IBM Software
Thought Leadership White Paper

January 2013

IT executive guide to security intelligence

Transitioning from log management and SIEM to comprehensive security intelligence

Contents

Introduction

Security intelligence, built upon the same concepts that have made business intelligence an essential enterprise technology, is the critical next step for organizations that recognize the importance of information security to their business health. This is especially critical on today's smarter planet, where instrumented, interconnected and intelligent businesses collect, process, use and store more information than ever before.

Too often, the response to new information security threats is a "finger-in-the-dam" approach with a particular point technology or reactive new policies or rules. This is in large part because a unified security program—based on automated analyses of unified information from across the IT infrastructure—is costly, complex, difficult to implement and inefficient. As a result, most organizations lack accurate threat detection and informed risk-management capabilities.

This white paper discusses how security intelligence addresses these shortcomings and empowers organizations—from Fortune Five companies to midsize enterprises to government agencies—to maintain comprehensive and cost-effective information security. In particular, it will show how security intelligence addresses critical concerns in five key areas:

- Data silo consolidation
- Threat detection
- Fraud discovery
- Risk assessment and management
- Regulatory compliance

Setting security intelligence goals

High-performance organizations excel at business in large part because they know how to put their information to work. Aided by the automated use of business intelligence technology, they apply analytics to extract maximum value from the massive amounts of data available to them.

They can apply the same approach to securing that information by implementing a security intelligence program. Just as business intelligence helps enterprises make decisions that maximize opportunities and minimize business risks, security intelligence enables them to better detect threats, identify security risks and areas of noncompliance, and set priorities for remediation.

The case for business intelligence is compelling. It enables organizations to support their critical decision making by automating the data analysis processes at a level that manual analysis can scarcely approach. By applying computer-based business analytics to their unique environments, successful organizations derive the greatest possible value from their amassed terabytes and petabytes of data, from sales revenue and customer demographics to the cost of shipping and raw materials.

The case for security intelligence is equally, if not more, compelling. Enterprises and government organizations have vast quantities of data that can help detect threats and areas of high risk—if they have the means and the commitment to collect, aggregate and, most importantly, analyze it. This data comes not only from point security products, but also from sources such as network device configurations, servers, network traffic telemetry, applications, and end users and their activities.

Security intelligence reduces risk, facilitates compliance, shows demonstrable return on investment (ROI) and maximizes investments in existing security technologies. The goals of security intelligence are to:

- Distill large amounts of information into an efficient decision-making process, reducing billions of pieces of data to a handful of action items
- Operationalize data collection and analysis through automation and ease of use
- Deliver high-value applications that help organizations derive the most benefit from their data to understand and control risk, detect problems and prioritize remediation
- Validate that the organization has the right policies in place
- Assure that the controls the organization has implemented are effectively enforcing those policies

Organizations have a long way to go in understanding their IT security environment. Consider a recent report on Advanced Persistent Threat Analysis by ESG, which found that 59 percent of organizations with more than 1,000 employees are either certain or fairly certain that they have been the target of an advanced persistent threat attack.[1] According to ESG, this leaves many CISOs in a no-win situation. On the one hand, they face a dangerous threat landscape and need to secure new IT initiatives such as cloud computing, mobile computing and social media. On the other hand, they continue to rely on discrete point tools, under-staffed organizations and manual processes as the basis of their security defenses.[2]

