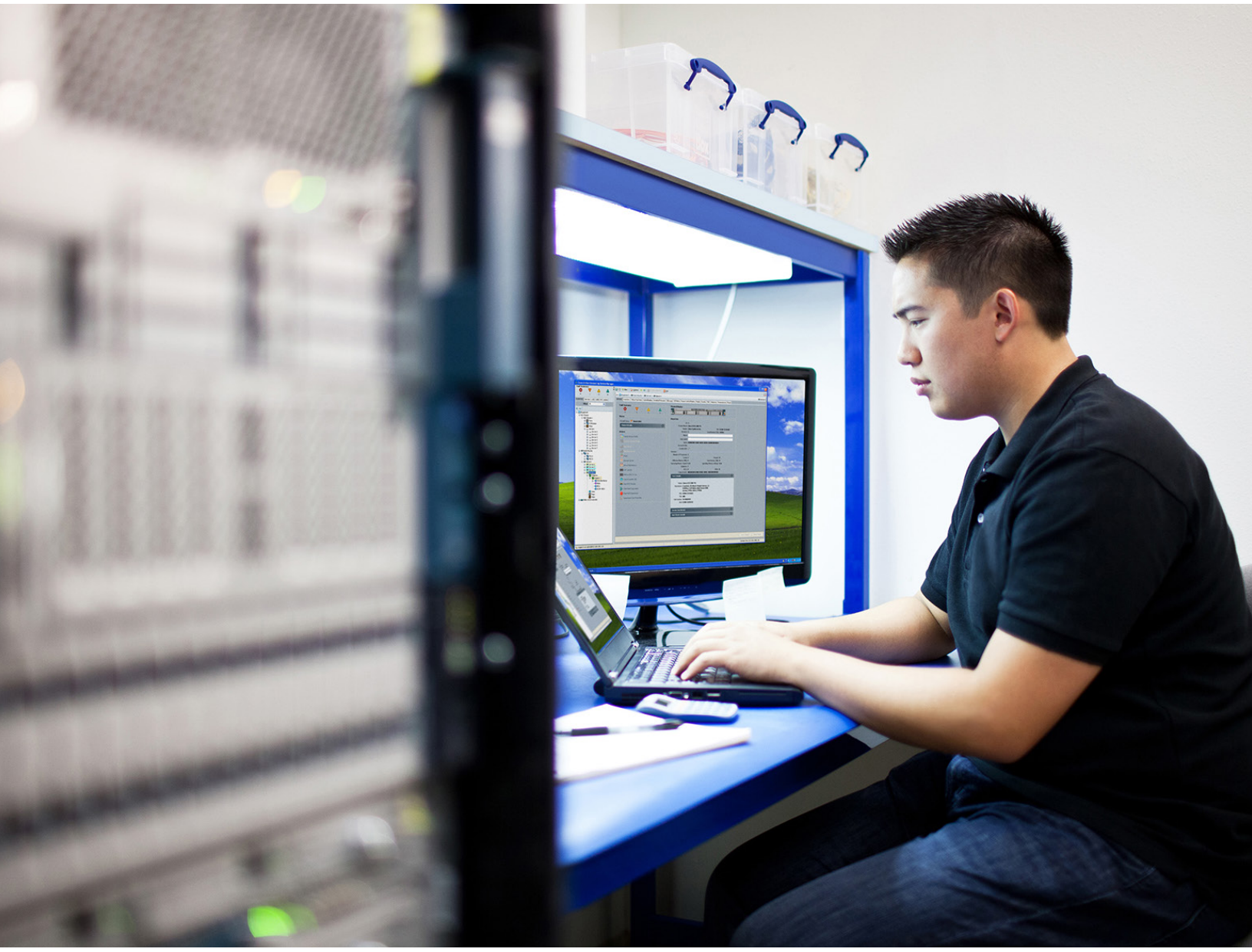
Unified Security Metrics

Vulnerability Metrics

Abstract

A paper about the development, deployment, successes, and lessons of a vulnerability security metrics framework



Gerwin Tijink, Information Security Architect
Hessel Heerebout, Manager Engineering
Cisco

Contents

Executive Summary 3
Intended Audience 4
Introduction 4
Historical Security Challenges 4
The Cisco IT Environment 4
- Security Primes 4

USM Concepts 5
- Example Use Case 5
- Vulnerability Metric Framework 5
  - Technical Vulnerability Measurements 6
  - Process Vulnerability Measurements 6
  - People Vulnerability Measurements 6
  - “Metrics” Defined 7
- USM Communication Framework 7

Putting It into Action and Proofing the Concept 7
- Tooling 7
- Managing the Measurement Data 8
- Using Existing Risk Management Frameworks 8
- Feedback Mechanisms 9
- CIO-Level Support and Visibility 9

Lessons Learned 9
- Cultivate Partnerships 9
- Speak IT Speak 10
- Start Small and Grow Organically 10
- Focus on Training 10
- Build Trust 10
- Construct a Communication Process Flow Loop 10
- Keep It Simple 10
- Some Challenges 10

Program Successes 11
Security Metrics Maturity Levels 11
Conclusion 11
Appendix A: Sample Questions That Lead to Vulnerability Metrics 11

Executive Summary

Unified Security Metrics (USM) is one of Cisco's governance programs. It helps a common set of security-leading indicators to be applied across the company's networks.

