BIG DATA FUELS INTELLIGENCE-DRIVEN SECURITY

Rapid growth in security information creates new capabilities to defend against the unknown

AUTHORS

Sam Curry, Chief Technology Officer, Identity and Data Protection business unit; Chief Technologist, RSA, The Security Division of EMC

Engin Kirda, Sy and Laurie Sternberg Associate Professor of Information Assurance, Northeastern University

Eddie Schwartz, Vice President and CISO, RSA, The Security Division of EMC

William H. Stewart, Senior Vice President, Booz Allen Hamilton

Amit Yoran, General Manager, Security Management and Compliance business unit; Senior Vice President, RSA, The Security Division of EMC

January 2013

WHAT IS BIG DATA?

Big data describes data sets that are too large, too unrefined or too fast-changing for analysis using relational or multidimensional database techniques. Analyzing big data can require dozens, hundreds or even thousands of servers running massively parallel software. What truly distinguishes big data, aside from its volume and variety, is the potential to analyze it to uncover new insights to optimize decision-making.

KEY POINTS

- The dissolution of traditional defensive perimeters coupled with attackers' abilities to circumvent traditional security systems requires organizations to adopt an intelligence-driven security model that is more risk-aware, contextual, and agile.
- Intelligence-driven security relies on big data analytics. Big data encompasses both the breadth of sources and the information depth needed for programs to assess risks accurately and to defend against illicit activity and advanced cyber threats.
- Within the next two years, we predict big data analytics will disrupt the status quo in most information security product segments, including SIEM; network monitoring; user authentication and authorization; identity management; fraud detection; and governance, risk & compliance.
- In the next three to five years, we predict data analytics tools will further evolve to enable a range of advanced predictive capabilities and automated real-time controls.
- Integrating big data analytics into business risk management and security operations will require organizations to rethink how information security programs are developed and executed. Six recommendations are presented in the section titled Building a Big Data Security Program.
- Security teams need analysts who combine data science with a deep understanding of business risks and cyber-attack techniques. Personnel with these skill sets are scarce, and they will remain in high demand. As a result, many organizations are likely turn to outside partners to supplement internal security analytics capabilities.

Contents

RSA Security Briefs provide strategic insight and technical guidance on today's high-stakes digital information risks and opportunities. This Brief is written by subject matter experts with deep technical knowledge and with broad exposure to how leading-edge organizations manage information security risks. Providing both big-picture context and practical technology advice, RSA Security Briefs are vital reading for today's forward-thinking security executives.

MOVING TO INTELLIGENCE-DRIVEN SECURITY

Intelligence-driven security is a modernized approach to security advocated by the Security for Business Innovation Council, a group of top security executives from Global 1000 enterprises that publish recommendations to advance the practice of information security worldwide. In an intelligence-driven security program, organizations evaluate all the security-related information available to them, both internally and externally, to maintain the visibility and control needed to protect an organization's most valued information assets. For guidance on implementing intelligence-driven security programs, please read the Council's report "Getting Ahead of Advanced Threats: Achieving Intelligence-driven Information Security" available on RSA.com.

BIG DATA HOLDS BIG PROMISE FOR SECURITY

Big data is transforming the global business landscape. Organizations are analyzing huge volumes of diverse, fast-changing data to gain new insights that help them run their businesses better and get an advantage over the competition. In the same way that big data has transformed competitive dynamics in industries from retail to biotech, we expect it will also transform the information security sector. Big data's new role in security comes at a time when organizations confront unprecedented information risk arising from two conditions:

1. Dissolving network boundaries – As organizations open and extend their data networks – allowing partners, suppliers and customers to access corporate information in new, dynamic ways in order to push collaboration and innovation – they become more vulnerable to data misuse and theft. Corporate applications and data are also increasingly accessed through cloud services and mobile devices, shattering what's left of enterprise network boundaries and introducing new information risks and threat vectors.

2. More sophisticated adversaries – Cyber attackers have become more adept at waging highly targeted, complex attacks that evade traditional defenses, static threat detection measures and signature-based tools. Oftentimes, cyber attacks or fraud schemes perpetrated by advanced adversaries aren't detected until well after damage has been done.

The dissolution of traditional defensive perimeters coupled with attackers' abilities to circumvent traditional security systems requires organizations to reinvent their security approach. In today's hyper-extended, cloud-based, highly mobile business world, security approaches solely reliant on perimeter defenses—or that require predetermined knowledge of the threat or direct control over all infrastructure elements—are being made obsolete. Instead, a more agile approach based on dynamic risk assessments, the analysis of vast volumes of data and real-time security operations will be essential to providing meaningful security.

