Maximizing ROI on Vulnerability Management

March 16, 2009
(Revision 1)

Carole Fennelly
Director of Content and Documentation

Brian Martin
Nessus Content Engineer

Table of Contents

Overview

Most organizations have some form of vulnerability management program, usually mandated by one of the myriad compliance standards. However, meeting a checklist of compliance standards does not make you secure. If you have to go through the expense of having a vulnerability management program anyway, it may as well be effective – and get a return on your investment.

Many businesses operate off simple economic principles: spend money to make money. This is often loosely translated into "return on investment," something that is measurable in the short term and results in profit. Getting a business to spend tens (hundreds?) of thousands of dollars in this economic climate without a demonstrable return is ludicrous. But, ask anyone in the security realm of the costs associated with a breach, forensic examination and cleanup, and a few thousand now is nothing. The trick? Explain that gamble to the executive board, between their forays to Vegas or the stock market. The DataLossDB.org project provides information that demonstrates how real these risks are:

Latest Incidents

twitter/ DataLossDB

RECORDS	DATE	ORGANIZATIONS
2,300	2009-03-11	Gwent Police
1,000	2009-03-09	Sonoma County Sheriff
59,000	2009-03-06	UPS, Idaho National Laboratory
50	2009-03-06	Federal Emergency Management Agency
60,000	2009-03-06	Bottle Domains
3,470	2009-03-06	New York City Office of Payroll Administration, The Organization of Staff Analysts
1,393	2009-03-05	Landlord's Source Centre
80,000	2009-03-04	New York City Police Department
242	2009-03-04	St. Rita's Medical Center
520	2009-03-04	Elk Grove Unified School District

Largest Incidents

RECORDS	DATE	ORGANIZATIONS
94,000,000	2007-01-17	TJX Companies Inc.
40,000,000	2005-06-19	CardSystems, Visa, MasterCard, American Express
30,000,000	2004-06-24	America Online
26,500,000	2006-05-22	U.S. Department of Veterans Affairs
25,000,000	2007-11-20	HM Revenue and Customs, TNT
17,000,000	2008-10-06	T-Mobile, Deutsche Telekom
12,500,000	2008-05-07	Archive Systems Inc, Bank of New York Mellon
11,000,000	2008-09-06	GS Caltex
8,637,405	2007-03-12	Dai Nippon Printing Company
8,500,000	2007-07-03	Certegy Check Services Inc, Fidelity National Information Services

DataLossDB is a research project aimed at documenting known and reported data loss incidents world-wide. The effort is now a community one, and with the move to Open Security Foundation's DataLossDB.org, asks for contributions of new incidents and new data for existing incidents. For any questions about this site or the data contained within the site, please contact curators@datalossdb.org.

Vulnerability Management Programs

Vulnerabilities are exposures that can be exploited. They can be in the form of a software defect, configuration error or basic human error. Vulnerability management programs provide a warm fuzzy feeling that somehow it is all under control: systems are scanned and patched and therefore everything is as secure as it can be.

Or is it? That really depends on the goal for your vulnerability management program: to reactively demonstrate compliance or proactively reduce risk to acceptable levels.

Demonstrate Compliance

Vulnerability management programs are often initiated to demonstrate compliance with regulations or industry standards or the fulfillment of contractual obligations. Many of these have been developed with the best of intentions, but it is like writing a shopping list for the store: inevitably something important won't make it to the list, an item will be too expensive or the friendly grocery clerk will give you the wrong item. Here is a list of some of the many compliance requirements organizations face:

Compliance Requirement	Related Links
BASEL II	http://www.bis.org/publ/bcbsca.htm
Control Objectives for Information and related Technology (**COBIT**)	http://www.isaca.org/cobit
DISA Security Technical Implementation Guides (**STIG**)	http://iase.disa.mil/stigs/stig/index.html
Federal Information Security Management Act (**FISMA**)	http://iase.disa.mil/fisma/index.html http://csrc.nist.gov/groups/SMA/fisma/index.html
Federal Desktop Core Configuration (**FDCC**)	http://cit.nih.gov/Support/FAQ/Fdcc/
Gramm-Leach-Bliley Act (**GLBA**)	http://www.ftc.gov/privacy/glbact/glbsub1.htm http://www.ftc.gov/privacy/privacyinitiatives/glbact.html
Health Insurance Portability and Accountability Act (**HIPAA**)	http://www.hhs.gov/ocr/hipaa/
ISO 27002/17799 Security Standards	http://www.iso.org/iso/catalogue_detail?csnumber=50297
Information Technology Infrastructure Library (**ITIL**)	http://www.itil-officialsite.com/home/home.asp
National Institute of	http://csrc.nist.gov/publications/PubsSPs.html

Standards (**NIST**) Special Publications	
National Security Agency (**NSA**) Security Configuration Guides	http://www.nsa.gov/SNAC/
North American Electric Reliability Council (**NERC**) Standards	http://www.nerc.com/page.php?cid=2
Payment Card Industry Data Security Standard (**PCI DSS**)	https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml https://www.pcisecuritystandards.org/pdfs/pci_audit_procedures_v1-1.pdf
Sarbanes-Oxley (**SOX**)	http://www.sarbanes-oxley.com/
Data Loss Prevention (**DLP**) Laws	http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm http://www.edps.europa.eu:80/EDPSWEB/edps

Secure Systems

If your goal is to secure your systems and reduce risk, chances are you will meet your compliance requirements as a side effect AND have a more secure infrastructure. New vulnerabilities and threats are discovered on a daily basis. Combine this with ever-changing business requirements and you have the perfect storm of security exposure. Relying on a checklist developed by a government agency isn't exactly going to have you on the leading edge of risk mitigation.

