protiviti®
Face the Future with Confidence

Sharpening the Focus on Cybersecurity: Insights From Active Directors

Below is the full summary, including key takeaways, of a discussion amongst active directors facilitated by Protiviti during a dinner roundtable at a December 2018 National Association of Corporate Directors (NACD) event. An abbreviated summary of this roundtable is provided in Issue 113 of Board Perspectives: Risk Oversight *(available at* **www.protiviti.com/US-en/insights/bpro113**) and *on NACD/BoardTalk (see blog at* **https://blog.nacdonline.org/posts/sharpening-cybersecurity-acumen**.

Much has been written, and important insights shared, on cybersecurity. The threat landscape continues to evolve, and the topic remains significant in the boardroom. But is there anything new to talk about?

To gain fresh perspectives on cybersecurity, an important area of board oversight, Protiviti met with 20 active directors to discuss their experiences. Below are some of the important points, including key takeaways, which were covered during that discussion.

Don't Let Overinvesting in Protection and Detection Lead to Underinvesting in Response and Recovery

Effective cybersecurity begins with *protection*, followed by *detection*, *identification*, *response* and *recovery*. Using these five cybersecurity pillars, as defined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework,[1] Protiviti sponsored and helped produce a global cybersecurity study in which executives were asked to rate their company's progress across these pillars.[2] The survey results indicated that most companies score highest on protection and

[1] The NIST Cybersecurity Framework offers computer security guidance for private sector organisations in the United States to use when assessing and improving their ability to prevent, detect and respond to cyber attacks. It is available at www.nist.gov/cyberframework.

[2] *The Cybersecurity Imperative: Managing Cyber Risks in a World of Rapid Digital Change* is a research report from a joint effort of ESI ThoughtLab, WSJ Pro Cybersecurity, Protiviti and a group of prominent organisations to conduct rigorous global research and analysis involving a survey of 1,300 global executives across multiple industries, advisory meetings and interviews with leading experts and practitioners, and analytical tools to benchmark approaches and assess performance impacts. The research is available at http://go.dowjones.com/cybersecurity-imperative.

detection and lowest on identification, response and recovery. As most cybersecurity investments address the protection pillar, the participating directors agreed that their organisations need a balanced programme to detect and respond to the inevitable cyber attacks. However, most of the board members report that they only see an overall cybersecurity budget; the company's investments across the five NIST domains are not transparent to them.

One board member spoke of a maturity assessment using the NIST framework and of monitoring of progress across the five domains to improve them to the desired maturity levels. The board reviewed management's assessment of each of these five areas, then evaluated the company's plan to improve them. With milestones set and a detailed plan developed, it was evident to the board that progress had to be reassessed continuously, with the intention of achieving the appropriate level of quality and protection relative to the cost incurred. In this respect, risk-based perspectives are very important. An organisation conceivably could spend millions of dollars to address one small area of the business, which would neither be cost-effective nor achievable in terms of meeting an unrealistic objective to maximise the security of that area. The point is that the five domains contributed to this assessment.

A shift is occurring in the nature and type of attacks companies experience. So-called identities, or certain personal information, are losing value on the black market. Credit monitoring, credit card alerts enabling card information to be frozen or closed instantly, and other measures are devaluing this information. That's a good thing. What is on the rise, however, is ransomware and intentional disruption that can shut a system or organisation down entirely until a ransom is paid. While protection and detection are crucial parts of a balanced programme, attackers often evade detection for long periods, allowing them to do more damage. These safeguards will not completely prevent hackers from breaking in. Accordingly, companies would be wise to focus more on response and recovery.

The bottom line is that attacks will happen. Today's cybersecurity measures are more about response than anything else. The organisation may have a recovery plan, but that does not necessarily mean the plan enables a timely recovery. One example raised by a board member was a ransomware shutdown that required the company to access backups stored on tape drives to restore the system. It worked as planned, but the effort took more than two weeks to complete. This experience underscores the point that important cybersecurity areas like recovery continue to be overlooked.

> **Key Takeaway:** Overall, it is important for organisations to move beyond the protection pillar when it comes to cybersecurity. The board should work with management to assess and monitor regularly the organisation's ability to identify, detect, respond to and recover from a cyber breach, as well as ensure that appropriate investment is supporting each pillar. One recommended and beneficial step is to conduct scenarios of cyber attacks that might occur and review the results. The outcomes can be enlightening when evaluating cybersecurity response and recovery capabilities.