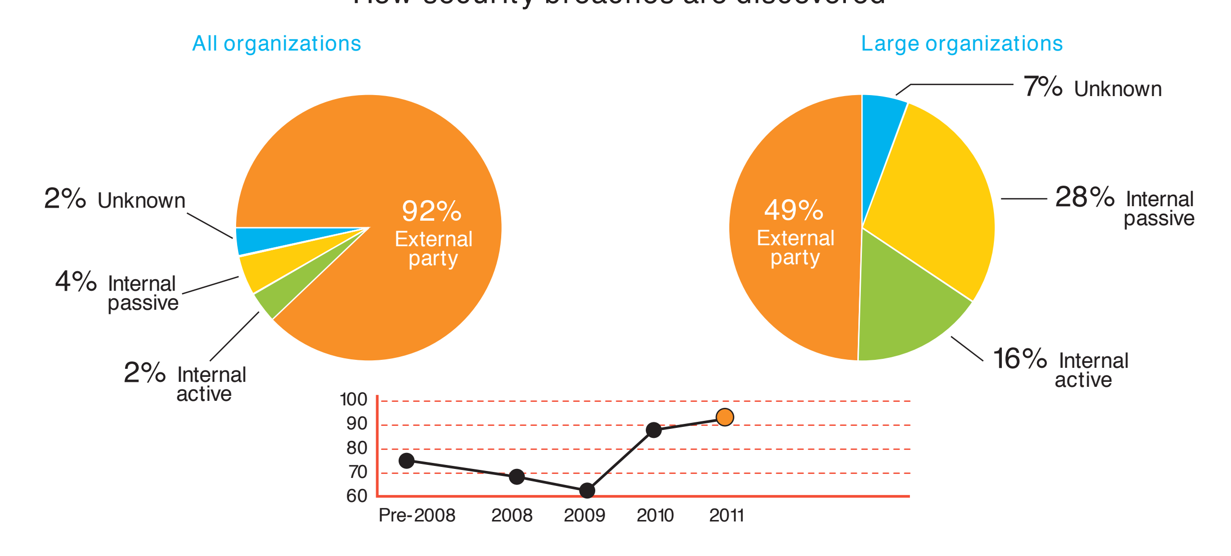
In addition, a Verizon Data Breach Investigations report revealed that more than half of data breaches investigated go undiscovered for months. As their research has shown for the last several years, third parties discover data breaches much more frequently than do the victim organizations themselves—and breaches discovered by external parties are at an all-time high, with more than 90 percent of all organizations being notified of a breach by external parties.[3]

Defining the problem

The security model of 10 to 12 years ago is no longer adequate to meet contemporary challenges, as “Internet hooliganism” has given way to organized criminal activity. The older model is outmoded and does not scale in the face of today’s threats and IT environment. Perimeter-based security has evolved to a highly distributed model as employees, partners and customers conduct business remotely across the Internet and criminals exploit new attack vectors and misplaced user trust. Government and industry regulatory mandates emerged and were given “teeth” through stronger penalties and more diligent enforcement.

The security industry has responded with new and enhanced products to meet each threat. All of these tools add value to overall enterprise security, but they are, in effect, islands of security technology. They are not conducive to a risk-based, enterprise-wide security program, and the overall effort tends to be fragmented.

How security breaches are discovered



Source: Verizon Risk Team, 2012 Data Breach Investigations Report, Verizon Communications, Inc., 2012

In many cases, organizations do not discover their own threats—the discovery is made by an external third party and then reported to the victim organization. When breaches are discovered internally, they typically come from either active methods designed specifically for detection or passive methods in which an incident is uncovered by a non-security process.

In many cases, organizations must deal with incomplete data because a given security tool may not recognize a threat or risk for what it is without correlation from other data sources. On the other hand, even when data is collected from disparate sources, analysts are challenged by the sheer volume, making it extremely difficult to distill actionable information.

Security intelligence addresses these problems across the spectrum of the security lifecycle, centralizing data from disparate silos, normalizing it and running automated analyses. This enables organizations to prioritize risk and cost-effectively deploy security resources for detection, prevention, response and remediation.

Moving beyond log management and SIEM

The concept of security intelligence is partially realized in security information and event management (SIEM) tools, which correlate and analyze aggregated and normalized log data. Log management tools centralize and automate the query process, but they lack the flexibility and sophisticated correlation and analysis capabilities of SIEM and, ultimately, security intelligence.