Many companies are requiring service providers who manage their confidential information to have formal vulnerability management programs and to provide reports on the state of the applications and systems that manage their data on a regular basis. Efficient vulnerability management is not just good business; it is a necessity for businesses.

Typical Problems in Vulnerability Management Programs

If simply having a vulnerability management program were enough to keep systems secure, we would not be hearing about so many data breaches. There are many reasons such programs fail to work, but the fundamental reason is the motivation in creating such programs. If the organization is initiating a vulnerability management program under duress, support for it will be lukewarm at best. Some of the reasons why vulnerability management programs typically fail are:

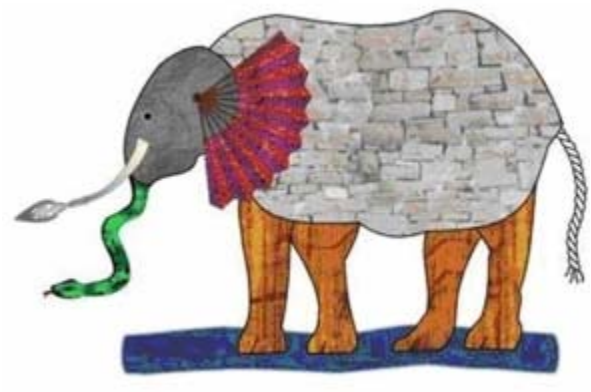
- Lack of corporate direction
- Lack of resources
- Ineffective scanning
- False sense of security
- Poor interpretation of the compliance guidelines

Lack of Corporate Direction

The primary problem with most vulnerability management programs is that management hasn't defined a clear-cut policy and direction. This leaves many organizations in a reactive mode of scanning for current vulnerabilities or responding to an executive's panicked email about a worm he read about on a blog. A reactive approach will always be behind the curve.

The most important management failure is the lack of a defined process. Organizations tend to focus on tools rather than the organization and processes that govern the use of the tools, reporting of vulnerabilities, mapping of risks, scheduling of scans, etc. A poorly defined methodology and process inhibits an organization's ability to have an effective vulnerability management program.

Often the person creating the vulnerability management does not get buy-in from IT, business units and executive management. Without a consensus on the approach, it is doomed to failure. For example, a set of systems for a particular business unit may have risks interpreted in several different ways. The business unit will attach significance to the type of data stored on the servers, while the IT department may be focused on risks to the Operating System. Auditors will have a different view and may consider a reported vulnerability to be of high importance since they are not considering the significance of the data and server it resides on. A "surprise" audit may make sense to an auditor but is horribly disruptive to IT and the business units. The lack of alignment of the various organizations is a classic case of blind men describing an elephant.



These are all problems management needs to solve at the executive level. Unfortunately, the frequent cop-out is to blame the security people for exposures when they haven't been empowered with a process that works.

Lack of Resources

Compliance regulations and guidelines do not specify the resources that must be committed to a vulnerability management program, leaving this up to interpretation – always a bad move when budgets are involved. This leads management to focusing commitment on the purchase of tools or a service, with little regard for developing a process for its use and committing people to supporting the process. Tools are only effective if they are used by staff trained in their use and following an established process governing how they are used.

Ineffective Scanning

Vulnerability management is considered a cost center – a necessary process to pass compliance audits that often gets in the way of business. This attitude results in a lukewarm support for the program so that components are weakened to the point of minimal effectiveness.

As part of the process to cut corners on the vulnerability management program, many organizations are only concerned with scanning for vulnerabilities and nothing more. "If it ain't broke, I don't want to know about it" is an expression that sums up their attitude. This reactive attitude results in missing many issues that a more proactive approach would detect. Many scanners have the ability to use credentials to log in to a system and get information that is not available on a network scan. This information is crucial to ensuring systems are secured, but management does not want to know about it since it would ruffle too many feathers. Even system administrators shy away from authenticated scans so they do not have to analyze and mitigate as much data.

Misleading Patch Audits

Vulnerability scanners can detect missing patches, but don't know what the official corporate policy is regarding patching. A configuration audit can be useful to ensure that it is part of the patching process.

Using a network scan to determine if a patch was applied is misleading. Just because the patch process was initiated does not mean the patch was applied. There are many reasons a scanner may report a system patched when it really isn't; Lack of disk space, buggy patches, security settings, loss of power during patch application, incorrect backup methods, systems not being rebooted and many other reasons can contribute to a patch that appears to be installed, but did not complete.

Another issue with patch audits involves older Operating Systems that no longer have patches available. If no patches are available, scanning for nothing will reveal nothing. For organizations that find need to use manually compiled programs, patch audits appear to paint a grim picture when in reality, the situation may not be bad at all.

Ignorance is bliss – until something happens.

Relying on Anti-Virus

Many organizations take comfort in their anti-virus (AV) program and feel it is sufficient to protect systems from exploit. However, anti-virus does not plug the actual attack vector. It may prevent a malicious site from spreading the latest Trojan to your vulnerable web browser, but it will not stop a custom exploit designed to grant access to your network from the outside. Further, AV does not protect against most "drive by malware" attacks that exploit vulnerabilities in client software. As with any agent, many commercial and open source AV solutions have vulnerabilities themselves. In addition, AV solutions are often not upgraded because of compatibility concerns or licensing issues.

