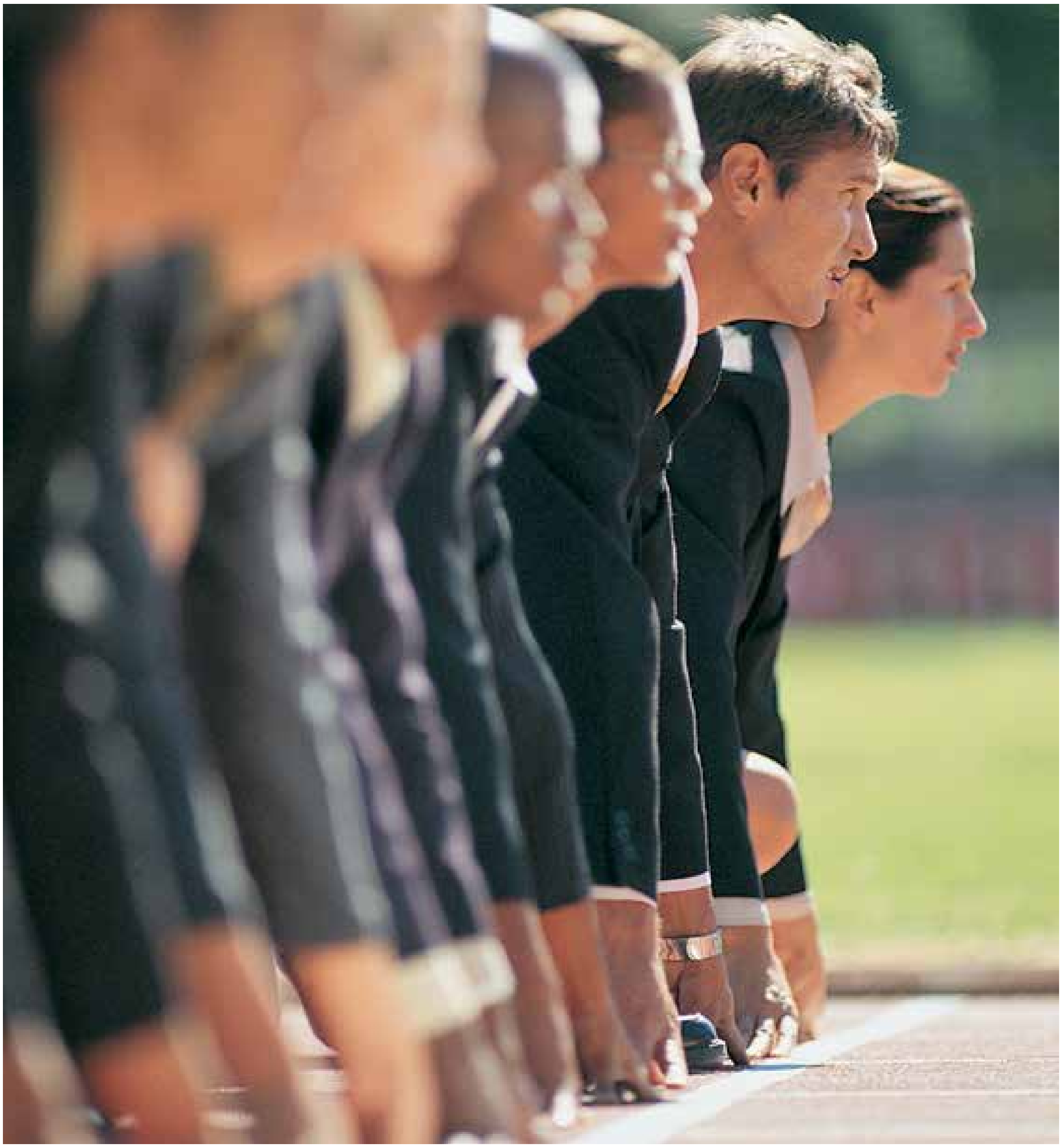
Report *based on* discussions *with the*

Security for Business Innovation Council

TRANSFORMING INFORMATION SECURITY

Designing a State-of-the-Art Extended Team



RECOMMENDATIONS FROM GLOBAL 1000 EXECUTIVES

INSIDE THIS REPORT:

The evolving information security mission	Required new skill sets	Emerging opportunities for collaboration	Insights into optimizing the use of resources	Actionable recommendations	Map of "who does what" on an extended team

An industry initiative sponsored by RSA

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

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

AstraZeneca
SIMON STRICKLAND, *Global Head of Security*

Automatic Data Processing
ROLAND CLOUTIER, *Vice President, Chief Security Officer*

The Coca-Cola Company
RENEE GUTTMANN, *Chief Information Security Officer*

EMC Corporation
DAVE MARTIN, *Vice President and Chief Security Officer*

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

Fidelity Investments
TIM McKNIGHT, *Executive Vice President, Enterprise Information Security and Risk*