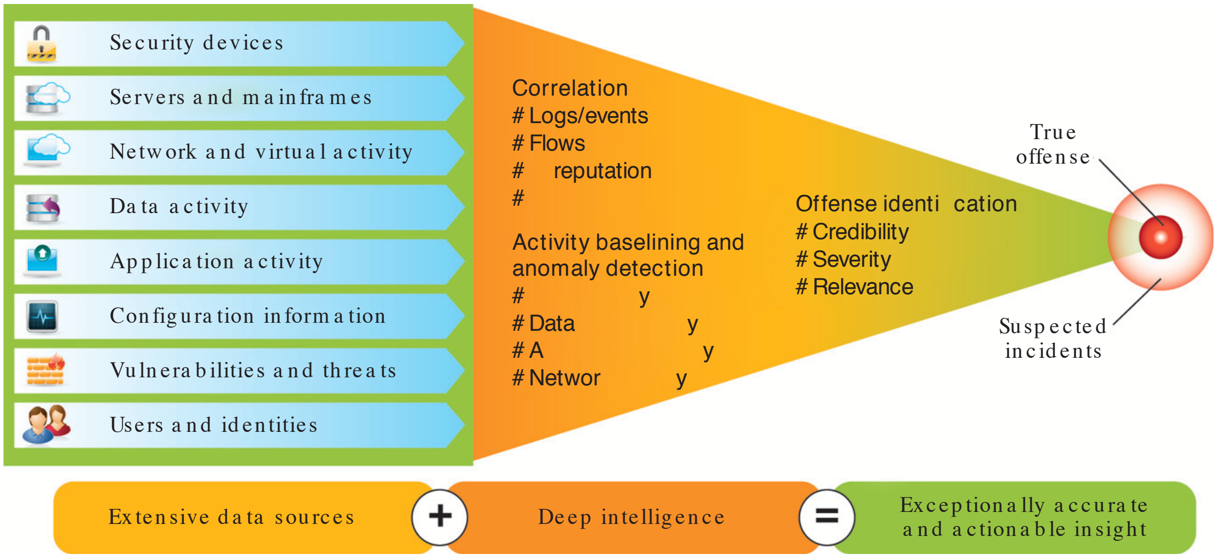
But SIEM should be regarded as a point along the way rather than a destination—the end goal is comprehensive security intelligence. SIEM is very strong from an event-management perspective and plays a particularly important role in threat detection. Comprehensive security intelligence, however, must encompass and analyze a far broader range of information. It requires continuous monitoring of all relevant data sources across the IT infrastructure, as well as evaluating information in contexts that extend beyond typical SIEM capabilities.

A key value point for security intelligence beyond SIEM is the ability to apply context from across an extensive range of sources. This can reduce false positives, tell users not only what has been exploited but also what kind of activity is taking place as a result, and provide quicker detection and incident response.

Security intelligence should include a much broader range of data, leveraging the full context in which systems are operating. That context includes, but is not limited to, security and network device logs, vulnerabilities, configuration data, network traffic telemetry, application events and activities, user identities, assets, geo-location, and application content.

This produces a staggering amount of data. Security intelligence provides great value in leveraging that data to establish very specific context around each potential area of concern and executes sophisticated analytics to accurately detect more and different types of threats.

For example, a potential exploit of a web server reported by an intrusion detection system can be validated by unusual outbound network activity detected by network behavioral anomaly detection (NBAD) capabilities.



IBM QRadar Security Intelligence Platform delivers comprehensive security intelligence.

Or, you have a report that a server has a potential vulnerability that has just been disclosed. But it's one of hundreds in your organization, so how do you evaluate the threat for this particular server? Security intelligence can analyze all available data and tell you:

- The presence or absence of the vulnerability
- The value the organization assigns to the asset or data
- The likelihood of an exploit based on attack-path threat models
- Configuration information, which may indicate, for example, that the server is not accessible because a default setting has been changed
- The presence of protective controls, such as an intrusion prevention system

Or, consider the insider threat. The 260,000 diplomatic cables on military issues given to WikiLeaks in 2010 were obtained by a U.S. Army insider with a security clearance who, according to charges, did "intentionally exceed his authorized access." According to news reports, he took advantage of a loophole in policies intended to prevent unauthorized downloading.[4] But analysis of correlated data, applying contexts from multiple sources, may have stopped the leak before it could cause damage.

Determining the business value of security intelligence

One of the most compelling arguments for security intelligence is operational efficiency, or better use of people, time and infrastructure. This is the ability to incorporate several security and network technologies into an integrated system rather than operating products independently.

