A Special Report by the

Security for Business Innovation Council

INFORMATION SECURITY SHAKE-UP:

Disruptive Innovations to Test Security's Mettle in 2013

FEATURING THE PERSPECTIVES OF C-LEVEL SECURITY EXECUTIVES FROM:

ABN Amro	Coca-Cola	Fidelity Investments	Johnson & Johnson	TELUS
ADP, Inc.	eBay	Intel	JPMorgan Chase	T-Mobile USA
Airtel	EMC	HDFC Bank	Nokia	Walmart
AstraZeneca	FedEx	HSBC Holdings plc.	SAP AG	

An industry initiative sponsored by RSA

Contents

Report Highlights

IN 2013, A CLUSTER OF disruptive innovations will continue transforming enterprise IT and hammering at the very foundations of information-security strategies

THIS YEAR PROMISES SEVERAL major developments in enterprise adoption of:

- **Cloud computing:** Many organizations are preparing to move more business processes – even mission-critical apps and regulated data – to the cloud.
- **Social media:** Based on social media's new-found powers to influence consumer purchasing behavior, many organizations are elevating it to a strategic endeavor.
- **Big data:** Evidence of competitive advantage is compelling more organizations to begin big data projects to gain market and business intelligence.
- **Mobile devices:** Organizations are experiencing a surge of consumer mobile devices accessing corporate networks and storing corporate data.

THESE TRENDS WILL HAVE A big impact on information-security programs, revealing significant and growing gaps including a lack of business skills, relationships, supply chain management, and tech-savvy action plans.

THE GAPS MUST BE ADDRESSED in order for information-security teams to keep pace with their organizations' technology aspirations.

BOOST RISK & BUSINESS SKILLS: Information-security teams have long lobbied to be perceived as business enablers not inhibitors. Now that many are, they don't have the right skills. To meet the swelling demands to enable innovation, security teams must rapidly attain risk management and business skills.

COURT MIDDLE MANAGEMENT: At most organizations, the C-suite "gets it" but security teams now face resistance from middle managers who don't want to expend their resources on security. Security teams must build these relationships, helping middle managers to understand security's value.

TACKLE IT SUPPLY CHAIN ISSUES: Organizations are accelerating the implementation of new technologies just as there is growing concern about the integrity of globally sourced IT components. Comprehensive programs are required to evaluate as well as demonstrate trustworthiness of hardware and software.

BUILD TECH-SAVVY ACTION PLANS: Security teams must build specific competencies and action plans for enabling these innovations:

For cloud computing focus on:

- optimizing cloud vendor management
- solving controls assurance
- realigning the IT budget to cover the costs of cloud security
- sharpening technical proficiency in virtualized environments

For social media focus on:

- working with a multidisciplinary executive team to develop policy and codes of conduct
- developing proactive incident response plans
- training end users
- monitoring social media channels

For big data focus on:

- understanding the complex security issues created by amalgamating and processing huge volumes of customer, market or business data
- getting in on the ground floor of big data projects
- ensuring access control governance
- developing a plan to leverage big data technologies for better threat detection

For mobile devices:

- Download the recent comprehensive report from the SBIC, *Realizing the Mobile Enterprise: Balancing the Risks and Rewards of Consumer Devices.*

1 2013 Promises a Fast and Bumpy Ride

In 2013, a cluster of disruptive innovations – cloud computing, social media, big data, and mobile devices – will continue transforming information systems. Conventional approaches to information security – such as perimeter protections, managed end-points, signature-based threat detection, and checklist risk evaluations – are breaking down. As the speed of technological advances continues to outpace information security, several major developments in enterprise technology adoption are exposing significant and growing gaps in information-security programs.

Based on the perspectives of 19 security leaders from global enterprises, the Security for Business Innovation Council (SBIC) has developed this Special Report to help navigate the shifting landscape. The report delivers specific guidance to fill the gaps and ensure that information-security teams have the "right stuff" in order to enable innovation over the next 12 months.

> *Information security isn't just about IT anymore. Trends like cloud computing and consumerization are quickly extending the information-security role. It's about business. It's about people. It's about risk management."*
>
> **DR. MARTIJN DEKKER**
> Senior Vice President, Chief Information Security Officer, ABN Amro

2 Technology Trends and the Impact on Information Security

Enterprises are looking to up the ante in technology adoption this year. Information-security teams should know what to expect and how they will be impacted.

1. Cloud Computing Adoption

Trend: Many organizations are preparing to move more business processes – even mission-critical apps and regulated data – to the cloud.