The Security for Business Innovation Council advises organizations to move to an intelligence-driven security model, which relies on security-related information from internal and external sources to deliver a comprehensive picture of risk and security vulnerabilities. (See sidebar titled Moving to Intelligence-driven Security.) As part of modernizing information security programs, organizations will have to reduce their reliance on signature-based scanning tools, which only detect limited-scope threats that have been encountered in the past. Instead, organizations need to cultivate security capabilities that will ultimately help them detect the unknown and predict threats in the future.

To move in this direction, organizations must gain full visibility into the security conditions of all IT assets handling valuable information. Today, however, most organizations effectively capture and analyze only a relatively small slice of security-related information. Such information sources include network logs, SIEM system alerts and application access records. Many sources of security-related information have not been used in security operations because their data formats are too variable and unpredictable, the data sets are perceived to be too large and/or the data changes too quickly. Now, with recent advancements in computing power, storage systems, database management and analytics frameworks, no data set is too big or too fast. Information such as full packet capture, external threat intelligence feeds, website clickstreams, Microsoft® Outlook® calendars and social media activity can be used for security–related analysis.

Author Commentary

"Intelligence-driven security reinforces the idea that no man is an island. When organizations combine outside information with all of their own data that's available to them they start to see a more informed view of threats. They correlate and detect faint signals that they couldn't see before. Tremendous value can be generated when all information within an enterprise with security relevance gets collected, organized, analyzed and leveraged."

—Eddie Schwartz
RSA, The Security Division of EMC

Despite the challenges of normalizing vast amounts of information from such diverse and dynamic sources, big data will play an increasingly important role in security. By incorporating big data into security programs, organizations gain richer context for assessing risk and learning what's "normal" for a particular user, group, business process or computing environment. As organizations develop fuller, more nuanced profiles of both systems and users, security teams can enhance their ability to spot aberrant activity or behaviors, which often indicate deeper problems.

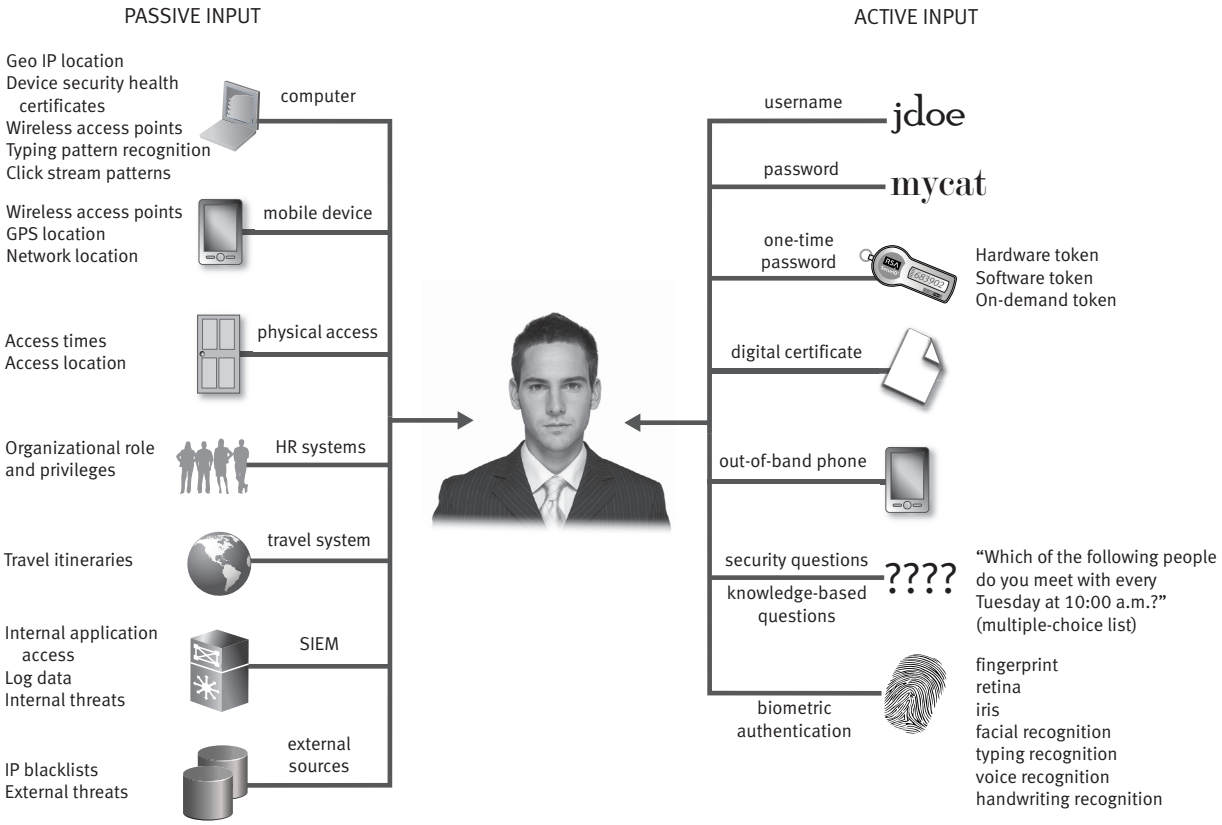
Big data analytics is expected to emerge as the cornerstone of an intelligence-driven security program for preventing, and even predicting, high-stakes security threats. In fact, the integration of big data into security tools represents a sea change in how information security programs may be designed and executed.

