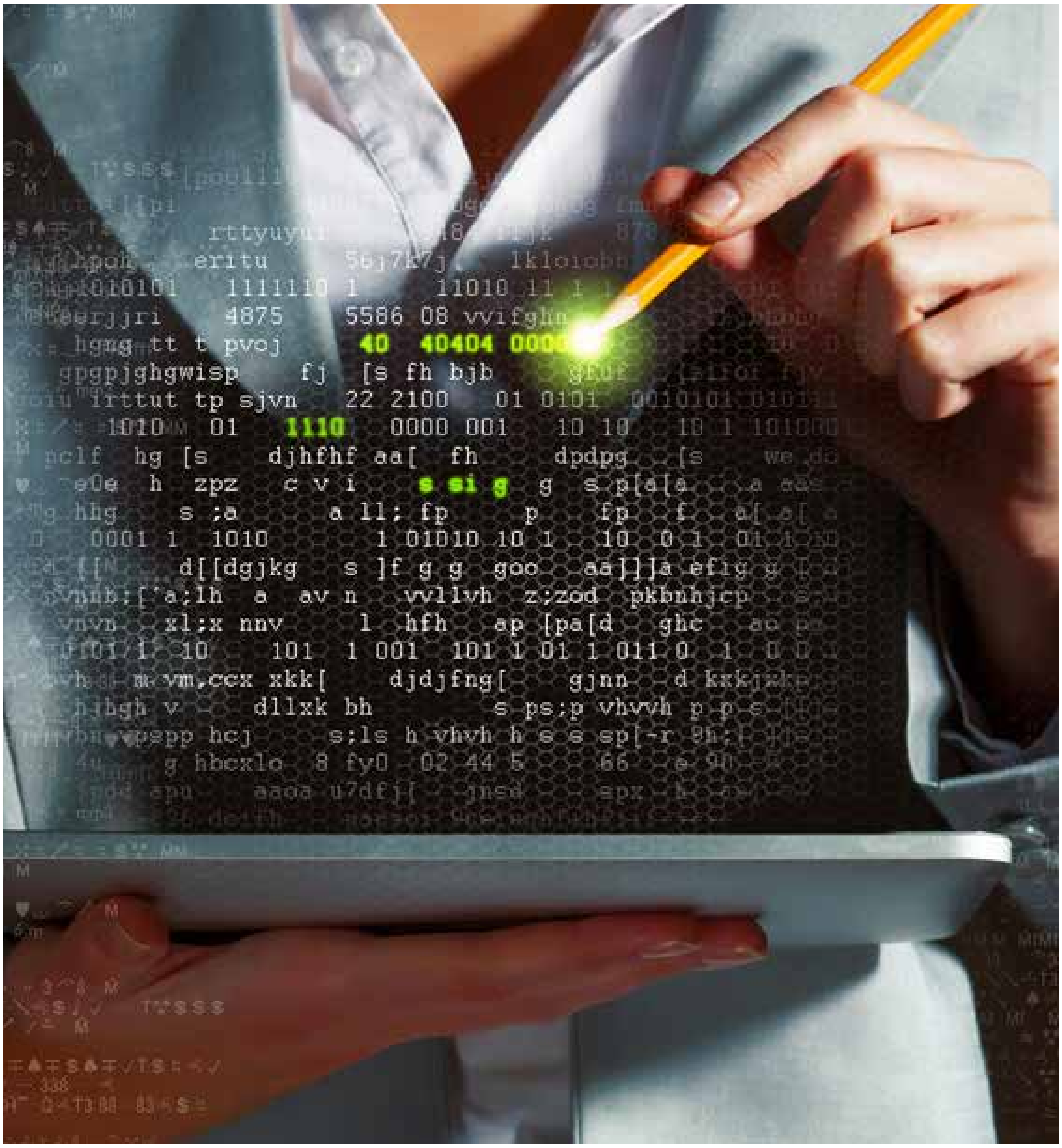
Report *based on* discussions *with the*

Security for Business Innovation Council

TRANSFORMING INFORMATION SECURITY

Focusing on Strategic Technologies



RECOMMENDATIONS FROM GLOBAL 1000 EXECUTIVES

INSIDE THIS REPORT:

- Identifying key areas to optimize threat resilience
- Creating an enterprise-wide big data strategy
- Guidance on making game-changing, detective investments
- Optimizing the end-user experience
- Improving visibility in the cloud
- Recommendations for leveraging advanced technologies

ABN Amro
DR. MARTIJN DEKKER, *Senior Vice President, 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*

eBay
LEANNE TOLIVER, *Office of the 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, CRISC, *Vice President Security, Processes & Compliance Office, SAP Cloud and Infrastructure Delivery*

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*

An industry initiative sponsored by RSA

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

LEADING INFORMATION security executives have identified opportunities to strengthen security capabilities in three key areas: cyber-threat resilience, end-user experience optimization, and cloud security.

