SANS

A SANS Whitepaper

How to Show Business Benefit by Moving to Risk-Based Vulnerability Management

Written by **John Pescatore**

August 2020

Sponsored by:

Tenable

For many years, cars had analog indicators on the dashboard, including the infamous "idiot light" which, loosely translated, meant: "You ignored the oil pressure and water temperature gauges and now will have an expensive engine repair." As microprocessors became common in automobile engine control systems, that glowing bulb was replaced by the dreaded "check engine" multi-indicator message, which largely meant: "You ignored the 27 little indicators of problems and now will have an expensive engine repair." Great for the towing and repair industry; not so great for businesses and families with vehicles stuck on the side of the road.

Flash forward to now. After-action reports reveal that well-known vulnerabilities were exploited by attacks, causing millions of dollars' worth of damage to businesses and their customers. The companies' security programs had discovered those vulnerabilities and notified IT operations and corporate management, but the vulnerabilities had not been remediated or mitigated. The check engine light had been turned on, but no connection had been made to business criticality. Again, great for the incident response and security consulting services; bad for the businesses' bottom lines.

Moving to a risk-based vulnerability program has helped many businesses avoid the check engine light trap. This paper provides SANS advice for actionable steps to enable security managers to reduce risk and demonstrate business value by increasing the maturity and effectiveness of their vulnerability management processes and controls. The main focus is on the key questions to ask of product and service providers to select the best approach for your organization.

From Vulnerability Scanning to Risk-Based Vulnerability Management

Security in any form is simple: Keep the bad guys from getting to your valuable stuff. It gets a bit more complicated when you add in "Make sure good guys can get to your valuable stuff." Addressing financial constraints adds another level of complications: "Within a real-world budget, make sure *only* good guys can get to my valuable stuff."

In the physical world, even this approach is still straightforward. We know the value of the physical goods we have locked away and where we put them. We know the strength of materials for walls, doors, locks and safes, and we know their vulnerabilities. The bad guys must physically get to our location. We can easily require strong authentication for access control and differentiation between good guys and bad guys.

Unfortunately, in cybersecurity everything changes. The value of information is hard to quantify, and many copies can exist in many places. There are no strength-of-materials tables for software. Vulnerabilities can show up at any time. Bad guys can be anywhere on the planet when they attack us. Simple and easily compromised reusable passwords are the dominant way of trying to discriminate between bad guys and good guys.

The security challenge is harder in the cyber realm, but established cybersecurity frameworks such as the Center for Internet Security (CIS) Critical Security Controls[1] point out that the same basic processes apply:

Step 1. Know where your crown jewels are (asset inventory, and prioritization by business criticality).

Step 2. Know where your weaknesses are (vulnerability discovery and assessment of high-level severity ranking).

Step 3. Know what threats are active (threat intelligence).

Step 4. Prioritize remediation or mitigation of vulnerabilities by criticality and threat activity (vulnerability management).

All too often, enterprises are doing only part of Steps 1 and 2—discovering assets but not determining business criticality; scanning for vulnerabilities and then notifying IT operations of the enormous volume of vulnerabilities discovered; and ranking by vendor-provided severity ratings. While standards such as the Common Vulnerability Scoring System (CVSS) have enabled more repeatable severity ratings, the CVSS relies on optional user-customizable environmental metrics to adjust severity scoring based on mission impact. In practice, however, the environmental scores are largely unused or used overly simplistically. This results in "grade inflation" in CVSS scores, diluting the usefulness of prioritization.

[1] www.cisecurity.org/controls/

Without any meaningful risk prioritization, IT tends to add those issues to its trouble ticket system, which already has a large backlog of service actions. A misconfiguration or missing patch is often not seen as an immediate priority, especially compared to trouble tickets with immediate impact on customers or business services.

That is why the other steps are critical:

- **Knowledge of asset criticality** (accurate identification of business-critical crown jewels, so that trouble tickets are associated with high business impact and prioritized)
- **Threat intelligence** (timely and detailed information on threats that are actively exploiting the discovered vulnerabilities)
- **Business impact-based prioritization** (combining accurate and fresh asset-criticality information and threat intelligence to determine which vulnerabilities should go to the top of the trouble ticket queue for immediate mitigation or remediation)

Those three steps are essentially the basis of risk-based vulnerability management—actions are prioritized by the severity of the likely impact to the business. The sign of a successful risk-based vulnerability management (RBVM) program is a demonstrable reduction in business impact from all forms of cyber incidents.