MORE DATA MEANS MORE SECURITY

In an intelligence-driven security model, the definition of "security data" expands considerably. In this new model, security data encompasses any type of information that could contribute to a 360-degree view of the organization and its possible business risks. For an illustration of how diverse information with security applications can be, Figure 1 charts data sources that could be mined by identity and access management systems in the near future.

Because potential sources of security-related data are nearly endless, intelligence-driven security models require scalable, big data architectures to be in place to store and manage all of the information that could prove helpful. Big data infrastructures will vary depending on each organization's unique business requirements and relevant data sources. While optimizing big data platforms is important, the information will yield no insight if organizations cannot integrate data and apply the right analytical techniques and context. Different methods of analysis can be applied to make smarter, more

Figure 1: Big data enhances identity verification



targeted types of decisions. Once these analytics are finely tuned, they can inform controls on the network to take action: lock accounts down, quarantine systems, change network device settings, require a second form of authentication, or tip off a fraud-monitoring system, for example. This increased automation reduces the workload for security analysts while accelerating the identification and mitigation of security threats.

When big data drives security, the result is a unified, self-evolving approach and a holistic awareness that discrete, stitched-together solutions can't begin to achieve. A big data-driven security model has the following characteristics:

- **Diverse data sources** – both internal and external – that multiply in value and create a synergistic learning effect as new security-related information is added
- **Automated tools** that collect diverse data types and normalize them so they're usable by analytics engines
- **Analytics engines** capable of processing vast volumes of fast-changing data in real time
- **Advanced monitoring systems** that continuously examine high-value systems and resources and make assessments based on behavior and risk models, not on static threat signatures
- **Active controls** such as requiring additional user authentication, blocking data transmissions or facilitating analysts' decision-making when high-risk activity is detected
- **Centralized warehouse** where all security-related data is made available for security analysts to query, either as a unified repository or, more likely, as a cross-indexed series of data stores
- **Standardized views** into indicators of compromise that are created in machine-readable form and can be shared at scale by trusted sources
- **N-tier infrastructures** that create scalability across vectors such as geography, storage and databases and have the ability to process large and complex searches and queries
- **High degree of integration** with security- and risk-management tools to facilitate detailed investigations of potential problems by analysts and to trigger automated defensive measures such as blocking network traffic, quarantining systems or requiring additional verification of user identity

When big data drives security, the result is greatly enhanced visibility into IT environments and the ability to distinguish suspicious from normal activities to inspire trust in our IT systems.

Author Commentary

"Collecting big data is the easy part. Understanding the data is the hard part. It's best to start out working on a sub-problem: for example pinpoint the command and control center of a botnet, and then take that information and correlate it against, say, connection information in your organization, to get better situational awareness."

– Engin Kirda,
Northeastern University

Author Commentary

"The game is changing. More and more data is going onto the Internet in automated forms, and that vector will continue. Therefore a security analysis tool that worked great two or three years ago doesn't work so well anymore. You now have to look through a whole lot more data, and you have to look for threats that are far more subtle. Commercial tools are changing to take advantage of these big data streams coming online."

– William H. Stewart, Booz Allen Hamilton

BIG DATA TRANSFORMS SECURITY APPROACHES

The quality and value of insight that can be derived from big data analytics is expected to spur dramatic changes in almost every discipline within information security. The changes have already begun, with an immediate need for advanced analytics arising in threat monitoring and incident investigations. These processes draw information from a variety of sources, analyzing both fresh and archived data to get a fuller, deeper view of security conditions (see Figure 2).