Understand the Paradox in Breach Detections Between Cyber "Leaders" and "Beginners"

Protiviti's research differentiates the maturity of cybersecurity capabilities amongst leaders, intermediates and beginners. Digital maturity is related to cybersecurity maturity, as they often go hand in hand. For example, according to the research, nearly 68 percent of digital beginners are also cybersecurity beginners and only 3 percent are cybersecurity leaders. Unsurprisingly, 46 percent of digital leaders are also cybersecurity leaders and only 6 percent of digital leaders are cybersecurity beginners. However, over half of digital leaders are not cybersecurity leaders, leaving them more vulnerable to cyber attacks because of their higher reliance on digital platforms.[3]

There is a "digital paradox" in business, and our research finds that digital leaders report more cyber attacks than beginners.[4] The roundtable discussion revealed several reasons for this:

1. Digital leaders likely are better at monitoring security activity and have stronger detection measures. Thus, they are more aware of attacks and breaches than other organisations that may be experiencing similar levels of attacks but are unaware of them.
2. Digital leaders are more likely to have an expanded attack surface, as they are leveraging, for various purposes, the Internet of Things, mobile platforms and other technologies with generally immature security.
3. There is greater complacency with greater connectivity, meaning that with greater connectivity comes greater security vulnerabilities. Younger generations with connected lives have become accustomed to this connectivity but may be somewhat blind to the related cyber and privacy risks.

The good news for digital leaders is that advanced technologies, such as artificial intelligence, machine learning and natural language processing, promise to enhance an organisation's cybersecurity capabilities. However, hackers and bad actors are leveraging these same technologies as well.

> **Key Takeaway:** Organisations need to stay focused and keep cybersecurity a critical priority as they advance their digital maturity. To minimise their risks, companies should build cybersecurity into each step along their digital transformation process.

[3] Ibid.
[4] Ibid.

Manage the "Cybersecurity Squeeze" on Innovation Funding

How does the board effectively address cyber risk without throttling innovation? This important question is a double-edged sword, as innovating creates more cyber risk because it almost always involves embracing new digital technologies. Cybersecurity presents a serious cost-benefit issue for management to consider. The organisation conceivably could spend an endless amount of money on cybersecurity if it wanted to, but this is not realistic. So, this discussion begins with the notion that cybersecurity must be cost-effective.

Agile and DevOps approaches, which an increasing number of organisations pursuing innovative products, services and operating practices are employing, move faster and frequently result in cybersecurity gaps. Agile focuses on collaboration, customer feedback and small, rapid releases, whereas DevOps brings development and operations teams together. Companies that use these approaches to achieve speed to market and sacrifice security may have cheaper products but will be at significant risk of major breaches and the attendant exposure to brand damage. It is therefore imperative for cybersecurity risk to be addressed early in the innovation process.

The roundtable discussion participants emphasised that innovation is about business strategy and should not be an IT or "innovation" budget item. Rather, it should be part of an overall budget for the enterprise's growth strategy. Ideally, these needs are addressed through different budgets so that IT and innovation teams are not competing for funding from a perceived single budget pool.

Also, risk and cybersecurity should be embedded into the design and developmental approach used by innovation teams, so that innovation is undertaken securely. Otherwise, much costlier and time-intensive retroactive work will be necessary to address security issues. Also, as part of innovation initiatives, it is important to involve the right people early, including cybersecurity, fraud and internal audit experts.

> **Key Takeaway:** As an organisation innovates, it must pursue secure innovation. Agile innovation and related processes must incorporate appropriate security designs.

Mind the Enemy Within

User error remains a consistent and persistent threat. In our study, most respondents expressed concerns about untrained company insiders and how easily they can be foiled. Human error is a significant challenge. Think about inadvertent or mistaken password disclosure, personally identifiable information being saved to a thumb drive, and the ever-increasing sophistication of social engineering to obtain the data needed to breach a target's systems. Also, there is the specific threat of attacks made by internal people, especially disgruntled employees.