Real-World Definition of Risk Analysis

There are many complex risk assessment and management frameworks available, almost all based on variants of the formula: "Probability of event times value of asset equals risk level," which came out of the physical risk-estimation world. The problem is that in the cyber world, the probability of the event is a very small imaginary number and the value of information assets is usually a very large imaginary number. The result is risk ranking based on medium-sized imaginary numbers that have little connection to real-world events or decisions.

One simple version has proven to work well over the years: **Risk = Threats x Vulnerabilities +/– Action** (see Figure 1). The most important component is **Action**. Business and security teams don't control the threats. Attacks will always occur—on the attacker's schedule and using increasingly sophisticated delivery mechanisms and evasion techniques. People and software will always have vulnerabilities. While there are actions we can take to avoid some vulnerabilities and mitigate many others, the reality of phishing and patching tells us that new vulnerabilities will always be discovered.

Figure 1. Simple Risk Assessment and Management Formula

The bottom line is that businesses can't control the risk-increasing (+) aspect of action. Risk increases when attackers launch and refine their attacks or when weaknesses in IT operations lead to misconfigured or vulnerable systems and/or applications. **What we *can* control are the risk-reducing (–) action components of the risk equation. That action is what reduces business impact.**

The key is for security teams to know which assets are critical to the business, which threats are active, and which are most likely to reach those business-critical assets. Because resources will always be limited, this approach prioritizes the use of staff and budget to enable accurate, timely and efficient action to fix the critical vulnerabilities or to segment or shield them until they can be fixed—that is what RBVM is all about. Industry analyst firms such as Gartner[2] and Forrester[3] (see Figure 2) have produced research with more details about the processes.

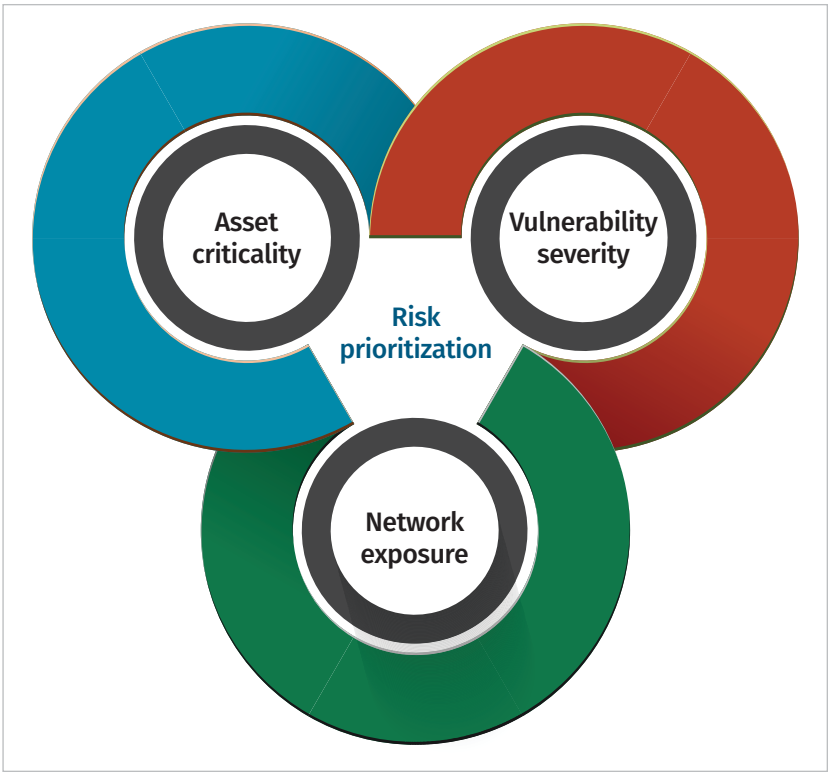

Figure 2. Three Attributes that Enable Risk-Based Prioritization, According to Forrester

Migrating to a Robust Risk-Based Vulnerability Management Program

Like everything else in cybersecurity, implementing RBVM will require a mix of:

- **People—**Organizations need sufficient staff with mixes of analytic and hands-on skills to keep up with changes in IT, business technology use, changes in threats, and modern tools and techniques.
- **Process—**Vulnerability management processes need to be comprehensive and integrated into both IT operations and business processes. Equally important and often problematic, those processes need to be both repeatable *and* adaptable to meet operational constraints while rapidly addressing changes in threats and risks.
- **Technology—**With a base of solid VM processes, cybersecurity products and services are used to both implement security controls and act as force multipliers for limited staff resources.