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

HSBC Holdings plc.
BOB RODGER, *Group Head of Infrastructure Security*

Intel
MALCOLM HARKINS, *Vice President, Chief Security and Privacy Officer*

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

JPMorgan Chase
ANISH BHIMANI, *Chief Information Risk Officer*

Nokia
PETRI KUIVALA, *Chief Information Security Officer*

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

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

T-Mobile USA
WILLIAM BONI, *Corporate Information Security Officer (CISO) and Vice President, Enterprise Information Security*

Walmart Stores, Inc.
JERRY R. GEISLER III, *Office of the Chief Information Security Officer*

Contents

Disclaimer – This Security for Business Innovation Council Report ("Report") includes information and materials (collectively, the "Content") that are subject to change without notice. RSA Security LLC, EMC Corporation, and the individual authors of the Security for Business Innovation Council (collectively, the "Authors") expressly disclaim any obligation to keep Content up to date. The Content is provided "AS IS." The Authors disclaim any express or implied warranties related to the use of the Content, including, without limitation, merchantability, suitability, non-infringement, accuracy, or fitness for any particular purpose. The Content is intended to provide information to the public and is not legal advice of RSA Security LLC, its parent company, EMC Corporation, their attorneys or any of the authors of this SBIC report. You should not act or refrain from acting on the basis of any Content without consulting an attorney licensed to practice in your jurisdiction. The Authors shall not be liable for any errors contained herein or for any damages whatsoever arising out of or related to the use of this Report (including all Content), including, without limitation, direct, indirect, incidental, special, consequential, or punitive damages, whether under a contract, tort, or any other theory of liability, even if the Authors are aware of the possibility of such errors or damages. The Authors assume no responsibility for errors or omissions in any Content.

Report Highlights

WHAT DOES IT TAKE TO manage the risks to information assets in a global enterprise today? Much more than it did just a few years ago. Especially in the past 18 months, requirements have been added driven by the escalation of cyber-attacks, fevered adoption of new technologies, heightened regulatory scrutiny, and a hyper-connected business environment.

THE INFORMATION SECURITY mission is no longer just "implementing and operating security controls," but has evolved to include advanced technical and business-centric activities such as: business risk analysis, asset valuation, IT supply chain integrity, cyber intelligence, security data analytics, data warehousing, and process optimization.

THERE ARE MANY NEW SKILL sets required so a significant challenge in building an effective team is the shortage of professionals with the right skills.

AN EMERGING OPPORTUNITY IS that, in many organizations, personnel outside of security are starting to recognize that they – not security – own the risks to their information assets and they need to actively partner with security to manage those risks.

TO BE SUCCESSFUL, THE information security function is a cross-organizational endeavor, with security processes deeply embedded into business processes.

THE EXTENDED TEAM includes personnel in IT, business units, and departments such as procurement, legal, and marketing.

THE "CORE" INFORMATION security team governs and coordinates the overall effort and performs tasks requiring specialized knowledge or centralization.

SEVEN RECOMMENDATIONS provide a playbook for building a state-of-the-art extended team to effectively manage cybersecurity risks and optimize the use of available human resources and for ensuring the team has the new skill sets that are required.

1. REDEFINE AND STRENGTHEN CORE COMPETENCIES: Focus the core team on increasing proficiencies in four main areas: Cyber Risk Intelligence and Security Data Analytics, Security Data Management, Risk Consultancy, and Controls Design and Assurance.

2. DELEGATE ROUTINE OPERATIONS: Allocate repeatable, well-established security processes to IT, business units, and/or external service providers.

3. BORROW OR RENT EXPERTS: For particular specializations, augment the core team with experts from within and outside of the organization.

4. LEAD RISK OWNERS IN RISK MANAGEMENT: Partner with the business in managing cybersecurity risks and coordinate a consistent approach. Make it easy for the business and make them accountable.

5. HIRE PROCESS OPTIMIZATION SPECIALISTS: Have people on the team with experience and/ or certifications in quality, project or program management, process optimization, and service delivery.

6. BUILD KEY RELATIONSHIPS: Be well positioned to have influence with key players such as owners of the "crown jewels," middle management, and outsourced service providers.

7. THINK OUT-OF-THE-BOX FOR FUTURE TALENT: Given the lack of readily available expertise, developing talent is the only true long-term solution for most organizations. Valuable backgrounds can include database administration, software development, business analysis, military intelligence, legal or privacy officers, data science, mathematics, or history.

1 Introduction: Teams in Transition

If you walked into an information security department a few years ago, you'd likely see a technically oriented team. You might hear conversations about perimeter protections, compliance checklists, and anti-virus updates. Walk through that same door today and you'd see a completely different picture. Teams are evolving into multi-disciplinary groups of specialists, including threat analysts, risk advisors, data scientists, and process experts. Discussions are shifting to topics like business risk management, data analytics, controls assurance, and service provider governance.

