



Dynamic Best Practices of Vulnerability Management

Executive Summary

Building a strong program based on mitigating known vulnerabilities has transformed from a security-centric process to an operational necessity for business success. Enterprises can build static perimeter defenses and scan for malicious code containing a known exploit, but the root cause of the problem is the existence of vulnerabilities in the corporate network. More than 80 percent of companies connected to the Internet experienced a disruption in business due to a worm or virus in 2003, even with ubiquitous antivirus deployments. Vulnerability management, the discovery of vulnerabilities and assessment of the risk to the network, is a critical part of both the security and business landscape that all enterprise security teams need to understand and implement for long-term success.

Vulnerabilities, usually expressed by a product vendor as a defect requiring a patch, upgrade or configuration change, are the weaknesses in a security profile that attackers target. Once a vulnerability is discovered, it is only a matter of time before an attacker develops the worm, virus or intrusion that can take advantage of the defect. Companies that rely totally on signature-based defenses against known exploits are helpless against fast-moving exploits and zero-day attacks that propagate globally at Internet speed. The goal of the security team is to reduce risks by identifying and eliminating weaknesses in an effort to reduce the window of opportunity in which an exploit or attacker could impact the organization.

Qualys, a leader in on-demand network security audits and vulnerability management, has published research based on analysis of years of vulnerability and exploit data. Their findings are internationally recognized as "The Laws of Vulnerabilities," which define vulnerabilities in the context of half-life, prevalence, persistence and exploitation. The Yankee Group puts "The Laws of Vulnerabilities" into action as our research, along with in depth customer interviews, serves as a basis for "Dynamic Best Practices of Vulnerability Management." The Yankee Group has identified four dynamic best practices and has defined a set of specific actions to represent the continual motion required from IT to adjust to the dynamics of networks, users and vulnerabilities.

1. **Classify.** Assign network resources a position in the hierarchy of assets, with the highest level in the hierarchy being the most critical resources.
2. **Measure.** Assess security team performances by their effectiveness in reducing exposures to key vulnerabilities.
3. **Integrate.** Vulnerability management bolsters the effectiveness of patch management, configuration control and early-warning services.
4. **Audit.** Security executives regularly audit the effectiveness of integrated vulnerability processes.

This special report, commissioned by Qualys, reviews "The Laws of Vulnerabilities" and applies these principles to the Dynamic Best Practices for Vulnerability Management. Information in this report derives from Yankee Group research and interviews with enterprise security officers of global organizations.

Table of Contents

I.	Introduction	3
II.	The Laws of Vulnerabilities	3
	The Law of Half-Life	4
	The Law of Prevalence	4
	The Law of Persistence	5
	The Law of Exploitation	5
III.	Dynamic Best Practices of Vulnerability Management	6
	Classify	6
	Measure	7
	Integrate	7
	Audit	8
IV.	Conclusions	8

I. Introduction

A common goal for IT departments is to achieve a 100 percent secure network, safe against business disruptions caused by misconfigurations, intrusions, worms and viruses. Security teams diligently update intrusion signatures and antivirus definition files, and apply patches to bolster their defenses against the next exploit that could rapidly disrupt business. However, it is all too likely that noncompliant systems on the network will provide the hole that unravels the entire security posture of the network. A network presumed to be secure when the security team goes home at night may be completely exposed by the time they arrive at work in the morning due to an overlooked vulnerability that an intruder exploited. All of the advances made by security teams in protecting business continuity can be lost quickly. Focusing strictly on exploits represents an eternal battle that IT can never win. IT simply cannot anticipate which vulnerabilities will have an exploit released against it, and signature-based anti-malware solutions cannot recognize the first instances of an attack until signatures are developed. It is, by definition, a reactionary policy that takes measurable control out of the hands of IT. Enterprises need to block exploits with up-to-date signature files; however, vulnerability management should be the cornerstone of the secure network policy.

The Dynamic Best Practices of Vulnerability Management reflects the variable dynamics associated with managing security measures required to identify and eliminate weaknesses effectively. This is an aggressive plan to remove vulnerabilities in key resources, in a timely manner, before attacker code can be developed to exploit the vulnerability.