Leading-edge security operations centers (SOCs)—especially those in defense and financial services organizations—are already discovering value from applying analytics to large sets of security data. They're analyzing massive archives of security data to understand attackers' techniques and to uncover subtle indicators that could help identify hidden threats faster, track cyber adversaries and perhaps even predict future attacks. They're applying fraud analysis techniques to reduce unauthorized access to user accounts and corporate resources.

While big data analytics tools for security were often custom-built in the past, this year leading security organizations will deploy commercial, off-the-shelf big data solutions in their SOCs. Within two years, we predict big data analytics will have disruptive impact on many categories in the information security sector, including SIEM; network monitoring; user authentication and authorization; identity management; fraud detection; and governance, risk and compliance systems. Longer term, big data is also expected to change the nature of conventional security controls such as anti-malware, data loss prevention and firewalls—essentially the entire security spectrum.

Figure 2: Security investigations rely on big data

Network/Host Traffic

Are there traffic anomalies to/from these servers?
- *Protocol distribution?*
- *Encryption?*
- *Suspicious destinations?*

Potential sources:
- SIEM
- Network monitoring
- Application monitoriing

Web Transactions

Has suspicious activity been observed in sensitive/ high value applications and assets?

Potential sources:
- Authentication data
- Transaction monitoring
- Application logs
- SQL server logs
- Network session data

Infrastructure

Has the server been manipulated?

Is it vulnerable? Has its configuration changed recently?

Is it compliant with policy?

Potential sources:
- IT assets
- GRC systems
- Configuration management
- Vulnerability management

Information

What kind of data does this system store, transmit, process?

Is this regulated information? High-value IP?

Potential sources:
- DLP
- Data classification
- GRC systems

Identity

Which users are logged in?

Have their privileges been escalated?

Where did they log in?

What other assets did these users touch?

Potential sources:
- Authentication data
- Microsoft Active Directory®
- Server logs
- Asset management
- SIEM
- Network monitoring

Author Commentary

"In the coming year, top-tier enterprises with progressive security capabilities will adopt intelligence-driven security models based on big data analytics. Over the next two to three years, this security model will become a way of life."

—Eddie Schwartz
RSA, The Security Division of EMC

Security management

SIEM and network monitoring capabilities have begun converging, creating a security analytics platform capable of massive and diverse real-time data collection and threat analysis. Security management driven by big-data analysis creates a unified view of multiple data sources and centralizes threat research capabilities, instead of forcing security analysts to deal with disparate tools that disrupt and potentially derail their workflows. The convergence of SIEM and network monitoring capabilities creates a unified security management system to assimilate all information that could possibly inform security. It ingests external threat intelligence and also offers the flexibility to integrate security data from existing technologies. Data processing happens on a much grander scale: today in the SIEM space, tools are capable of correlating thousands of events per second; going forward, security management platforms will correlate hundreds of thousands, even millions, of events per second without the need to expand the hardware footprint.

Identity and access management (IAM)

Next-generation tools enable risk-based, adaptive identity controls that continuously evaluate and adjust the level of protection and access based on asset criticality and risk. By enabling situation-aware IAM, such tools provide continuous risk assessment of user activity, especially when accessing sensitive resources, even after initial authentication. Profiles are based on historical behavior; a deep, complex user profile; a richer view of identities and a data-driven perspective of what normal behavior looks like.

Provisioning is done on demand, based on enforcement policies that are created on the fly. Today, access control is based on rigid policies that say this person is allowed to do specific things. Next-generation access control systems acknowledge that an organization can't foresee all possible scenarios and instead allows operators to describe the kind of behavior that's desired, with the system working out the related rules.

Fraud prevention

Whether it's financial fraud, transaction fraud or the fraudulent use of corporate resources, advanced security technologies analyze massive amounts of behavioral data and other diverse indicators to distinguish between malicious and legitimate business activities. We predict that session intelligence and behavioral and click-stream analysis will combine to stop business logic abuse in which attackers find a flaw in the functioning of an IT-based system and exploit it for illicit gain.

Governance, risk and compliance (GRC)

As organizations expand the scope of their GRC programs—bridging organizational siloes and business functions with a unified GRC system—the amount of data that such systems can handle will need to grow exponentially. We predict that GRC platforms will evolve to provide real-time access to the entirety of information relevant to understanding business risks and to prioritizing security activities. They'll analyze larger volumes of data to facilitate better, smarter decisions about the level, sources and criticalities of risk facing an organization. They'll also inform SOCs about valuable assets that are at high levels of risk and help prioritize steps that an organization should take to mitigate those risks.