Different organizations are at different stages of transformation, but most have recognized the need for new approaches to information security. In fact, in a recent security survey, the second-highest ranked spending priority for global enterprises was a fundamental redesign of their information security programs.[1] Simply adding point solutions or working on incremental improvements is no longer sufficient. **But what exactly does an effective and forward-leaning information security program look like?**

This report is the first of a series on transforming enterprise information security programs that intends to answer that question, drawing from the expertise and vision of some of the world's leading information security executives on the Security for Business Innovation Council (SBIC). This first report describes essential new skill sets and explains how responsibilities for information security are being distributed throughout the enterprise. It gives specific and actionable recommendations for designing a state-of-the-art extended team.

[1] E&Y Global Information Security Survey, November 2012

2 The New Statement of Work

The information security mission is no longer just "implementing and operating controls," but has evolved to include a much broader set of activities. Building an optimized team with the best people for the job requires an understanding of the scope of work.

What does it take to manage the risks to information assets in a global enterprise today? Much more than it did just a few years ago. Especially in the past 18 months, requirements have been added driven by the escalation of cyber-attacks, fevered adoption of new technologies, heightened regulatory scrutiny, and a hyper-connected business environment.

Organizations are now under immense pressure to achieve a proactive stance regarding cybersecurity risks. To make this change requires new approaches to defending against advanced threats, integrating information security into business and technology strategies, and ensuring that security processes are effective and efficient.

Advanced technical and business-centric activities are now required including:

→ Information Risk Management/Business Risk versus Reward Analysis
- To systematize risk/reward decision-making

→ Asset Inventory and Valuation
- To prioritize protection strategies and focus on safeguarding the crown jewels

→ Third-Party Risk Management/IT Supply Chain Integrity
- To assess the growing number of globally sourced service providers and system components

→ Cyber Risk Intelligence and Threat Analysis
- To understand the adversarial landscape and recognize attack indicators

→ Security Data Analytics
- To apply advanced analytics techniques in detecting anomalous system or user behavior within IT environments

→ Security Data Management and Data Warehousing
- To develop an overarching strategy and infrastructure for collecting data from various inputs to be used for various purposes such as threat detection, controls monitoring, and compliance reporting

→ Security Process Optimization
- To formalize improving the efficiency of security processes

→ Controls Agility
- To achieve objectives for security controls using new methods in response to trends such as cloud and mobile computing

A keystone of a team strategy is defining the mission in order to determine "who does what." Chart 1 is a depiction of the information security mission at leading organizations today, listing the more conventional to increasingly advanced activities. Organizations with a converged program might also include related tasks such as fraud, e-Discovery, privacy, product quality, and/or physical security in the mission. This report covers the information security components, bearing in mind the necessary coordination with other related activities.

Chart 1

TODAY’S INFORMATION SECURITY MISSION

Activities are roughly listed from more conventional to increasingly advanced.

Program Management	• Determine overall strategy and plan for the information security management program • Ensure program meets organization’s most critical business needs • Coordinate with related tasks such as fraud, e-Discovery, physical security, product security, and/or privacy
Security Policy and Standards	• Develop and document the overall directives and rules that prescribe how the organization protects information • Elaborate the complete set of administrative, technical, and physical information security controls used by the organization (i.e. the controls framework) including access controls, encryption, identification and authentication, configuration management, monitoring, audit logging, application security, and awareness training (of staff and customers) • Consider requirements of various laws and regulations (e.g. SOX, HIPAA, PCI) • Ensure controls are agile and track with changes in business and threat landscapes
Controls Implementation	• Implement controls based on policy and standards and on internal and external environmental factors
Controls Operation	• Operate the controls based on policy and standards and on internal and external environmental factors
Controls Design (Security Architecture)	• Develop new controls or new ways of implementing controls based on changes to business, IT, and threat landscape • Includes application-development techniques; specifying, deploying, customizing, and/or developing new security technology; and new end-user agreements and procedures
Controls Oversight/ Assurance	• Assess all controls to ensure they conform to policy and standards • Verify all controls are present and performing as intended • Ensure all controls are consistently monitored and attested
Incident Response/ Resiliency	• Coordinate and manage the organization’s response to security incidents, including business continuity/disaster recovery
Information Risk Assessment	• Evaluate the risks of a program, process, project, initiative, or system based on the value of information, data assets, applicable threats and vulnerabilities, likelihood of compromise, impact to organization (e.g. reputation, revenue, regulatory non-compliance), and estimated losses
Information Risk Management/ Business Risk vs. Reward Analysis	• Establish risk owners’ risk appetites and authorized risk acceptance levels • Based on risk assessment for particular program, process, project, initiative, or system, formulate risk mitigation and remediation strategy • Have a consistent process to weigh the information security risks against the business rewards • Determine required controls to bring risk to acceptable level • Integrate information risk with enterprise risk management framework/program