USM was specifically designed to promote the continuous improvement of an IT service, to measure its security posture over time, and to provide a two-way feedback mechanism to IT service owners and leaders on a quarterly basis. Greater visibility of security indicators provides system vulnerability intelligence that can be used for:

- Preventive or prescriptive remediation
- Risk management and security posture assessment
- Improved security hygiene
- Operational and business decision making

More importantly, the introduction of USM represents a paradigm shift at Cisco. Security issues are now handled much more strategically than reactively, and departments are given expanded operational control and flexibility in managing their security investments, actions, and processes.

With USM measures in place, we are able to quantify Cisco's security health. We saw a 65 percent reduction in vulnerabilities in the first year of the program. On-time closures improved from 15 percent to 80 percent within a year. The success also led to more security investment (increase of 50 percent year over year) and stronger support of the next phase of the program.

You can't manage what you don't measure. The policies Cisco uses for maintaining security hygiene—patching systems, embedding security, and managing vulnerabilities—have existed for many years. However, when we started measuring these activities, few teams were doing it well.

This white paper explains how USM combines multiple sources of individual data to create high-value actionable business metrics. It helps our executives make better decisions to protect Cisco's data, business processes, operational integrity, and brand from security incidents.

Intended Audience

Security professionals, IT staff, and business people with an interest in security metrics will find this paper of most interest. It showcases how Cisco has set up its own metrics program for other companies to benefit from. A basic understanding of security fundamentals is expected.

Introduction

This white paper introduces a framework to set up a security metrics program for your organization or business. It explains how security can be made a shared responsibility between your IT staff and other departments. The scope of security and risk metrics is large. We focus on one aspect of information risk metrics: vulnerability measurements.

At Cisco, the Information Security (InfoSec) group is responsible for protecting the integrity, confidentiality, and availability of information and computing assets while supporting business productivity. We address the phases that InfoSec had to go through, from identifying the problem and the solution, to implementing the solution and defining the value to gain executive buy-in. In addition, this paper describes some of the lessons learned and the envisioned future of the program.

Historical Security Challenges

Before InfoSec launched the USM program, Cisco IT service owners and executives had limited visibility into their security posture and often assumed that their IT ecosystem was uncompromised and secure. In the past, business units were not highly integrated, and everything within the logical and physical perimeters of the enterprise was assumed safe.

Over the last several years, businesses around the world have been changing, causing a shift in information security. Disruptive trends like digitization, virtualization, collaboration, bring-your-own-device (BYOD) workplaces, and cloud adoption shook up the information risk landscape and required a different approach from traditional security models, including security metric reporting.

Digitization is increasing digital information. More and more businesses are dependent on the digital information in applications, and the volume and complexity of this data are rapidly growing. A good percentage of this information is business critical and would cause an enormous impact if it were lost or compromised.

Other disruptive trends, like cloud use and collaboration, caused significant additional changes in the threat landscape. With the eroding of logical perimeters and the adoption of clouds to allow for highly integrated business models, applications and data can no longer be considered “internal only.”

At Cisco, security vulnerabilities were seen as InfoSec’s responsibility, not the IT group’s. The security analysis, metrics, and communication coming from the InfoSec department was inconsistent and fragmented. Another approach to security metrics and shared accountability was required.

The Cisco IT Environment

The IT group’s core responsibility is to build, deliver, and maintain capabilities to continuously deliver business outcomes with speed, integrity, and simplicity. Most of Cisco’s business processes depend on capabilities delivered by the IT staff, and 99 percent of its data assets are stored, communicated, and processed by the capabilities that the IT group is responsible for.

Cisco IT is focused on services. Everything that the group delivers is a service. Currently there are more than 150 services with more than 2000 applications. In addition, Cisco uses more than 400 cloud providers.

Security Primes

Everyone is responsible for security. InfoSec can’t manage this alone. It depends on cooperation and expertise from other teams. This shared accountability is essential, because without it nothing will change. Part of our success has come from the creation of two newly defined roles: **security primes**, the IT managers or directors who act as the chief security officer of their respective IT service area, and **partner security architects**, who are subject matter experts (technical leads).

Neither is part of the InfoSec organization, but they’re fully trained on security and have broad responsibility to govern security. Designating this virtual team of trusted advisors throughout the IT staff helps the relatively small InfoSec team scale and embed security into the department’s DNA.