Not Using Credentials

Scanners that support the use of credentials to log in to a system can provide information about configuration settings that would not be visible from the network. For example, a

credentialed scan can get information about the type of hardware that is running. Hardware drivers have life cycles just like any other type of software, and are subject to the same security issues. The Center for Internet Security (CIS) provides consensus benchmarks that set security hardening standards. A credentialed scan can verify that systems are configured in accordance with a known "gold standard". Often configuration standards are not established which impacts uptime and reliability.

Making Vulnerability Management Pay Off

If you want to get the most out of your vulnerability management program, you need to take a proactive approach. This involves a lot of planning, but once the process is in place it will be much more effective and will save a lot of time in responding to compliance requests – not to mention saving the cost of a data breach.

Perform Risk Analysis

A vulnerability rated as "critical" by a scanner does not have the same importance on all systems. Throw away systems, such as a test box that is isolated from critical systems, can easily be reloaded and probably do not have any important data. The same cannot be said for a system that houses a customer database.

Identify Assets

It is important to identify what you are trying to protect to ensure critical assets are protected. For large organizations, this can be a huge challenge. It is often helpful to group assets by common functions and features, such as OS platform or business function. This facilitates vulnerability scanning and remediation by ensuring that scans are configured to probe for common weaknesses in the platform or application. Systems may be classified in multiple asset lists. For example, a Solaris web server on the DMZ may be listed under "Solaris Systems", "Web Servers" and "DMZ Systems". This ensures that scans are targeted appropriately. Create asset lists that logically group assets, such as:

- Critical business servers
- Critical infrastructure devices
- Managed servers
- User / Desktop
- Off-site (VPN, Managed)
- Production servers
- Development servers
- Test systems

Classify Data

Data leakage is a growing problem that is getting a lot of media attention these days. Organizations have a lot of data flowing through the network and not all of it is of equal importance. Technology does not have ESP. Unless the data has been identified and classified, the system administrator has no idea of the significance of the data. This requires some effort from the business owner. Once the data has been classified, the network and security devices can be designed to segregate data flows and monitor for data patterns. Some typical classifications are as follows:

- Patient Health Information
- Credit Card Data
- Client Financial Data
- Intellectual Property
- Material Non-public
- Business Critical Data

Define Requirements

What do you want from your vulnerability management program? This question is not as easy to answer as you might think. You need to consider a number of factors such as compliance requirements, business objectives and contractual obligations.

Define an effective process for gathering information, performing scans and creating meaningful reports before deploying tools.

Create a Vulnerability Program Blueprint

Create a blueprint document for the vulnerability management program before purchasing or even test driving vulnerability scanning tools. The advantage of creating such a blueprint is that all aspects of the program (e.g. vulnerability research, scanning requests, tools and tool deployment, operational components, remediation SLAs) can be clearly documented and vetted. A comprehensive blueprint allows the organization to put the program through peer and executive management review to identify critical assets and build consensus on the direction of the program. This aids greatly in setting expectations for the impact of vulnerability scanning and identifies potential risks of scanning before it becomes an issue.

A Vulnerability Program Blueprint may contain the following items:

Area	Description
Business Requirements	The drivers behind the creation of the program, such as: • Compliance • Policy • Contracts • Standards • Business Initiatives
Technical Requirements - (network, web application, non-web application, database, passive scanning, configuration and patch audits)	Create evaluation charts with criteria for products. Break down the requirements by type of scanner as the different types of scanners have different features. Some examples of requirements are: • Features and functionality • Reporting (internal vs. exportable) • User Interface (yes, look and feel does matter) • Costs (including ongoing operations and maintenance) • Automatic and manual scanning

	capabilities
Product requirements	Larger organizations often require that product installation involve multiple organizations (operations, networking) so they need to be involved to determine what is required to install the product.
Vulnerability research	Review reported vulnerabilities and correlate them with patches. The types of vulnerabilities reported can determine the course of action taken to remediate the issues.
Scanning and reporting process	Develop a comprehensive process to do the following: • Information gathering for scans • Scheduling and performance of scan • Conversion of scan report to risk assessment report (involve the development groups) • Delivery of report to business owner • Establishment of SLA for remediation and mitigation • External reporting (e.g. customers)
Administration and Operations requirements	Large IT organizations typically require a detailed list of what is required of them to manage the devices. Among the requirements are: • Network • System • Data Center • Support
Change management	Some companies require a change request to run a scan.
Roles and Responsibilities	Clearly lay out who is responsible for what.
Documentation	All the other auxiliary documents that will be required: • change management • user documentation • scanning process
Audit	Verify technology solutions are being operated as required.
Budget	Equipment, software, personnel – tell them how many hours are required for installation and ongoing monthly support.
Service Level agreements	Scanning, remediation, mitigation timelines.

Metrics	Risk metrics show many vulnerable applications you have, the level of vulnerability and the remediation status. Status metrics show how far the program has spread through the company.
Resources	Process diagrams, descriptions of reports, etc.

Analyze Solutions

All solutions have limitations. Do not be pushed by the sales reps -if a sales rep will not admit to at least one weakness, walk away. Be objective in the analysis and do not try to fit the program to the tools. Perform a bake-off between qualified parties to better judge their skill. Do not rely on marketing materials to evaluate a product.