In addition to transforming existing categories of security tools, we also believe that big data will inspire the development of new tools that have yet to be conceived. Tools driven by big data security analytics will inform where and when to apply controls—or how to change them—to better protect information, identities and infrastructure.

Author Commentary

"Until very recently in security we've had to do all sorts of complicated things to filter, preprocess and ultimately reduce our visibility to get down to a manageable data set, perform analytics and make decisions. But with extremely high-speed, scalable big data platforms, we have a much richer set of visibility tools to begin the whole security process. Once you have the data in the platform, you can then go through a number of different analytical methods and techniques, based on what you're trying to accomplish."

– Amit Yoran
RSA, The Security Division of EMC

BUILDING A BIG DATA SECURITY PROGRAM

Integrating big data analytics into security operations—the cornerstone of an intelligence-driven security model—will require organizations to rethink how security programs are developed and executed. In updating security programs to take advantage of big data, organizations should consider the following steps:

1. Set a holistic cyber security strategy – Organizations should align their security capabilities behind a holistic cyber security strategy and program that's customized for the organization's specific risks, threats and requirements. The security strategy should integrate big data analytics as part of a broader array of technical solutions, combined with tailored processes and expert staff. In most cases, a detailed assessment of an organization's current security posture, including an industry peer comparison, lays the groundwork for an effective cyber security program.

2. Establish a shared data architecture for security information – Because big data analytics require information to be collected from various sources in many different formats, a single architecture that allows all information to be captured, indexed, normalized, analyzed and shared is a logical goal.

3. Migrate from point products to a unified security architecture – Developing a unified security analytics framework will require a big-picture, more disciplined approach to security investments than most organizations have shown in the past. Organizations need to think strategically about which security products they will continue to support and use over several years, because each product will introduce its own data structure that must be integrated into a unified analytics framework for security—or deliberately omitted as a potential blind spot. In many cases, the TCO benefits of unifying the data architecture for security analytics may outweigh the benefits of preserving existing point products. Conversely, if a particular product isn't compatible with a given security data architecture, it's unlikely to deliver long-term value.

4. Look for open and scalable big data security tools – Organizations should ensure that ongoing investments in security products favor technologies using agile analytics-based approaches, not static tools based on threat signatures or network boundaries. New, big data-ready tools should offer the architectural flexibility to change as the business, IT or threat landscape evolves.

5. Strengthen the SOC's data science skills – While emerging security solutions will be big data ready, security teams may not be. Data analytics is an area where on-staff talent is lacking: a recent survey conducted by IDC-Computerworld of analytics professionals found that 70 percent identified "lack of a sufficient number of staff with analytics skills" as a key challenge to delivering a successful business intelligence and analytics solution in their organizations.[1] Security leaders should consider adding data scientists to their teams. Such specialists will not only need to manage the organization's big data capabilities efficiently, but they will also need to understand business risks and cyber-attack techniques in sufficient depth to develop analytical models that detect, and even predict, illicit activities. Data scientists with specialized knowledge in security are scarce, and they will remain in high demand. As a result, many organizations are likely turn to outside partners to supplement internal security analytics capabilities.

6. Leverage external threat intelligence – Augment internal security analytics programs with external threat intelligence services. Often threat indicators, attack forensics or intelligence feeds from outside sources are not machine-readable and require extensive manual processing by SOC analysts. SOCs should evaluate service providers aggregating threat data from many trustworthy, relevant sources. Data from these sources should be in formats that can be automatically ingested by security analytics platforms for correlation with internal data.

Author Commentary

"Defending against sophisticated adversaries requires advanced analytics to help narrow the field and focus around advanced threats. This technology is necessary to help analysts solve the hardest security problems. You're reacting to a mind and a person, and therefore you need creative and empowered people to defend yourself. Analytics tools inform analysts, provide scale and identify patterns of behavior too subtle to be otherwise observed."

– William H. Stewart
Booz Allen Hamilton

[1] IDC Link: Analytics Education – Does One Size Fit All?, Doc #lcUS23882612, December 2012

Author Commentary

"Traditional security controls are like a machine that you put a recipe into and they always make exactly the thing that you ask for. The new security world is like looking in your fridge and having it tell you, based on what's available, what would taste good and then it makes it for you. For example, think about adaptive access control, cutting off the bad guys before they have even gotten into the network because you can tell where they're going to be. That's cool stuff."