Every IT service is captured in the service portfolio, every IT application in the application portfolio, with both being hosted in the same database. Every service has a quarterly risk review with the CIO. Security is discussed there, among other risk measures like compliance with the Sarbanes-Oxley Act (SOX), resiliency, and audits. IT services have dedicated security primes and partner security architects (roles explained in the sidebar). There's also the dedicated InfoSec team, which closely aligns with the IT organization but is not a part of it.

Cisco's mission is to innovate and adopt the most effective information security technologies and policies, share them with our customers, and reflect them in our people, products, and services. To meet our objectives, InfoSec requires close alignment with other departments. We provide security guidance during the architecture, change management, and operational IT processes. InfoSec maintains a set of security policies and standards to impose consistency with the IT processes.

USM Concepts

If security is to become a shared accountability, security concerns need to be heard, seen, and acted on in an acceptable timeframe. They need to take into account the exploitability of the vulnerability, the threat landscape, and potential impact or value of the information.

A focused, accelerated security initiative led to the creation of Unified Security Metrics (USM). The industry defines several variations of information risk, but in building out a USM framework, we adopted a basic definition:

Risk = (Vulnerability * Threat) * Impact

Against this definition we set our goals for the security metrics program, and we are working to deliver a comprehensive information risk metric. In this paper we cover vulnerability measurements only and not topics like types of threats and their impacts. The USM program reports on service levels and collects information on host, application, and service-offering levels.

Two frameworks mark the boundaries of the problems to be solved. One framework, the vulnerability metric framework, defines the capabilities needed to produce security metrics consistently and in good time. A second framework, the USM communication framework, defines how the metric can be delivered to the right audience. It is designed to assign accountability throughout the IT organization.

Example Use Case

Many critical business services have been designed, implemented, and expanded over time. A service that started well over 10 years ago as a minor business dependency may have evolved into a mission-critical and enterprisewide integrated service. Over the last decade, as the IT service developed and matured and the business changed, the security question to ask is, Do the leaders and decision makers have insight into the shifts in the risk landscape and the information to make educated security decisions?

Let's take the example of one IT service to illustrate the importance of security metrics. A little over 15 years ago Cisco saw a need to set up a file-sharing service, like FTP, so that it could exchange files with other businesses. The scope of use was limited to a few small business groups. Traditionally files were sent over email, but as their size grew, email was no longer meeting the organization's needs. You could describe this as a first step in business-to-business collaboration. Since then the service has developed into a collaboration service that includes enterprise document management systems and cloud integration. Many business units in the enterprise are now using this service, and gigabytes of data are exchanged on a quarterly basis with other companies. Over the years, the support and the development of the systems have been made more efficient and been outsourced to third parties or cloud providers.

In this changed threat landscape, the service is fully externally facing and accessible on the Internet. The total value of the data in the system has increased, and a good percentage of that data is business critical or falls under legislative responsibilities.

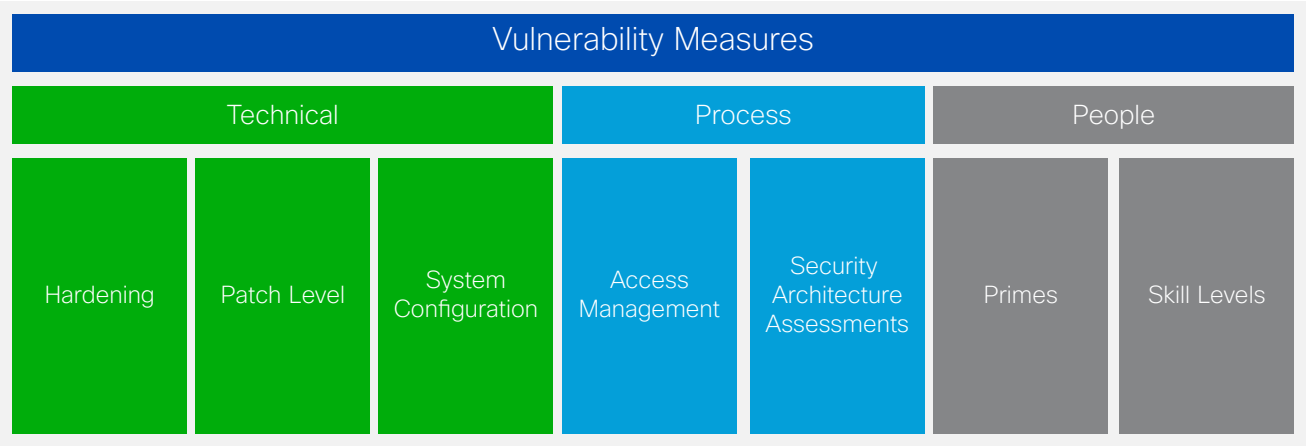
Security metrics can provide ongoing insight into the strengths and weaknesses of a system and determine whether the risk is at an acceptable level. The vulnerabilities of the system will define its overall strength and its ability to defend against attacks and misuse.

