The Essential Building Blocks for Cyber Security
Best Practices in Building an Effective Cyber Defense Strategy

Torsten George
Chief Security Strategist, RiskVision
June 2015
Executive Summary

In this paper, RiskVision® is providing insight into the essential building blocks to create a sound cyber security strategy. These best practices are based on the company’s engagement with Global 2000 companies, government agencies, fellow security vendors, industry analysts, and security consultants; as well as market research it conducts on a regular basis.

The data breaches at Target, Home Depot, Staples, Michaels, Kmart, eBay, Anthem, Sony Pictures Entertainment, and the U.S. Office of Personnel Management, were just the tip of the iceberg. Despite increased investments in preventive security measures, many organizations are losing the war against cyber criminals. New methodologies developed by the National Institute of Standards and Technology (NIST) and other industry standards bodies (e.g., the Payment Card Industry) are being implemented by many organizations, but best practices for addressing cyber security threats remain vague. At the same time, board members are demanding quantitative risk data that spans all business operations, while business units need to neutralize the impact of cyber-attacks. So what can be done to minimize cyber security threats?

It’s clear that the dynamics of the threat landscape have changed, and that organizations need to respond accordingly. An effective starting point is to focus on the essential building blocks of any cyber threat defense strategy, namely: Data Integrity, Continuous Monitoring, Cyber Risk Visualization, Risk-Based Prioritization, and Closed-Loop Remediation.

About RiskVision

RiskVision, the Big Data Risk Company™, is the leading independent provider of integrated solutions for Operational and Security Risk Intelligence. RiskVision is automating how Global 2000 companies and government agencies continuously monitor big data for risks across financial, operations, and IT domains to increase operational efficiency and orchestrate incident, threat, and vulnerability actions in real time. RiskVision® customers demonstrate automation use cases within 30 days on-demand, and within 60 days on premise, made possible by a configurable platform and applications, broad library of technology integrations, as well as vast domain and regulatory content. RiskVision scales with businesses, effectively managing assets, data, people, and processes to achieve 100 percent risk and compliance coverage. Its real-time risk analysis leads to optimized business performance and better investment decisions. For more information, please visit www.RiskVisionInc.com.
# Table of Contents

Executive Summary ............................................................................................................................................. 2

About RiskVision ................................................................................................................................................ 2

1.0 Introduction ................................................................................................................................................. 4

2.0 The Essential Building Blocks for Cyber Security ......................................................................................... 7
   2.1 Data Integrity ................................................................................................................................................ 7
   2.2 Continuous Monitoring ............................................................................................................................... 7
   2.3 Cyber Risk Visualization ............................................................................................................................. 9
   2.4 Risk-Based Prioritization .......................................................................................................................... 10
   2.5 Closed-Loop Remediation ........................................................................................................................ 12

3.0 Incident Risk Response ................................................................................................................................ 13

4.0 Conclusion .................................................................................................................................................... 15
1.0 Introduction

The data breaches at Target, Home Depot, Staples, Michaels, Kmart, eBay, Anthem, Sony Pictures Entertainment, and the U.S. Office of Personnel Management, were just the tip of the iceberg. Despite increased investments in preventive security measures, many organizations are losing the war against cyber criminals. New methodologies developed by the National Institute of Standards and Technology (NIST) and other industry standards bodies (e.g., the Payment Card Industry) are being implemented by many organizations, but best practices for addressing cyber security threats remain vague. At the same time, board members are demanding quantitative risk data that spans all business operations, while business units need to neutralize the impact of cyber-attacks. So what can be done to minimize cyber security threats?

As news of more data breaches and third-party originated cyber-attacks make the news, businesses and regulators alike are sharpening their focus on how to report on and mitigate these risks. According to Gartner (“Gartner Says Worldwide Information Security Spending Will Grow Almost...” , Gartner, August 2014) worldwide spending on information security will reach $76.9 billion in 2015, an increase of 8.2 percent over 2014.