SECURITY LEADERS TODAY speak in terms of resilience against cyber threats: in the face of ongoing intrusions, their goal is to prevent attackers from achieving their outcomes, manage the inevitable breaches, and minimize their impact.

BIG DATA ANALYTICS AND next-gen anti-malware are considered fundamental to developing cyber-threat resilience.

FULLY IMPLEMENTED, Big Data analytics enables organizations to continuously monitor for cyber threats throughout the business environment and detect, understand, and respond to incidents in real time.

MOST LEADING-EDGE implementations are based on homegrown solutions but are moving to commercial, off-the-shelf security analytics platforms.

SINCE COMMERCIAL SOLUTIONS are now widely available, it is expected that many more organizations will begin to implement a security analytics program within the next 18 months.

This report provides a valuable set of recommendations from 18 of the world's leading security officers to help organizations build security strategies for today's escalating threat landscape.

NEXT-GENERATION anti-malware technologies do not rely on signatures; they detect malware by analyzing patterns of behavior for suspicious characteristics and are therefore more effective against zero-day attacks.

CYBER-THREAT RESILIENCE requires game-changing investments: leading security teams today are focusing investments on controls that detect rather than prevent intrusions.

MANY LEADING SECURITY teams consider it a top priority to bring the UX for security systems up to the new bar that has been set by smartphones, tablets, and popular consumer apps.

TODAY, USERS EXPECT FEWER and faster sign-ons, quicker access to data and applications, and the freedom to move between devices, locations, and platforms.

BETTER UX IS BEING DRIVEN by advances in risk-based authentication techniques and identity and access management.

TO HELP SOLVE SOME OF THE thorniest security issues related to enterprise cloud usage, a range of services has become available. Many leading security teams see real promise in these new cloud security services and plan to implement at least one over the next year.

THESE SERVICES CLAIM TO BE able to solve issues such as shadow IT, risk assessment and controls assurance, identity and access management, data leakage, protection of user credentials, and encryption in the cloud.

THE SBIC PROVIDES ITS TOP three recommendations for leveraging advanced technologies to build better defenses and improve business productivity:

1. **Look at Least Three Years Ahead:** A three-year rolling plan is a useful tool to help focus limited capital on forward-leaning security investments. Specific guidance includes: use SWOT analysis, align with IT and the business, create an enterprise-wide big data strategy, and get auditors engaged.

2. **Achieve a Bigger Picture through Integration:** When investing in security technologies today, the greatest payoffs often come from connecting and consolidating multiple applications. Technologies now make it easier to meaningfully integrate systems; for example, security teams are more fully integrating threat detection with prevention technologies or risk management with business applications.

3. **Maximize Value Through Formalized Technology Developments:** Deploying technology effectively is a huge challenge given the pace of change and limited budgets. To proactively manage the risks, predict and track total costs and value, scale deployments for quick wins, employ judicious cloud vendor management, and approach maintenance strategically.

1 Introduction: Strengthening Capabilities

> *The speed of change is quicker than it's ever been. You've got to inject flexibility and innovation into your strategy. Because 18 or even 12 months down the line, technology will have moved, your adversaries will have moved on, and you can pretty much guarantee there will be questions about why you're not keeping up with developments.*

SIMON STRICKLAND,
Global Head of Security,
AstraZeneca

The Security for Business Innovation Council (SBIC), a forward-thinking group composed of some of the world's leading information security executives, has identified opportunities to strengthen security capabilities as a result of technology advances. These opportunities focus on three key areas: cyber-threat resilience, end-user experience optimization, and cloud security.

The security leaders who comprise the SBIC said that enormous changes in security are underway, but, in some ways, developments are not happening fast enough. They would like to see continued advances in security technology that would not only build better anticipatory defenses but also improve business productivity.

This report, the third and final in a series on Transforming Information Security, combines perspectives on technologies with experience in strategy to help security teams navigate complex decisions regarding technology deployments while maximizing investments.