II. The Laws of Vulnerabilities

Gerhard Eschelbeck, CTO of Qualys, defined the “Laws of Vulnerabilities” from a statistical analysis of vulnerabilities collected on an aggregate basis from millions of scans performed across thousands of networks (see Exhibit 1). From this research, Eschelbeck determined the laws that govern vulnerabilities' life cycle. It is important to understand these laws before developing corporate best practices, because they provide a framework of how pervasive vulnerabilities have become and why dynamic best practices are a necessity.

Exhibit 1

Laws of Vulnerabilities

Source: Qualys, 2004

Laws of Vulnerabilities

Half-Life

The half-life of critical vulnerabilities is 30 days and doubles with lowering degrees of severity

Prevalence

50% of the most prevalent and critical vulnerabilities are being replaced by new vulnerabilities on an annual basis

Persistence

The lifespan of some vulnerabilities is unlimited

Exploitation

80% of vulnerability exploits are available within 60 days of the vulnerability release

The Law of Half-Life

The half-life of critical vulnerabilities is 30 days and doubles with lowering degrees of severity.

The half-life law reflects the difficulties in successfully patching large networks. The data shows that in the first month of a critical vulnerability, IT, on average, only mitigates the vulnerability in half of its network. The second month finds half of the remaining vulnerable systems protected, and so on. The half-life law points to a need in organizations to understand all their network assets and identify unpatched weaknesses as quickly as possible. The half-life of vulnerabilities implies lessons to be learned in deriving the best practices of vulnerability management, including:

- **You can't patch them all at once.** There always will be systems not connected to the network, or new assets added to the network that do not reflect the latest patch or upgrade. These systems will be more vulnerable to exploit code.
- **Mitigate more than the remaining half of the vulnerabilities over the next month.** Half of the network resources are protected in the first 30 days of a critical vulnerability, so the patch and distribution procedures are known to work. More than 50 percent of the remaining resources should be treated in the subsequent months.
- **Improve reduction of risk in the enterprise by shrinking the half-life to less than 30 days.** Security teams should strive to make improvements that reduce the current half-life of vulnerabilities. In other words, since the current half-life is 30 days, security teams should work to reduce vulnerability half-lives in their organization.

***Dynamic Best Practices Action:** Patch all systems within 30 days of the release of a critical vulnerability. The Yankee Group recommends 21 days for critical systems and a rollout procedure to other assets based on their priority level. This is a dynamic best practice since the rate in which vulnerabilities are exploited continues to get shorter; therefore, this further reduces the time frame to fix vulnerabilities.*

The Law of Prevalence

Fifty percent of the most prevalent and critical vulnerabilities are replaced by new vulnerabilities on an annual basis.

- **New critical vulnerabilities occur throughout the year.** Left undetected and unpatched, new vulnerabilities can undo all of the security team's hard work. Keep vigilant and adjust assessment cycles according to the value of the network resources to be protected. Again, what is safe today may be vulnerable tomorrow.
- **Half of the vulnerabilities still exist in the network a year later.** Be sure management processes completely remove a vulnerability. This includes updating configurations for new devices placed on the network as well as implementing management metrics to drive the vulnerability risk to zero. Effective security teams will drive down the persistence of vulnerabilities.
- **Vulnerability management is a never-ending process.** Implement management metrics to refine the best practices for vulnerability management. It is very difficult to manage what you cannot measure, which is one of the problems of total reliance on hit-or-miss, exploit-oriented signature-based products.

***Dynamic Best Practices Action:** Continually test assets for weaknesses. Test critical assets a minimum of every 5 to 10 days. This is a dynamic best practice as the frequency may increase as the number of vulnerabilities rises and the trend in time to exploitation gets shorter.*

The Law of Persistence

The lifespan of some vulnerabilities is unlimited.

A few vulnerabilities never totally disappear from the network security profile. Scanning after patching still catches vulnerabilities recurring in the network. These vulnerabilities could reappear for a variety of reasons. For example, they may be borne in application code, reintroduced via new system installations, or come from computing devices added to the network that did not meet the latest security level.