Vulnerability Metric Framework

Often vulnerabilities are immediately associated with weaknesses in technology, application, and infrastructures, but vulnerabilities can also relate to processes and people. For example, a lack of segregation of duty in a process is considered a process vulnerability; a lack of skilled and trained administrative personnel, a weakness in people.

Accordingly, the list of vulnerability measurements was divided into three categories: technology, process, and people (Figure 1).

Figure 1. Vulnerability Measurement Categories and Their Components



Technical Vulnerability Measurements

Technical vulnerability measurements aim at finding weaknesses in information systems. Information systems require software in all the layers of the stack to operate. Logical controls built into applications and infrastructures use software to perform their function. It is often said that no software is without flaws, and new bugs, weaknesses, and errors are discovered on a daily basis. Software companies harden and fix their software on an ongoing basis and release new versions and patches.

A second aim is finding weaknesses in information system defenses. These could include a misconfiguration of software, or a lack of security controls protecting the systems. For the USM program the list of technical vulnerability measurements was narrowed down to the following set:

- **Stack compliance:** The number of vulnerabilities found on the TCP/IP stack (network devices, operating systems, application servers, middleware, etc.)
- **Antimalware compliance:** Assessment of whether malware protection software has been properly installed and is up to date
- **Baseline application vulnerability:** Determination of whether automatic vulnerability system scans have been performed in accordance with Cisco policy and, after a scan, whether any open security weaknesses remain
- **Deep application vulnerability:** Determination of whether penetration testing has been performed on our most business-critical applications in accordance with Cisco policy and, after testing, whether any open security weaknesses remain
- **Design exceptions:** The total number of open security exceptions, based on deviations from established security standards and best practices

Process Vulnerability Measurements

Processes require administrative controls so that changes are consistently managed and have predictable and secure outcomes. These controls consist of approved written policies, procedures, standards, and guidelines. Administrative controls are also used to inform the people operating the processes how the business is securely run and how day-to-day operations are to be conducted. Process vulnerability measures aim to reveal weaknesses or a lack of administrative control. Because the volume of processes in large companies like Cisco is enormous, the USM program focuses on two security-related processes in its measurement portfolio:

- **Architectural assessments:** Processes that influence the design, adoption, and delivery of applications and infrastructure
- **Access authorizations:** Processes responsible for governing the access to applications and data

People Vulnerability Measurements

People, largely trusting, are often seen as the weakest link within the security spectrum. In addition, employees such as sysadmins have unrestricted access to critical systems and data, so they are obviously a top target for attacks and data disclosure. Education and awareness are the main

ways we can try to limit the ability of employees to compromise network security. We focus on questions in two areas:

- **Security commitment:** How many service team members are security service primes or partner security architects?
- **Security awareness:** How many users with sensitive business roles (controllers, HR staff, managers) have gone through security awareness training?

Appendix A has more examples of questions we want to answer through our measures.

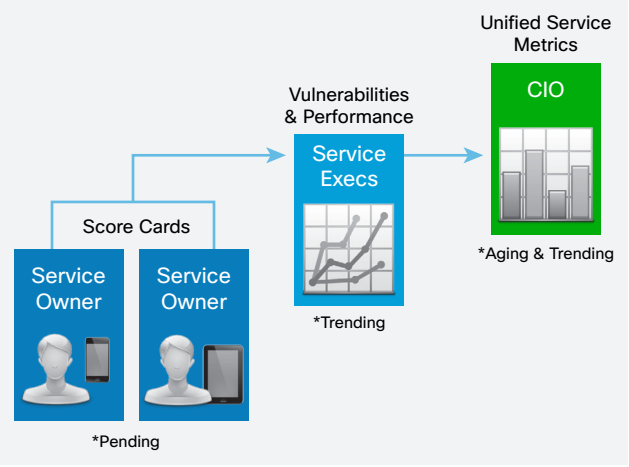
"Metrics" Defined

For vulnerabilities in particular we have identified two metrics that are helpful in security reports. A **vulnerability metric** shows the total number of vulnerabilities as well as the percentage of pass or fail among the five technical vulnerability measures. An **on-time closure metric** shows whether IT teams managed to close the vulnerabilities within an agreed-upon timeframe.

USM Communication Framework

To deliver the metrics to the right audience and impose accountability, a communication framework has to be defined. The main objective of this framework is to deliver the metric at the right time to the right person. To also ensure accountability, the communication model was broken down into three tiers, as shown in Figure 2.

Figure 2. Communication Model



Service owners: Directors and senior managers receive timely metrics about the pending vulnerabilities of the systems they are responsible for. More information about the type of vulnerability is available so the service owner can have the vulnerability remediated. Each vulnerability has to be remediated within an agreed-upon timeframe. Security primes and the partner security architect help remediate the vulnerability of the service, and where needed they collaborate with InfoSec.