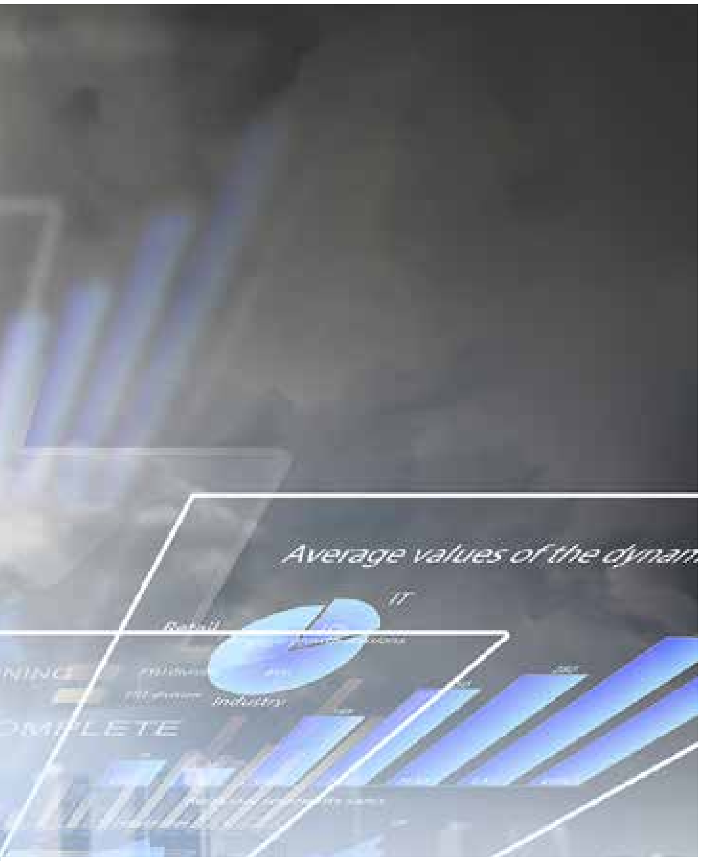
What does an effective and forward-leaning information security program look like?

The Security for Business Innovation Council (SBIC) has produced a series of three reports on "Transforming Information Security" to answer that question. Fusing the knowledge and vision of top information security leaders, the reports deliver actionable recommendations for achieving a strategic program. The first report was a playbook for designing a state-of-the-art extended team; the second explored the forefront of information security processes. The third identifies some of the essential technologies for evolving information security programs.

Read the first two reports →

2 Developing Cyber-Threat Resilience

It is widely recognized that current implementations of cyber defense are often insufficient. The Verizon Data Breach Investigation Report reveals 66% of breaches take months or even years to discover.[1] Security leaders today speak in terms of resilience against cyber threats.



Although they still seek to deter cyber adversaries from gaining entry into their organization, they acknowledge the likelihood of compromises. In the face of on-going intrusions, their goal is to prevent attackers from achieving their outcomes, manage the inevitable breaches, and minimize their impact. To achieve cyber-threat resilience, security leaders require technologies that provide comprehensive situational awareness, effective threat detection, and the ability to respond to incidents quickly.

It is important to keep in mind, however, that new technologies will not entirely replace existing security controls but rather serve as a critical component of an organization's overarching, multi-layer defense and protection framework. For example, performing basic security hygiene practices —and doing them well—is still essential.

Security Analytics: A Foundational Technology

Increasingly, big data analytics technology is being embraced by leading-edge security teams as a fundamental component of their multi-layer information security programs. Threat detection is the primary area of information security where big data analytics is being applied. When fully implemented, big data analytics enables organizations to continuously monitor for cyber threats throughout the business environment and detect, understand, and respond to incidents in real time. By drawing together data on threats and business processes, it allows an organization to form a more complete picture and significantly increases visibility across the global enterprise. Those features, along with the unique ability to adapt to changes in the threat landscape over the long term, make big data analytics a cornerstone of cyber defense.

Today's Programs

Leading security teams with relatively mature analytics programs have not only been able to attain significant value from these programs but are "doubling down" on their investments. Current efforts include adding more sophisticated data visualization techniques to provide additional context about an incident and help investigators better understand which events might be related. Some organizations are working towards deeper integration of business event and business process data into their analytics system to automatically increase protection for the most critical business resources. Others are focused on cutting their reaction time when detecting attacks and enriching their analysis with external threat data.

Although most of the leading-edge implementations of security analytics to date have been based on homegrown solutions, many organizations are now looking at migrating to commercial solutions. They anticipate that the complexity of implementing security analytics will be reduced as vendors provide more complete platforms. In fact, first-generation commercial, off-the-shelf security analytics platforms are available now, and vendors are building in more advanced functionality such as support for integrated incident response workflow. Since these commercial solutions are widely available, it is expected that many more organizations, especially large enterprises, will begin to implement a security analytics program within the next 18 months.

[1] 2013 Verizon Data Breach Investigation Report

LONG-TERM VISION

Leading security *teams have plans for increasingly automated and powerful analytics systems. The table describes some of the capabilities they expect to add to their analytics programs over the long term.*

