White Paper

Leveraging Security Risk Intelligence

The strategic value of measuring Real Risk™
Introduction

Every battlefield commander understands the strategic necessity of reliable intelligence. Winning battles depends on accurate understanding of enemies, their tactics and goals, weighing risks against potential damage, and deploying resources to mitigate or neutralize threats. Gathering information is just a starting point; more importantly, is any of it relevant or meaningful? Within all the chatter and noise, effective commanders discern the one percent of useful intelligence and follow through with action.

Every IT security professional knows that the battle to protect IT resources and data is fully engaged. In its 2011 Data Breach Investigations Report, Verizon studied 761 data compromise incidents that occurred in 2010, compared to just over 900 total breaches studied between 2004 and 2009. Verizon reported that of all breached records, 50 percent involved some form of hacking and 49 percent included use of malware.

The ongoing struggle to prevent hackers from breaching assets and malware from gaining a foothold requires a vulnerability management strategy that begins with a comprehensive measurement of security risk. Organizations must examine the entire IT stack, including the operating system, network, applications, and databases. The cycle of discovering assets, capturing and processing vulnerability data, identifying actual risks, testing and prioritizing mitigation tasks, and verifying effective controls grows more complex with every new technology that adds convenience but multiplies risk of a breach or incident. These new technologies include dynamic, virtualized environments and services outside traditional physical IT infrastructures, such as virtualized, cloud-based services and social networking.

Figure 1: The Security Risk Intelligence cycle - a holistic approach to minimizing risk

Rapid7 addresses the need for dynamic, in-depth risk management with Security Risk Intelligence, a holistic approach to minimizing risk (Figure 1). It is based on a unified solution set that includes vulnerability management, penetration testing, and best practices. Security Risk Intelligence helps organizations detect vulnerabilities, prioritize risks, and validate threats in a closed-loop system.
Beginning with an understanding of the need for effective risk management followed by a definition of the elements of risk, this discussion presents the advantages and strategic value of Rapid7 Security Risk Intelligence for your environment and illustrates its operation.

**Situation report: State of the Battlefield**

Attacks are smarter, sneakier, and easier to perpetrate than ever. The Verizon report found that “96 percent of breaches were avoidable through simple or intermediate controls,” that 50 percent of records breached used some form of hacking, and 49 percent of records breached incorporated use of malware. Incidents investigated during 2010 presented “the largest caseload ever; it was also extremely diverse in the threat agents, threat actions, affected assets, and security attributes involved.”

Security professionals struggle to reduce risk with limited staff and budget. To achieve effective risk management, they must abandon the limitations and expense of traditional, reactive approaches in favor of a proactive, data-driven investment model. They must overcome several challenges: interpreting massive amounts of data, monitoring dynamic assets, incorporating both compliance and security into best practices, moving beyond traditional “scan-and-patch” approaches to implement security best practice programs, and trusting conventional prioritization methods beyond their scope.

**Data through a fire hose.** Most security policies address some form of vulnerability management. Security professionals depend upon accurate assessments to determine whether intervention is necessary and implement proper steps for mitigation or remediation. There is no problem obtaining data: security devices and scanners generate terabytes of it. The challenge is interpreting data: identifying those specific vulnerabilities that truly represent a clear and present risk to security.

Security operators need solutions that help them distinguish the danger signals from the noise. For example, a mission-critical Web server may have ten known vulnerabilities, but which of those ten present genuine risk? Vulnerability management solutions should identify and dismiss seven of those attacks as “noise” and flag the other three as “signals” that require their attention.

**Dynamic assets, static tools.** Virtualization is re-defining how IT operations build and deliver services, but vulnerability scanners have not kept up. Traditional scanners provide a snapshot that goes obsolete within hours or minutes within a virtualized environment where VMs go online and offline or change hosts all day long. Virtualized environments—and the risks they present—are constantly changing, and scanners need a continuous discovery feature that tracks these changes as they occur.

**Compliance does not equal security.** Another challenge is the perception that attaining compliance (e.g., PCI, HIPAA, NERC, FDCC) reduces risk to acceptable levels. A breach of an asset unrelated to compliance can lead to the compromise of assets deemed compliant. Organizations spend billions of dollars on security solutions to address compliance, but most of them do not focus on deploying those solutions for maximum benefit beyond compliance.