The focus on security intelligence is particularly relevant, as operational responsibility for security is increasingly being placed in the hands of network operations teams. It makes sense to mirror this consolidation of operational responsibilities with consolidation at the intelligence layer. Think in terms of enabling multiple tasks in single-platform and cross-functional development of skills across the organization, and then deploying access based on roles.

Further, security intelligence adds value in other areas of IT, such as troubleshooting system problems, network issues, and user support and authorization analysis.

Security intelligence enables organizations to use integrated tools across a common framework and to leverage a unified data set to address problems along the entire security spectrum. This can be illustrated in five of the most prominent use cases in which security intelligence provides high value.

Data silo consolidation

Without automated technology, business intelligence analytics are difficult to execute. The data that would enable users to understand inventory returns, supply chains and more is available, but it is siloed in different applications and databases. It falls upon the analyst to compile data from all those sources and pour them into spreadsheets or databases to perform manual analyses. Security analysis poses similar problems, and security intelligence provides similar efficiencies. From a security perspective, data can exist in three types of silos:

- Data locked up in disparate security devices, applications and databases
- Data that is collected from point products, applications and more, creating, in effect, yet another silo; that data is stored in another database, but there is no communication or coordination between the configuration databases
- Organizational silos of data segregated by business unit, operations group, department or other group

In the first two cases, security intelligence breaks down the silos by integrating data feeds from disparate products into a common framework for automated analysis across different security and IT technologies. From a security perspective, this brings in all the enhanced detection and risk assessment capabilities the consolidated telemetry of security intelligence can deliver. From a CIO perspective, reducing these silos enables the rationalization of security products that would otherwise have to be managed on a point-product basis. The third case requires considerable cooperation among groups that are typically separated, meaning a realigning of processes and responsibilities, and perhaps some pressure exerted by management.

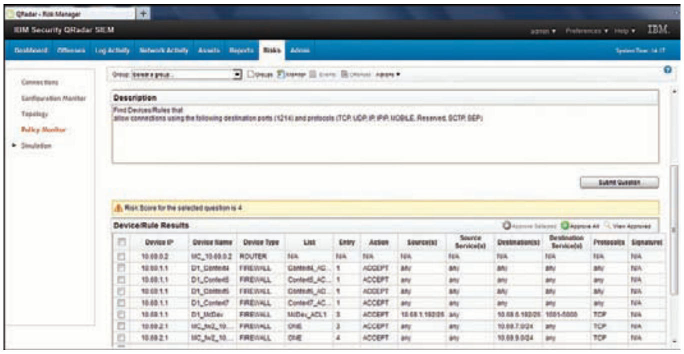
The crushing cumulative volume of all this disparate data exacerbates the problem exponentially. Each of these silos can create enormous volumes of data, in different formats, for different purposes. In some cases, they can create different policies or compliance requirements. Only automated security intelligence can effectively manage petabytes of security-related data and analyze it across organizational and operational silos.

Threat detection

In a few short years, as enterprises have opened themselves to Internet-based commerce and remote users, security has moved from a perimeter-based model with all policy centered on the firewall to distributed security. Security is now focused on hosts, applications and the content of information moving out of the organization.

Moreover, we're seeing growing incidences of highly targeted attacks, including attacks on high-profile companies. Sophisticated, targeted intrusions are typically multistaged and multifaceted, difficult to detect and very difficult to eradicate; advanced persistent threats are characterized by the tenacity of the attackers and resources at their disposal.

An overarching intelligence should be applied to the diverse security technologies that have been developed in response to the evolving threat landscape. As noted in the discussion of security context, an activity that appears innocuous to one part of an infrastructure may be revealed as a threat when that data is correlated with other sources. For example, an attacker may disable logging, but can't shut down network activity.