Asset Inventory and Valuation	• Delineate the complete inventory of business processes, sensitive data, and information systems used by the organization • Perform comprehensive business process documentation and data flow mapping in order to understand the processes and data that need protecting and formulate protection strategies • Identify the privileged users throughout the extended enterprise who have access to critical systems • Determine the value of assets in order to prioritize protection strategies
Third-Party Risk Management/ IT Supply Chain Integrity	• Ensure a risk evaluation is performed prior to the organization establishing a relationship with a third party • Develop a due diligence process to assess vendors, partners, and suppliers • Evaluate the risks involved in doing business with vendors, partners, and suppliers on an ongoing basis • Understand the IT supply chain and evaluate the security of hardware and software used in the enterprise IT environment • Increase efficiencies through shared assessments and continuous controls monitoring
Cyber Risk Intelligence and Threat Analysis	• Understand the adversarial landscape relative to business assets (identity, capabilities, motivations, targets) • Gather intelligence data regarding threats to the organization • Manage sources of intelligence data, interpret data, perform analysis, and produce threat intelligence reports and alerts • Integrate threat modeling and intelligence into entire security management process and lifecycle
Security Data Analytics	• Use advanced analytics techniques and data science to analyze security data enriched by intelligence data • Develop queries, algorithms, and data models used to detect or predict malicious activity
Security Data Management and Data Warehousing	• Develop a data management strategy and infrastructure for aggregating and analyzing security data from various inputs (security systems, databases, applications, threat feeds) for various purposes (e.g. threat detection, enterprise risk management and compliance, continuous controls monitoring) • Architect a data warehouse for security data
Security Process Optimization	• Consistently track and measure the efficiency of security processes and implement improvements using formalized quality management, project management, and service delivery methodologies
Long-Range Planning	• Look at future trends in business, technology, and regulation in order to formulate proactive security strategies. For example, technology developments such as the “Internet of Things” and wearable computing are bringing new security challenges

3 Challenges and Opportunities

Creating an effective information security team comes with a number of current challenges:

- Expertise is in short supply and talent is hard to keep
  - Specialized security and business risk experts are in high demand
- Budget is limited
- Security teams are already at full capacity
- Boardroom attention demands business acumen
  - As information security becomes a more critical component of business strategy, security practitioners require more in-depth knowledge of the business

The good news is that there are also some emerging opportunities:

- Awareness is expanding
  - At every level from end users to leadership, awareness of security issues is higher than ever due to media attention, actual experience with cyber attacks, or regulatory pressure.
- The "business" is taking ownership of risks
  - In many organizations, a fundamental shift in thinking is occurring whereby personnel outside of security are starting to recognize that they – not security – own the risks to their information assets and they need to actively partner with security to manage those risks.
- Security careers have a growing cachet
  - It's an exciting time to be in information security, as it takes on new aspects such as business risk analysis, cyber intelligence, and data science. News reports and Hollywood portrayals of defending cyberspace are also creating more interest in the field, which can help attract talent.
- The range of service providers is increasing
  - As the market responds to growing demands, it is becoming more feasible for organizations to turn to external security service providers to reduce costs, obtain specialized expertise, help accomplish a surge of activities, or provide independent assessments.

DAVE MARTIN
Vice President and Chief Security Officer,
EMC Corporation

> *"It's amazing to see. We've gone from, 'You security guys are getting in our way, why do we have to do this?' to the business units using our central consultancy services to roll out risk mitigation strategies. It's picking up speed because the business units are realizing they need to manage their risks, not rely on somebody else to try and fix it or stick their head in the sand."*

4 Recommendations

To be successful, the information security function must be a cross-organizational endeavor, with security processes deeply embedded into business processes. The extended information security team might include the following:

- Personnel in IT implementing and operating security controls
- Risk managers in business units remediating risks
- Purchasing professionals implementing vendor assurance and risk assessment protocols for evaluating suppliers
- The privacy office tracking regulations
- Marketing staff monitoring social media for information on possible threats

The "core" information security team governs and coordinates the entire effort and performs tasks requiring specialized knowledge or centralization. Some personnel performing security tasks outside of the core team may be direct or dotted line reports; others may be operating to security standards or Service Level Agreements (SLAs). Chart 2 in the Appendix illustrates who does what on an extended team, including core information security, IT, business, and service providers.

The following recommendations provide a playbook for building a state-of-the-art extended team to effectively manage information security risk and make optimal use of available human resources. Depending on an organization's level of maturity, this guidance could help to get started, validate an approach, or accelerate progress in particular areas.