**Risk reduction encompasses more than “scan-and-patch.”** Many enterprises trust that “scan-and-patch” methods keep them secure. Patching inherently keeps hackers ahead, because vendors typically issue patches in response...
to hacking incidents. While patching remains an important security step, security professionals need a variety of proactive solutions and best practices to put them ahead of hackers and malware.

**Conventional risk prioritization doesn’t tell you enough.** For example, many enterprises rely solely on CVSS scores to define thresholds for mitigation. These base CVSS metrics measure only the potential risk (likelihood plus impact) of a given vulnerability, not requiring temporal or environmental metrics to calculate its score. As such, base metrics CVSS scores do not consider the whole context of the identified vulnerability to the organization. Consider two vulnerabilities: one with a base metric CVSS score of 9 that is not exploitable, versus one with a CVSS score of 5 that is exploitable. A CVSS score of 9 may prompt a network operations manager to prioritize the fix of that vulnerability over the vulnerability with a score of 5. However, when the local environment is taken into consideration, and it becomes known that the higher CVSS scored vulnerability is not exploitable, while the lower vulnerability is, then it becomes obvious that the exploitable vulnerability should take priority.

For example: MS10-022: “Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution” has a CVSS score of 7.6. This score is deceptively low, because this particular vulnerability is exploitable by a malware kit. Rapid7 Metasploit software can exploit it. The actual risk associated with this particular vulnerability is greater than its CVSS score indicates and the Rapid7 Real Risk score of 867 (out of a total of 1000) more accurately reflects the severity of this particular vulnerability.

**Elements of Risk**

The battlefield commander relies upon useful intelligence to help determine the most effective way to deploy assets and forces. The commander needs to understand the advantages and limitations associated with terrain: desert or forest, mountains or plains; where the enemy is most likely to attack: by air, water, or land, across a field or bridge; what the enemy wants to accomplish: blow up the bridge or cross it and blow up a munitions depot; predict the consequences of a potential enemy incursion; and what to do to win the battle.

On the IT battlefield, security professionals need to measure the likelihood that a given vulnerability will be exploited and the potential impact such an exploit would cause. It is the security professional’s mission to identify the critical vulnerabilities, quantify unacceptable risk levels, and then decide what, if anything, to do. It is impractical, and unnecessary, to attempt to remediate every vulnerability listed on a scan report. Most vulnerabilities present low risk for various reasons. Perhaps the asset is non-critical, or it is not exploitable by a malware kit, or compensating controls, such as a firewall, protect it.

Security professionals measure risks using four parameters: Exposure, Likelihood, Impact, and Mitigation (see Figure 2 below). A combination of automated and expert risk intelligence methods qualifies and quantifies actual risk. Automated risk intelligence is vulnerability scanning with a solution such as Rapid7 Nexpose. Expert risk intelligence is penetration testing with a solution such as Rapid7 Metasploit. The depth and breadth of these methods determines the success of the risk assessment and mitigation process. Following is a chart of questions associated with each parameter, followed by a list of capabilities that will support security professionals in their quest to answer those specific questions.
Figure 2: Accurate risk measurement requires both automated and expert risk intelligence.

**Risk Exposure**

Exposure determines where an attack might occur.

- Have I identified all potential risk exposure across my environment?

<table>
<thead>
<tr>
<th>Automated Risk Intelligence</th>
<th>Expert Risk Intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environment attack surface discovery and analysis</td>
<td>Threat attack surface discovery and analysis</td>
</tr>
<tr>
<td>Network, OS, database, and application vulnerabilities</td>
<td>Social engineering</td>
</tr>
<tr>
<td>Web application scanning</td>
<td>Network, OS, database, and application vulnerabilities</td>
</tr>
<tr>
<td>Policy and configuration compliance</td>
<td>Advanced exploit research</td>
</tr>
<tr>
<td>0-day coverage</td>
<td>Breach path analysis</td>
</tr>
<tr>
<td>Vulnerability chaining</td>
<td>Controls assessment and validation</td>
</tr>
<tr>
<td>Support for virtualized environments</td>
<td>Exploitations</td>
</tr>
<tr>
<td></td>
<td>Brute force password audits</td>
</tr>
<tr>
<td></td>
<td>Cross-site scripting</td>
</tr>
</tbody>
</table>
**Risk Likelihood**

Likelihood assesses whether an identified vulnerability presents an actual danger, accounting for the complexity of actually exploiting a given vulnerability (access complexity), the difficulty in reaching the specific vulnerability (access vector), and authentication requirements needed to exploit the vulnerability.