Layout a comparison chart, looking for the following:

- What is already in-house?
- Is it supported on/can scan multiple platforms?
- How well does it scale?
- Do the features align with technical and business requirements?
- What are the costs (both one time and recurring)?
- What is the long-term viability of the product?
- What is the update process?
- What is the learning curve?
- What could it break?
- How effective and flexible is the reporting?
- Who else uses it?

Do not just look at the short-term costs. Some solutions may be a bit more expensive up front, but are more inexpensive over time. Unless you are the government, you do not have to go with the lowest bidder. Look for solutions that you can leverage for other areas of the organization. Go beyond just looking for vulnerabilities.

Third Party Solutions

Identify what can be done in-house versus outsourced. Do you really need to have a third party analyze 100K systems? Use third parties to spot check systems or as needed to fulfill client contracts. Consider using third parties to learn methodologies to enhance your own internal processes.

Managed Service

- Subscription based that can get expensive over time
- May put valuable resources out of your immediate control
- Possible delays reaching managed service if something goes wrong

Penetration Testing / Vulnerability Assessments / Compliance Audits

- Only a “snapshot in time”
- Must provide value beyond scanner results (experienced human insight)
- Costly if done very well
- Costly if done thoroughly (e.g., network, application, host level)

In-House Solutions

Integrate the vulnerability management program with some of your other in-house processes. A proactive vulnerability management program can do much more than just find software bugs. It can identify other risks and help mitigate them before they become costly mistakes.

Leverage the program to aid in supporting and validating other efforts, such as:

Patch Management

Identify the priority of deploying patches during a normal schedule or in an emergency based on the threat level defined in the vulnerability research part of the program. Use the tools to provide verification that patches have been fully applied to the systems they are supposed to be applied to.

Configuration Management

Establish "gold" standards and then perform credentialed audits against those standards. Make sure they are *your* standards! Use the vulnerability management tools to provide independent verification of any patches or security issues and adherence to configuration standards in accordance with an established security and configuration management plan.

Incident Response

Monitor networks for potential security incidents. Correlate events over time to detect anomalies that can indicate a pending attack or the presence of an attacker who already has a foothold in the door.

A Security Incident and Event Management (SIEM) system simplifies incident reporting by gathering IDS and netflow data, operating system logs and many other disparate pieces of information into one place.

Organizations that have an effective vulnerability management program can quickly provide a global picture of system activity to those responding to an incident.

Software Development

In organizations that develop applications, it is typical to find the same types of vulnerabilities across many application segments, begging the following questions:

- **Why do they keep occurring?**
- **Who is responsible for detecting and preventing?**
- **What steps can be taken to change programming behavior to reduce vulnerabilities in applications?**

Integrate scanning into the Software Development Life Cycle (SDLC) and train developers to run scans (source code audits, vulnerability scans of development builds) *during* development. This will help reduce the number of QA cycles and allow developers to fix problems earlier. Detecting vulnerabilities early in the development cycle saves costly efforts to mitigate a problem after the software has been released.

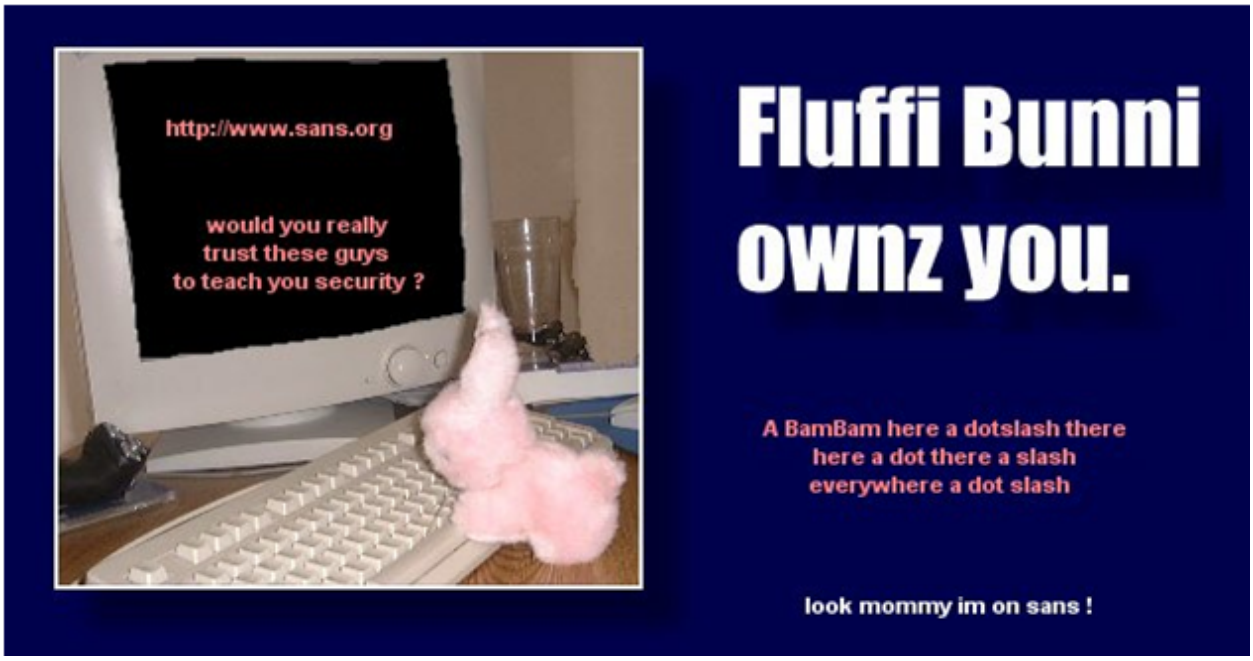
Organizations that create Security Application Coding standards and train their developers on secure coding practices can use the vulnerability scan metrics to show trends in vulnerabilities to measure the effectiveness of the program.