Redefine and Strengthen Core Competencies 1

Delegate Routine Operations 2

Borrow or Rent Experts 3

Lead Risk Owners in Risk Management 4

Hire Process Optimization Specialists 5

Build Key Relationships 6

Think Out-of-the-Box for Future Talent 7

1. Redefine and Strengthen Core Competencies

Within leading organizations, core information security teams are currently focused on increasing proficiencies in four main areas: Cyber Risk Intelligence and Security Data Analytics, Security Data Management, Risk Consultancy, and Controls Design and Assurance.

Depending on the size of the core team and level of specialization, individual members may cover very specific tasks or multiple areas. Each area requires a set of key skills that are often new for team members. Going forward, existing personnel will need to develop the requisite skills through training and/or the core team will need to add new members or engage with service providers.

1. Cyber Risk Intelligence and Security Data Analytics

Given the escalating threat landscape, improving threat detection is paramount for most organizations worldwide, specifically developing an intelligence-driven approach (see SBIC report, "Getting Ahead of Advanced Threats: Achieving Intelligence-Driven Information Security"). This requires collecting and amalgamating cyber intelligence data from internal sources (e.g. sensors in IT systems and business applications) and external sources (e.g. government or commercial threat feeds) and using advanced data analytics techniques to spot attack indicators or anomalous behavior patterns. The core team should have the capabilities to achieve situational awareness across the organization.

Determining relevant sources of data and performing meaningful analysis necessitates developing an in-depth understanding of the true business environment, assets to be protected, and cyber adversarial landscape. Security teams are beginning to tap into the power of Big Data technologies, with the objective to not only detect but also predict attacks.

- Key People Skills: Internal and external networking for developing good sources of intelligence, communication for developing reports and presenting intelligence briefings
- Key Process Skills: Designing an end-to-end intelligence process including obtaining and filtering data, performing analysis, communicating results, making a risk decision, and taking action
- Key Technical Skills: Analysis (drawing connections between seemingly disconnected data), data analytics techniques, and data science

2. Security Data Management

As they pursue data analytics for threat detection, organizations are realizing the need for an overarching security data management strategy and infrastructure. This entails aggregating security data from across the IT environment including logs, full packet data streams, and unstructured data from systems, databases, and business applications. The data can be applied beyond threat detection to be used for purposes such as enterprise risk management and compliance and continuous controls monitoring.

- Key People Skills: Interfacing with IT and the business including enterprise data management architects
- Key Process Skills: Mapping security data flows throughout the organization's IT environment
- Key Technical Skills: Core IT skills such as storage architecture, processing architecture, database schema, normalization, and dealing with networking bottlenecks

3. Risk Consultancy

The core team acts as a consultancy, advising the business on managing the risks to information assets, including those related to security, privacy and legal issues, regulatory compliance, and e-Discovery. The core team must have a keen awareness of business processes. They must be able to collaborate with stakeholders to assess risks, gauge the value of assets, determine risk mitigation strategies, and ensure that risk conversations take place when projects are first initiated. A fast-growing set of risks to manage stems from third parties. Global sourcing and cloud computing strategies are driving organizations to further increase their use of outsourced service providers and to take on new business partners and suppliers. Having the know-

> *"The core security team's expertise should be primarily focused on delivering consulting, providing direction, driving strategy, identifying and explaining risks to the business, understanding threats, and moving the organization forward – not be encumbered by the day-to-day routine operational activities."*

BOB RODGER
Group Head of Infrastructure Security, HSBC Holdings plc.

how to perform efficient and effective third-party due diligence, ongoing assessments, and evaluation of hardware and software is critical.

- Key People Skills: Leadership, internal networking for awareness of business strategies, communication (listening, verbal articulation, handling difficult conversations, sensitivity to cultural and organizational nuances)
- Key Process Skills: Business process mapping and documentation, risk management frameworks, protocols for third-party risk assessments and controls assurance (including shared assessments), managing outsourced service providers and supply chain communities
- Key Technical Skills: Risk evaluation, measuring diverse risks and risk appetites across an organization with a standardized method, automating risk management and vendor assessment activities, continuous controls monitoring

4. Controls Design and Assurance

Designing innovative controls aligned with business goals and devising advanced testing techniques for controls assurance should be major focus areas for the core team. This work includes research and development and the evaluation and deployment of new security technologies. Controls analysts must engineer the gathering of evidence to not only prove controls are working as intended but also ensure they are optimal to defend against the latest threats and enable business agility.

- Key People Skills: Translating business and compliance requirements into security requirements, liaising with enterprise architecture
- Key Process Skills: Documenting the organization's controls framework, developing protocols for controls assessment and attestation
- Key Technical Skills: Security architecture, application security, mobile security, cloud security, continuous controls monitoring, advanced testing and analysis of security controls

2. Delegate Routine Operations

Traditional security teams are more comfortable doing things themselves. But that has to change. Delegating routine security operations to other internal groups or external service providers allows the core team to focus on being more proactive and strategic, maximizing their technical expertise and business risk management capabilities. Moreover, through scalability and specialization, the right service providers cannot only lower costs but also increase quality.