Description

Find Devices/Rules that
allow connections using the following destination ports (1214) and protocols (TCP, UDP, IP, IPIP, MOBILE, Reserved, SCTP, SEP)

Risk Score for the selected question is 4

Device/Rule Results

□	Device IP	Device Name	Device Type	List	Entry	Action	Source(s)	Source Service(s)	Destination(s)	Destination Service(s)	Protocol(s)	Signature(s)
□	10.69.0.2	MC_10.69.0.2	ROUTER	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
□	10.69.1.1	D1_Context4	FIREWALL	Context4_AC...	1	ACCEPT	any	any	any	any	any	N/A
□	10.69.1.1	D1_Context5	FIREWALL	Context5_AC...	1	ACCEPT	any	any	any	any	any	N/A
□	10.69.1.1	D1_Context6	FIREWALL	Context6_AC...	1	ACCEPT	any	any	any	any	any	N/A
□	10.69.1.1	D1_Context7	FIREWALL	Context7_AC...	1	ACCEPT	any	any	any	any	any	N/A
□	10.69.1.1	D1_McDav	FIREWALL	McDav_ACL1	3	ACCEPT	10.69.1.192/26	any	10.69.6.192/26	1001-5000	TCP	N/A
□	10.69.2.1	MC_fw2_10...	FIREWALL	ONE	3	ACCEPT	any	any	10.69.7.0/24	any	TCP	N/A
□	10.69.2.1	MC_fw2_10...	FIREWALL	ONE	4	ACCEPT	any	any	10.69.9.0/24	any	TCP	N/A

The Prioritize Risk screen shows a user query for risk scoring.

Proprietary applications may not produce logs; some parts of the network may be without firewalls. Security intelligence can still identify the applications and services running between that host and the network, in these cases, and flag a potential threat.

Fraud discovery

Security intelligence is absolutely essential for effective fraud detection. Besides network telemetry, data from the switching and routing fabric, and the security-device enforcement layer, the key ingredient is an understanding of the users and the application data.

Fraud detection requires monitoring everything that goes on across the network: network activity and events, host and application activity, and individual user activity. Security intelligence enables organizations to bind the user to a particular asset. By tying together network, DNS server and application activity with directory information, for example, security intelligence can tie a specific user to a specific IP address for a specific VPN session.

Risk assessment and management

Security intelligence provides the backbone for risk management through impact analysis and threat modeling. It is the difference between reacting to attacks on the network and proactively protecting one's most important assets.

Impact analysis is based on the value an organization assigns to a particular asset and negative consequences to the business if it is compromised. Security intelligence addresses this by asset and data discovery and classification to identify critical assets. Further, it answers questions such as, how exposed is the asset? Does it have direct access to the Internet? Does it have known vulnerabilities for which there are known exploits?

Threat modeling takes into account all these factors and more, identifying not only vulnerabilities on the target system, but also possible attack paths based on exploiting weaknesses between the target and the Internet—poorly designed firewall rules, badly configured router access control lists and more.

Regulatory compliance

Compliance is a foundational use case for security intelligence. Security intelligence addresses many compliance requirements, particularly all aspects of security monitoring. For example, security intelligence does not meet all Payment Card Industry (PCI) requirements, but it does meet all PCI monitoring requirements in a way that SIEM and log management alone cannot. Security intelligence provides the data that serves as a foundation to deliver and demonstrate audit requirements for all regulations.

By monitoring broadly across the IT infrastructure—across events, configuration changes, network activity, applications and user activity—security intelligence consolidates compliance capabilities in a single product suite rather than relying on multiple point products, each delivering its own piece of the audit puzzle.

Addressing the bottom line

Security intelligence, like business intelligence, enables organizations to make smarter business decisions. It enables organizations to process more information more efficiently across the entire IT infrastructure. Applying business intelligence technology enables organizations to do more with less: Instead of having analysts devote expensive hours manually poring over a fraction of the available data, business intelligence automates analysis across all available data and delivers role-based information specific to the task.

Information technology is about automating business processing—for purchasing, logistics, enterprise resource planning and more. Security intelligence is about automating security, including understanding risk, monitoring the infrastructure for threats and vulnerabilities, and prioritizing remediation.

By centralizing security tools and data from the IT infrastructure, security intelligence enables consolidated management and more efficient use of resources devoted to security. Organizations can improve their security posture without additional operational and personnel costs or the expense of purchasing, maintaining and integrating multiple point products.