![FIGURE 1: Total IT Security Spend; Source: Gartner, “Gartner Says Worldwide Information Security Spending Will Grow Almost...”, August 2014](image-url)
However, at the same time we’re seeing an increase in security incidents, which are raising doubts about the effectiveness of these investments. A PwC survey (“Managing Cyber Risk in an Interconnected World”, PwC, 2015) of 9,700 companies found that they had detected nearly 43 million security incidents in 2014, a compound annual growth rate of 66 percent since 2009.

![Compound Annual Growth Rate of Security Incidents since 2009](image)

FIGURE 2: Compound Annual Growth Rate of Security Incidents since 2009 and Number of Security Incidents; Source: PwC, “Managing Cyber Risk in an Interconnected World”, 2015.

Cyber-attacks have become part of the day-to-day operations of many businesses and public sector agencies. As frequency and sophistication has increased dramatically over the last two years, many organizations are struggling to align their cyber security strategy with the new threat realities. Those seeking guidance and assistance from the government have been disappointed. Political gridlock in Washington has hampered progress on passing a Cyber Security Information Sharing Act that would at least enable cyber threat data exchange across different industry sectors to improve cyber resilience.

To show some momentum, the White House mandated the development of a voluntary risk-based Cybersecurity Framework – a set of industry standards and best practices to help organizations manage cyber security risks. This Cybersecurity Framework, developed by the National Institute of Standards and Technology (NIST) with the collaboration of other government agencies and the private sector, was introduced more than a year ago. Notwithstanding some anecdotal evidence presented to members of a Senate committee at a February 4th hearing, there has been no measurable proof that using the framework can help prevent cyber-attacks.
In addition, the White House recently signed another executive order that strengthens the authority of federal offices to collect and aggregate cyber threat information from across the government and the private sector. At the same time, the President and his staff members announced the creation of three new US cyber groups -- the National Cybersecurity and Communications Integration Center, the Cyber Threat Intelligence Integration Center, and the Cyber Response Group.

While these initiatives might strengthen the government’s threat awareness, the average company will most likely not benefit from these efforts. Unless, of course, they’re exposed to state-sponsored cyber-attacks, as in the case of Sony Pictures Entertainment, which would draw the attention of the government. Otherwise, it will remain an organization’s sole responsibility to build an effective cyber security strategy that meets today’s unique threat requirements.

So what can be done to minimize cyber security threats? There are five essential building blocks to build a sound cyber security strategy, which this paper will review in depth.
2.0 The Essential Building Blocks for Cyber Security

2.1 Data Integrity

Undeniably, data is the prime target for attackers. Therefore, if we can prevent data from leaving the organization or being modified, protecting against network breaches becomes less critical. Unfortunately, data is often left unsecured. For example, a quick web search for “data breach and unencrypted data” produces thousands of results that illustrate how many organizations fail to protect the integrity of their data and don’t even encrypt sensitive information.

The first step to assure data integrity is to classify data into categories that reflect the business need to protect them, such as “public”, “internal use”, “confidential”, and “top secret”. Unfortunately, data classification is often abandoned due to the manual efforts required to maintain the constantly changing classification states. However, emerging big data risk management systems come with so-called dynamic grouping capabilities that provide drag and drop capabilities to realign classifications and then propagate changes to all associated nodes.

Data classification will subsequently determine what data should be encrypted, which typically applies to all personal identifiable information (PII). Innovations in encryption technology over the past few years have eliminated many of its earlier performance and deployment roadblocks. Organizations should place special emphasis on developing well-documented and properly implemented encryption policies which should be applied to all sensitive data, wherever it resides and however it is transmitted.

Access control is the Achilles heel of many security programs, since practitioners have to balance data availability versus unauthorized data usage (e.g., theft, disclosure, modification, destructions). Meanwhile, hackers often target privileged users since their accounts provide a beachhead into the entire network. Therefore, strict enforcement of well-defined access control policies and continuous monitoring of access paths to ensure they are working as intended are essential for the success of data integrity initiatives.