- Is there a clear path to the assets in question?
- Are the vulnerabilities exploitable?
- What is the level of authentication required in order to exploit a given vulnerability?

<table>
<thead>
<tr>
<th>Automated Risk Intelligence</th>
<th>Expert Risk Intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consistent, single point of view</td>
<td>Determination of access complexity</td>
</tr>
<tr>
<td>Risk scoring determination based on vulnerability age, existence of known exploits and malware kits integrated with CVSS metrics</td>
<td>Confirm exploitability of identified vulnerabilities</td>
</tr>
<tr>
<td></td>
<td>Assess the level of authentication required to successfully exploit this vulnerability</td>
</tr>
</tbody>
</table>

**Risk Impact**

Impact measures the consequences of a security incident resulting from exploitation of a vulnerability. It considers asset or data confidentiality, integrity, and availability.

- How business-critical are the assets at risk?
- What data or information does an attacker gain access to when a vulnerability is exploited?
- What are the consequences if an incident occurs?

<table>
<thead>
<tr>
<th>Automated Risk Intelligence</th>
<th>Expert Risk Intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset criticality: weighting the importance of this asset</td>
<td>Post-exploitation analysis and VPN pivoting</td>
</tr>
<tr>
<td>Vulnerability chaining: assessing the “ripple-affect” of an exploited vulnerability</td>
<td>Automated reporting for all stakeholders</td>
</tr>
</tbody>
</table>

**Risk Mitigation**

After determining what Real Risks are present in your environment, you will want to determine what mitigation and remediation efforts you want to take.

Risk mitigation takes steps to prevent or allay security incidents.
• What actions should I take? Should I remediate, mitigate, defer, transfer, or accept this risk?

• When do I need to take this action?

• What is my acceptable level of risk? And, am I adding in any new risk with my proposed solution?

<table>
<thead>
<tr>
<th>Automated Risk Intelligence</th>
<th>Expert Risk Intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Remediation reporting</td>
<td>• Root cause analysis</td>
</tr>
<tr>
<td>• Integration with best-of-breed penetration testing and mitigation systems</td>
<td>• Mitigation verification</td>
</tr>
</tbody>
</table>

Assessing the Battlefield: Security Risk Intelligence

Combining vulnerability management, penetration testing, and best practices, Rapid7 Security Risk Intelligence re-defines and improves risk management. Security Risk Intelligence delivers the combination of qualitative and quantitative risk analysis that security professionals need to tackle the multi-faceted challenges of achieving useful information about risk. It measures contextual risk, provides step-by-step mitigation instructions, and enables rapid, trustworthy verification.

Security Risk Intelligence generates a Real Risk score. A Real Risk score adjusts a CVSS value based on contextual elements that analyze each risk element separately, for the first time incorporating both temporal and governance parameters. This provides greater insight into overall risk posture and drives more efficient risk reduction practices.

\[
\text{Rapid7 Real Risk} = \frac{\text{CVSS Impact Metrics}}{\text{CVSS Likelihood Metrics}} \times \text{Exposure} \left( \frac{\text{Malware Kits}}{\text{Exploit Rank \times time}} \right)
\]

Figure 3: Calculating Real Risk utilizes both standard and environmental metrics for contextual insight

Temporal parameters weigh the age of a vulnerability against the likelihood that a hacker tool or malware exists to exploit it. The temporal score increases over time, bringing vulnerabilities to the attention of security managers before an incident occurs.

For example, the Troj/Protux-Gen attack in 2009 exploited MS06-028, a seemingly innocuous vulnerability in Microsoft PowerPoint patched in June 2006. The rising temporal score would have flagged that vulnerability, enabling remediation before the attack commenced.

**Governance parameters** follow internal policies that qualify the criticality of assets, raising or lowering risk scores accordingly and establishing where compensating controls should be put in place.

For example, a company has a proprietary software application that runs on a 2003 version of Microsoft Windows NT. Patching the server would cause the application to crash. The company is unwilling to invest millions of dollars in an application upgrade with minimal business value. The security team implements compensating controls such as an intrusion protection system and a dedicated firewall, tests the
effectiveness of these measures, and if successful, files an exclusion for this specific vulnerability. This governance process reduces the Real Risk score by including the vulnerability exception put in place in response to the old OS version.