- **Scan configurations of new equipment to be sure they do not reintroduce old vulnerabilities to the network.** Be sure processes for deploying new equipment require scans for vulnerabilities after all software is installed and configured.
- **Be alert for vulnerabilities that may be lurking in application code.** It was relatively easy to find SQL servers during the SQL Slammer attack, however it was very difficult for IT departments to determine which applications had embedded the Microsoft database engine, MSDE. When old vulnerabilities recur, one possible source is application upgrades.

Dynamic Best Practices Action: *Continually test assets to uncover reintroduced weaknesses. Scan critical assets a minimum of every 5 to 10 days. It is an ongoing process to identify and eliminate weaknesses.*

The Law of Exploitation

Eighty percent of vulnerability exploits occur within 60 days of the vulnerability release.

The announcement by a product vendor about a security patch or upgrade starts the race between enterprises deploying corrections and attackers exploiting the vulnerability. Traditionally, there is a period of several weeks before an exploit is unleashed. However, this time frame is shrinking rapidly and security teams can no longer count on the 6-month interval that worms such as SQL Slammer gave us. Today, most product vendors do not announce a vulnerability until there is a patch available to protect enterprise customers. However, the race continues and tips in the favor of attackers if vulnerabilities are left unpatched for more than 60 days.

- **Keep an eagle eye on key vendors for early warnings of available patches for critical resources.** Build the vulnerability review process to quickly get information on the severity of the vulnerability, available patch, and where in the network the company is most at risk. Proper vulnerability management solutions have this mechanism built in to the auditing solution; therefore, each time a network audit takes place, it automatically incorporates the latest vulnerabilities, ensuring proactive identification of security issues.
- **Make a team decision on when to patch.** In some unintentional situations, the patch may place the company's business processes more at risk than the vulnerability itself. This is especially the case when the patch is part of a bundle of related patches. Therefore, it is important to put a process in place to quickly determine if the patch is going to be applied, if the vulnerability can be mitigated by configuration control, or if the security team will assume the risk that an exploit will not cause serious damage.
- **Integrate with automated procedures.** Time is of the essence when a "go" decision is made on applying a patch. Integrate information from your vulnerability management system with patch management and configuration control systems to accelerate the accurate remediation of the vulnerability. Use the network auditing solution to verify the patch has eliminated the weakness.

- **Be prepared to scan for vulnerabilities on an attack basis.** Some day zero exploits may strike before the patch has been widely deployed. Have escalation procedures in place to immediately scan, on demand, the network for vulnerable points on an attack basis.

Dynamic Best Practices Action: *This is a reinforcement of the previous actions (i.e., scan frequently and remediate weaknesses proactively) to prevent inevitable exploits from adversely affecting business continuity. Maintain awareness and have procedures in place to mitigate urgent risks.*

III. Dynamic Best Practices of Vulnerability Management

The Dynamic Best Practices of Vulnerability Management are based on key findings from the Laws of Vulnerabilities. The best practices apply vulnerability management as one solution IT can use to measure and manage the effectiveness of a network defense program. Vulnerability management alone does not fix vulnerabilities—patch and configuration management does that while antivirus software seeks to block identified malware. Simply stated, vulnerability management helps managers understand network assets, identify weaknesses, measure security effectiveness, enforce policy and assess the success of patching efforts. The Dynamic Best Practices of Vulnerability Management refers to the security team's actions to classify, measure, integrate and audit.

Exhibit 2 shows the enterprise goals for vulnerability management that outperform what the Law of Half-Life would predict. To remove vulnerabilities in key assets before an exploit can strike, IT needs to establish goals to lower the enterprise Law of Half-Life by patching and updating critical resources in a timely manner. This is especially important for networked resources that are vital to business operations.