Executives: The executive is provided with trending metrics for all the services within his or her portfolio. The executive is able to see the overall vulnerability management performance over time and the best and worst performances within the service portfolio.

CIO: The chief information officer is presented with both aging and trending metrics across all IT services.

Putting It into Action and Proofing the Concept

Tooling

It became evident during the framework building that tools had to be created to scale the program. The tools had to have the following functionalities:

- **Speed and flexibility:** The tooling had to be flexible enough to adopt new measurements and scoring methods without going through a redesign. In addition, it had to have automated extract, transform, and load capabilities to import and normalize measurements from any source.
- **Accuracy:** The tooling had to provide accurate results with low error threshold. It had to require little human involvement in the processing of measurements into metrics. The role of the human was to validate the tooling accuracy.
- **Metrics:** The USM program would have little involvement in delivering the metrics to service owners. A portal would allow service owners and other audiences to collect the metrics.
- **Secure Design:** Because the tool was going to process and store vulnerabilities across the enterprise, the system had to be hardened and secure.

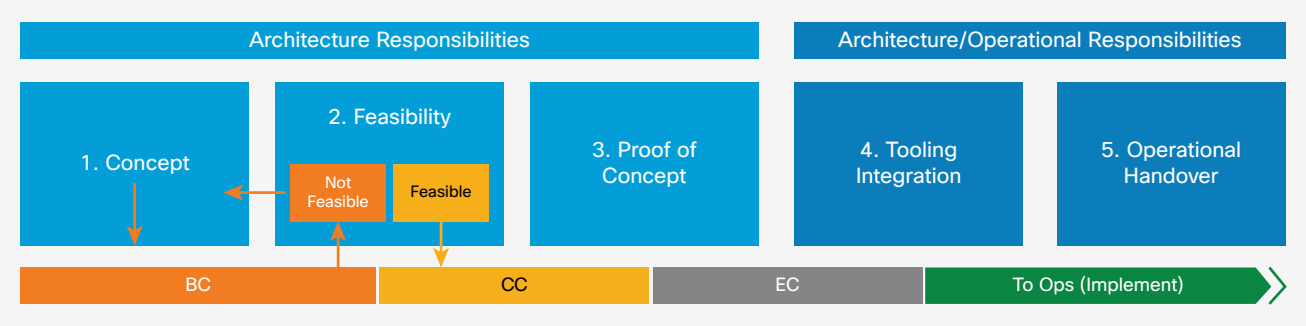
To meet these requirements, a tool was created that included a modular and flexible database backend, with ETL (extract, transform, load) functionality integrated into a data visualization application. Audiences use the application to collect the relevant security metrics.

Managing the Measurement Data

There are plenty of statistical data sources to mine information from, particularly from IT system logs and dashboards. In fact, early research identified 30 types of meaningful data to track. Comprehensive, yes, but not realistically feasible or sustainable to implement long-term across Cisco.

Providing consistent, transparent, and actionable vulnerability metrics requires an assessment of the data sources and their usefulness. Furthermore, the ongoing extracting, loading, processing, and transforming of the raw measurement data into a vulnerability metric had to scale, and automation of this process had to be considered. Additional measures will have to be added to adjust and mature the metrics over time. To manage this process, a workflow for adding and changing measures was created (Figure 3).

Figure 3. Managing the Workflow



Note: "BC" refers to "business commit." "CC" stands for "concept commit," and "EC" is the "execute commit."

It is beyond the scope of this document to go into detail of every aspect of this workflow, but the high-level stages are as follows:

- **Measurement concept:** Define and plan what changes are needed.
- **Feasibility:** Perform a feasibility analysis on the measurement data to understand whether measurements are available, trusted, and accessible, and whether the collection, transformation, and loading of the measures can be automated. A playbook was created to consistently and efficiently assess the feasibility of measurement candidates.
- **Proof:** Proof the concept by pulling a first set of measures. Then proof the tool's readiness and its impact on scoring. This step requires a staging environment of the USM tools and systems.
- **Integration:** Prepare the production tooling, and test the automation of the measurement collection. Also plan for additional staff.
- **Operational handover:** Finalize the operational documentation, hire staff where needed, and train the staff about the changes made. Most important: Inform all stakeholders about the changes in metrics and when they are to be expected.

Using Existing Risk Management Frameworks

Having a well-defined library of common controls to manage risk is important, particularly in a fast-changing IT environment that includes cloud computing, virtualization, and mobile computing. Cisco's IT Risk Management (ITRM) department uses a universal framework to manage risk globally in the areas of resiliency, SOX requirements, internal audits, ISO 9001 certifications, relationships with cloud and application security providers, and security.