Last but not least, organizations should implement practices to certify uncorrupted data transmission. Worst case scenarios here include the manipulation of stock market data by cyber-attackers before it is publicly disseminated.

2.2 Continuous Monitoring

To ensure proper cyber security visibility, many organizations are relying on multiple, best-of-bread, silo-based tools (e.g., fraud and data loss prevention, vulnerability management, or SIEM) to gather the necessary security data. This only adds to the volume, velocity, and complexity of data feeds that must be analyzed, normalized, and prioritized. Unlike adaptive authentication, which is being used to automate behavioral pattern analysis for fraud prevention in the payments industry, most security tools lack the capability to provide self-analysis. Instead, security operations staff members are often required to piece together data from different sources, connect the dots, and detect suspicious patterns that would indicate a cyber-attack or data breach. Unfortunately, relying on manual processes to comb through mountains of logs is one of the main reasons that critical issues are not being addressed in a timely fashion. The Target breach was a good example. The right tools were in place and reported the intrusion, but due to the volume of data that the outsourced security operations team needed to assess on an ongoing basis, the data breach was not detected in a timely fashion. In fact, authorities were alerted to the breach by a third-party that, which according to the Verizon Data Breach Investigation Report is not uncommon.
Big data in security becomes even more daunting when you consider that cyber criminals increasingly targeting third-party vendors to gain backdoor access to data at large, well-protected global organizations. As a result, it is no longer sufficient to simply focus on an organization’s internal security posture. We also need to safeguard against third-party related control failures. This adds a whole new dimension to the scope of what an organization has to frequently monitor and assess.

Following a continuous monitoring approach as propagated by NIST only adds to the big security data conundrum, as an increase in frequency of scans and reporting exponentially increases the data volume. This, in turn, requires security data aggregation and normalization from a variety of sources such as security information and event management (SIEM), asset management, threat feeds, and vulnerability scanners.

At the end of the day, the ultimate goal is to shorten the window attackers have to exploit a software or network configuration flaw. Big data sets can assist in putting specific behavior into context, but there are some real technological challenges to overcome. Big data risk management software can assist organizations in aggregating the different data sources, leading to reduced costs by unifying solutions, streamlining processes, creating situational awareness to expose exploits and threats in a timely manner, and gathering historic trend data, which can assist in predictive security.

FIGURE 3: RiskVision screen shot: dashboard view, showing aggregated security and threat information over time to assist with predictive security.
2.3 Cyber Risk Visualization

As news of more data breaches and third-party originated cyber-attacks make the news, businesses and regulators alike are sharpening their focus on how to report on and mitigate these risks. Meanwhile, corporate boards are demanding quantitative risk data that spans all business operations, while business units need to neutralize the impact of cyber-attacks. In this context, it is important to visualize, measure, and action cyber security operational risk intelligence in real time.

The most efficient way to identify imminent threats to an organization is to create a visual representation of the company’s IT architecture and associated risks. This approach provides security operations teams with interactive views of the relationships of systems to their components, systems to other systems, and components to other components. Ultimately, it enables security practitioners to rapidly distinguish the criticality of risks vis-à-vis the affected systems and components. This allows organizations to focus mitigation actions on the most sensitive / at risk business components and increase board / auditor transparency.

FIGURE 4: RiskVision screen shot: cyber systems visualization, illustrating an organization’s enterprise architecture and distinguishing the criticality of systems and their components, adjacent systems / components, and types of relationships to allow focus of mitigation actions on business critical issues.
2.4 Risk-Based Prioritization

Effective prioritization of vulnerabilities and incidents is essential to staying ahead of attackers.

While security monitoring generates big data, in its raw form it remains only a means to an end. Ultimately, information security decision making should be based on prioritized, actionable insight derived from the data. To achieve this, big security data needs to be correlated with its business criticality or risk to the organization. Without a risk-based approach to security, organizations can waste valuable IT resources mitigating for instance vulnerabilities that in reality pose little or no threat to the business.