Classify

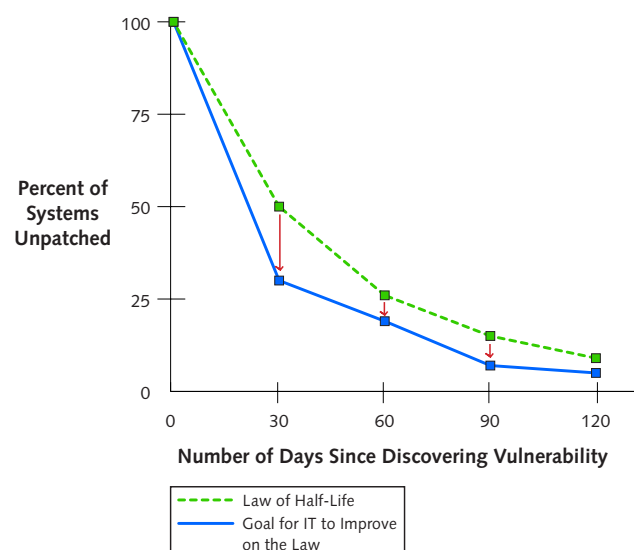
Identifying and classifying network resources is the first best practice to implement. The Law of Half-Life tells us that only about 50 percent of network resources will be protected within the first 30 days an enterprise is aware that a vulnerability exists. Understanding and classifying assets to a category allows IT to apply policies more efficiently and, if the organization is time or resource constrained, enables the security team to focus on patching the most critical assets first.

- **Classify network resources.** Most enterprises will have 5 to 20 categories of network assets prioritized by value to the business and by the ability to manage the assets as a group. There are far too many assets in an enterprise network to manage individually, and at an average cost of \$235 to patch a desktop, patching all vulnerabilities as rapidly as possible becomes cost prohibitive. Classifying resources by categories is the best practice for vulnerability management (see Exhibit 3 on next page).
- **Tier the hierarchy of assets by value to the business.** Critical databases, financial systems and other business critical assets must be in a higher category than clerical desktops, non-production servers and remote laptops.

Exhibit 2

Enterprise Goals of Improving on Law of Half-Life for Vulnerability Management

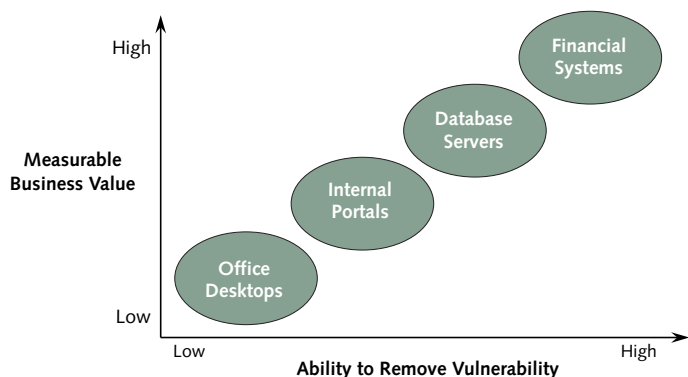
Source: Qualys, 2004



- **Limit the higher priority categories by the ability to manage vulnerabilities.** It is vital to patch the most critical assets before an exploit is released. The Yankee Group recommends that enterprises completely protect the higher priority categories against vulnerabilities within 21 days to defeat the law of prevalence by a healthy safety margin.
- **Classify asset priority based on the value to the business and do not give critical assets a lower categorization because you assume they are safe.** Exploits will find their way through your network—in other words, do not place critical business processors in a lower priority because you think they are safely tucked away behind the DMZ.
- **Scan the highest categories regularly for vulnerabilities.** The Yankee Group has discovered that enterprise customers following the current best practices guidelines are auditing their critical assets every 5 to 10 days—with the average being weekly. These are your most important assets and you must protect them. Lower categories of assets can tolerate somewhat less frequent scanning.

Exhibit 3
Classify Network Resources

Source: The Yankee Group, 2004



Measure

Vulnerability management solutions test network resources for the presence of known vulnerabilities. This produces a record per scan of the number of vulnerabilities discovered, their severity, and the categories affected. It is the true measurement of a patch and configuration control program. Measuring the effectiveness of a vulnerability management program is the next best practice.