As noted by several directors, there are solutions to help combat internal threats, but the board is typically not aware of how effective they are. Exposure to attacks by nation-states and sophisticated external attackers is compounded in that these groups often exploit untrained insiders.

Key Takeaway: According to Protiviti's research, nearly all firms (87 percent) see untrained general staff as the greatest cyber risk to their business because they may provide a conduit for outside attackers.[5] The directors agreed that boards need to turn up the volume on their inquiries of cybersecurity management as to what is being done about insider risk, including exposure to third parties. One tried-and-true, not to mention low-cost, cybersecurity measure — at least for insiders — remains employee training and communication.

Know How Much — Quantify Cyber Risk to Put a Value on the "Crown Jewels"

Organisations must understand what data and information they need to protect (e.g., know your "crown jewels"). But it has been well-documented that not all data is created equal. How can board members satisfy themselves that management understands and distinguishes the different types of data and information systems the organisation is creating and managing and the business outcomes the organisation must address?

For example, a key question to answer is, "Do we understand the *unfavourable business outcome* that would result from the loss of certain data?" Can the organisation quantify that risk? Quantification will help management and the board significantly as they work to understand the different types of data and systems assets the organisation maintains. More importantly, it will help them understand what needs to be protected most and oversee how asset protection is being prioritised. The Factor Analysis of Information Risk (FAIR) methodology[6] can assist with this analysis, as it employs risk quantification software to analyse risk using techniques such as the Monte Carlo method, which simulates risk scenarios. Also, data loss prevention software enables identifying where sensitive data is stored and transmitted, including the volume of that data, and detecting possible security breaches. Quantitative analysis is then required to put a business value to that data. The software continues to be refined and eventually may offer better control over data and its security.

Key Takeaway: Conducting a quantitative risk analysis forces IT and security teams to set risk appetite thresholds, which enhances cybersecurity communications with the board. Qualitative risk maps, numerical rating scales and other similar tools may be useful in fostering risk awareness and prioritisation. However, risk management, including risk-based decisions, is enhanced if risk is quantified in financial terms.

[5] Ibid.

[6] The Factor Analysis of Information Risk (FAIR) is an international standard quantitative model for understanding, analysing and quantifying information risk in financial terms. FAIR uses an enterprisewide portfolio approach to analyse and aggregate potential loss events and vulnerabilities based on their likely frequency and magnitude. See www.fairinstitute.org/what-is-fair.

Increase the Board's Confidence in Its Cybersecurity Oversight

How can boards increase their confidence enough to oversee cybersecurity threats and management's countermeasures? Although directors may not have direct knowledge of the cyber threat landscape, they can take steps to sharpen their oversight in this area. The NACD's Cyber-Risk Oversight Resource Center offers relevant questions for assessing the board's cybersecurity literacy.[7] If the board could benefit from more IT and security expertise, there may be a need for a technology expert, either a director on the board or an objective party advising the board. The NACD's resource center also offers questions for discussing with management the company's cybersecurity situational awareness, strategy and operations, and incident response, and inquiring of management following discovery of a cyber breach.

The key is to position the board to gain more clarity around the company's cybersecurity by asking direct questions regarding its oversight preparedness and management's cybersecurity capabilities. These questions should be directed to, amongst others, the chief financial officer (CFO), the chief information officer (CIO) and/or the chief technology officer (CTO), and leaders in the security function.

In addition, one director noted that the board has four independent resources it can use to enhance its understanding and assessment of the effectiveness of cybersecurity measures and the overall health of IT security — Payment Card Industry Data Security Standard (PCI DSS) compliance assessments (to the extent applicable), ISO 27001 certifications, internal audit cybersecurity assessments, and the use of outside consultants to evaluate specific areas and provide independent assessments and analysis. Consultants may include "white hat" hackers and penetration testers hired to attack the organisation, report on the company's vulnerabilities and make recommendations to address them. These reports offer board members an opportunity to ask pointed questions.

Cybersecurity reporting can also enhance the board's confidence level. If cyber risk is measured quantitatively and risk thresholds are established, directors can then ask for metrics to be provided periodically depicting the health of the security programme. Such metrics might include the following: how many incidents (e.g., breaches, protocol violations and near misses) are detected every quarter, how many high-risk third parties have not been assessed or have outstanding issues, the number of patches exceeding agreed-upon patch time frames, the length of time it takes to respond to a breach, and the length of time it takes to remediate audit findings. The board can use these and other metrics as a barometer and look for changes that signal a need to dig deeper. Management can then determine the budgets appropriate to secure the organisation from cyber attacks and breaches.