Future Capability	Description
Apply machine learning to the development of threat detection rules	The system automatically suggests what rules need to change or what correlations might be useful. For example, it can suggest adjusting the threshold in a detection rule if the current behavior of normal users is generating too many false positives. With machine learning, the system can also discover which previously unnoticed parameters are useful for detecting an attack. Early prototyping has been very successful and indicates that machine-learning systems are extremely adept at refining threat detection rules.
Automate response and containment	When the system detects a problem, it automatically provides a response to contain and limit the impact without requiring human intervention. Automated response would work particularly well for situations where the steps for response are well-defined, such as Distributed Denial-of-Service (DDoS) attacks.
Anticipate attacks	Prioritization system that sets threshold for priority risks. The system provides alerts if it detects behavior that could indicate an attack is being planned, such as detecting multiple failed authentication attempts in quick succession. While reactive alerts inform analysts that an attack is occurring, predictive alerts inform analysts of behavior that holds a certain index risk value indicative of a future breach, including the reasons and context.
Support community defense	The system has built-in mechanisms to automatically exchange threat intelligence data with other organizations. It includes refined masking capabilities and high levels of trust in the information sharing network.
Automatically move resources and instantiate controls	The system uses virtualization to allow resources to be moved easily. If a target is under attack, the system automatically moves the attacked resource to a different physical location. At the new location, the system instantiates controls around the resource specific to the type of attack underway.

Challenges

Big data analytics is challenging to implement, even for highly sophisticated security teams. Some of these challenges should lessen as the technology matures. Current challenges include:

- Best-in-class analytics programs typically require specialized expertise. Given the shortage of available experts, many organizations may have to turn to service providers for particular skills. (For guidance regarding the required skill sets, see the first report in the series, Designing a State-of-the Art Extended Team.)
- End-user privacy must be considered when collecting and storing data that can reveal a great deal about individuals and their work and personal habits. This requires organizations to develop competencies in "privacy by design." See the sidebar in Section 3 for further discussion.
- The data warehouse used in an analytics program is a critical resource containing information from security systems and business processes, such as logs and other sensitive data. Therefore it needs effective security controls to protect it. The amalgamation of data into one place creates a new target for cyber criminals.
- Substantial work is required to parse data from various systems so that it can be loaded into the analytics platform.
- The processing power and storage requirements for big data analytics are considerable. Organizations need to ensure they can meet the compute scale requirements and have the necessary platform elasticity in order to handle large surges of data that can take place during an attack.
- Commercial security analytics solutions are not yet pre-configured to handle many common use cases; therefore, much customization is still needed.
- Security analytics requires focused and dedicated resources. To avoid conflicts of interest and situations where employees are shifted to areas such as IT operations, leaving a gap, security monitoring must be separate from other monitoring-like availability.

> Next-generation anti-malware technologies have been adopted by many forward-thinking companies and are expected to go mainstream within the next 18 months.

Next-Gen Anti-Malware: Key Part of Cyber-Defense

Several products have come on the market in recent years that serve to detect and stop malware without relying on signatures. They can be deployed as software or appliances on the network and can be effective against certain types of threats. Next-generation anti-malware technologies are now considered essential parts of cyber-defense strategies.

Malware Analysis

Most next-generation anti-malware technologies detect malware by analyzing patterns of behavior for suspicious characteristics, such as a process trying to execute at a kernel level rather than an application layer. This makes them effective against zero-day attacks that purely signature-based tools cannot detect. Solutions can use the following techniques:

1. Payload analysis: Running incoming traffic in a virtual environment and dropping the traffic before it reaches the endpoint if it appears to be malware.
2. Network analysis: Checking for whether a process is trying to connect to an IP address that is known to be associated with a botnet command-and-control center.
3. Memory analysis: Examining memory on endpoints to determine whether the device is infected.

A key advantage of these solutions is that the time span between malware coming in and detecting it can be dramatically reduced, allowing rapid blocking and cleaning and preventing possible data leakage or other malicious activities. However, a drawback is that these solutions do not completely replace AV solutions; as a result, organizations must continue to operate their existing AV alongside the new technology. Next-generation anti-malware technologies have been adopted by many forward-thinking companies and are expected to go mainstream within the next 18 months.

RALPH SALOMON

Vice President Security, Processes & Compliance Office, SAP Cloud and Infrastructure Delivery, SAP AG

"If you look at APTs, there is a lot of money behind them. To really identify all of the zero-day and APT attacks, organizations definitely need to move to a more proactive approach and invest in analytics and non-signature-based defense technologies."

Game-Changing Investments Required

Leading security teams today are focusing investment on controls that *detect* rather than prevent intrusions. Detective controls are designed to generate alerts that require follow-up in order to distinguish false positives from actual threats and to respond to the threats. This requires a highly qualified staff and robust incident-handling processes for following up on alerts. The need for new skills and processes, and the time needed to respond to incidents, makes the newer analytic and anti-malware technologies more expensive to operate relative to many conventional security technologies.

It can be tempting for some security teams to defer investments in cyber-defense given the expense of advanced detective technologies and the pace of technological change in this area. However, leading security teams are steadfast in choosing to invest now in newer, strategic technologies to protect against cyber-threats. In particular, it is crucial that organizations targeted by advanced persistent threats (APTs), involved in critical infrastructure, or needing to protect valuable intellectual property, implement better cyber-threat detection technologies, including advanced anti-malware solutions and big data analytics. When considering the alternative costs of investigating and recovering from escalating incidents, security teams can often build a strong business case for investing in detective technologies that can discover attacks before they result in significant damage.