– Sam Curry
RSA, The Security Division of EMC

LOOKING AHEAD: BIG DATA IN FIVE YEARS?

If many information security products are enhanced with big data analytics within the next couple of years, what will happen down the road when such products take root and are broadly deployed? In the next three to five years, we predict data analytics tools will advance rapidly and enable the following security capabilities:

- Security analysts will be able to use tools with intuitive interfaces to spot relationships among data sets and create correlations that build upon themselves, painting the most complete security picture possible.
- SOCs will gain the requisite expertise, processes and tools to make the most of the security data available to them. They consistently collect data from the right internal and external sources and use analytics to detect many, if not most, attacks and prevent unwanted outcomes. Some SOCs will develop advanced data models that are accurate enough to predict certain types of cyber attacks.
- Data analytics systems will empower users with decision-support capabilities at crucial times—usually before damage can be done. Analytics systems will inform real-time decision making, triggering automated tools such as risk-aware user authentication systems or notifying SOC analysts so they can take action based on detailed reports of what's happening in the moment.
- Security management tools will automatically share relevant threat data with trusted partners and creatively reuse big data in different security scenarios.

Big data analytics, when used within an intelligence-driven security program, automates many risk assessments and threat detection processes and puts the advantage of time back in an organization's hands. Big data analytics also help enhance situational awareness and shorten reaction times to potential risks and problems. We believe it will prove instrumental in helping the global security community bring about a more trusted digital world.

About the Authors

Sam Curry
Chief Technology Officer, Identity and Data Protection business unit
Chief Technologist
RSA, The Security Division of EMC

Sam Curry has more than 20 years of experience in security product management and development, marketing, engineering, quality assurance, customer support and sales. His experience also includes cryptography and research, and he is a regular contributor to a number or journals and periodicals. Prior to his current role, Mr. Curry was CTO, Marketing and Vice President of Product Management at RSA, charged with leading the strategic direction for all RSA solutions. Before joining RSA, Mr. Curry was Vice President of Product Management and Marketing for a broad information security management portfolio at CA. Previously, Mr. Curry served as Chief Security Architect and led Product Marketing and Product Management at McAfee. He holds degrees in English and Physics from the University of Massachusetts and from Mount Allison University and has founded successful security startups.

Engin Kirda
The Sy and Laurie Sternberg Associate Professor of Information Assurance
Northeastern University

Engin Kirda is the Sy and Laurie Sternberg Associate Professor of Information Assurance at Northeastern University and also holds the position of director of the Northeastern Information Assurance Institute. Previously, Dr. Kirda held faculty positions at Institute Eurécom on the French Riviera and the Technical University of Vienna, where he co-founded the Secure Systems Lab that is now distributed across five institutions in the U.S. and Europe. Dr. Kirda is interested in systems, software and network security with specific focus on web security, binary analysis and malware detection. He is a co-founder and Director of Research at Lastline, a company specializing in advanced threat detection based on cutting-edge research conducted at Northeastern University.

Eddie Schwartz
Vice President and Chief Information Security Officer
RSA, The Security Division of EMC

Eddie Schwartz is Chief Information Security Officer for RSA and has 25 years of experience in the information security field. Previously, he was Co-Founder and Chief Security Officer of NetWitness (acquired by EMC), CTO of ManTech, EVP and General Manager of Global Integrity (acquired by INS), SVP of Operations of Guardent (acquired by VeriSign), CISO of Nationwide Insurance, a Senior Computer Scientist at CSC, and a Foreign Service Officer with the U.S. Department of State. Mr. Schwartz has advised a number of early stage security companies, and served on the Executive Committee for the Banking Information Technology Secretariat (BITS). Mr. Schwartz has a B.I.S. in Information Security Management and an M.S. in Information Technology Management from the George Mason University School of Management.

William H. Stewart
Senior Vice President
Booz Allen Hamilton

William Stewart is a Booz Allen Hamilton senior vice president with more than 25 years of professional experience designing, developing and deploying cyber solutions. In his current role, he leads the Cyber Technology Center of Excellence (COE), which includes more than 3,000 staff and provides consulting and systems integration expertise to public and private sector clients. Mr. Stewart and his team offer strategy and implementation for today's most complex security problems. Prior to joining Booz Allen Hamilton, Mr. Stewart worked for a major electronics firm and also served as a signal officer in the U.S. Army. Mr. Stewart holds a MS in Electrical Engineering from Drexel University and a BS in Engineering from Widener University.