IT Support

A nice side effect of vulnerability scanning is that it can help identify bugs or problems in the network, which aids system and network administrators in troubleshooting problems. A passive scanner can identify new devices on the network that otherwise may go unnoticed, except for a sudden spike in network traffic. A close relationship between the IT support and IT security teams can greatly improve efficiency.

Deploy Solutions

Many people are gun shy about rolling out their vulnerability management program. What if something breaks? Or the head of a business unit has a fit about a negative report? The only way to be sure of no problems is to do nothing and wait for a malicious hacker to demonstrate the need for a proactive program.



Sadly, this is often the motivation that generates support for the program. The best time to deploy a vulnerability management program is before the need for one is publicly demonstrated. There are some measures that can be taken to reduce the pain of deploying a vulnerability management program.

Establish a Baseline

Executive management loves metrics and this starts by establishing a baseline vulnerability analysis report at the commencement of the program. Don't worry if it paints a dismal picture of the organization's security posture – you can only go up from here. The baseline provides the foundation for demonstrating progress.

Tune Scanning Parameters

Any vulnerability scan - manual or automated - needs to be tuned. Tuning scans makes them more efficient, faster to accomplish and generates more accurate results (less false positives). Some points to get the most from your scanning:

- Tune the scan to the target: a thousand database checks against a web server with no databases is about as effective as banging your head against the wall.
- Figure out false positives: one hundred findings sounds bad, until you figure out only 30% are valid.
- Audit companies and scanners assign risk levels to vulnerabilities based on their standards/experience. Weigh the risks reported, adjust according to *your* organization and **then** act on them.

Scan Scheduling

Avoid ad hoc scanning as it is typically very disruptive and difficult to manage. Set a schedule for scanning systems and stick to it. Work with your IT organization so that scans are not disruptive to operations. Ad hoc scans should generally be used only to test administrative response to an unplanned test. However, unscheduled tests can lead to Bad Things™. Resentful administrators, unnecessary escalation and law enforcement are a few of your least favorite things.

Correlate Results

Large organizations often do not communicate well between organizations. This creates redundancy in software, personnel, scanning and remediation. Sharing information, at all levels and processes, benefits the organization. Sharing includes, but is not limited to:

- Solutions in place (e.g., AV, FW, IDS, IPS, SIM)
- Players involved (e.g., Managed, Auditors)
- Schedules for testing
- Scanning results
- Logs (daily, during testing, correlated and monitored)
- Network data (you are sniffing your network, right?)

Analyze Results

Use standard report templates for the vulnerability report, detailed risk report and summary risk reports. Standard templates provide a mechanism for consistent reporting of vulnerabilities and risks. They help establish a level of efficiency in understanding risks. Anyone can read a vulnerability report, not everyone can understand one.

- Analyze and research the results! Many scanners provide a brief description and suggested remediation of the detected vulnerability, but don't take this at face value. Remember, they are giving the 'best' recommendation for the masses, not the recommendation that may be most suitable for your company.
- Follow-up on the issue. Did it really get patched? Or did it get addressed through other means without fixing the underlying issue?
- Anomaly Detection
- Create risk reports based on vulnerability reports and nature of the data

Communicate Results

Once all of the reports have been created, make sure they are communicated to the appropriate parties. More importantly, ensure that they are drafted in a format that is readable to the intended audience. Most importantly, ensure that they **will** be read by the audience. Length and technical scope must be tailored for all levels of the organization. Executive management does not understand what a `fingerd` vulnerability is. Make sure the report is worded in terms they can understand.

Mitigation and Remediation

Share risk reports with business owners and gain consensus on remediation and mitigation efforts. Establish Service Level Agreements with business owners and enforce them. Gain buy-in from senior management to meet these objectives. Remember, finding issues are not "gotchas". Lay out an objective reports describing the risk if these vulnerabilities are left unmitigated. If management is held accountable and understands the facts, they will make the right decisions. Developers are interested in technical details. Business owners are interested in the risk to their livelihood.

Develop Trending Reports

Define status and risk metrics to show the progress of the program and the amount of risk to the organization. Ensure that everyone involved in the process is aware of progress, not just executives.

Status Metrics vs. Risk Metrics

Status metrics demonstrate the state of the program and are organized in the following categories:

- Information gathering
- Vulnerability scanning
- Remediation and Mitigation efforts

Risk based metrics demonstrate the overall posture of the risk to applications and are organized as follows:

- High, medium and low vulnerabilities
- Critical, high, medium and low risks
- Compliance issue
- Score between vulnerability and criticality of the data

There are several risk scoring systems available (e.g., Microsoft STRIDE and DREAD rating systems, CVSS2, etc.) that can be used as a template. Develop a consistent scoring system that is in line with business objectives and stick to it. This helps demonstrate improvements that save money and demonstrates ROI.