These investments should be approached as a key component of a multi-layer defense and protection framework. Advanced anti-malware solutions can be deployed relatively quickly, whereas big data analytics can be a multi-year project. To realize benefits as soon as possible, best-in-class organizations carefully scope the project and maintain momentum. They build their initial system to address a few use cases with a minimal number of data sources, stabilize the system while it is still small, and then add more sources and use cases gradually.

3 Optimizing End-User Experience

Bring-your-own-device programs and cloud computing applications have reshaped user expectations in the corporate landscape. Today's workers have little patience for the archaic user experiences (UX) that are still common in enterprise applications. Many leading security teams consider it a top priority to bring the UX for security systems up to the new bar that has been set by smartphones, tablets, and popular consumer apps.

In information security, better UX has little to do with surface gloss. It primarily means having less in the way: fewer and faster sign-ons; quicker access to data and applications; and the freedom to move between devices, locations, and platforms. It also means minimizing mental effort, such as the need to memorize complex passwords and numerous username/password combinations. Better UX can quickly translate into increased efficiencies for enterprise employees. UX is even more highly valued in customer-facing applications, where it easily pays for itself through increased customer satisfaction. End-user experience is now critical to the success of the security model for both enterprise and consumer applications.

> End–user experience is now critical to the success of the security model for both enterprise and consumer applications.

Analytics Drive Flexible Authentication Methods

A goal for many organizations is to lower the authentication effort required by the typical user by presenting a quick and easy process in low-risk situations and a more challenging process in higher-risk situations. This type of risk-based authentication has already been deployed extensively in consumer banking. For instance, a user on their usual laptop, paying a bill that they pay every month, might go relatively unchallenged, whereas a user attempting to make a large cash transfer using an unfamiliar device would be required to verify their identity. Advanced authentication techniques that use multiple factors for risk-based identification drive higher levels of trust and less user interaction, which makes for more secure transactions and greater end-user satisfaction.

Complex risk calculations

Big data analytics makes more complex risk calculations possible in analyzing aspects of the user and his or her behavior. Many factors can be taken into account to determine the degree of confidence in the user's identity and overall trust level of a transaction, such as the user's physical location, time of access, requested activity, the value of the assets they are trying to access, and the security characteristics of the user's device (e.g., whether it is password-protected or jailbroken). Leading organizations have begun to implement these increasingly sophisticated, risk-based authentication systems for consumer and enterprise applications.

Optimizing the authentication experience often requires trade-offs that can be challenging to manage. The use of analytics requires careful consideration of privacy (see sidebar). But analytics also enables personalization. Some users may opt for two- or three-factor authentication in order to do higher-value transactions online. Others may choose to register their device and allow more intrusive inspection and tracking of their behavior in order to perform transactions without prompts to verify their identity.

Improvements in Identity and Access Management

Recent developments in the area of identity and access management (IAM) are helping to fulfill the long-standing goals of getting new hires, contractors, and partners up and running as quickly as possible, ensuring the right access for roles, and terminating access immediately once it is no longer required. Most IAM systems now provide out-of-the-box connectors to various systems, making them much easier to integrate with authoritative business databases such as HR systems.

Identity brokerage services now enable third-party access to enterprise applications, without the enterprise having to take on the burden of validating the identity or issuing and managing the credentials. Technologies for identity federation have also matured, making it easier to connect enterprises to business partner organizations and cloud providers. However, some security leaders are cautious about whether current enterprise IAM solutions will be suitable as organizations dramatically increase use of public cloud services. Another potential source of disruption for IAM technologies is the growing use of social media logins for federated identity amongst consumer sites, which could spread to the enterprise realm.

PRIVACY AND DATA PROTECTION IMPLICATIONS

Advanced authentication and situational awareness of cyber-threats are both powered by extensive data collection and analytics. The privacy implications for this data will receive increasing attention as the technologies become more widely used.

In a security analytics program, machine data gathered over long periods of time reveals an individual's pattern of work, what applications and device settings he or she uses, where he or she works, and when. In some countries, this data is considered "personal data" and must be protected accordingly. Even if the data is not locally regulated, security teams must find a balance between the usefulness of the user information they can gather and the sensitivities of those users with respect to that data.

The security development lifecycle should embed hooks for designing for privacy, particularly when setting up an analytics program. Consider questions such as the following:

Have promises been made to your customers and/or employees with respect to what types of data you may collect and how that data will be used?

Do you need all the machine data you are collecting?

How secure is the repository where you store the data? Note that when you aggregate data in a big data repository, you lose the controls that were originally on the information and your ability to apply granular controls may be limited.