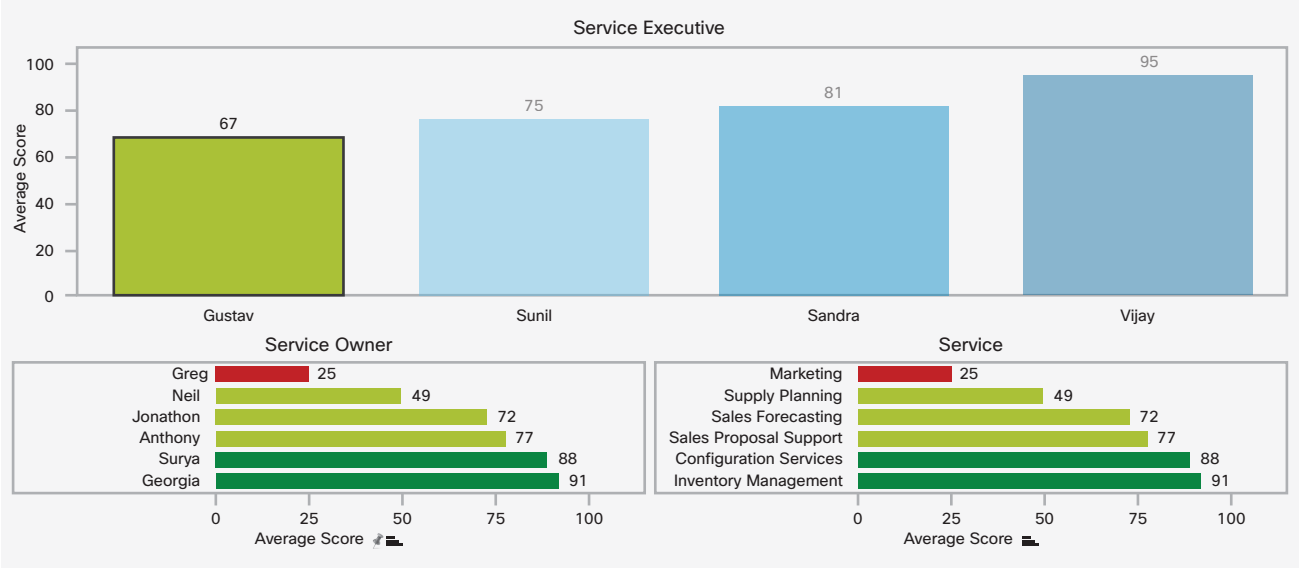
ITRM's risk management reporting dashboards provide tremendous insight and visibility at both the service and the application portfolio levels. By incorporating security metrics into the ITRM framework, IT functions and service areas can more effectively (and efficiently) make risk-aligned investment decisions and satisfy regulators; auditors (internal and external); and governance, risk, and compliance requirements.

Feedback Mechanisms

Quarterly reports provide detailed security analyses, such as vulnerability and on-time closure metrics, at three levels: service owner, service executive, and CIO. The analyses are designed to assist these groups in implementing remediation efforts, identifying trending activities, and assessing risk. For IT service owners, these transparent reporting systems are vital to making corrective actions in a timely manner. Now service owners are evaluated not only on their services' operational performance but also on their ability to make their services secure (Figure 4).

This nonpunitive approach has increased program adoption among the IT service areas. Surprisingly, it has also created a sense of competition between teams within IT for improved performance.

Figure 4. Example of Service Executive and Service Owner Scores



CIO-Level Support and Visibility

Gaining an overall picture of the business risk, including what's happening at the IT enterprise level, assists CIOs in making decisions. Critical business decisions can affect a department's reputation management, intellectual property, disaster recovery planning, marketing, human resources, legal issues, and even finance activities.

Security metrics from the quarterly USM dashboard give the CIO a consolidated picture of Cisco's security posture from disparate IT systems. These metrics help enable prompt, responsive remediation efforts from the IT service owners and the CIO. Ultimately, their interactions lead to improved security performance.

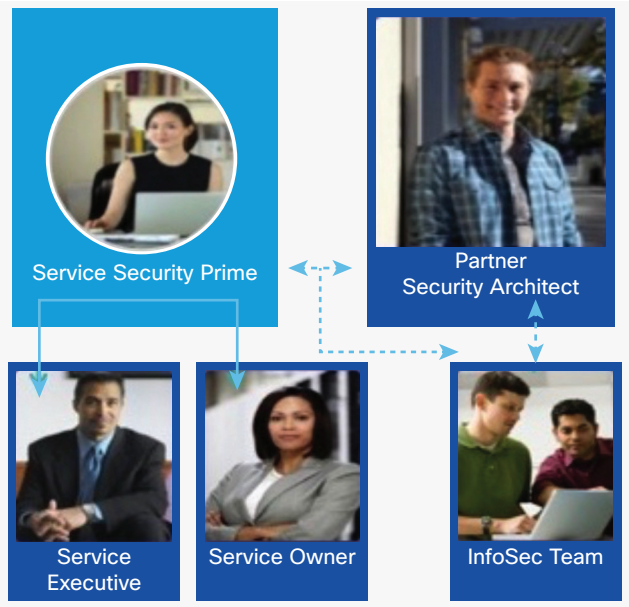
Cultivate Partnerships

Working relationships are the cornerstone of InfoSec's USM program, beginning with service security primes and partner security architects, who are a virtual team of trusted security advisors. They, in cooperation with the IT service owners, risk management groups, and decision makers (including the CIO), work with InfoSec to safeguard Cisco (Figure 5). Because of InfoSec's tight alignment with these groups, it can more effectively manage security investments, actions, and processes globally. This alignment also opens the door to advance metrics beyond basic security hygiene to more sophisticated posture assessments (for example, risk determination) within IT and with other departments.