For many years, businesses either focused on achieving compliance or taking preventive measures to strengthen their security posture. Endless data breaches have proven that neither approach is necessarily effective in minimizing risk. In fact, you could even argue that for years organizations may have misaligned their resources and funds in fighting threats.

What does this mean? Well, when an organization is solely focused on strengthening its compliance posture to pass an audit, they primarily look at control failures and gaps and try to mitigate them. However, if there is no threat that could reach the vulnerability in the context of the control gap, why bother? The same applies to vulnerabilities discovered by an organization focused on improving their security posture. Even if a vulnerability can be reached by an existing threat, choosing the right remediation method should also take into account whether any compensating controls are in place that might mitigate the risk. Furthermore, any decision related to resource allocation should be driven in conjunction with the business criticality a compliance or security shortcoming poses.
Furthermore, big security data needs to be filtered to just the information that is relevant to specific stakeholders’ roles and responsibilities. Not everyone has the same needs and objectives when it comes to leveraging big data.

**FIGURE 6:** RiskVision screen shot outlining information such as normalized vulnerabilities, assets in the environment affected by the vulnerability or the threats, ticket information, assets where the vulnerability or threat is fixed, patch availability to identify future remediation actions.

**FIGURE 7:** RiskVision screen shot: contextualized view, correlating asset criticality with vulnerability and threat data to provide a prioritized, actionable picture of the risk posture.
2.5 Closed-Loop Remediation

Lastly, closed-loop, risk-based remediation leverages subject matter experts within business units to define a risk catalog and risk tolerance. This process entails asset classification as outlined under ‘Data Integrity’ to define business criticality, continuous scoring to enable risk-based prioritization, and closed-loop tracking and measurement. By establishing a continuous review loop of existing assets, people, processes, potential risks, and possible threats, organizations can dramatically increase operational efficiency, while improving collaboration among business, security, and IT operations. This enables security efforts to be measured and made tangible (e.g., time to resolution, investment into security operations personnel, purchases of additional security tools).

FIGURE 8: Closed-loop remediation concept, covering setting risk tolerance and risk catalog, survey and data-driven gap assessment, correlation of compliance and security posture (both vulnerabilities and threats) with business criticality, subsequent remediation actions, and finally re-assessment to determine if mitigation steps were effective.
3.0 Incident Risk Response

Even with the five essential building blocks in place, there will never be 100% protection. With data breaches becoming an understandable consequence of interconnected business, with the use of big data risk management systems a breach is no longer the death knell it once was though. How you respond to a breach has everything to do with the depth and severity of its effect on your business. Do it wrong and you face huge liability and reputational penalties - do it right, and draw praise from your customers, business partners, and regulators in your execution. You can’t control a breach, but you can control your destiny. In this context, big data risk management systems like RiskVision provide the essential building block for your well-choreographed response actions.

In the midst of a breach, it is extremely difficult to effectively prioritize the remediation response. In today’s dynamic risk ecosystem, even smaller organizations face hundreds of incidents on an ongoing basis. Organizations must determine the order in which the incident needs to be remediated. Similar to cyber security remediation, this should be done based on the level of risk and business impact. Calculating risk and business impact is difficult, if not impossible, without input from and analysis across the organization’s infrastructure. Automated big data risk management tools can assist with risk determination and prioritization. Once the organization has determined its incident remediation strategy, the next step is to track the process of remediation – how long it will take, who is responsible, and who will take action to ensure remediation is accomplished within the timeframe established.
Ultimately, the biggest challenge associated with incident response management is documenting the entire process. In many instances, once an incident is identified by one group, the remediation actions are executed by a different group. Without interconnectivity into remediation systems and a centralized repository for capturing this data, it becomes almost impossible to establish an audit trail and determine how effective remediation actions were, whether they were brought up to compliance, or how they could be or must be improved or rectified.