Conclusion

Compliance requirements can provide useful checklists to ensure you've addressed specific security concerns, but it is dangerous to base a vulnerability management program solely

on a checklist. A proactive vulnerability management program that addresses specific business needs of the organization will do far more to provide real value to the organization. Planning requires effort, but poor planning results in wasted resources.

Appendix: NIST Special Pub 800-53 and DOD 8500.2

In the process of scanning for vulnerabilities, a lot of data is gathered that can be analyzed for purposes other than searching for vulnerabilities. This is particularly important in meeting compliance requirements. The following table is an example of mapping NIST and DoD controls to vulnerability management measures. Such measures can easily be mapped to other compliance requirements.

NIST ID	Control Name	DOD 8500.2 ID	Vulnerability Management Measures
Access Control			
AC-1	ACCESS CONTROL POLICY AND PROCEDURES	**ECAN-1** **ECPA-1** **PRAS-1** **DCAR-1**	Test for default accounts and process logs and/or network activity to audit the access control policies in use. Detect changes to network access control policies through the use of repeated network scans, passive network monitoring and log analysis. Correlate logs from systems and devices across the network. Detect for violation or change to access control policies (user account permissions) through network monitoring and log analysis.
AC-2	ACCOUNT MANAGEMENT	**IAAC-1**	Test for the presence of inactive, suspended or terminated accounts and determine if they have been disabled. Check audit logs for creation of new accounts and tie account creation with the permissions the accounts can have.
AC-3	ACCESS ENFORCEMENT	**DCFA-1** **ECAN-1** **EBRU-1** **PRNK-1** **ECCD-1** **ECSD-2**	Test servers and desktops to ensure they are configured with the proper level of access control. Monitor network data flows for specific data types (e.g., credit card data, patient health information, etc.). Check audit logs for all policy changes to access control, or attempt to increase access level.
AC-5	SEPARATION OF DUTIES	**ECLP-1**	Test servers to ensure they are configured and maintained with the proper level of access control, including separation of duties for default and new accounts.
AC-6	LEAST PRIVILEGE	**ECLP-1**	Test servers to ensure they are configured and maintained with the proper level of access

			control and locked down to a least level of privilege.
AC-7	UNSUCCESSFUL LOGIN ATTEMPTS	**ECLO-1**	Test to ensure that systems are configured to log all successful logins and login failures.
AC-8	SYSTEM USE NOTIFICATION	**ECWM-1**	Audit network devices to ensure a default warning banner message is displayed before users can login.
AC-9	PREVIOUS LOGON NOTIFICATION	**ECLO-2**	Audit operating systems to ensure a previous login notification setting is enabled.
AC-13	SUPERVISION AND REVIEW - ACCESS CONTROL	**ECAT-1** **ECAT-2** **E3.3.9**	Provide continuous and automated log monitoring and analysis to identify specific users who are abusing their privileges.
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	N/A	Identify applications that offer data without requiring a unique user login.
AC-17	REMOTE ACCESS	**EBRP-1** **EBRU-1**	Audit the security of remote access infrastructure for vulnerabilities.
AC-18	WIRELESS ACCESS RESTRICTIONS	**ECCT-1** **ECWN-1**	Test for unauthorized wireless devices on the network.
AC-19	ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES	**ECWN-1**	Provide continuous monitoring to discover when new hosts are added to the network including new laptops. Use Windows Management Instrumentation (WMI) functionality to monitor local and remote systems for USB device, CD-ROM disc and DVD disc activity.
AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	N/A	Use asset discovery and system analysis to detect systems that were not configured to be part of the normal infrastructure.
Audit and Accountability			
AU-2	AUDITABLE EVENTS	**ECAR-3**	Enable full logging capabilities wherever possible and use a log aggregation tool to normalize and correlate log data.
AU-3	CONTENT OF AUDIT RECORDS	**ECAR-1** **ECAR-2** **ECAR-3** **ECLC-1**	Ensure that log correlation methods store the full log of each event received in sufficient detail that can be used for analysis or incidence response at a later time.
AU-5	RESPONSE TO AUDIT PROCESSING FAILURES	N/A	Monitor system status, including CPU, memory and disk utilization. Check for attacks that overflow logs, poison caches and log files to hide their track.
AU-6	AUDIT MONITORING, ANALYSIS AND REPORTING	**ECAT-1** **E3.3.9**	Ensure log correlation solutions have the ability to normalize log events, search for correlated events of interest or detect anomalies. Configure alerting for critical events that are audited so they can get timely and proper attention.