Lessons Learned

During the creation and implementation of the USM program, we learned a number of lessons. Here are the most important ones.

Figure 5. Collaborators in the USM Program



Speak IT Speak

When sharing vulnerability data with senior IT leadership, discuss it as part of "operational effectiveness." Make security hygiene the same as uptime, bugs introduced and closed, and other IT metrics. The lesson for security people is that, to be understood, they need to map to IT speak and not security speak.

Start Small and Grow Organically

As with any new endeavor and, in particular with massive, complex organizations such as Cisco, it's best to start small before launching at "full throttle," so you can properly monitor, manage, or adjust your security metrics program accordingly. This experience will help you standardize your processes. It will also create IT service owner "champions" that can evangelize your security program for broader adoption and long-term sustainability.

Focus on Training

Formalized, ongoing training, such as that provided by Cisco's global internal Security Knowledge Empowerment program, expands security knowledge across the organization. Its courses range from as little as 4 to 6 hours of security basics to more than 120 hours of in-depth classroom, mentoring, and group projects. When combined with the advocacy of service security primes and partner security architects, it provides a potent conduit to expand security DNA throughout Cisco.

Build Trust

Keeping the USM process open, transparent, and nonpunitive is crucial to building trust and credibility with multiple stakeholders. Stakeholders can count on InfoSec to consistently deliver reliable, unbiased metrics every quarter. Ample time is also provided for broad internal team reviews and remediation efforts, along with clear communication for next steps. As a result of these collective activities, shared responsibility and accountability become the norm, fueling early program adoption among IT service areas. Ultimately, security performance improves.

Construct a Communication Process Flow Loop

Communication process flow loops are essential for security metrics "consistency" across a department. Establish a quarterly timeline so that IT service owners know when they can expect their security data, where they can find it (dashboards), and how to interpret it (reports). Users can access vital information in real time. Better synergy and dialogues between groups ensue to remediate security issues.

Keep It Simple

Most IT organizations track risk metrics routinely. Start by pulling data from IT system logs and dashboards. InfoSec narrowed its data sources from 30 to 5 and, in doing so, improved security process behaviors and actions within the IT department. Figure out what you want to achieve. Innovation does not always involve the newest and shiniest things. It often comes from new ways to get the basics right.

Some Challenges

Our stakeholders did not understand the vulnerability metric. They didn't know how to interpret the percentages, nor was the data particularly actionable. We removed it and focused on the on-time closure metric instead.

When we started measuring whether security checks were performed according to policy, we overloaded certain downstream processes. Even though this was anticipated, the extra load was higher than expected and those teams were not necessarily ready to manage it.

Program Successes

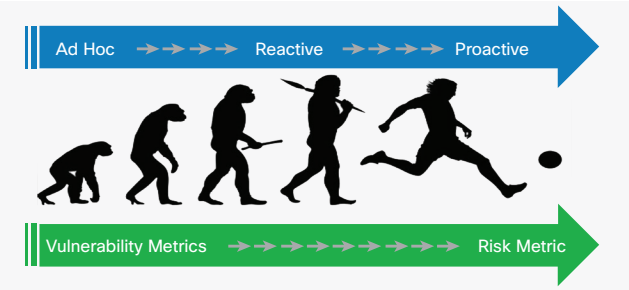
Before USM, the IT staff took an ad hoc approach to security across the service portfolio. The department was unable to manage and assess security vulnerabilities due to a lack of measures. Internal security vulnerabilities received marginal executive attention.

Since USM, "operational security" has become a responsibility shared between the CISOs and their peers at the IT executive level. This had a big impact. With USM measures in place, we are able to quantify Cisco's security health. We saw a 65 percent reduction in vulnerabilities, and on-time closure improvement rose from 15 percent to 80 percent within one year. The success led to a greater investment in security (up 50 percent year over year) and to support of the next phase of USM development.

Security Metrics Maturity Levels

When a department decides to adopt a Unified Security Metric program, one of the first things to determine is its existing maturity level. Here are some descriptions of security maturity (Figure 6).