Metrics can be presented through a focused dashboard addressing the organisation's major cyber threats and highest-risk third parties and how well they are being managed. Protiviti's research

[7] This resource center is at www.nacdonline.org/insights/resource_center.cfm?ItemNumber=20789 and is available to NACD members. It is a repository for all NACD content, services and events related to cybersecurity oversight and includes practical guidance, tools and analyses tailored to the full board, relevant committees and individual directors.

indicates that organisations that perform quantitative risk analysis excel in all cybersecurity categories — time to detect incidents, number of incidents, time to patch and so on. One of NACD's publications on cyber risk oversight includes examples of cyber risk reporting metrics and dashboards.[8]

One director noted that many boards do not receive third-party risk reports from management. The board needs to have a better understanding of the organisation's data to which third parties have access and how these third parties are using, managing and protecting that data. That need applies to fourth parties as well (i.e., a vendor's vendors). The organisation itself can suffer reputational damage in the event of a cyber attack or breach to any of its third or fourth parties.

In addition to asking appropriate questions, leveraging independent sources of assurance and receiving focused dashboards, the board should clarify expectations with management, particularly concerning cyber threats and incidents that can affect the company's reputation and standing with customers, regulators and investors. During the roundtable conversation, reference was made to a blog written by a director asserting that the levers for creating value in an organisation offer a framework for setting management expectations in the cybersecurity space — strategy, structure (including information flows and decision rights), culture (including values and behaviours), metrics and incentives, business processes and information technology, leadership, and skills and competencies.[9]

Application of these levers can bring clarity to the board's cyber risk oversight. The first three lay out the board's expectations (and, incidentally, should be incorporated into the company's risk appetite statement), and the last four set the bar for accountability. The point is, how can the board be sure that the CIO or chief information security officer (CISO) won't get conflicted about certain priorities as the executive weighs competing demands and metrics and, as a result, loses sight of the forest for the trees? And how can directors satisfy themselves that the chief executive officer (CEO) won't fail to set the right tone for resolving these conflicts with clarity?

For example, if a company's brand promise — implicit or explicit — is that it can be entrusted with sensitive consumer information, should the board use the first three levers — strategy, structure and culture — to set expectations with the CEO and senior leadership team? Should directors make it clear that the strategic value of individual consumer information is such that, effectively, the company needs to adopt a "zero defects" approach to keeping that information safe? Should they also make it clear that this imperative is a top priority of every single employee, consistent with the behaviours associated with an organisation committed to a zero defects philosophy? Such expectations should be articulated up front, so the board is not at risk of becoming involved too late after the fact.[10]

[8] See Appendices E and F, *NACD Director's Handbook Series on Cyber-Risk Oversight*, 2017, available for purchase at www.nacdonline.org/Store/ProductDetail.cfm?ItemNumber=10687.

[9] "Where's the Board? Questions for Equifax," Gary Cook, Harvard Law School Forum on Corporate Governance and Financial Regulation, October 24, 2017, available at https://corpgov.law.harvard.edu/2017/10/24/wheres-the-board-questions-for-equifax/.

[10] Ibid.

As one director noted, the management team should understand cybersecurity risks in the same way it understands the overall competitive landscape. CEOs typically know or want to know the organisation's top five competitors; however, do they know the organisation's top five cybersecurity adversaries? This knowledge presents a challenge to obtain, as the list of the most dangerous hackers and attackers changes regularly. That said, management would be well-served to keep as close an eye on these threats as it does on the company's competitors.

> **Key Takeaway:** Cyber threats represent a legitimate concern. A company's reputation that has been established and nurtured for 100 years can suffer severe and lasting damage following just one high-profile cyber attack. As a result, it can be difficult for boards to feel fully confident in how they are monitoring and keeping tabs on cybersecurity risk, both within the organisation and amongst third parties. Ultimately, directors must rely on management for this information but should be proactive in refreshing the board's oversight capabilities, asking appropriate questions, receiving independent assurances, monitoring focused dashboards, and setting clear expectations regarding the need to preserve reputation and brand image.