Familiarity Breeds Trust

By now, most companies have deployed some form of cloud computing, including Software-as-a-Service (82% of companies), Infrastructure-as-a-Service (51% of companies), and Platform-as-a-Service (40% of companies),[1] to capture benefits such as cost savings, agility, and scalability. Over the next few years, spending on public cloud services is predicted to increase at 19% per year.[2]

Although supplier lock-in and system availability are some of the big concerns with the cloud, security remains the number one obstacle to adoption. But trust in the cloud is growing. In a recent survey, 50% of respondents were confident that the cloud is now viable for mission-critical business applications.[3] Even regulators are getting more comfortable with the cloud. The Dutch banking authority has given Dutch banks the green light to use cloud services.[4] Given this confidence, many organizations are ready to move more business processes to the cloud. But surprisingly, only 30% of organizations have implemented a cloud security strategy[5] even though cloud computing has been a growing phenomenon for years. And even many cloud vendors don't have sufficient security programs.

Impact: The security concerns hindering cloud adoption will come to a head. The increasing demand for cloud computing will force organizations to find effective ways to evaluate their providers' security controls to ensure they meet requirements, including implementing continuous monitoring.

2. Social Media Adoption

Trend: Social media has become a major influencer of consumer purchasing decisions, setting it on course to become a strategic endeavor.

Serious Business

Organizations will be looking at social media with a more strategic eye in 2013. A recent survey indicates brand following has doubled in the past two years by Americans who use social media. And of those who use social networking sites at least once a month, 47% say that Facebook has the most influence on purchasing.[6]

The opportunities to reach customers and create positive brand awareness with social media are huge. The problem is that social networking sites also present enormous opportunities for misuse and misinformation as well as malware distribution and fraud. In fact, 66% of organizations name social media as a significant or critical risk to their brand.[7] Yet only 38% of organizations have a security strategy in place for social networking.[8]

As organizations increase their use of social media to capture the business benefits, they must also put in place strategies to manage the risks. Expectations should be set regarding allowable activity on social sites and policy viewed broadly, balancing corporate interests with freedom of expression. Tools and techniques will also be required to mitigate the risks of incidents and guard against social-media-based attacks.

Impact: Information-security teams must work to actively manage the risks of social media, including comprehensive policies and effective security controls.

1 *Future of cloud computing survey*, North Bridge Venture Partners, June 2012
2 *Gartner: Public cloud spending to increase 19 percent annually to 2016*, FierceEnterprise Communications, October 23, 2012
3 *Future of cloud computing survey*, North Bridge Venture Partners, June 2012
4 *DNB neemt hobbel weg voor 'outsourcen in the cloud'*, Nieuwsbericht, De Nederlandsche Bank NV, (DNB), November 6, 2012
5 *The Global State of Information Security® Survey 2013*, a worldwide survey by CIO, CSO and PwC, October 2012
6 *The Social Habit*, Edison Research, July 2012
7 *Guarding the Social Gates: The Imperative for Social Media Risk Management*, Altimeter, August 2012
8 *The Global State of Information Security® Survey 2013*, a worldwide survey by CIO, CSO and PwC, October 2012

3. Big Data Adoption

Trend: Evidence of competitive advantage is compelling more organizations to begin big data projects to gain market and business intelligence.

Better Threat Detection

In the information-security community, "big data" is generating considerable hype. The power of analytics can greatly improve the ability to detect cyber attacks. Big data can be used to spot malicious activity by amalgamating and analyzing system and user behavior data. It will play a major role in changing the information-security model to be more effective.

Good for Business

It's not only security that is excited about big data. So are marketing departments and many other areas of business. Big data can be used to gain deep market insight, provide tailored customer service, and create operational intelligence. A survey of executives worldwide found that the use of big data has improved their businesses' performance, on average by 26%. The majority of these companies (58%) claim they will make a bigger investment in big data over the next three years.[9] This evidence of competitive advantage will spur more organizations to invest in big data. But the relative newness of the space means most do not fully understand the privacy and security risks when customer and business information is being collected, combined, processed, and stored at unprecedented scales and speeds.

Impact: Information-security teams must recognize the value of big data for security and develop a multi-year plan to evolve their security management model to utilize big data to detect and remediate security threats. They also must get in on the ground floor of any new big data projects that the business takes on, in order to understand the risks and develop strategies to manage them.

"When thinking about big data, information-security teams should not only consider how they can use powerful analytics to detect security events but also realize that business overall is shifting towards the use of big data. Securing big data will require an evolution in data protection controls."