4 Securing Enterprise Cloud Usage

The impact of cloud computing on enterprise IT is well illustrated by the fact that many companies, big and small, are questioning whether to have their own IT infrastructure or instead use cloud services. Between 2013 and 2017, public IT cloud services are forecasted to have a compound annual growth rate of 23.5%—five times that of the IT industry as a whole.[2]

Amidst this remarkable rate of uptake, the fundamental question for organizations remains, "How do we as an enterprise actually keep control of our data if it is not in our IT infrastructure?"

Security issues only become more difficult to manage as enterprise cloud usage grows. In addition to the concerns that enterprises have always had about the cloud, a relatively new area of attention is the potential vulnerability of cloud-hosted data to government surveillance. In particular, many organizations are reluctant to send sensitive data to cross-border cloud services, where the data could be placed within infrastructure that is monitored by a foreign government.

New Cloud Security Services Promise Visibility and Control

A range of services has recently become available to help solve some of the thorniest security issues related to enterprise cloud usage. Many leading security teams see real promise in these new cloud security services and plan to implement at least one of them over the next year. Overall, the market is predicted to grow from $2.1 billion in 2013 to $3.1 billion in 2015.[3] It's still early days and therefore the jury is still out on whether or not this new crop of cloud security services will be able to fully deliver on their promises. The chart shows some of the promised valuable capabilities.

Cloud Security Issue	Example of New Cloud Security Service Offerings
Shadow IT: Employee usage of cloud services for work without organizational approval	• Analyze enterprise environments to detect what cloud services are being used by employees. Restrict or block usage of certain cloud applications. For example, the security team can disallow sharing of specific documents with certain file-sharing services.
Risk assessment and controls assurance	• Rate the security of individual cloud applications. • Perform continuous controls monitoring on cloud services. • Measure key risk indicators in real time.
Identity and access management	• Conveniently provision and de-provision employee accounts for multiple cloud applications using Active Directory or LDAP accounts. • Enable employees to access multiple cloud-based applications with single sign-on. • Support strong authentication. • Restrict access based on the user's device and geographic location.
Preventing data leakage	• Extend the reach of data leakage prevention (DLP) or information rights management (IRM) to the cloud.
Protection of user credentials	• Provide an audit trail of login attempts and successful application logins. • Analyze user behavior and alert the enterprise if an account appears to be compromised.
Encryption of data in the cloud to meet regulatory requirements or to protect it from surveillance	• Enable encryption of data with an enterprise-controlled key before it is sent to the cloud so that governments or other entities cannot read it without permission from the enterprise. (Some security teams remain skeptical of vendors' claims to provide encryption that is robust while allowing the data to be fully used within cloud-based applications for functionality such as sorting and searching.)

[2] IDC, September 2013

[3] Gartner Research, October 2013

5 Recommendations

The leading security executives of the SBIC were asked to confer on key questions such as:

- What factors do we need to consider when developing a technology strategy?
- How can we get the most value out of the technology we buy?
- What is essential to have in the budget? What could we leave out?
- What are some of the most important aspects of technology planning, acquisition, and deployment?

Based upon their years of experience, these are their top recommendations in trying to meet enterprise requirements in the current, rapidly changing environment.

1. Look at Least Three Years Ahead
2. Achieve a Bigger Picture Through Integration
3. Maximize Value Through Formalized Technology Deployments

1. Look at Least Three Years Ahead

A three-year rolling plan is a useful tool to help focus limited capital on forward-leaning security investments.

Use SWOT Analysis

As part of a regular strategic planning exercise, the security team should forecast the strengths, weaknesses, opportunities, and threats (SWOT) that its organization will be facing one, two, and three years or more from now. These assumptions should guide investments in solutions, with the understanding that confidence in predictions will decline further along the time span.

FIVE STRATEGIES TO STAY AHEAD OF THE CURVE

1 ENSURE THAT YOUR SECURITY program includes a strong architecture voice to counter-balance the tendency for people to advocate for more of the technology that they are used to.

2 FRAME YOUR REQUIREMENTS in terms of what capabilities you need from technology rather than in terms of what existing products or product groups are due to be replaced.

3 WATCH EMERGING SECURITY vendors. Innovative new ideas from startups might not yet be mature enough to deploy at scale, but in two years their solutions could evolve to meet your need.

4 ARTICULATE THE BUSINESS problems that you will need to solve in three years and start now to push vendors to provide the tools you'll need then.

5 SEEK OUT INFORMATION on technology trends from resources such as the Institute for the Future (www.iftf.org).

Consider "threats" broadly, not only security threats but also anything that could negatively affect the business. Opportunities should include advances in security technology that forecast where security technology will be on a one-to-three years' horizon. Also consider disruptive technological advances that will come with technology generally, such as in mobile platforms, cloud computing, the Internet of Things, and consumer identity. How will technology evolve and what risks will it create or change?