AU-7	AUDIT REDUCTION AND REPORT GENERATION	**ECRG-1**	Use filters and analysis tools to simplify log analysis and generate concise reports. Normalize logs into convenient types that align with common reporting requirements such as login failures, software installations, compromises and port scans.
AU-8	TIME STAMPS	**ECAR-1**	Ensure all events logged events uniquely time-stamped and that Network Time Protocol (NTP) is in use.
AU-9	PROTECTION OF AUDIT INFORMATION	**ECTP-1**	Ensure users can only see vulnerabilities, IDS events and logs for the range of IP addresses that they are responsible for. Ensure archived audit logs are protected with appropriate controls Ensure systems that store audits logs are protected. Ensure purging of audit logs is done in a secure manner.
AU-10	NON-REPUDIATION	**DCNR-1**	Ensure each individual has a unique account to ensure accountability. Ensure there are separate accounts for administrative activities. Provide the ability to track multiple log types from a variety of devices, including netflow data, firewall logs, operating system logs and even honeypot logs. This builds a better picture of what has occurred during an event where some logs could be forged at the source.
AU-11	AUDIT RETENTION	**ECRR-1**	Save all log files to a separate archiving device.
Certification, Accreditation and Security Assessments			
CA-2	SECURITY ASSESSMENTS	**DCII-1** **ECMT-1** **PEPS-1** **E3.3.10**	Establish a third party security assessment plan to review critical systems on a regular basis. Establish a periodic assessment plan to identify and resolve issues until the third party assessment date comes up. Identify gaps between internal assessment process and external assessment, and improve the internal process to close the gaps.
CA-3	INFORMATION SYSTEM CONNECTIONS	**DCID-1** **EBCR-1** **EBRU-1**	Monitor network connections, data flows and trust relationships through direct network analysis, netflow analysis and log analysis.

		EBPW-1 **ECIC-1**	
CA-7	CONTINUOUS MONITORING	**DCCB-1** **DCPR-1** **E3.3.9**	Use a combination of monitoring techniques and aggregate the data in a central Security Information Management system.
Configuration Management			
CM-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	**DCCB-1** **DCPR-1** **DCAR-1** **E3.3.8**	Define specific asset classes of servers or network devices to perform specific audits. Use real-time network analysis to discover new hosts as well as hosts operating outside of configuration guidelines.
CM-2	BASELINE CONFIGURATION AND SYSTEM COMPONENT INVENTORY	**DCHW-1** **DCSW-1**	Discover the baseline of a network footprint with active and passive vulnerability analysis.
CM-3	CONFIGURATION CHANGE CONTROL	**DCPR-1**	Detect configuration changes in the network through real-time network and log monitoring, as well as through subsequent vulnerability and configuration audits.
CM-4	MONITORING CONFIGURATION CHANGES	**DCPR-1** **E3.3.8**	Use data collected from ongoing network scans, passive network monitoring and log analysis to continuously assess the amount of risk that has been exposed.
CM-5	ACCESS RESTRICTIONS FOR CHANGE	**DCPR-1** **ECSD-2**	Log access control changes on specific servers. Audit the configurations of key assets to determine if they have the proper access control settings.
CM-6	CONFIGURATION SETTINGS	**DCSS-1** **ECSC-1** **E3.3.8**	Perform configuration audits to determine if systems are configured in compliance with established standards.
CM-7	LEAST FUNCTIONALITY	**DCPP-1** **ECIM-1** **ECVI-1**	Identify if an asset class is not supposed to have a specific setting, running service or open port. Determine what user id running processes and network daemons are operating as.
Contingency Planning			
CP-7	ALTERNATE PROCESSING SITES	**COAS-1** **COEB-1** **COSP-1** **COSP-2**	Monitor alternate processing sites to ensure that they are secure and are running the same software versions as the primary site. Backup sites are often not maintained with the same level of diligence as the primary site. This can lead to problems if it needs to be deployed as the operational site. Ongoing monitoring will ensure that the alternate site contains the required resources to resume operations with minimal downtime.
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	**COTR-1** **ECND-1**	A SIEM is a valuable tool in the system recovery process that provides a record of the vulnerabilities, configuration settings and installed software that existed on a host prior

			to its reconstitution. It can also be used to scan recovered systems for vulnerabilities and to ensure the latest patches and appropriate configuration settings have been deployed. Finally, it can be used to monitor for signs of repeated disruption.
Identification and Authentication			
IA-2	USER IDENTIFICATION AND AUTHENTICATION	**IAIA-1**	Any system that logs user activity by user name also produces access control (login and login failures) logs. These can be used for log analysis, raw pattern searches and anomaly detection. Ensure attempts to bypass user authentication are logged, alerts are issued and logs are audited.
Incident Response			
IR-5	INCIDENT MONITORING	**VIIR-1**	Monitor networks for potential security incidents. Correlate events over time to correlate anomalies that can indicate a pending attack.
IR-6	INCIDENT REPORTING	**VIIR-1** **E3.3.9**	A SIEM simplifies incident reporting by gathering IDS, netflow, operating system logs and many other disparate pieces of information into one place.
IR-7	INCIDENT RESPONSE ASSISTANCE	N/A	Organizations that have an effective vulnerability management program can quickly provide a global picture of system activity to those responding to an incident.
Maintenance			
MA-4	REMOTE MAINTENANCE	**EBRP-1**	Perform a before and after configuration audit of systems undergoing maintenance.
Physical and Environmental Protection			
PE-2	PHYSICAL ACCESS AUTHORIZATIONS	**PECF-1**	Monitor user access by IP address to detect attempted access violations. Note when a user changes IP addresses.
PE-5	ACCESS CONTROL FOR DISPLAY MEDIUM	**PEDI-1** **PEPF-1**	Scan systems to ensure that screen lock capabilities are enabled.
PE-6	MONITORING PHYSICAL ACCESS	**PEPF-2**	Any device that generates logs files for specific user data can be monitored. Windows servers can also be monitored for USB device usage.
Risk Assessment			
RA-1	RISK ASSESSMENT POLICY AND PROCEDURES	**DCAR-1**	Monitor configurations, manage vulnerabilities and monitor for security and compliance events. Share security events and reports with authorized users to aid in coordination efforts. Map all vulnerabilities discovered to the risk they pose to the environment based on the systems they are discovered on.