DAVE MARTIN
Vice President and Chief Security Officer, EMC Corporation

4. Mobile Devices Adoption

Trend: More employees are using their smartphones and tablets for work, creating a surge of consumer mobile devices accessing corporate networks and storing corporate data. Organizations have to prepare for a world where the dominant endpoint is not a desktop PC, but a mobile device.

Risks Mounting

Heading into 2013, consumer mobile devices continue to create worrisome risks for organizations – ranging from loss of confidential information to high-profile security breaches. Research shows that 70% of all smartphone-owning professionals are now using their personal devices to access corporate data, yet almost 80% of that activity remains inadequately managed by IT departments.[10] The potential benefits of mobile devices can include improved productivity and reduced costs. Capitalizing on these opportunities is only possible if enterprises know how to manage the risks.

Impact: Mobile risks are reaching a critical mass. To avert major incidents, information-security teams must implement strategies that manage the risks while enabling the rewards. Security strategies should assume the end-point is untrusted.

9 *The Deciding Factor: Big Data & Decision Making*, Capgemini, June 2012
10 *Multi-market BYOD Survey*, Ovum, September 2012

3 Addressing the Gaps

In 2013, as enterprise adoption of technology intensifies, information-security teams face significant gaps, including a lack of business skills, relationships, supply chain management, and tech-savvy action plans. Addressing these gaps will take a commitment to rapid-fire change.

Boost Risk and Business Skills

As the need to protect information has become increasingly vital, at most global organizations the information-security role has become more strategic and is transitioning to an "information risk management" role. Enabling a set of disruptive innovations is accelerating that trend, forcing a risk management perspective versus a security "lock-down" mentality. To capture the business benefits of new technologies, each organization must accurately evaluate how much risk it is willing to take on to capture those benefits. The information-security team must work with the business in order to understand the risks and develop protection strategies to mitigate them to an acceptable level. This includes identifying the key information assets and assessing their value to the organization.

For years, security professionals have been lobbying to be perceived as business enablers rather than inhibitors. Now many information-security teams are bombarded with requests to enable innovation. But as information security migrates from being an IT-focused to a business-focused problem, many teams lack the required skillset. Security professionals must become risk managers and business consultants – translating business requirements into security requirements. More and more, the performance of security teams will be measured on their ability to enable business, which requires knowing how to tie security programs to business outcomes.

Court Middle Management

As we begin 2013, most C-suites and Boards "get it." The growth of information protection regulations and the escalation of cyber threats mean that most of them understand the importance of information security and consider it a priority. Today, it is common for CISOs to meet regularly with executive leadership and the Board. In many cases, information security has attained the sought-after attention from the top.

The current resistance to information-security efforts is two levels down from the executive level. Middle managers don't want to use their resources on security. They are incentivized by timeline and budget; adding security doesn't fit into their objectives. Security teams need to build relationships with middle managers, helping them understand the value of information security. It may be a harder nut to crack than the C-suite.

Tackle IT Supply Chain Issues

Organizations are accelerating the implementation of new technologies within their IT environments just as there is growing concern about the integrity of hardware and software components. Many of these components are globally sourced, creating complex supply chain issues. Going into 2013, organizations must increasingly question whether their IT supply chain can be trusted. However the approach should evolve from banning gear to a more holistic risk management approach to adopt technology with appropriate security safeguards. Organizations should seek assurances regarding all of their suppliers' technology-development and -delivery practices.

As well, most organizations not only implement IT products developed by others but also develop IT, such as custom applications for use by business partners and customers. Whether they develop commercial or custom hardware or software, organizations must be able to demonstrate that they are a trustworthy supplier of IT. Comprehensive programs will be required to evaluate and demonstrate the integrity of the entire IT supply chain, downstream and upstream.

Build Tech-Savvy Action Plans

Solving all of the security issues that disruptive innovations are creating isn't going to happen in 2013, but security teams have to make large strides or fall even further behind their organizations' plans for technology adoption. Security teams must build competencies and specific actions plans in each area.

1. Cloud Computing Competencies

Cloud Vendor Management

Organizations are ultimately accountable for safeguarding the information handled by their cloud service providers. Cloud computing is forcing information-security teams to switch their focus from implementing controls to assuring that the controls implemented by others meet requirements. Security teams need to determine "How can we ensure that cloud providers can meet our trust level? How do we know they are attuned to our particular threats? Can they meet our regulatory compliance and e-Discovery requirements?"