The fact that organizations are relying on human interaction and dispersed systems can lead to major deficiencies and slow down an organization’s responsiveness. To overcome these shortcomings and streamline the overall process, some organizations are turning to big data risk management software with built-in incident response capabilities. A software-based approach helps organizations collect data from a variety of security and IT tools as well as other applications such as spreadsheets. It can aggregate the data and calculate the preliminary risk and business impact, enabling an organization to more effectively prioritize their response plan actions and timing. These systems also route and assign incidents based on type, severity, or affected assets; alert the assigned stakeholders, and provide for escalation if needed. Ultimately, all remediation efforts are tracked and all of the collected data is leveraged to measure controls and policy effectiveness as part of the incident post-analysis.

By making incident response a top priority and developing a well-documented policy and process that is understood by stakeholders, organizations can limit or even prevent reputational and share price erosion caused by a breach, as was the case with Target. Using software to automate and centralize manual incident response management processes can help reduce human error to ensure a timely, well executed response if a data breach occurs.
4.0 Conclusion

By leveraging the five cyber security building blocks plus a well-orchestrated incident risk management foundation, organizations can reduce risk, reduce costs, improve response readiness, and increase risk-posture visibility. However, without the commitment of management and board of directors to provide adequate resources for risk management, organizations’ cyber security posture won’t significantly improve. The current climate is ripe for implementing a transformational approach to security.

Many Global 2000 companies and government agencies worldwide are turning to RiskVision and leverage its RiskVision big data risk management to implement these best practices. With RiskVision, organizations can not only fulfill their board requirements for quantitative risk reporting that spans all business operations, but also serve their business units’ need to neutralize the impact of cyber-attacks. RiskVision helps break down security silos, improve time-to-remediation, and increase visibility into enterprise risks.

RiskVision is a purpose-built, context-aware software platform that transforms cyber operational security risk management into a pro-active, collaborative, and real-time discipline. Risk is influenced by three key factors: compliance posture, threats and vulnerabilities, and business impact. RiskVision aggregates critical intelligence about risk and compliance postures with current, new, and emerging threat information to calculate impacts on business operations and prioritize remediation actions. To provide organizations with a holistic view of risk, RiskVision harmonizes multiple frameworks to marry top-down risk modeling with bottom-up controls automation. It enables ongoing risk measurement across financial, operational, and security domains.

![RiskVision - Cyber Security Operational Risk Intelligence.](image-url)
RiskVision uses patented technology to identify, monitor, and mitigate risks by correlating security posture, assessing business unit criticality, and remediating physical and virtual assets within an organization’s infrastructure. It preserves investments in best-of-breed IT and security tools, using flat files, XML feeds, Web Services APIs, and 70+ connectors to leading asset and configuration management tools, threat feeds, vulnerability scanners, SIEM and DLP systems, plus privileged identity, ticketing, and patch management tools.

RiskVision solves a big data analytics problem with a discovery-based risk management database, time-proven data schema, and dynamic risk grouping. RiskVision has field-proven success in scaling with key performance indicators covering tens of thousands of live assessments, threats, and incidents; hundreds of thousands of vulnerabilities and configurations; and millions continuously monitored assets, conducting more than 300 million daily control checks.

RiskVision has been granted four patents; six additional are pending— all of which are a reflection of the innovative character of the RiskVision platform. In turn, the company and its RiskVision earned 32 industry accolades in 2014 alone, including the Security Products Magazine’s 2014 Govies Platinum Award, 2014 Cyber Defense Magazine Most Innovative InfoSec Award, Government Security News 2014 Homeland Security Award, 2014 International Business Awards Stevie Winner, 2014 American Business Awards Stevie Winner, and 5-Star Rating in 2014 SC Magazine’s Risk and Policy Management Group Test. The 2014 Deloitte Fast 500 ranked RiskVision one of the top 20 fastest growing security software companies for the second year in a row and the analyst community (e.g., Gartner and Forrester Research) describes RiskVision as the leading product in its category.