**Tactical: Components of Rapid7 Security Risk Intelligence**

Rapid7 Security Risk Intelligence is a combination of award-winning solutions and expertise that enable closed-loop risk verification and risk validation (see Figure 4 below):

**Rapid7 Nexpose**—Provides automated risk intelligence. It presents reports that prioritize critical and non-critical vulnerabilities using a contextual Real Risk score, provides step-by-step instructions for mitigation or remediation, and directly integrates with Metasploit. Its comprehensive vulnerability scanner uses one of the world’s largest databases of known vulnerabilities. The Nexpose database lists more than 75,000 vulnerability checks for more than 22,000 vulnerabilities. A large or mid-sized business easily generates a vulnerability report with 5,000 identified vulnerabilities, but only a fraction of them are exploitable and present a current and concrete risk. Rapid7 worked with VMware to build the first vulnerability-scanning solution that offers continuous discovery of dynamic assets in virtualized environments. It is the first vulnerability management solution included in the VMware security reference architecture.

**Rapid7 Metasploit**—Provides expert risk intelligence. Its powerful penetration-testing capabilities think like a hacker, using the world’s largest database of known exploits. It allows security operators to validate critical vulnerabilities, verify successful mitigation, and automatically update Nexpose to reduce false positives.

**Self-serve expertise**—Enhance your own skills with Rapid7 training in best practices, world-class customer support, and straightforward user interface in Rapid7 solutions. The Rapid7 Community ([https://community.rapid7.com/index.jspa](https://community.rapid7.com/index.jspa)) empowers security professionals with a forum for sharing content, collaborating on best security practices, and providing feedback.

**Rapid7 Professional Services**—Provide expertise for periodic assessments, testing, mitigation, and application of security best practices.

![Figure 4: Closed-loop Security Risk Intelligence from Rapid7](image-url)
Benefits of Security Risk Intelligence

The benefits of implementing a Security Risk Intelligence strategy include:

**Improve business decision-making through better insight.** High-quality risk intelligence helps security professionals improve operational practices and technology investment. For example, server managers can work with the security manager to test and harden servers and virtual machines before they go online. Business intelligence; security information and event management; and governance, risk-management and compliance tools can use security risk information to determine the success of risk-management and compliance-management practices and whether a risk requires further mitigation.

**Create operational efficiencies with repeatable best practices.** Nexpose reports help security managers deliver clear, correct, prescriptive advice to server and network administrators tasked with mitigation and remediation. Metasploit helps security professionals validate vulnerabilities and verify that mitigation steps provide protection. This closed-loop system is more effective than the endless “scan-and-patch” cycle that often plagues network administrators using other vulnerability scanning solutions, allowing them to meet the needs of the security team along with their other IT infrastructure responsibilities.

**Incorporates compliance requirements.** Security Risk Intelligence helps security managers view compliance as one aspect of a security practice, not the end goal. Enlarging the perspective of what needs securing also leads to compliance.

**Measurably reduce risk level over time.** When Security Risk Intelligence is the basis of regular vulnerability management operations, organizations can substantially reduce their overall risk posture over time. Using an iterative approach to continuously identify the highest risks alongside risk trending for critical assets, organizations can establish best practices for risk reduction.

**Reduce signal-to-noise ratio.** With Real Risk scoring, Nexpose and Metasploit provide reliable intelligence that quantifies the criticality of a given risk and supports threshold-based management decisions to cost-effectively reduce risk and strengthen security postures.

**Improve existing investments in third party security solutions.** Both Nexpose and Metasploit are essential intelligence systems that feed data into third-party systems such as Governance, Risk Management & Compliance solutions (GRC), security information and event management (SIEM) and intrusion prevention system (IPS) solutions, such as Sourcefire, making those tools more effective. For example, Rapid7 vulnerability data can be imported into the Sourcefire Defense Center® (http://www.sourcefire.com/security-technologies/cyber-security-products/3d-system/centralized-management). The vulnerability data adds to visibility gathered by Sourcefire RNA (http://www.sourcefire.com/products/3D/rna). At the same time, administrators can use Metasploit to verify correct configuration of third-party systems, such as testing the effectiveness of a given mitigating control.

Security Risk Intelligence in Action

Two use cases illustrate the value of Rapid7 Security Risk Intelligence.

**Use Case: Cloud Services**

A sales representative in Paris selects an applet in the corporate cloud that copies a virtual machine (VM) image from a server in New York onto her hard drive. The VM spins up on her laptop in Paris. Back at the IT operations center in New York, the Nexpose continuous discovery feature finds the new image and reports it to the security console, triggering an alert.
The alert is used to trigger a suspension of the new VM until the security manager can verify its security posture. Using Nexpose, the operator scans the VM and determines that the image is five patches behind. A critical vulnerability, MS06-071, with a Real Risk score of 918 and a CVSS value of 7.6 is present that a hacker could exploit and allow remote code execution within the private cloud. The higher Real Risk score is a result of its consideration of the environmental metrics associated with MS06-071: the age of the vulnerability (5 years since it was identified) and the fact that known exploits exists for this specific vulnerability.

