How Cisco IT and InfoSec Partner to Protect Our Infrastructure and Data

Operationalizing security with trusted people, process, policy, and technology

EXECUTIVE SUMMARY

CHALLENGE

- Protect infrastructure and data
- Ensure that security controls do not make it more difficult to do work or run the business

SOLUTION

- Embedded security throughout our infrastructure
- Implemented policies and processes
- Fostered a security-conscious culture

RESULTS

- Reduced vulnerabilities by 65 percent in the first year
- Improved rate of on-time closure of vulnerabilities from 15 percent to 84 percent
- Provided online training to more than 25,000 employees to be mindful of security

LESSONS LEARNED

- Include security experts on IT teams
- Enforce policies with technology whenever possible
- Measure success by tracking and publishing security metrics

NEXT STEPS

- Continue educating employees on security threats and precautions
- Introduce new technology as the threat landscape continues to evolve

Background

Customers often ask how Cisco protects our global enterprise. We prepared this case study to answer that question.

Cisco's goal is to be not only the world's number-one IT company but also the number-one cybersecurity company. Protecting infrastructure and data requires a close partnership between our IT and Information Security (InfoSec) organizations. InfoSec has more than 350 employees. Part of Cisco's Security and Trust Organization (STO), InfoSec works with Cisco IT to ensure that the products we build and the infrastructure we operate are secure. The ultimate goal is to protect our customers' investments and our business.

"We strive to be trustworthy, transparent, and accountable," says Michele Guel, distinguished engineer and chief security architect at Cisco. "That means leaving no stone unturned in our search for threats to our infrastructure or data."

Challenge

Organizations today must contend with a rapidly evolving cybersecurity landscape. Attacks continually grow more persistent, sophisticated, damaging, and frequent. Executing attacks has become easier: point-and-click software that exploits OS and application vulnerabilities is often available within days of the vulnerability's discovery.

Defending the Cisco® enterprise is a significant undertaking, involving 122,000 workers in 170 countries, 3 million IP addresses, more than 40,000 routers, approximately 26,000 remote office connections, and 75 million web transactions each day (Cisco 2016 Annual Security Report). Compounding the challenge, year by year the number of devices connected to our network increases, an outgrowth of the Internet of Things and our bring-your-own-device (BYOD) program. By the year 2020, an estimated 50 billion devices will connect to the Internet.

Growing interconnectedness and escalating cybersecurity challenges compel Cisco and other organizations to rethink their approach to security.

Solution

A Holistic Approach

Cisco IT and InfoSec work together to enable business productivity while protecting our systems and data from internal and external threats. Instead of focusing on security hardware and software alone, we take a holistic, pervasive approach to security by:

- Fostering a security-conscious culture to reduce the attack surface and ensure a robust security posture
- Implementing security-focused policies and processes
- Embedding security throughout our infrastructure

We take care to make sure that controls don't make it more difficult for employees to do their work or run the business. "Some people view IT as the organization that says no and InfoSec as the organization that says no even when IT says yes," says Marisa Chancellor, senior InfoSec director at Cisco. "We don't want employees to think they need to go around Cisco IT and InfoSec to conduct business."

Our holistic approach to security spans people, process, policy, and technology.

People

Our people are a critical first line of defense in protecting Cisco. We fund security advisors and work to foster a security-conscious culture across the company.

Security Advisors

Two types of security advisors work within our IT organization:

- Security Service Primes are accountable for the end-to-end security of one or more of our nearly 200 IT services, such as collaboration or data-as-a-service. The Security Service Prime is essentially the chief security officer for the service.
- Partner Security Architects (PSAs) serve as the technical security leads responsible for reviewing the security architecture for IT projects and applications.

Although security advisors are not direct InfoSec employees, they receive 25 hours of training from InfoSec and take ongoing 1-hour courses. "Security Service Primes and PSAs help the InfoSec team scale and embed security into the IT organization's DNA," says Sujata Ramamoorthy, director of information security for InfoSec.

Security-conscious Culture

Many vulnerabilities can be reduced or eliminated when employees are mindful of cybersecurity issues and their own role in protecting the organization. InfoSec and IT also work together to foster a security-conscious culture. Programs include:

- Online cybersecurity training program: More than 25,000 global Cisco employees and contractors have participated in an online training program called the Security Ninja program. Employees earn a white, green, brown, or black belt certification in various security topics by completing a series of 20-minute modules developed by Cisco experts. Tracks are available for managers, software engineers, hardware engineers, and non-technical employees. To date, approximately 60 percent of Cisco engineers have completed the white-belt training.
- Anti-phishing training: Every quarter we send a test phish to all 130,000 employees and contractors who have a Cisco email address. Employees who click the link see a web page explaining that if the link had been real, the employee could have put Cisco at risk. The site goes on to explain how to recognize phishing emails. Three weeks after the test, employees who clicked through the first time receive another test phish. Some

phishing emails are very convincing, and our first test had a high click rate. Education helped. “Across all companies, the average click rate for phishing emails is 30 percent,” says Dave Vander Meer, Cisco InfoSec service manager. “We’ve dramatically reduced that rate for our workforce.”

- Code of business conduct: Each year Cisco employees sign a code of business conduct. Data protection is as important a part of the code as acting ethically and using corporate resources responsibly. In agreeing to the code of business conduct, employees acknowledge that they are responsible and accountable for the data they handle, whether it pertains to customers, partners, or the company.