Controls Assurance

The conventional controls-assurance model is not sustainable in the cloud. Client organizations can't go on site to examine the security controls of every cloud service provider, so they expect the providers to provide assurance by answering questionnaires. This is an inefficient process, since the cloud providers' customers all ask the same questions.

Standardized assessments would help. Industry initiatives, to achieve large-scale sharing of assessments, have not had a lot of success so far. It's hard for a large number of organizations to agree on a standard set of controls that will satisfy everyone's requirements. Some organizations are beginning to turn to small-scale sharing of assessments. This might follow the same model as intelligence sharing whereby exchanging information among a small set of trusted individuals grows over time. Another possible approach is third-party assessments or certification of service providers, such as the AICPA's SOC 2 Report on Controls at a Service Organization or the upcoming ISO 27017 Standard for Security in Cloud Computing.

In moving to the cloud, security teams need to find effective ways to measure the health of controls and detect failures. The building blocks for attestations through governance, risk, and compliance (GRC) technology are there, but the process needs to mature. Automated and transparent controls assurance and continuous monitoring will be an important part of the solution.

Budget Realignment

The assurance process adds cost on both sides (for the cloud provider and the enterprise). Organizations should recognize that the increasing costs of assurance can reduce any cost savings from moving to the cloud in the first place. As with outsourcing, if the process is mismanaged the cost savings may be neutralized. Organizations also need to understand that in a highly virtualized environment more of IT's budget will be needed to address cloud security. One solution is budget realignment – reinvesting a portion of the IT savings the organization achieves by moving to the cloud into managing the risks.

Technical Proficiency

In order to evaluate the controls, security teams will need a high level of technical proficiency within virtualized environments. When servers and applications are decoupled from hardware, the security controls framework is completely different than in conventional IT environments. For example, software controls (such as hypervisor security modules) replace hardware controls.

Many security teams are still not convinced regarding the efficacy of cloud security controls. They need to validate the security model for themselves, understanding the advantages and limitations, in order to oversee cloud providers. Especially in public clouds, data co-mingling and data remanence remain big concerns. Security teams don't yet have an acceptable level of assurance that cloud service providers can protect data integrity and confidentiality in a multi-tenant environment. Proficiency in cloud security controls is critical not only for public/hybrid clouds but also private clouds. Security teams must have the know-how to secure virtualized environments within their own data centers.

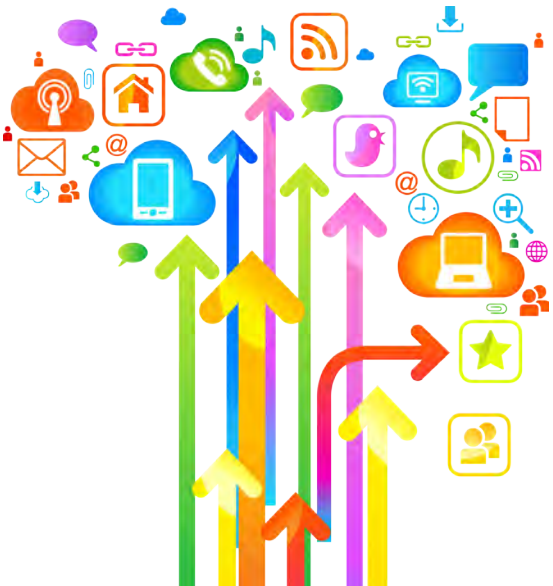
Cloud Computing Suggested Actions:

• Plan for increasing resources for cloud vendor management.	• Make it a general rule to segregate the role of controls implementation from controls assurance to ensure impartial controls oversight.	• Leverage technologies such as GRC solutions that can perform automated assurance and continuous monitoring and provide visibility into cloud environments.
• Make the case to earmark a portion of IT savings that result from moving to cloud computing for information-security oversight.	• Work with auditors in the early stages of public or private cloud computing initiatives, to educate them about the new security controls in virtualized environments.	• Ensure your team has the technical proficiency to evaluate software controls and secure the virtualized environment.
• Factor in IT savings/ security oversight offset when making decisions regarding moving to the cloud.	• Investigate the possibility of sharing cloud vendor assessments with a small number of trusted partners to reduce redundancy and costs.	• Investigate next-generation encryption solutions that can be used to protect your sensitive data in the cloud.