Take Stock of a Changing Cyber Threat Landscape

Throughout the roundtable discussion, numerous comments were made regarding the changing cyber threat landscape and the importance of staying informed as it evolves. For example:

- Ransomware is now a critical issue on the minds of board members. Organisations can protect against these attacks through regular backups. But ransomware campaigns still present significant threats, especially if they result in a system shutdown or an inability to interact with clients and/or customers.
- Today, it is not just about protecting credit card data; rather, the focus should be on any information that might be of value to hackers or third parties (e.g., medical records, intellectual property [IP] and customer files). Accordingly, the organisation must understand its data as well as the exposure created from having it. Boards should be inquisitive about possible data targets.
- One of the biggest cyber risks for an organisation could involve mobile devices, especially those with software not approved by the organisation.
- Third-party threats loom large and warrant more attention, as discussed earlier.

The above issues are company-specific examples raised during the discussion. Another significant concern for board members is also a legitimate and serious national security issue: the threat of state-sponsored cyber attacks. These perpetrators have unlimited resources, and a growing number of their attacks are directed at specific companies.

Some believe we are not doing enough as a nation to combat cyber attacks from China, Iran, North Korea, Russia and other nations at odds with the United States, and that the threats to our national infrastructure — energy, utilities, water and more — have a potentially devastating impact if realised and thus supersede threats at the corporate level. Threats to our national power grid and other key infrastructure raise serious concerns about how companies would be affected if they were attacked or shut down. Some organisations believe a major attack is yet to come, either in the financial services industry, which is a prime target for many reasons, or elsewhere.

Regarding this issue, the organisation, specifically the CISO, should have a relationship with the Federal Bureau of Investigation (FBI). Of note, the FBI has stated it wants companies to reach out to them with information about attacks they have experienced, which can help the FBI's investigative efforts and, by extension, the overall national security. The FBI is looking for partnerships and cooperation between the public and private sectors.

However, many believe that such partnerships and disclosures present a bit of a Catch-22 for companies. Many are reluctant to disclose information about cyber attacks or breaches, as the FBI has requested, because companies could then face penalties from other parts of the public sector — for example, prosecution by the U.S. Department of Justice or fines from the U.S. Securities and Exchange Commission. The NACD has proposed safe harbour for companies disclosing attacks without penalty or prosecution. Progress with respect to securing safe harbour, however, is unlikely to be made in the near term.

An information sharing and analysis center (ISAC)[11] can be beneficial for obtaining insights regarding computer security threats and is an example of cooperation and two-way sharing of information between the private and public sectors. It is good for the entire industry in which the organisation operates and can help reduce the overall industry's profile as a target. That involves industry information-sharing, which helps everyone. While leveraging insights from an ISAC is highly recommended, a challenge for an ISAC is the restraint on sharing due to concerns over disclosing confidential and sensitive information.

> **Key Takeaway:** Regarding strong cybersecurity measures, some organisations are "later to the game" than others. For example, consumer packaged goods companies have been slow to address cyber threats, as they typically do not harbour customers' personal data or credit card information. But the game has now changed. Virtually any organisation is susceptible to cyber attack. Hackers now pursue far more than credit card numbers. In fact, considering that ransomware is essentially a moneymaking activity for hackers, any organisation is a target.

[11] As attacker resources and sophistication have increased over time, regulators and various government agencies in the United States have formed an information sharing and analysis center (ISAC) for multiple industries. An ISAC is a nonprofit organisation that provides a central resource for gathering and sharing information on cyber threats to critical infrastructure.

Questions for Boards

The following are some suggested questions that boards of directors may consider, based on the risks inherent in the entity's operations:

- Is the company a possible nation-state target based on what it represents, what it does or the value of its IP? If so, does the company have the advanced detection and response capabilities it needs? Given the increasing sophistication of threat actors, are simulations of likely attack activity performed periodically to ensure defences can detect a breach and respond in a timely manner?
- Does the board define its expectations for management regarding cybersecurity and establish clear accountabilities for results? If the organisation has a risk appetite statement, are the board's expectations for cybersecurity incorporated therein?
- Is the board satisfied with the reporting and metrics used by management for cybersecurity matters? Do the metrics used provide supporting key performance and risk indicators as to how top-priority cyber risks are managed and address areas that inform the board's oversight? Are the metrics refined over time to provide added insights as threats change?
- Is the board satisfied that there is an effective response and recovery plan? Is the plan evaluated through tabletop exercises, tested periodically and adjusted as necessary?
- Is the IT budget separated from the funding supporting the innovation needed to support the growth strategy? If not, is the spend on operational risk proportionate and focused on protecting what's important (the "crown jewels"), keeping up with the cyber threat landscape to identify the kinds of attacks that are most likely to occur, and being proactive about incident response so that systems can be put back online with minimum impact to the business?
- How alert is the organisation regarding patches? Is the organisation up to date with them? If cost-cutting efforts are underway across the organisation, is care taken to ensure they do not affect the frequency and/or timeliness with which patches are applied?

How Protiviti Can Help

Protiviti works with organisations to focus on foundational information security questions:

- Do we know what we need to protect (e.g., the data and information systems assets that are most important — the "crown jewels"), and where those assets are located? Concerning these assets:
  - Are we properly caring for them? How do we know?
  - Who are we protecting them from, to whom should we permit access, and how can we tell the difference?
  - Are our defences effective? Are they working as intended?
  - How will we know if things are not working as we planned?
- Are we able to recognise a new threat to our environment and detect likely attack techniques on a timely basis and align our protection measures to meet the threat?
- Are we ready to respond if something bad were to happen? Are we capable of managing such incidents? And when incidents occur, are we able to keep them from happening again?

Protiviti provides a wide variety of security and privacy assessment, architecture, transformation, and management services to help organisations identify and address security and privacy exposures (e.g., loss of customer data, loss of revenue or reputation impairment) before they become problems. Working with companies in all industries, we evaluate the maturity of their information security programmes and the efficacy of their controls — and help them design and build improvements when needed. We have a demonstrated track record of helping companies react to security incidents, establish proactive security programmes, deal with identity and access management, and handle industry-specific data security and privacy issues. Our experience and dedication to developing world-class incident responses have resulted in deep expertise in security strategies, response execution, forensic analysis and response plan development.

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 its 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 70 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.

Contacts

United Kingdom

Roland Carandang
Managing Director
London
+44.20.7389.0443
roland.carandang@protiviti.co.uk

Thomas Lemon
Managing Director
London
+44.20.7024.7526
thomas.lemon@protiviti.co.uk

United States

Cal Slemp
Managing Director
Security and Privacy Program and Policy Services Segment Lead
New York City
+1.203.905.2926
cal.slemp@protiviti.com

Scott Laliberte
Managing Director
Global Leader of Security and Privacy
Philadelphia
+1.267.256.8825
scott.laliberte@protiviti.com

Michael Ebert
Managing Director
Healthcare Industry Cyber Lead
Philadelphia
+1.267.234.9735
michael.ebert@protiviti.com

Andrew Retrum
Managing Director
Financial Services Industry Cyber Lead
Chicago
+1.312.476.6353
andrew.retrum@protiviti.com

Jeffrey Sanchez
Managing Director
Data Security and Privacy Segment Lead
Los Angeles
+1.213.327.1433
jeffrey.sanchez@protiviti.com

David Taylor
Managing Director
Response and Recovery Segment Lead
Orlando
+1.407.849.3916
david.taylor@protiviti.com

Michael Walter
Managing Director
Cyber Intelligence and Response Center Lead
Atlanta
+1.303-898-9145
michael.walter@protiviti.com

Australia

David Adamson
Managing Director
Sydney
+61.2.8220.9500
david.adamson@protiviti.com.au

China and Hong Kong

Michael Pang
Managing Director
Hong Kong
+852.2238.0438
michael.pang@protiviti.com

Germany

Kai-Uwe Ruhse
Managing Director
Frankfurt
+49.699.6376.8148
kai-uwe.ruhse@protiviti.de

Italy

Enrico Ferretti
Managing Director
Rome
+39.346.7981427
enrico.ferretti@protiviti.it

Japan

Fumihito Fujiwara
Managing Director
Tokyo
+81.70.6962.9797
fumihito.fujiwara@protiviti.jp

Masato Maki
Managing Director
Tokyo
+81.80.1177.3674
masato.maki@protiviti.jp

protiviti®