Align with both IT and the Business

An organization's overall technology direction will be a major determinant of what security controls and systems will provide the most value. It is essential that security architecture and technology architecture teams tightly coordinate their planning efforts. In some companies, one person is the overall head of both functions. In others, there are two separate teams but they work in lockstep.

Any successful security strategy must also map to the business. The security team must successfully demonstrate how its vision not only aligns, but enables, business strategy.

Create an Enterprise-wide Big Data Strategy

A key area for technology alignment is in creating an overall big data strategy for the enterprise. In many cases, the logs from IT infrastructure, databases, and business applications that are valuable for security are also useful to IT and other business units. Big data analytics can benefit a wide variety of business processes ranging from IT support to optimizing the manufacturing supply chain. In companies with a commitment to an analytics program, the Chief Information Officer generally drives strategies to centralize big data and to optimize its use overall in the enterprise – having some of the data in a silo for one department will not work. The security team is in a position to help define the overall big data strategy for an enterprise because it is likely to have some of the first use cases. Ensure that when choosing technologies and partners, the solution provides a path towards an enterprise-wide big data strategy. Big data technologies that are specific to security might meet the functional requirements of the security team but at the cost of losing an opportunity to enable broader business objectives.

Big data analytics can benefit a wide variety of business processes ranging from IT support to optimizing the manufacturing supply chain.

Big data adoption offers a significant competitive advantage, not only through better threat detection, but by way of deeper market insight, tailored customer service, and valuable operational intelligence. It's vital that information security teams develop new security controls to allow for the fast adoption of big data techniques enterprise-wide while ensuring the protection of the company's big data assets.

> *If you want to be forward-leaning, you need a very strong architecture voice. You need your team looking out on a three-year horizon. You have to be willing to make bets on where you think technology will land.*

KENNETH HAERTLING,
Vice President and Chief Security Officer,
TELUS

Get Auditors Engaged

If you work with external auditors, keep them abreast of the new technologies you will be implementing over your three-year plan. The audit frameworks that companies are graded against typically come from security textbooks that could be three or more years old. If you want your use of newer technology to be accepted, it is helpful to regularly re-educate your auditors and keep them up-to-date with technology. Storing regulated information in the cloud, such as payment card industry (PCI) data, is a particularly challenging issue, because even if the cloud environment is more secure than what it replaces, auditors may not know how to confirm that it is secure.

If you are considering using cloud technology or virtualization in a way that could pose difficulties with audits, develop a partnership with your auditors well in advance to establish meaningful audit criteria. In the meantime, plan moves to the cloud in a graduated fashion. One leading organization meets quarterly with its auditors to try to resolve issues around cloud usage, with the goal of storing regulated data in the cloud by 2015.

2. Achieve a Bigger Picture Through Integration

When investing in security technologies today, the greatest payoffs often come from connecting and consolidating multiple applications. Most security organizations get a fraction of the potential value from the security data that they have because it tends to stay inside dozens of siloed applications that were not designed to work together.

Technologies are now available which make it easier to meaningfully integrate systems. For example, big data analytics; security intelligence; and Governance, Risk, and Compliance (GRC) platforms now provide a path to more fully integrate threat detection or risk management with business applications or prevention technologies. The following examples illustrate integration of:

Business process data with security data warehouse

To incorporate real business context into security events, a leading organization recognized that it needed to analyze data from not only security systems, but also business applications and databases. It created a common logging service to feed relevant data from business applications into its security data warehouse. Analysts following up on incidents can now see a comprehensive view of the business environment, enabling them to complete investigations more quickly and thoroughly.

Real-time application testing with security intelligence platform

Dynamic Application Security Testing (DAST) systems check live web applications for security flaws. A leading organization has integrated its DAST system with its firewall via its Security Intelligence Platform (SIP), enabling the firewall to provide optimal protection to web applications. If the DAST system finds a flaw in an application, it categorizes the type of vulnerability according to the National Vulnerabilities Database and passes a vulnerability index number to the SIP. The SIP sends the firewall the name of the flawed application, its IP, and the vulnerability index number. This tells the firewall that a particular application has a flaw and can be attacked by a certain kind of malware or protocol. The firewall, knowing what type of traffic is a threat, blocks that type of traffic to that application.

GRC with project management

Business units must be able to view all of the information security risks associated with their business processes holistically, in order to manage all of them. To meet this objective, some leading organizations are implementing GRC tools with project management systems so that for all new projects, a risk assessment will be automatically requested. As projects continue through their lifecycles, the business units can keep track of overall risks as they change or are remediated.

GRC with mobile devices

A leading organization has developed a mobile app that gives personalized views of risks in the enterprise GRC system. Board members and staff can access the app via an iPad or other mobile device and see a list of risks that are in their area of responsibility or that are assigned to them. They can also use the app to drill down into details on particular risks, such as what has been done to mitigate the risk and what its current status is.