Repeatable, well-established processes are good candidates for delegation. Examples include allocating the operation of firewalls, authentication, intrusion prevention systems, and/or antivirus software to groups in IT or managed security service providers (MSSPs). Allocate application-level user access provisioning and user account administration to the business units. Train developers in application security and provide them with tools to find vulnerabilities. Consider using security-as-a-service for scans and testing.

As the core team allocates activities, they will need to retain an adequate level of command and control through comprehensive requirements, standards, and SLAs. The core team must also have sufficient technical security expertise as well as vendor management skills to ensure effective oversight. Organizations which are apprehensive about outsourcing security to external third parties can often achieve the same goals by "outsourcing" to internal IT groups; however, the same level of oversight is required regardless of the type of service provider.

Over time, the core team should continually evaluate what would be more efficiently or cost-effectively done by others. For example, the core team may initially handle the deployment and operations of a new security technology, but eventually it becomes standardized and ongoing operations can be delegated.

3. Borrow or Rent Experts

A common challenge is that the core team doesn't have expertise in particular specialized areas. Experts from outside of the security department can fill the gap. For example, some security teams are engaging data analytics personnel from service providers or other parts of the organization such as fraud or marketing. Big Data may be new to security but other areas of business have been using data analytics techniques for years.

When it is infeasible or simply too expensive to have certain experts on staff full-time, such as malware forensics specialists or cyber threat intelligence analysts, organizations may turn to external service providers on an ongoing basis. Core teams may bring in extra talent to handle a surge of activities or to assist when team members leave. Forming a partnership with a security consulting company, which can provide multi-faceted, high-level security professionals on retainer, is another good option. They can augment the core team's abilities and offer an independent perspective.

For solving particularly complex problems, it often makes sense to bring in subject matter experts such as a security architect consultant specializing in a specific technology. Keep in mind that the core team still needs enough knowledge in-house to apply outsourced expertise.

> *"If I don't have a critical skill I build it or buy it. You have to know when to build or buy based on the total cost of ownership. For some skills, it may make more sense to go to a service provider."*

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

4. Lead Risk Owners in Risk Management

Typically, senior managers within the business are responsible for owning the risk management decisions associated with initiatives such as launching a new product or service, programs such as BYOD, information assets such as customer-facing web sites, or business processes such as financial reporting. As business leaders increasingly recognize their responsibility to manage cybersecurity risks, a growing number of organizations have dedicated "information security risk managers" in the business units, responsible for risk remediation.

The core team's role is to lead information risk management activities and partner with the business in managing its cybersecurity risks. This includes coordinating a consistent approach to risk identification, assessment, mitigation, remediation, and reporting; gauging risks against rewards; establishing risk appetite and acceptance levels; and incorporating information risk into the overall enterprise risk management program. Key aspects are to make it easy for the business and make them accountable for managing risks by providing self-service tools, integrating risk management into business processes, and implementing automation.

> ***"Traditionally the information security team was more focused on technology. But an increasingly important role is to liaise with the business, bring their requirements into the security organization, and in turn carry the security perspective to the business."***

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

5. Hire Process Optimization Specialists

Process expertise has become an essential aspect of a state-of-the-art team. Have people on the team who are adept at quality, project, or program management; process optimization; and service delivery, and who can be trained in security. Consider hiring people who have credentials in Six Sigma Process Improvement, ITIL's IT Service Management (ITSM), COBIT IT Governance, and/or TOGAF's Enterprise Architecture. Some core teams have been able to leverage process experts or program management professionals from other areas of the organization, such as the Quality Department or Enterprise Program Office.

Having process expertise on board will help meet the growing demands for process improvements. For example, given the threat landscape, some organizations would like to see patching of all critical systems in hours not weeks. Business units want to reduce the impact of security on business processes, minimizing the friction for end users and downtime for servers. Regulators want tighter controls on access to information, such as revocation of expired entitlements in minutes not days. Increasingly, the security department will be expected to measure the productivity of security investments and deliver quantifiable improvements over time. This includes process repeatability, agility, and the ability to scale.

For an extended cyber enterprise, look at who your critical service providers are and establish a solid working rapport with them. Give the bad guys no place to hide because you have raised the standard of conformance to a good practice of security across your ecosystem.”

WILLIAM BONI
Corporate Information Security Officer (CISO),
Vice President, Enterprise Information Security,
T-Mobile USA

“We have a fundamental cornerstone to our security organization, and it says, ‘Formality matters.’ Our processes have to be highly documented and reviewed. How can we make them more efficient? More effective? Did we miss anything? You need people with a strong process and quality background if you want credibility with your business leaders.”