[2] www.gartner.com/document/3887782 [Membership required for access.]

[3] www.forrester.com/report/The+Forrester+Wave+Vulnerability+Risk+Management+Q4+2019/-/E-RES152075

The first step toward implementing an RBVM approach is an accurate and thorough understanding of the gaps in your current staffing, processes and technology needed for an effective program. In working with businesses and government agencies, SANS has seen six distinct patterns of readiness or maturity with regard to RBVM (see Figure 3).

Figure 3. Patterns of RBVM Effectiveness

Organizations that match Patterns 1 (Greenfield) or 2 (Vulnerability Assessment [VA] Owned by IT Ops) will need to make progress in several areas before being able to implement RBVM. This paper focuses on organizations that match Patterns 3 and 4:

- **Pattern 3: Security Scans and Tosses—**Because most compliance regimes (such as PCI DSS, Federal Information Security Management Act [FISMA] and HIPAA) require vulnerability scanning to be done, most larger organizations have at least reached this level. To move up in readiness for RBVM, Pattern 3 organizations have to get better at prioritizing assets by business criticality and support multiple methods of vulnerability assessment. Analyst skills should be good enough to at least manually integrate key elements of threat intelligence into vulnerability alert criticality levels with trouble ticket system integration.
- **Pattern 4: Formal Vulnerability Assessment and Management (VAM)—**Pattern 4 capabilities provide a solid starting point for implementing RBVM processes backed by RBVM products and services. At this level, the major efforts required are staff skills and tools for rapid assessment of high criticality threats and vulnerabilities, working processes that address cloud-based assets, and the acquisition and deployment of tools to support the functions of RBVM.

With the people and process aspects addressed, technology can be selected to increase both the effectiveness and the efficiency of your RBVM approach. The following section provides guidance on how to evaluate potential RBVM products and vendors.

Select the Optimum Technology

Risk-based vulnerability management consists of a number of integrated functional areas. Table 1 shows the Gartner, Forrester and SANS lists of RBVM functional areas used in this paper. Key definitions follow.

Asset Discovery/Classification—Discovery of devices and software elements within the boundary of responsibility and characterization or classification of the functions performed and the level of business criticality

Vulnerability Assessment and Rating—Assessment of each discovered asset to discover vulnerabilities, such as misconfigurations, missing patches, etc., as well as the severity rate of vulnerabilities using standard approaches, including but not limited to the Common Vulnerability Scoring System.[4] This rating includes an estimation of the exposure of the vulnerability to known threat paths.

Table 1. Risk-Based Vulnerability Management Functional Areas

Gartner	Forrester	SANS
• Assess • Prioritization - Value - Threat - Exposure • Compensate - Remediate - Mitigate - Accept	• Asset Management • Vulnerability Enumeration • Prioritization - Value - Threat - Exposure • Remediation	• Asset Discovery/ Classification • Vulnerability Assessment and Rating • Prioritization - Value - Threat - Exposure • Remediation - Fix/Patch - Mitigate/Shield - Accept/Monitor

Prioritization—Using business criticality, threat intelligence, vulnerability severity and exposure information, rank vulnerabilities by likely risk to critical business functions. This process includes groupings of related vulnerabilities. This process also includes dashboard functions for measuring, monitoring and communicating overall risk levels as well as supporting ad hoc queries.

Remediation Support—Diagnostic detail and guidance to aid in remediation, support for manual and automated shielding or mitigation approaches, as well as for enhanced monitoring/reassessment of vulnerabilities that must be accepted

Skilled cybersecurity staff is a scarce resource; mature RBVM products and services can provide support and some level of automation across all of the functional areas. Many organizations have existing criteria and processes for cybersecurity vendor/ product evaluations. Two efforts are key to selecting the best RBVM technology for your organization:

- Developing a set of weighted evaluation criteria that map business and cybersecurity needs to the key features of an RBVM product or service
- Using hands-on testing and evaluation or demonstration of the product in real-world use in your environment or on a testbed similar to your operational environment

[4] https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System

This section provides a starting point for development of RBVM-specific evaluation criteria by listing the key questions to ask in each functional area.