- **Measure your network against the half-life and persistence curves.** Beat the half-life curve by graphically tracking the percentage of vulnerabilities mitigated within each 30-day cycle and the number of vulnerabilities that extend past 180 days. Tracking total vulnerabilities is also useful, but be sure to account for the rate of announced vulnerabilities from the vendors (a climbing rate of exposed vulnerabilities may be a function of vendor quality announcements and not a function of an inferior patching process). Evaluate process changes against these metrics to measure best practices.
- **Measure team performance by the half-life results and the treatment of the persistence law.** Chart the performance of each security team by asset category, with comments in performance reviews based on competition with peers for protecting the business processing environment. The goal of a security team is to reduce risks, particularly to critical assets. Therefore, place such security metrics into the human resources performance review process and make people accountable once they have the proper tools in place to quickly and accurately audit the network on an ongoing basis.
- **Use gathered metrics to communicate the security problem to senior management.** Lines of business managers can understand the trend of vulnerabilities and the efforts of the security team to minimize the risk to the enterprise. Use actual performance measurements to educate your executive management team and show the value of security best practices in maintaining business continuity, reducing risks and maintaining a secure infrastructure.

Integrate

Vulnerability management provides the common measurable indication that the network is as secure as IT can make it. The best practice of leading enterprises is to integrate the intelligence gained into the entire security team cycle of identifying assets and removing vulnerabilities.

- **Integrate with discovery systems such as network integrity systems** to find new servers and desktops on the network, and schedule a vulnerability scan upon detection. A single vulnerable computer can compromise the entire network.
- **Integrate with patch management systems to confirm completion of the task.** Most enterprises do not trust patches enough to automate distribution of patches upon a recognized vulnerability. However, scanning to confirm completion of an upgrade or patch distribution to a class of resources is a pragmatic check and balance.
- **Integrate into management reporting portals.** Take the mystery out of security by reporting on operational progress achieving vulnerability goals based on the Laws of Vulnerabilities. This is a best practice for raising the level of awareness among executive management for the accomplishments of the security team.

Audit

Vulnerability management delivers the fundamental metrics management needs to understand the state of the corporation's network security program. Use the metrics to evaluate successes and failures of various efforts to improve performance.

- **Evaluate actual vulnerability management results against targeted metrics.** Get in the habit of setting, and exceeding, performance goals for reducing the level of critical vulnerabilities in the network.
- **Regularly review vulnerability management reports with the security teams.** Understand what could be affecting the results and brainstorm better methods to handle vulnerabilities. Be sure to conduct postmortems when vulnerability management events are triggered by the sense of urgency brought on by a new exploit.

- **Measure the performance of security teams by the reduction of critical vulnerabilities.** Compare distributed teams performance, recognizing leaders and followers. Peer pressure will encourage security teams to share experiences of actions, leading to a more rapid reduction in vulnerabilities.

IV. Conclusions

The Dynamic Best Practices of Vulnerability Management provides a framework for organizations to create their own best practice-based system to minimize risks to their network and maintain business continuity (see Exhibit 4). When considered in relation to the Laws of Vulnerabilities, the impact of an organization's effectiveness in identifying risks and reducing vulnerabilities serves as a true measure of a security team's performance. The best practices of the enterprises we interviewed all involve using vulnerability management to measure and monitor security of their internal infrastructure and extended network of business associates. They also use it to enforce security procedures for patching, upgrading and deploying networked systems. Understanding the underlying lessons of the Laws of Vulnerabilities and applying this knowledge to a dynamically changing network yields an effective methodology for identifying and eliminating weaknesses, which should reduce the window of opportunity in which security could be compromised.

Exhibit 4

Dynamic Best Practices of Vulnerability Management

Source: *Qualys, 2004*

Best Practices of Vulnerability Management

Classify network assets to more efficiently prioritize vulnerability mitigation programs, such as patching and system upgrading.

Measure the effectiveness of risk mitigation by setting goals of reduced vulnerability exposure and speedier mitigation.

Integrate vulnerability management with discovery, patch management, and upgrade management processes to close vulnerabilities before exploits can strike.