RA-4	RISK ASSESSMENT UPDATE	**DCAR-1** **DCII-1**	Network monitoring can help discover changes in the network such as new devices or network paths. Changes in access control lists, running software and different types of detected vulnerabilities can indicate when risk assessment policies and procedures need to be updated. Update risk assessment process to accommodate changes to the type of data that resides on a system and its availability requirements as well as new business and compliance requirements.
RA-5	VULNERABILITY SCANNING	**ECMT-1** **VIVM-1**	An effective vulnerability management system can manage dozens of active or passive scanners, schedule scans, correlate IDS and log data and share information securely to authorized users across large networks.
Systems and Services Acquisition			
SA-5	INFORMATION SYSTEM DOCUMENTATION	**DCCS-1** **DCHW-1** **DCID-1** **DCSD-1** **DCSW-1** **ECND-1** **DCFA-1**	Leverage asset discovery capabilities to maintain an up-to-date network list. It can also help in detecting new devices added to the system and old devices that have been retired (due to end of life). Any information about running processes, known vulnerabilities, configuration information, WMI data, system BIOS data and more can be used to classify systems into one or more different asset groups.
SA-6	SOFTWARE USAGE RESTRICTIONS	**DCPD-1**	Use credentials to log into servers and obtain a list of installed software. If host credentials are not available, monitor network traffic to detect traffic patterns.
SA-7	USER INSTALLED SOFTWARE	N/A	Leverage vulnerability management tools to find new types of software installed by users as well as monitor network traffic and logs to discover newly installed applications.
SA-10	DEVELOPER CONFIGURATION MANAGEMENT	N/A	Use the vulnerability management tools to provide independent verification of any patches or security issues and adherence to configuration standards in accordance with an established security and configuration management plan.
SA-11	DEVELOPER SECURITY TESTING	**E3.4.4**	Vulnerability management tools can be used to manage scans of software under development so developers can address any vulnerabilities in their software early in the development process. Monitor any logs generated by the software, which can aid in documentation of security testing. VM tools can help to run scans on

			servers/systems that host developed applications, identify issues and provide potential of securely locking down the systems.
Systems and Communication Protection			
SC-5	DENIAL OF SERVICE PROTECTION	N/A	Use network scanning tools to perform Denial of Service tests. Normalize IDS and other types of logs that may indicate denial of services attempts. Use the tools (log correlation) to identify an active denial of service event so that timely response can be provided.
SC-7	BOUNDARY PROTECTION	**COEB-1** **EBBD-1** **ECIM-1** **ECVI-1**	Multiple scans can be performed across an enterprise to simulate remote network scans. This can determine if certain parts of the network have excessive trust relationships with other parts. Analyze logs from any systems monitoring the boundaries of a network. Monitor traffic on boundary networks to detect if specific types of network data are being transmitted in violation of policy (credit card data or personal health information).
SC-14	PUBLIC ACCESS PROTECTIONS	**EBPW-1**	Provide ongoing external and internal assessments of public data systems. Scanners can be placed outside of the network to simulate public access.
System and Information Integrity			
SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	**DCAR-1**	Monitor for compliance with any policies and procedures that specify configuration of key assets or how events from those assets are monitored and logged. Unauthorized change is the leading issue for degradation of server integrity.
SI-2	FLAW REMEDIATION	**DCSQ-1** **DCCT-1** **VIVM-1**	Update vulnerability scanners on a regular basis to detect the latest system flaws and recommended security patch levels.
SI-3	MALICIOUS CODE PROTECTION	**ECVP-1** **VIVM-1**	Aggregate logs from virus and malware tools. Audit registry settings or file content to look for viruses and check to make sure the AV system is operational and updated. Scan systems to ensure they are not distributing malicious code. Set up rules to monitor for signatures on commonly known or newly discovered malicious code patterns in the industry, and monitor logs for detection of any identified

			patterns.
SI-4	INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES	**EBBD-1** **EBVC-1** **ECID-1**	Log monitoring tools provide event collection, normalization and correlation for hundreds of different types of devices. These events can be quickly analyzed by large and small enterprises. Use vulnerability scanning tools to actively and passively monitor network activity. A SIEM collects data from a wide variety of security devices to provide a correlated view of the enterprise security posture.
SI-5	SECURITY ALERTS AND ADVISORIES	**VIVM-1**	Update scanners on a daily basis to detect the latest security vulnerabilities. Automate this capability, if possible.
SI-6	SECURITY FUNCTIONALITY VERIFICATION	**DCSS-1**	Use distributed scanners to streamline vulnerability scanning and provide redundancy. Correlate to monitor for security function failures such as the failure of a security test to launch.
SI-7	SOFTWARE AND INFORMATION INTEGRITY	**ECSD-2**	Correlate logs with user logins to detect suspicious events or anomalies. Perform checksums of Unix servers to ensure that the files being monitored have not been changed.

About Tenable Network Security

Tenable, headquartered in Columbia, Md., USA, is the world leader in Unified Security Monitoring. Tenable provides agent-less solutions for continuous monitoring of vulnerabilities, configurations, data leakage, log analysis and compromise detection. For more information, please visit us at http://www.tenablesecurity.com/.

TENABLE Network Security, Inc.
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
TEL: 1-877-448-0489
http://www.tenablesecurity.com/