DENISE D. WOOD
Corporate Vice President, Information Security, Chief
Information Security Officer, Chief IT Risk Officer,
FedEx Corporation

6. Build Key Relationships

Strong relationships throughout the organization are essential for the core team in order to rally the growing number of personnel with security responsibilities, create a collaborative environment, and ensure members of the extended team understand and perform their tasks. The core team must reach out to all areas of the enterprise and be engaging at all levels. They must be well-positioned to have influence with the key players, such as those who control technology investments and make strategic business decisions.

One of the most important relationships is with those who own the “crown jewels” of the organization, for example the data sets and business processes with intellectual property or proprietary data. Another is with middle management – significant inroads can be made when middle management is won over. Business process outsourcing (BPO) providers should also be a key target. The core team should build a strong network of security contacts from BPOs and work with them to ensure high security standards and information sharing within the entire community.

7. Think Out-of-the-Box for Future Talent

Interest in the field of information security is growing, but over the near term there will be a shortage of professionals with "ready-to-go" cybersecurity and risk advisory skills. It is especially challenging to find talent with know-how in emerging security technologies. Some organizations are turning to MSSPs in the interim, because it is difficult to recruit and/or retain talent with certain technical skills. Furthermore, security teams also need professionals who can transcend technical expertise to have fruitful business risk conversations with key stakeholders.

An ongoing recruiting strategy is essential for building an effective security team. Work with the business units and Human Resources to evaluate needs and possible sources of talent. Increasingly, organizations are recruiting people who don't have a security background but who have valuable skills and can be trained in security. One approach is to form an internal "cybersecurity academy." Another is to provide support for individual team members to pursue external training courses and certifications, and/or set up mentoring programs. Besides new grads, new recruits can be internal people from IT or other areas who might be interested in a security career. They are often the best recruits since they bring knowledge of the organization and established networks.

Given the lack of readily available expertise, developing talent is the only true long-term solution for most organizations.

Given the lack of readily available expertise, developing talent is the only true long-term solution for most organizations. Keep an open mind when looking for people to train for security roles. There is a wide range of valuable backgrounds such as database administration, software development, business analysis, military intelligence, or legal and privacy officers. Some core teams have recently hired data scientists who have backgrounds in DNA sequencing. People who have theoretical knowledge in areas like econometrics or mathematics can grow their practical technical abilities. Others with a background in history or journalism may offer excellent investigative skills. As retention is a big challenge when training people to have sought-after security skills, it is important to provide a foreseeable and attractive career path for individual team members and to ensure market-level compensation.

"When adding people to your organization, you absolutely want diversity of thought. It's more critical today than ever because the change on the business side is outpacing security's capabilities and it's going to require innovative thought to solve these problems."

JERRY R. GEISLER III
Office of the Chief
Information Security Officer,
Walmart Stores Inc.

Many organizations are also partnering with universities to ensure the growth of the security talent pool. This can include creating leadership development programs, helping to drive curricula to suit industry needs, or offering internship/co-op opportunities. Outreach programs at the university and even high school levels can help to educate the potential workforce about cybersecurity careers.

Conclusion

Information security teams are evolving to meet the demands of an increasingly challenging business environment, threat landscape, and regulatory regime. Awareness of security issues is enabling a shift in information security's position within organizations, away from being a technical silo towards a truly collaborative endeavor. Organizations are also discovering that meeting security requirements requires more attention to process. An effective security team today has a keen understanding of business processes and of the importance of good security processes in achieving its own mandate. The next report in this three-part series on transforming information security will further explore how leading organizations are rethinking and optimizing processes. The third report will address how new technologies fit into the picture of a modern information security program with a creative and forward-looking team as its foundation.

About the Security for Business Innovation Council Initiative

Business innovation has reached the top of the agenda at most enterprises, as the C-suite strives to harness the power of globalization and technology to create new value and efficiencies. Yet there is still a missing link. Though business innovation is powered by information and IT systems, protecting information and IT systems is typically not considered strategic – even as enterprises face mounting regulatory pressures and escalating threats. In fact, information security is often an afterthought, tacked on at the end of a project or – even worse – not addressed at all. But without the right security strategy, business innovation could easily be stifled or put the organization at great risk.

At RSA, we believe that if security teams are true partners in the business-innovation process, they can help their organizations achieve unprecedented results. The time is ripe for a new approach; security must graduate from a technical specialty to a business strategy. While most security teams have recognized the need to better align security with business, many still struggle to translate this understanding into concrete plans of action. They know where they need to go, but are unsure how to get there. This is why RSA is working with some of the top security leaders in the world to drive an industry conversation to identify a way forward.