Figure 6. The Evolution of Security Metrics



1. **Ad hoc:** Security metric reporting is performed organically. Typically, security metrics are not validated. They are communicated in standalone reports, and they are inconsistent and nontransparent.
2. **Reactive:** Security metric reporting is structured, and metrics have been defined. Security metrics are consistently delivered to decision makers and are acted upon. The scope of the metrics is toward vulnerability measurements. Communications to IT staff aim to ensure system hardening and compliance.
3. **Proactive:** Security metrics include people, process, risk, user behavior and cost. Besides the IT group, business and data owners are also provided with consistent security metrics and influenced in their security decision making, and they apply security best practices and efficiency throughout the organization. This level of maturity is out of scope for this paper.
4. **Predictive:** Security metrics include business behaviors and industry trends. They predict risks before they occur. This level of maturity is out of scope for this paper.

Conclusion

Today, with USM, the Cisco IT staff and InfoSec have greater confidence and insight into what's happening within the enterprise. They can quickly diagnose, remediate, and fix security issues.

Done right, it works! Make sure you get buy-in from upper management. Build those partner teams to create security synergy and governance and embrace talent outside your immediate security and IT staffs.

Always make sure you use measurements that are meaningful, accessible, quantifiable, and actionable. Start small and build trust across stakeholders and, if possible, use "IT as a service" building blocks.

Score results, and score them objectively. Consider introducing weighting over time. Finally, report results using the existing reporting structures wherever possible.

Appendix A: Sample Questions That Lead to Vulnerability Metrics

Every organization is different, and every organization has different needs for security metrics. When an organization chooses to adopt a Unified Security Metrics program, it should start by defining a set of security questions so that it can determine what its security posture is today. This appendix provides a starting point for organizations in the process of defining a set of questions that will lead them to the security metrics they need.

The list of question is broken down into three categories: Technology, Process, and People as described in the section "Vulnerability Metric Framework." When a list of questions has been decided upon, a concept is created that captures how and with what measurement data these questions can be answered. The most relevant questions will differ from organization to organization, but in principle the measurement data must be available, accessible, reliable, and usable. If possible, it should also be automated and scalable.

Questions	Category	Measurement	Measurement Data		
			Availability	Quality	Scalability
What kind of application vulnerabilities do we find through periodic application vulnerability scans, how severe are they, and how quickly do we fix them?	Technology	Number and severity of application vulnerabilities; number of on-time closures	Partly	Partly	Manual
What kind of infrastructure vulnerabilities do we find through periodic infrastructure vulnerability scans, how severe are they, and how quickly do we fix them?	Technology	Number and severity of infrastructure vulnerabilities; number of on-time closures	100%	100%	Partly automated
Is there an antivirus tool on the system and does it adhere to the antivirus update schedule?	Technology	Number of noncompliant hosts	100%	100%	Partly automated
What kind of vulnerabilities do we find through our penetration tests (destination available, or DAVA), how severe are they, and how quickly do we fix them?	Technology	Number of total findings versus closed findings; number of on-time closures	Partly	Partly	Partly automated
How many design exceptions are beyond their agreed-upon remediation date?	Technology	Total number of expired exceptions	Partly	Partly	Manual
How is the internal service externally exposed in any of our firewalls?	Technology	Number of permit statements per access control list	Partly	Partly	Partly automated
What is the desktop compliance for service administrators and developers (end-user device vulnerability)?	Technology	Percent of desktop compliance per admin/dev	Partly	Partly	Manual
Are exceptions stored in a central repository and follow-up tracked?	Process	Number of exceptions; number of closed actions, number of open actions	Partly	Fair, not all exceptions in same format	Manual
Are architectural assessments stored in a centralized place?	Process	Number of architectural assessment documents		Partly	Manual

Questions	Category	Measurement	Measurement Data		
			Availability	Quality	Scalability
Does the service have a risk rating and/or data classification captured in a service catalog?	Process	Actual risk rating, data classification	Partly	Partly	Manual
Are the root cause and long-term fix of incidents identified and tracked to closure?	Process	Number of closed and open incidents	100%	Partly	Partly automated
When administrators or developers change roles, is their access profile changed accordingly?	Process	Number of admins and developers; number of active admins and developers versus elevated access rights	Partly	Partly	Manual
For the service, is all data in the service portfolio, application portfolio, and Configuration Management Database kept up to date?	Process	Yes or no	Partly	Partly	Manual
How many generic passwords are being used for a service?	Process	Number of generic passwords	Partly	Partly	Manual
What percentage of service teams are security service primes and partner security architects?	People	Percent of PSAs and primes	Partly	100%	Manual
What percentage of security service primes and partner security architects have been provided with the appropriate training?	People	Percent of security primes and partner security architects	Partly	Partly	Manual
What percentage of administrators are trained on appropriate security topics?	People	Percent of administrators trained	Partly	Partly	Manual
What percentage of application developers are trained on appropriate security topics?	People	Percent of developers trained	Partly	100%	Manual
What percentage of users with sensitive business roles (controllers, HR staff, managers) have gone through security awareness training?	People	Percent of users	Partly	Partly	Manual

C11-737409-00 07/16