2. Social Media Competencies

Executive Treatment

The potential scenarios are nightmarish: insiders tweeting pre-released earnings data, developers inadvertently disclosing confidential intellectual property in peer forums, employees making inappropriate comments to customers or re-tweeting rumor as fact, hacktivists hijacking corporate officers' social networking accounts, cyber-threat agents using social sites for reconnaissance or spreading malware. The security team must carefully articulate the risks of social media to the business – including data loss, damage to reputation, regulatory issues, malware infections, and targeted spear-phishing campaigns – and design and implement controls to manage the risks.



It will require an organizational strategy, including a defined code of conduct and an incident response plan. Defining social media policy takes a cross-functional team of executives from security, IT, legal, HR, and communications. It can be a long process, taking months to set up the initial policy and requiring ongoing iterations based on learnings and the evolution of the social space. For example, users will be testing the limits/parsing definitions.

Determining areas of responsibility can be an area of tension. It's not always straightforward whether certain aspects of social media risks are security, PR, or legal matters. The policy should cover who owns what. For example, legal/compliance owns the liability issues, marketing owns sentiment management, and security owns technical monitoring solutions.

Response Plan

Traditional incident-response methods that may have worked with conventional media don't work with social media because of the extreme audience reach and speed of communications. Often, organizations are forced to think through a social-media response only when they experience a watershed event like a major outage or flash event. To avert a social media crisis, an organization needs to plan responses to various scenarios ahead of time.

End-User Behavior

End-user training specific to social media is essential. It's not just about what employees do at work but also on their personal time. Training should help them understand the policy and internalize the consequences of non-compliance, making them safer Internet citizens overall.

Organizations need to set constructive boundaries through training and technical controls – although technical controls available today lack the granularity needed. Some organizations may have a very open culture where blocking of social media channels is not a viable option. Programs can also include moderating an organization's Facebook page and monitoring employees' postings on social sites.

Threat Management

Brand monitoring on social sites is commonly used by corporations to help manage reputational issues. Customer care teams also monitor social sites to address specific customer issues before they escalate. The information-security team needs to work with the corporate marketing teams. Monitoring social media sites can also be a valuable source of threat intelligence. Social media threats (YourCompanySucks.com) are not necessarily cyber-security issues, but security should be informed of anything that points to possible cyber threats, such as hacktivist postings or discussions regarding possible targeted attacks directed at the company. Some organizations have a team that specifically monitors social media channels for security threats.

Social Media Suggested Actions:

• Develop a social media risk management strategy involvingamultidisciplinary team.	• Mature the incident-response process and include crisis management and surprise drills that test performance of the response team.	• Gain threat intelligence from reputation/brand-monitoring services.
• Have a clear policy which delineates responsibilities and covers code of conduct and incident response.	• Develop a plan to monitor the corporate social media presence for hijacking, malware, misrepresentation, and other public-facing threats.	• Create Facebook and Twitter accounts for leadership to pre-empt others from creating falsified accounts.
• Deliver ongoing end-user awareness training programs including educating employees on what information is appropriate to post on social channels and monitor employees' social media activities.	• Create policy regarding when and how to respond to rumors/misleading statements regarding your organization, such as its security posture.	• Work with vendors to develop more advanced, flexible technologies for fine-grained social media access control and monitoring.

"For social media response planning, one of the most useful things is a table-top exercise. Create scenarios and go through simulated events in real time with all of the stakeholders – such as IT, Communications, HR, Legal – in order to train and test the response of the team. You'll quickly learn how different social media events are compared to other events."

VISHAL SALVI
Chief Information Security Officer and Senior Vice President, HDFC Bank Limited

3. Big Data Competencies

Increased Complexity

Big data technologies such as Hadoop go well beyond conventional database engines. They allow organizations to amalgamate data sets and run powerful analytics at unprecedented volumes and speeds. Rapidly amassing and processing customer and business information increases the complexity of security issues such as access governance, confidential data exposure, regulatory compliance, and data integrity.

For example, as data sets grow, without robust access controls, individuals could easily be over-provisioned access. If not carefully tracked, confidential information could be combined with other data sets and inadvertently exposed. As personally identifiable information (PII) is processed in new ways, organizations run the risk of breaching privacy laws which require that data remain in particular geographical locations. Analyzing blended data sets to produce business insights may lead to new intellectual property (IP) that will need protecting. As well, data integrity issues arise when data from different sources gets combined; organizations must consider whether all of the data is from trusted sources and if the resulting analysis can be trusted.

Formulating Security Strategies

As organizations begin big data projects, security teams must get involved early on, in order to understand the risks and devise strategies to manage them. To protect information in a big data context, a major focus area must be access control governance. Unfortunately not many specialized tools are available yet. Limited data masking and coarse data access control are some of the currently available techniques, but they're not sufficient. Better methods for sanitizing aggregations and fine-grained access controls for large data sets are needed.