Systems are often not designed to connect seamlessly out-of-the-box, therefore integrating them can be challenging. For example, fully implementing a Security Intelligence Platform with every application, firewall, access control, and so on is an effort comparable in scale to deploying an enterprise resource planning (ERP) system, but it results in an integrated system that is far more powerful than the sum of its parts. To reap the rewards of advancements in security technologies today, keep a mindset of favoring solutions that can be part of an integrated architecture and use point solutions only where necessary to meet niche requirements.

> *"Security organizations need to look at the security solutions that they have in place today most of which are not connected or talk to each other and figure out, how do we consolidate these technologies? How do we integrate them to give us context, make things more actionable, and get an aggregated view?"*

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

3. Maximize Value Through Formalized Technology Deployments

Even with the most perceptive radar for new products, deploying technology effectively is a huge challenge. Given the current pace of technological change, getting a system fully implemented can take so long that technology might have advanced measurably by the time the project is complete. New products, selected with care and attention, do not always live up to expectations. And with limited budgets, it's difficult to keep day-to-day operations going, let alone keep up with exciting technological developments or the long-term business strategy. Leading security teams, familiar with these pitfalls, advise having formal approaches to deployment in order to proactively manage the risks.

Have formal approaches to deployment in order to proactively manage the risks.

Predict and Track Total Costs and Total Value

One of the most common causes of technology failure is not planning for how much the technology will cost to operate. Having appropriately trained professionals running security technology is critical to its success and is often expensive due to the expertise involved. Before investing in any new technology, be sure you understand the total cost of ownership and have an ongoing operating budget for its lifecycle.

A formal process to articulate and track expected costs and benefits can also help security teams to work with vendors to maximize success with the vendor's product. Make sure vendor contracts define what value the product should be delivering in a specified time period, say six months, and then conduct a review. If after the six-month time period, an organization has not seen the expected value or if they have encountered unexpected costs, they should have a process to ask, "Is the problem with us? With the technology? With the way we deployed it?" and enter into a remediation phase. After nine to 12 months, if the organization is still not seeing the value expected, consider options that include parting ways with the vendor, reducing payment, or deploying the technology differently.

Scale Deployments for Quick Wins

Many organizations have found that trying to do all-at-once, "big bang" deployments in a large enterprise is too slow and expensive. To meet the challenge of keeping up with technology change while still deploying something that will make a difference to the business, look for ways to make initial deployments smaller. Can you deploy a new anti-malware control to only certain critical data assets that need it the most? Is there an opportunity to gain momentum by having a single team or department use a new authentication system? If the technology proves itself in a small implementation, it can grow organically to wider use.

Employ Judicious Cloud Vendor Management

Formalized processes are not only key for the deployment of on-premises technologies. As organizations adopt more cloud security service providers, it is critical that these vendor engagements are judiciously managed. Carefully consider how to assess the trustworthiness of cloud security services.

This includes monitoring the effectiveness of security controls on an ongoing basis using evidence-based controls assurance. (See the second report of this series, Future-Proofing Processes.) Organizations will need to set up agreements requiring the vendor to regularly provide evidence that its controls are working. With new features and competitors emerging frequently amongst cloud security services, organizations must also consider the possibility that they will need to change providers down the road and therefore must have an exit strategy upfront.

> *"With limited budget, it's a balancing act. You have to reduce the costs of the existing security infrastructure while still keeping the risks to an acceptable level and then use the savings to invest into some of the new technologies."*

PETRI KUIVALA
Chief Information Security Officer,
Nokia

Approach Maintenance Strategically

All teams want better versions of the technology that they already know. Some security team members would prefer to keep running AV, for instance, if that is where their expertise is. To conserve limited capital for moving technology forward, push back on this natural tendency and look critically at how much the security team is investing in upgrades and point releases for existing technology. For example, ask yourself whether you can accept the risks of not doing every software update or hardware upgrade for older technologies that may be reaching end-of-life. Strategic cost-cutting can free up resources to get more advanced technologies in place.

Conclusion

Information security teams are implementing leading-edge technologies in order to turn the tide against advanced attacks and enable business innovation. As security teams map out their strategies, it's not sufficient to pick the right technologies. To get the most value, they must also develop comprehensive, multi-year plans to integrate new technologies with the organization's existing infrastructure. Building out a multi-layer defense and protection framework takes deep understanding of the business environment and the critical assets that need protecting, as well as knowledge of the specific threats the organization faces. Successful technology deployments are supported by robust processes that leverage the new tools and a staff capable of operating them. The SBIC's "Transforming Information Security" series provides a route to successfully protect today's enterprises, by advancing and aligning people, processes, and technologies.

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.

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**

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

RALPH SALOMON CRISC
Vice President Security, Processes & Compliance Office, SAP Cloud and Infrastructure Delivery, **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
Office of the Chief Information Security Officer,
eBay

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*

EMC^2

RSA