Audit the performance of security policy implementations, security team performance, and process improvements to build a culture of refining security operations.

The Yankee Group

World Headquarters

31 St. James Avenue

BOSTON, MASSACHUSETTS 02116-4114

T 617.956.5000

F 617.956.5005

info@yankeegroup.com

Regional Headquarters

North America

31 St. James Avenue

BOSTON, MASSACHUSETTS 02116-4114

T 617.956.5000

F 617.956.5005

info@yankeegroup.com

951 Mariner's Island Boulevard, Suite 260

SAN MATEO, CALIFORNIA 94404-5023

T 650.522.3600

F 650.522.3666

info@yankeegroup.com

EMEA

55 Russell Square

LONDON WC1B 4HP

UNITED KINGDOM

T 44.20.7307.1050

F 44.20.7323.3747

euroinfo@yankeegroup.com

For More Information

T 617.956.5000

F 617.956.5005

E-mail: info@yankeegroup.com

Web site: www.yankeegroup.com

Advisory Services

Yankee Group AnalystDirect advisory service annual memberships offer clients access to research and one-to-one expert guidance.

Advisory services represent our best value for clients. The services help our members understand industry, regulatory, competitive and market-demand influences, as well as opportunities and risks to their current strategies.

Membership includes an invaluable in-person strategy session with Yankee Group analysts, direct access to a team of analysts, research reports, forecasts, research notes and regular audioconferences on relevant topics.

We offer advisory services on almost 30 selected topics in Telecommunications; Wireless/Mobile Communications; Consumers, Media & Entertainment; and Information Technology Hardware, Software & Services.

Decision Instruments

The Yankee Group offers a full portfolio of technology and market forecasts, trackers, surveys, and total cost of ownership (TCO), return on investment (ROI), selection and migration tools. Decision instruments provide our clients the data required to compare, evaluate or justify strategic and tactical decisions—a hands-on perspective of yesterday, today and tomorrow—shaped and delivered through original research, in-depth market knowledge and the unparalleled insight of a Yankee Group analyst.

Trackers

Trackers enable accurate, up-to-date tactical comparison and strategic analysis of industry-specific metrics. This detailed and highly segmented tool provides discrete proprietary and performance data, as well as blended metrics interpreted and normalized by Yankee Group analysts.

Surveys

Surveys take the pulse of current attitudes, preferences and practices across the marketplace, including supply, delivery and demand. These powerful tools enable clients to understand their target customers, technology demand and shifting market dynamics.

Forecasts

Forecasts provide a basis for sound business planning. These market indicators are a distillation of continuing Yankee Group research, interpreted by our analysts and delivered from the pragmatic stance our clients have trusted for decades.

Signature Events

The Yankee Group's signature events provide a real-time opportunity to connect with the technologies, companies and visionaries that are transforming Telecommunications; Wireless/Mobile Communications; Consumers, Media & Entertainment; and Information Technology Hardware, Software & Services.

Our exclusive interactive forums are the ideal setting for Yankee Group analysts and other industry leaders to discuss and define the future of conversable technologies, business models and strategies.

Consulting Services

The Yankee Group's integrated model blends quantitative research, qualitative analysis and consulting. This approach maximizes the value of our solution and the return on our clients' consulting investment.

Each consulting project defines and follows research objectives, methodology, desired deliverables and project schedule. Many Yankee Group clients combine advisory service memberships with a custom-consulting project, enabling them to augment our ongoing research with proprietary studies.

Thousands of clients across the globe have engaged the Yankee Group for consulting services in order to hone their corporate strategies and maximize overall return.

Understand the Company You KeepSM

The Yankee Group believes the statements contained in this publication are based on accurate and reliable information. However, because our information is provided from various sources, including third parties, we cannot warrant that this publication is complete and error-free. The Yankee Group disclaims all implied warranties, including, without limitation, warranties of merchantability or fitness for a particular purpose. The Yankee Group shall have no liability for any direct, incidental, special, or consequential damages or lost profits. This publication was prepared by the Yankee Group for use by our clients.