Product/Service Questions

1. How does the product perform asset discovery, identification and classification? Is the solution integrated with ITSM or other asset/configuration management products used by IT operations? Does the supported asset list include all technology and services in use, such as devices, operating systems, containers, cloud services and applications used on your business-critical segments?
2. What mechanisms (network scanning, agent-based, credentialed agentless, passive monitoring) does the product support for vulnerability discovery? What factors and granularity are included in ranking of vulnerabilities (CVSS or vendor score, current threat activity, asset criticality, current exposure level or others)? How frequently are these factors updated? Does the VA function support "assess again at remediation due date" logic?
3. How are vulnerabilities prioritized using the information from vulnerability assessment and rating, and other factors? Does the reporting support critical cybersecurity readiness metrics, at a minimum time to discover and time to mitigate? What higher level metrics are provided to demonstrate overall business-level risk, both current and trending? What risk management framework standards are supported for visualization and reporting? What custom risk-ranking features are provided?
4. What level of remediation guidance is provided beyond links to vendor patching guidance or CVE reports? What level of granularity is provided in identifying the location of the vulnerability? What grouping of vulnerabilities is supported to reduce the IT operations workload in implementing fixes? What mitigation/shielding guidance is supported for the firewall/IPS or segmentation measures you have available? Does the product include enhanced monitoring for risks that must be accepted?
5. For each major function (asset discovery and classification, vulnerability assessment, business impact/risk prioritization), what level of automation (versus manual analyst effort) is supported?
6. What level of ad hoc/what if/change assessment type queries are supported? What mechanisms for alerts, trouble tickets and other information-sharing are supported? Does the integration between the RBVM product and ITSM systems provide bidirectional integration with sufficient security/privacy controls?

RBVM-Specific Vendor Questions

1. What formal technology partnerships exist with other vendors or information sources related to asset identification, vulnerability and threat information, and industry-specific risk information?
2. How many people and what percentage of revenue are dedicated to active and proprietary (beyond aggregation of open source information) vulnerability and threat research, and mitigation development and testing? Do vendor employees contribute to and participate in open source vulnerability research efforts and does that information feed back into RBVM product updates?
3. What percentage of revenue comes from a) product installation support, and b) from custom security services, such as penetration testing, risk analysis and incident response support?
4. Does the company support customer benchmarking and best practices groups to enable information-sharing across the user community?

Summary

Vulnerability discovery products have been around for more than 30 years, and regular vulnerability assessment has been a requirement of every major compliance regime for more than 15 years. Yet, most after-action reports of serious breaches still find that the cause of millions of dollars in damage to the business was a failure to patch or reconfigure a known vulnerable computer or service. As it is with termite infestations, finding vulnerabilities is just the first step—without mitigation, the damage will continue and be severe.

SANS defines the success of security operations as:

> "... when it **intervenes** in adversary efforts to impact the availability, confidentiality and integrity of the organization's information assets. It does this by **proactively** making systems more resilient to impact and reactively **detecting, containing and eliminating** adversary capability."[5]

Corporate or agency management will not consider security operations to be valuable or successful if vulnerabilities were discovered but attacks succeeded nevertheless. Security teams need to be able to reduce the friction for IT and business operations to make the changes necessary to remediate or mitigate business-critical vulnerabilities. That task requires expressing danger in business terms and prioritizing vulnerabilities by true business risk, in language and displays that speak to the business side of the organization. Back up this communication with accurate and detailed mitigation advice that reduces the obstacles to effective, efficient and timely risk reduction. This approach enables you to convey risk metrics and timelines in business-relevant terms and enables proactive vulnerability-avoidance by working across the company's operations and supply chain. Risk-based vulnerability management provides a measurable and adaptive way of meeting these needs.

[5] "The Definition of SOC-cess? SANS 2018 Security Operations Center Survey," August 2018, www.sans.org/reading-room/whitepapers/analyst/definition-soc-cess-2018-security-operations-center-survey-38570, p. 4.

About the Author

John Pescatore joined SANS as director of emerging security trends in January 2013 after more than 13 years as lead security analyst for Gartner, running consulting groups at Trusted Information Systems and Entrust, 11 years with GTE, and service with both the National Security Agency, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and surveillance systems and "the occasional ballistic armor installation." John has testified before Congress about cybersecurity, was named one of the 15 most-influential people in security in 2008 and is an NSA-certified cryptologic engineer.

Sponsor

SANS would like to thank this paper's sponsor: