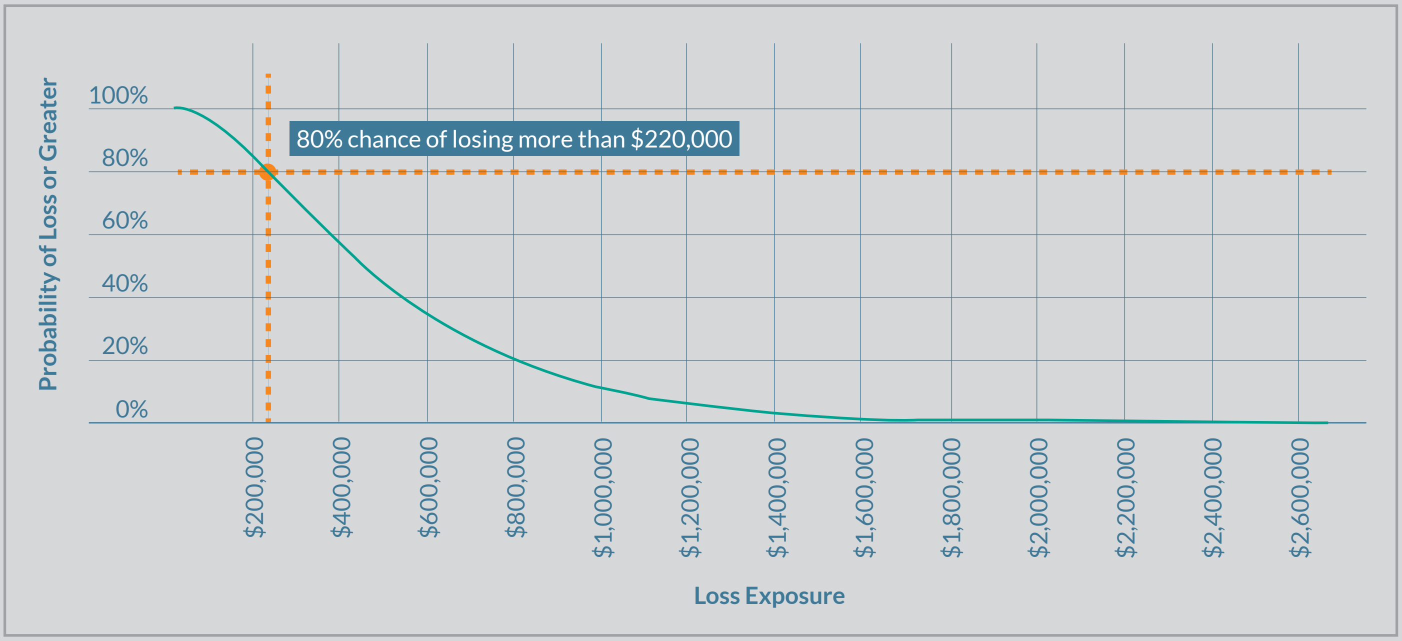
The team found this decomposition to be a useful approach to its analysis because it permitted a more granular understanding of data that could also be aggregated as they saw fit.

The ontology also helped the team evaluate each loss event scenario in multiple dimensions — anticipated frequency of a threat and a service's vulnerability to that threat, as well as the magnitude of any loss — measured in financial terms. Losses included primary ones directly attributed to each loss event scenario (such as incident response and lost business productivity), as well as secondary losses (e.g., time spent responding to inquiries about the loss event, potential fallout from regulatory response and loss of customers and future business). All losses were quantified as anticipated costs.

FAIR prompted a thorough analysis by disclosing all forms of loss that could result from a loss event scenario, including lost productivity, replacing a system or service, the cost of responding to a loss event, reductions to the organization's competitive advantage, damages to the organization's reputation, and fines and judgments.

Now supplied with an understanding of potential losses in terms of financial costs, the team was ready to establish target risk parameters for each service. These parameters were measured in time but translated directly to costs. The team worked with leaders to establish the *recovery point objective* (RPO) for each service — the acceptable duration of a loss event scenario. They also used FAIR simulations to determine the *recovery time objective* (RTO) — the duration that each service could remain unavailable before business operations were significantly impaired. They calculated the *maximum tolerable period of downtime* (MTPOD), after which the organization's viability would be threatened to the point of possibly never resuming. The costs associated with the MTPOD were the organization's stated loss capacity. This

Loss Exceedance Curve — The Monte Carlo simulation can be used to produce loss exceedance curves, which describe the impact and likelihood of a cyber event. Below is an example of a loss exceedance curve.



exercise also considered the timing of a loss event scenario; the team acknowledged that costs would be different if the event occurred, for example, on a Sunday morning versus a payday afternoon.

By using FAIR methods, the team completed an analysis that determined whether — and for how long — the losses calculated would be sustainable. The analysis provided answers to these complex questions:

- How long before unavailability of our consumer debit card services exceeds what we've defined as an acceptable loss?
- If, at 16 hours of downtime, we would have a 20% chance of losing $100 million, would a $15 million cyber resilience initiative be a good investment if it would reduce those losses by half?

The insights the organization gained stood in stark contrast to the traditional risk assessments that previously had guided its decisions. Now, management had objective numerical data to:

- Establish the organization's risk management priorities:
- Select the most effective cyber resilience-oriented projects
- Measure projects' effectiveness post-implementation
- Report on overall cyber resilience portfolio effectiveness to their executives and board — and to regulators.

"This kind of in-depth analysis is like gold," said one senior executive at the firm. "The exercise was extremely rigorous, and we stand on firmer ground now that we really know where the threats are and how best to invest our cyber resilience dollars."

How to Win With FAIR

Quantifying the numerous risks faced by your organization will help prioritize efforts, support your decision-making and refresh your organizational priorities. Shifting from a controls-focused orientation to a business risk orientation — and optimizing cyber resilience frameworks based on FAIR — may demand special effort to spur and strengthen adoption. Organizations contemplating whether to implement FAIR should consider how they would manage a significant change to the well-established risk assessment approach. Conducting training, workshops and presentations for decision-makers, cybersecurity professionals and business stakeholders will support the organizational change required for success with FAIR.

Proper presentation of results is another important aspect of the overall FAIR cyber risk analysis process. Firms will have the opportunity to replace legacy PowerPoint decks and spreadsheets with interactive, data-driven reports and dashboards. Larger organizations with a higher degree of complexity should consider specialized data marts to collect, process and store relevant metrics for analysis and reporting. The benefit of effective presentation is twofold: It helps everyone in the organization understand their overall risk profile, and it underscores dramatically the value achieved via an organization's investment in FAIR.

Conclusion

Cyber risk is best evaluated through a probabilistic, quantifiable approach like FAIR, which allows organizations to understand potential financial outcomes from rigorously evaluated loss event scenarios. Understanding the point at which a loss event will exceed the organization's risk threshold or capacity to sustain those losses would put decision-makers in a better position to make well-informed decisions and make more impactful investments to mitigate cyber risk.

ABOUT PROTIVITI

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 75 offices in over 20 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.

Protiviti is a leader in applying FAIR methods to quantifying cybersecurity and other risks. The firm works closely with regulators around the world and understands what they're looking for. We educate organizations about the applications, benefits and best practices around FAIR and deliver programs, strategy, and processes required to shift from a controls orientation of cybersecurity to a business risk orientation and optimize compliance frameworks based on risks. We assist organizations in building cybersecurity datamarts to collect, process and store relevant metrics for analysis and reporting and to manage overall organizational change surrounding transition to a FAIR approach, including training, workshops and socialization exercises to support the organizational change required to adopt cyber risk quantification.

CONTACTS

Ron Lefferts
Managing Director, Global Leader of Technology Consulting
+1.212.603.8317
ron.lefferts@protiviti.com

Andrew Retrum
Managing Director, Security & Privacy
+1.312.476.6353
andrew.retrum@protiviti.com

Curt Dalton
Managing Director, Global Leader of Security & Privacy
+1.617.330.4801
curt.dalton@protiviti.com

Vince Dasta
Associate Director, Security & Privacy
+1.312.476.6383
vince.dasta@protiviti.com

THE AMERICAS

UNITED STATES
Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Denver
Fort Lauderdale
Houston
Kansas City
Los Angeles
Milwaukee
Minneapolis
New York
Orlando
Philadelphia
Phoenix
Pittsburgh
Portland
Richmond
Sacramento
Salt Lake City
San Francisco
San Jose
Seattle
Stamford
St. Louis
Tampa
Washington, D.C.
Winchester
Woodbridge

ARGENTINA*
Buenos Aires

BRAZIL*
Rio de Janeiro
Sao Paulo

CANADA
Kitchener-Waterloo
Toronto

CHILE*
Santiago

COLOMBIA*
Bogota

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE, MIDDLE EAST & AFRICA

FRANCE
Paris

GERMANY
Frankfurt
Munich

ITALY
Milan
Rome
Turin

NETHERLANDS
Amsterdam

SWITZERLAND
Zurich

UNITED KINGDOM
Birmingham
Bristol
Leeds
London
Manchester
Milton Keynes
Swindon

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

EGYPT*
Cairo

SOUTH AFRICA *
Durban
Johannesburg

ASIA-PACIFIC

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*
Bengaluru
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

*MEMBER FIRM

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. PRO-1119-103143