For big data, security teams will also need to get a handle on information life cycle. It's important to understand what data is being collected and stored, including the queries: "What returns large amounts? Small amounts?" As well, the individuals performing the analytics will need to be monitored. A possible solution may be a peer review of query results to check, for example, for access to PII.

4. Mobile Competencies

A recent comprehensive report from the SBIC, *Realizing the Mobile Enterprise: Balancing the Risks and Rewards of Consumer Devices,* identifies today's major sources of risk for the mobile enterprise and the outlook for the near future and presents concrete recommendations for managing mobile risks.

Big Data Suggested Actions:

• Ramp up technical knowledge in big data.	• Monitor what's being requested and what's going out including anomalous access or queries.	• Educate analysts regarding risks to various types of data and make clear what can be shared and with whom.
• Ensure proper information classification which covers legal and regulatory compliance and considers country-specific requirements.	• Watch carefully for over-provisioning of access and segregate roles for different types of access, such as those who ask for queries and those who run them.	• Move toward data-centric security, protection that travels with the information.
• Develop data-flow mapping as a core competency of the security team.	• Evolve access control governance by tracking the types and levels of data requests and queries.	• Work with vendors to develop technologies required for managing the risks of big data, such as better data masking, meta-tagging, data classification, and fine-grained access control.

6 Conclusion

Expect cloud computing, social media, big data, and mobile devices to be on the radar as disruptive forces for all of 2013 and beyond. As enterprises accelerate implementation, the information-security team needs to ensure it has what it takes to enable innovation – including people, processes and technologies. It is critical for the security team – as risk management partners – to develop a keen understanding of business goals and engage multiple departments and levels of management. It will require developing or honing skills, especially the ability to engage and influence stakeholders from across the organization, in order to ensure that information security has a seat at the table as the business moves forward.

About the Security for Business Innovation Council Initiative

The Security for Business Innovation Council (SBIC) is a group of top security leaders from Global 1000 enterprises committed to advancing information security worldwide by sharing their diverse professional experiences and insights. The Council produces periodic reports exploring information security's central role in enabling business innovation.

Report Contributors

Security for Business Innovation Council

MARENE N. ALLISON,
Worldwide Vice President of Information Security, **JOHNSON & JOHNSON**

ANISH BHIMANI, CISSP, Chief Information Risk Officer, **JPMORGAN CHASE**

WILLIAM BONI, CISM, CPP, CISA, Corporate Information Security Officer (CISO), VP, Enterprise Information Security, **T-MOBILE USA**

ROLAND CLOUTIER,
Vice President, Chief Security Officer, **AUTOMATIC DATA PROCESSING, INC.**

DR. MARTIJN DEKKER, Senior Vice President, Chief Information Security Officer, **ABN AMRO**

JERRY R. GEISLER III, GCFA, GCFE, GCIH, Office of the Chief Information Security Officer, **WALMART STORES, INC.**

RENEE GUTTMANN, Chief Information Security Officer, **THE COCA-COLA COMPANY**

MALCOLM HARKINS,
Vice President and ~~Chief Information Security Officer, General Manager, Information Risk and Security,~~ **INTEL**

KENNETH HAERTLING,
Vice President and Chief Security Officer, **TELUS**

PETRI KUIVALA,
Chief Information Security Officer, **NOKIA**

DAVE MARTIN, CISSP, Vice President and Chief Security Officer, **EMC CORPORATION**

TIM McKNIGHT, CISSP, Executive Vice President, Enterprise Information Security and Risk, **FIDELITY INVESTMENTS**

FELIX MOHAN,
Senior Vice President and Global Chief Information Security Officer, **AIRTEL**

ROBERT RODGER, Group Head of Infrastructure Security, **HSBC HOLDINGS PLC.**

RALPH SALOMON, CRISC, Vice President IT Security & Risk Office, **SAP AG**

VISHAL SALVI, CISM, Chief Information Security Officer and Senior Vice President, **HDFC BANK LIMITED**

SIMON STRICKLAND,
Global Head of Security, **ASTRAZENECA**

~~**LEANNE TOLIVER,** CISA, CISSP, Interim Chief Information Security Officer, Global Information Security, **EBAY**~~

DENISE D. WOOD, Corporate Vice President, Information Security, Chief Information Security Officer, Chief IT Risk Officer, **FEDEX CORPORATION**

To see SBIC members' full bios, please visit emc.com.