RSA has convened a group of highly successful security executives from Global 1000 enterprises in a variety of industries which we call the "Security for Business Innovation Council." We are conducting a series of in-depth interviews with the Council, publishing their ideas in a series of reports, and sponsoring independent research that explores these topics. Go to www.rsa.com/securityforinnovation to view the reports or access the research. Together we can accelerate this critical industry transformation.

A Appendix

Illustration of a State-of-the-Art Extended Information Security Team

Chart 2

Executive management and board of directors oversee the program.

TEAM MEMBERS	CORE INFORMATION SECURITY	IT	BUSINESS	SERVICE PROVIDERS (*COMMON USES*)
	• A wide range of specialists • Individuals may take on more than one role • May be converged with e-Discovery, physical security, and/or product security teams	Personnel involved in strategic and operational security roles	Lines of Business (LOBs) and Functional Areas (e.g. Privacy, HR, Marketing, Legal, Audit, Procurement)	Consultants with subject matter expertise (SMEs), managed security service providers (MSSPs), and cloud vendors (SAAS)
Activities	*Specific Responsibilities*			
Program Management	CISO leads program and chairs cross-functional "Information Risk Committee"	CIO participates in "Information Risk Committee"	Certain business executives participate in "Information Risk Committee"	
Security Policy and Standards	Develop policy and standards	Consult on policy and standards	Consult on policy and standards	
Controls Implementation	• Manage and oversee controls implementation • Perform controls implementation in more complex cases	Implement controls to security standards or provide services meeting security SLA	Facilitate controls implementation	MSSPs provide controls implementation services meeting security SLA
Controls Operations	• Manage and oversee controls operations • Operate newer or more complex controls	Operate controls to security standards or provide services meeting security SLA	Ensure business operations meet security control requirements	MSSPs provide controls operation services meeting security SLA
Controls Assurance	• Perform controls assessment and develop advanced tools for controls testing and analysis • Implement continuous controls monitoring			MSSPs provide services, e.g. source code reviews, vulnerability scanning
Controls Design (Security Architecture)	• Drive design of new security controls • Work with enterprise IT architecture	Consult on design of new security controls	Consult on design of new security controls	
Incident Response/ Resiliency	Manage and coordinate cross-organizational response	Work on technical aspects of response	Work on legal, PR, HR aspects of response	SMEs provide forensics and malware analysis

Information Risk Assessment	• Manage risk assessment program • Perform risk assessments in more complex cases • Provide tools to ease risk assessments	Perform risk assessment using tools provided by the core team	• Perform risk assessment using tools provided by the core team • Legal personnel consult on legal and compliance risks	Emerging trend is risk assessments performed by service providers meeting security SLA
Information Risk Management/ Business Risk Versus Reward Analysis	• Drive risk management activities • Engage with IT and the business • Consult on risk management • Provide tools to ease risk management	• Work with core team to manage risks • Facilitate remediation of identified risks • Regularly report on status of risks	• Work with core team to manage risks • Facilitate remediation of identified risks • Regularly report on status of risks	
Third-Party Risk Management/ IT Supply Chain Integrity	• Drive third-party risk management and supply chain integrity program • Develop standards and provide tools for third-party assessments and evaluation of hardware and software	• Perform due diligence and third-party assessments using tools provided by the core team • Perform evaluation of hardware and software using tools provided by the core team	• Perform due diligence and third-party assessments using tools provided by the core team • Procurement builds security assessments into procurement process • Legal personnel consult on legal and compliance risks and write contracts	SMEs perform due diligence and third-party assessments using standards provided by the core team
Asset Inventory and Valuation	Drive development of registry	Engage with core team to list and value assets	Engage with core team to list and value assets	
Cyber Risk Intelligence and Threat Analysis	• Manage intelligence program • Coordinate sources	Share intelligence data such as phishing emails	Share intelligence data such as social media monitoring	SMEs provide sources and threat analysis
Security Data Analytics	Drive development of queries and models	Consult and/or provide data analytics services	Consult and/or provide data analytics services	SMEs and/or MSSPs provide data analytics services
Security Data Management and Data Warehousing	Drive security data management strategy and architect security data warehouse	• Drive organization's overall data management strategy • Consult on security strategy and data sources such as network logs	Consult on data sources such as application and database logs	• SMEs provide threat feeds • MSSPs provide feeds from security system logs
Security Process Optimization	Drive security process optimization throughout organization	Consult and facilitate implementation of improvements	Consult and facilitate implementation of improvements	
Long-Range Planning	Look at future trends in business, technology, and regulation in order to formulate proactive security strategies	Collaborate on future trends and proactive strategies	Collaborate on future trends and proactive strategies	

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, Chief Security and Privacy Officer,
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 and 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

DENISE D. WOOD
Corporate Vice President, Information Security, Chief Information Security Officer, Chief IT Risk Officer,
FedEx Corporation

To see *the SBIC members' full bios, please visit EMC.com*