Security intelligence yields key benefits in business cost and efficiency. It can:

- Reduce costs associated with deployment and operations; rather than add people, organizations use existing staff to help make security relevant to the business
- Make product acquisition simpler and cheaper; organizations can purchase a single platform, rather than multiple products
- Facilitate deployment through a unified platform rather than multiple products, which then must be integrated even to approach an acceptable security intelligence capability
- Give a broad class of organizations security capabilities that were formerly possible only for the most sophisticated organizations
- Automate the collection, normalization and analysis of massive amounts of security data from technical and organizational silos; this capability applies rich context to every analysis
- Enhance threat detection, applying context to detect possible attacks that might go unnoticed by a particular security technology
- Improve incident response through accurate and quick detection
- Realize staffing ROI; organizations can implement new security services, such as worldwide threat monitoring, without requiring additional staff
- Empower enterprises to run highly robust security programs, processing billions of records daily and producing a score of high-priority action items every 24 hours

Enabling security intelligence

IBM® QRadar® Security Intelligence Platform provides a highly integrated set of solutions designed to help organizations achieve comprehensive security intelligence implemented on a unified operating system and managed through a single console.

Anchored by a powerful SIEM, this platform presents a unique security intelligence capability, integrating a set of high-value security and network-monitoring applications into a unified solution that empowers organizations to deploy security and network operations resources based on analysis of a comprehensive set of data sources.

The platform is built on the IBM QRadar Security Intelligence Operating System, which enables IBM to deliver a set of common services around data integration, normalization, warehousing and archiving, and analytics. This unified structure produces uniform workflow, reporting, alerting and dashboarding capabilities. These support organization-wide policies and processes, rapidly identify threats and assess risk, and support audit-, operational-, managerial- and executive-level security information and response requirements.

On top of strong core SIEM and log management capabilities, IBM Security QRadar QFlow technology provides deep network monitoring with sophisticated anomaly detection capabilities that add rich context to analyses that might otherwise rely solely on log data. QRadar QFlow application-aware network monitoring enables stateful information about all conversations at the application layer.

Further, the QRadar Security Intelligence Platform extends its security intelligence capabilities into virtual network environments with its IBM Security QRadar VFlow technology, assuring a high level of threat detection and risk management in support of data center consolidation and private and public cloud initiatives.

The IBM Security QRadar Risk Manager risk assessment module provides detailed configuration auditing that adds risk posture context that SIEM alone cannot provide. QRadar Risk Manager evaluates risk and models potential threats against high-value assets, determining possible attack paths based on the wealth of data it draws upon.

The QRadar Security Intelligence Operating System provides a platform on which users can continue to add new security modules to accommodate new use cases around the intelligent securing and intelligent risk assessment of the enterprise infrastructure. This eliminates the burden of new data-integration layers, different storage requirements, new analytics engines and different reporting infrastructures to accommodate new security applications and potential data sources.

Conclusion

Forward-thinking organizations have recognized and embraced the value of business intelligence technology, as their success is predicated on the ability to analyze and act upon the essential information derived from staggering volumes of data. Similarly, security intelligence is essential because information security is integral to doing business in the 21st century. Powerful, automated analytics for centralized data from sources that cover the entire spectrum of the IT infrastructure make a high level of cost-effective security not only possible, but indispensable.

For more information

To learn more about IBM security intelligence offerings, please contact your IBM representative or IBM Business Partner, or visit **ibm.com**/security

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We’ll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
January 2013

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.

♲ Please Recycle

[1] Jon Oltsik, “Research Report: U.S. Advanced Persistent Threat Analysis,” Enterprise Strategy Group, November 1, 2011. http://www.esg-global.com/research-reports/research-report-us-advanced-persistent-threat-analysis/?keywords=advanced%20persistent

[2] Jon Oltsik, “Enterprise Information Security in Transition: An Opportunity for IBM,” Enterprise Strategy Group, October 15, 2012. http://www.esg-global.com/briefs/enterprise-information-security-in-transition-an-opportunity-for-ibm/

[3] Verizon RISK Team, “2012 Data Breach Investigations Report,” *Verizon*, 2012. http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

[4] Thomas Shanker, “Loophole May Have Aided Theft of Classified Data,” *The New York Times*, July 8, 2010. http://www.nytimes.com/2010/07/09/world/09breach.html