Amit Yoran
Senior Vice President
General Manager, Security Management & Compliance business unit
RSA, The Security Division of EMC

Amit Yoran oversees RSA's Security Management and Compliance business unit. He is a Commissioner of the CSIS Commission on Cyber Security advising the 44th Presidency and serves on several industry and national advisory bodies. Mr. Yoran came to RSA through EMC's acquisition of NetWitness in 2011. Prior to NetWitness, Mr. Yoran served as Director of the National Cyber Security Division at the Department of Homeland Security. Formerly, he served as the Vice President of Worldwide Managed Security Services at the Symantec Corporation. Mr. Yoran was the co-founder of Riptech, a market-leading IT security company, and served as its CEO until the company was acquired by Symantec in 2002. He also served as an officer in the U.S. Air Force in the Department of Defense's Computer Emergency Response Team. Mr. Yoran received a Master of Science degree from the George Washington University, a Bachelor of Science from the United States Military Academy at West Point, and an honorary Doctorate from the University of Advancing Technology.

SECURITY SOLUTIONS & PROGRAMS

The offerings described below align with the recommendations presented in this RSA Security Brief. The following overview of products and programs is not intended to provide a comprehensive list of applicable solutions. Rather, it's intended to serve as a starting point for security technology practitioners and compliance officers wanting to learn about some of the options available to them.

From Booz Allen Hamilton

Booz Allen Hamilton (Booz Allen) helps clients evolve cyber security programs to reduce risk to their business operations and critical digital assets posed by increasingly severe cyber threats. Booz Allen's approach is informed by a deep understanding of sophisticated adversary behavior, anchored by the current state of the art in cyber security technology and practice, and balanced with a strong focus on clients' business needs. Booz Allen's Intelligence Driven Dynamic Defense Framework helps clients shift from largely static, perimeter-based cyber defenses to active, operationally focused capabilities that employ big data analytics capable of anticipating and reacting to evolving threats.

Booz Allen's Intelligence Driven Dynamic Defense Framework includes the following offerings:

Threat Intelligence: Booz Allen's Cyber4Sight™ managed service delivers predictive cyber threat intelligence 24 hours a day, 7 days a week. Cyber4Sight delivers near-real-time cyber threat intelligence to protect clients' entire business operations across the global Internet. The service correlates anomalies observed within our clients' networks with the techniques, motivations, objectives and intentions seen in human cyber threat actors across the globe.

Incident Response: Booz Allen provides full-suite triage capabilities, with experts in critical response delivering effective solutions for DDoS, insider threats, advanced persistent threat compromises and other security breaches. Incident response services are often enhanced with Automated First Responder (AFR), a non-signature-based approach to uncovering an adversary's presence, threat origins, and the methods for controlling and remediating attackers' activities while preventing further intrusions.

Preemptive Response: Booz Allen leverages its long heritage as a management and technology consulting firm to help clients gain a greater understanding of the business challenges and opportunities related to cyber security programs. Our preemptive response services are built around our Cyber M3: Measure, Manage, and Mature model. Booz Allen offers a range of Cyber M3 diagnostic and strategy services to help clients advance their security capabilities. At the premier level, services help clients: 1) create holistic cyber security programs aligned with business needs, 2) develop a balanced portfolio of complementary capabilities, and 3) prioritize how to satisfy the diverse needs of stakeholders through justifiable resource expenditures.

Integrated Remediation: Booz Allen uses a multi-disciplinary approach encompassing policy, operations, technologies, management and people to synchronize remediation efforts. This ensures that cyber protection is fully integrated and effectively achieved. Booz Allen services range from "design" partnerships, in which Booz Allen experts work hand-in-hand with clients to develop comprehensive capabilities (e.g., End-to-End Hunt Team Operational Operating Models), to "implementation" engagements, in which Booz Allen provides world-class services in execution and delivery of cyber services (e.g., PKI solution integrations, network segmentations, etc.).

From Northeastern University

Northeastern University offers Master of Science and Ph.D. programs in Information Assurance (IA). The specialized field of IA protects information systems by ensuring data privacy and integrity, user authenticity and legitimate use of system resources. IA professionals understand the relationships between information technology and people, systems, society, policy and law. Northeastern University's interdisciplinary IA programs are offered jointly by the College of Computer and Information Science, the College of Engineering and the College of Social Sciences and Humanities and are the only such programs in New England. Program graduates typically work in government agencies, as well as in commercial and financial organizations. The National Security Agency/Department of Homeland Security has designated Northeastern University as a Center of Academic Excellence in Information Assurance Research and Education.