Nexpose recommends remediation steps for patching the VM. The security manager forwards this information to the server administrator, flagging it for immediate attention. The server administrator patches the original VM in New York and reports task completion to the security manager. Using Metasploit Pro, the security manager verifies that the patches are effective for stopping an attack. He sends an email to the representative in Paris indicating that she can use the updated applet.

**Use Case: Malware Exploit**

An email with an Excel attachment is delivered to the corporate server. Employees know not to open files from untrusted sources, but this email looks like it came from the recipient’s college buddy.

The Excel attachment contains a macro that contains malware that exploits a known vulnerability in Windows to propagate itself and set up a bot network. The vulnerability exploited in this attack, MS06-014, has a Real Risk score of 760, because any kid with a computer can “weaponize” an Excel file using a malware kit. The base metric CVSS score of 5.1 for this specific vulnerability would not flag the danger within this environment, but the Rapid7 Real Risk score identifies the malware kits that have been known to exploit this vulnerability, combines it with other known exploits for this vulnerability, and increments the score appropriately.

Just last week, the security manager used Metasploit to send a malicious email and verify that antivirus software on the email server detects this macro and deletes it before delivering the message to the user. Knowing that compensating controls are in place, the security manager used Metasploit to mark the Windows vulnerability as “acceptable” within Nexpose.

**Why Choose Rapid 7 Security Risk Intelligence**

Rapid7 offers all the solutions and best practices that support comprehensive Security Risk Intelligence. Built upon award-winning Rapid7 Nexpose and Metasploit solutions, Security Risk Intelligence helps organizations make better business decisions related to IT security with specific guidance to answer: “What do we fix first? How do we fix it? What level of risk are we willing to accept?”

Central to Security Risk Intelligence is the Rapid7 Real Risk™ score, a contextual risk metric that accurately prioritizes mitigation tasks to reduce overall risk as quickly as possible. More informative than conventional risk prioritization schemas such as the Common Vulnerability Scoring System (CVSS), Real Risk incorporates criteria specific to each IT environment and its security policies.

Rapid7 Security Risk Intelligence delivers strategic advantages in the battle for control of your IT environment. In an industry crowded with vendors claiming to deliver proactive vulnerability management, only Rapid7 has everything you need for continuous security improvement. Only Rapid7 offers unified vulnerability-scanning and penetration-testing solutions, customer training in best practices, and professional expertise that organizations need to implement Security Risk Intelligence. Security Risk
Intelligence helps organizations implement operational best practices in closed-loop vulnerability management, build productive relationships with IT operations, and achieve measurable drops in risk exposure over the shortest period of time.

IDC agrees: “Rapid7’s leadership and strong growth indicate that it is on solid ground, and it can meet the requirements to succeed in its markets. Rapid7 has critical awareness of market forces and vendor competitive positioning and is focused on leveraging its strengths to increase its share. The overarching strategy that centers around converged vulnerability management and penetration testing, context-rich security intelligence, and testing of security controls outside of patch distribution creates a compelling strategy that has the potential to redefine Rapid7’s segment.”

For More Information

To learn more about Security Risk Intelligence and Real Risk scoring, contact Rapid7 sales at 866.772.7437 or online at sales@rapid7.com.

About Rapid7

Rapid7 is a leading provider of IT security risk management software. Its integrated vulnerability management and penetration testing products, Nexpose and Metasploit, and mobile risk management solution, Mobilisafe, enable defenders to gain contextual visibility and manage the risk associated with the IT environment, users and threats relevant to their organization. Rapid7’s simple and innovative solutions are used by more than 2,000 enterprises and government agencies in more than 65 countries, while the Company’s free products are downloaded more than one million times per year and enhanced by more than 175,000 members of its open source security community. Rapid7 has been recognized as one of the fastest growing security companies by Inc. Magazine and as a “Top Place to Work” by the Boston Globe. Its products are top rated by Gartner®, Forrester® and SC Magazine. The Company is backed by Bain Capital and Technology Crossover Ventures. For more information about Rapid7, please visit http://www.rapid7.com.