From RSA

RSA® Adaptive Authentication, with its advanced self-learning risk engine, calculates a risk score based on the user behavior profile, the device profile and the eFraudNetwork™ match. This risk score is provided to a policy engine and the user is either granted access, required to provide an alternate authentication credential or denied access. RSA Adaptive Authentication is a proven solution protecting thousands of organizations and users worldwide today.

The RSA® Advanced Cyber Defense Practice provides a complete range of innovative consulting and professional services to organizations needing to mitigate cyber threats while pursuing their business objectives. Using RSA's proven Total Threat Visibility & Mitigation methodology, practice consultants help organizations strengthen their operational security programs by optimizing how their people, processes and technology solutions work together. Consulting services include conducting breach readiness assessments to minimize exposure to attacks; fortifying approaches to identity/access management; unifying governance, risk and compliance practices; and redesigning SOCs/CIRCs. The RSA Advanced Cyber Defense Practice also provides expert counsel and hands-on assistance with all aspects of advanced threat detection, response and remediation.

RSA® Archer™ GRC Suite is the market-leading solution for managing enterprise governance, risk and compliance (GRC). It provides a flexible, collaborative platform to manage enterprise risks, automate business processes, demonstrate compliance and gain visibility into exposures and gaps across the organization. The RSA Archer GRC platform is designed to draw data from a wide variety of systems to serve as a central repository for risk-, compliance- and security-related information. The RSA Archer Threat Management solution is an early-warning system for tracking threats. The RSA Archer Incident Management solution helps organizations escalate problems, track the progress of investigations and coordinate problem resolution. The platform's ability to integrate information on security alerts and threats, to gather and present metrics about the effectiveness of security controls and processes and to analyze contextual information about the security and business environment helps create actionable, real-time intelligence across the enterprise.

RSA® Cloud Trust Authority (CTA) is a collection of cloud-based services to simplify and enhance identity, information and cloud infrastructure security, as well as compliance reporting. With RSA Cloud Trust Authority, public cloud service providers and their customers do not need to establish individual point-to-point integrations to establish trust; instead, participants can establish many cloud security relationships simultaneously through a single integration with the CTA service. Enterprises can manage secure user access and user provisioning to multiple public cloud service providers via federated single sign-on and directory synchronization with options for strong authentication.

The RSA® Live platform operationalizes threat intelligence by consolidating information from the global security community and fusing these external data sets with an organization's internal data. The platform gathers security information from the industry's most trusted and reliable sources, including proprietary RSA® FirstWatch research. RSA's expert security analysts consolidate and evaluate threat data from diverse sources to illuminate the information most relevant to your organization. The data is then distributed and operationalized via correlation rules, blacklists, parsers, views and feeds. This automated approach allows organizations to take advantage of the intelligence that others have already found and to discern what they should look for in applying threat intelligence to current and historical data.

RSA® Security Analytics is designed to provide organizations with the situational awareness needed to deal with their most pressing security issues. By offering enterprise-wide visibility into network traffic and log event data, the RSA Security Analytics system can help organizations gain a comprehensive view of their IT environment, enabling security analysts to prioritize threats quickly, investigate them, make remediation decisions and take action. The RSA Security Analytics solution's distributed data architecture is engineered to collect and analyze massive volumes of information – hundreds of terabytes and beyond – at very high speed using multiple modes of analysis. The solution is also capable of integrating external threat intelligence about the latest tools, techniques and procedures in use by the attacker community and of helping organizations track and manage responses to security issues identified through the solution. The RSA Security Analytics platform is planned for commercial release in early 2013.

RSA® Silver Tail software and SaaS solutions protect organizations from cyber attack, cybercrime, and fraud by analyzing web sessions and mobile traffic to distinguish suspicious or malicious activities from legitimate ones. The Silver Tail platform collects and analyzes massive amounts of real-time data from web and mobile traffic to power the platform's behavioral analysis engine. The behavioral analysis engine creates heuristics and rules to learn the typical conditions and behaviors within any IT-based system and to detect anomalies that signal IT security threats, fraud, insider threats, business logic abuse and other malicious activity.

ABOUT RSA

RSA, The Security Division of EMC, is the premier provider of security, risk and compliance management solutions for business acceleration. RSA helps the world's leading organizations solve their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, encryption & key management, SIEM, data loss prevention, continuous network monitoring, and fraud protection with industry leading GRC capabilities and robust consulting services, RSA brings visibility and trust to millions of user identities, the transactions that they perform and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

www.rsa.com

168628 H11437 BD BRF 0113