Process

Examples of processes we use to protect our infrastructure include publishing Unified Security Metrics (USMs) and conducting ongoing penetration testing.

Quarterly Unified Security Metrics

Without meaningful statistics about a service’s security posture, IT service owners and executives might incorrectly assume that their service is uncompromised and secure. InfoSec provides statistics by publishing USMs on a quarterly basis (Table 1). We calculate the metrics by combining multiple data sources, such as IT logs and penetration test results. For each metric we report the number of vulnerabilities and the on-time closure rate for vulnerabilities reported the previous quarter.

Table 1. InfoSec Reports Unified Security Metrics to IT Service Owners and Executives

Unified Security Metric	What It Measures
Stack compliance	Vulnerabilities found in network devices, operating systems, application servers, and middleware
Anti-malware compliance	Whether malware protection software has been properly installed and is up to date
Baseline application vulnerability assessment	Whether automatic vulnerability system scans have been conducted Security weaknesses that remain following the scan
Deep application vulnerability assessment	Whether penetration testing has been performed on business-critical applications in accordance with Cisco policy Security weaknesses that remain following the scan
Design exceptions	Number of open security exceptions, defined as deviations from established security standards and best practices

The goal of publishing USMs is to help IT service owners quickly diagnose, remediate, and fix security issues. “When USM revealed that only 15 percent of vulnerabilities were closed on time, leaving Cisco exposed, IT service owners stepped up to raise the percentage to 84 percent within a year,” says Ramamoorthy.

> “When Unified Security Metrics revealed that only 15 percent of vulnerabilities were closed on time, leaving Cisco exposed, IT service owners stepped up to raise the percentage to 84 percent within a year.”
>
> — Sujata Ramamoorthy, Director of Information Security, Cisco InfoSec

Cisco Attacks Its Own Enterprise

We regularly attack our own enterprise to expose security gaps before attackers can exploit them. With this proactive approach, InfoSec continually gathers intelligence about operating system and application vulnerabilities. We scan the network on a regular schedule to find and remediate vulnerabilities. Areas of highest risk are scanned daily and the entire enterprise is scanned monthly.

Vulnerability reports generated by the scans are automatically sent to the IT service owner. InfoSec and the service owner jointly review the findings because Cisco IT owns the assets at risk. “We look at which systems and data are at risk and how important they are to Cisco,” says David Bell, manager of InfoSec’s Vulnerability Management team. “Then we tell IT which systems need to be patched today versus, say, in 30 days.”

IT service managers sign into InfoSec’s scanning system to see the vulnerabilities that have been discovered in their area of responsibility, such as desktops or routers. The service owner uses Cisco IT’s asset management tool to identify all devices with the vulnerability, for example, storage with a particular operating system. Then service owners close the case themselves without involvement by InfoSec. The rate of resolution appears in the USM.

Policies

In conjunction with our focus on people and process, we enforce security-focused policies. Table 2 lists the policies that InfoSec applies to protect our infrastructure and data.

Table 2. A Holistic Approach to Security Includes Security Policies

Policy	Content
Acceptable Use	Requirements for acceptable use of information, electronic and computing devices, and network resources in conjunction with our established culture of ethical and lawful behavior, openness, trust, and integrity.
Access Management	Requirements for managing user and administrative access to information assets and information systems through proper controls for authentication, authorization, and auditing.
Application Security	Requirements that an application must satisfy to reduce the exposure of critical infrastructure and information assets to risk caused by vulnerabilities in application design, code, and infrastructure.
Audit	Requirements for audits and risk assessments to be conducted to ensure compliance with security policies, data integrity, incident investigation, or the monitoring of user / system activity where appropriate.
Cloud Security	Minimum security requirements for clouds we consume to conduct Cisco business or clouds we build (hosted services).
Computer Security Incident Management	Requirements for managing computer security incidents, including but not limited to detecting, responding, investigating, monitoring, and logging.
Cryptographic Controls	Requirements for the use of cryptographic controls to protect the confidentiality, integrity, and availability of information assets.
Data Protection	Requirements for classifying, labeling, and protecting data. Determines the relative sensitivity of information and how this information should be treated and disclosed to Cisco employees and other parties.
Information Security	Requirements for the management of Information Security and for the confidentiality, integrity, and availability of information assets.
Intellectual Assets Protection	Requirements for the protection of Cisco intellectual assets.
Lab Security	Information security requirements to manage and safeguard lab resources and Cisco networks by minimizing exposure of critical infrastructure and information assets to threats that may result from unprotected hosts and unauthorized access.
Network Access	Requirements for authorized users and devices to access corporate networks.
Password	Requirements for the creation, protection, and management of strong authentication credentials.
Server Security	Server equipment requirements to minimize the exposure of Cisco critical infrastructure and information assets to threats that may result from unprotected hosts and unauthorized access.

The policies in Table 2 are consistent with recognized best practices and industry certifications such as ISO 27001. “InfoSec is accountable for the policies, and we partner with Cisco IT and other organizations to put the right controls in place,” Vander Meer says. For example, InfoSec specifies required password strength. Cisco IT enforces the policy by setting up the password-reset and device-management solutions to reject passwords that don’t meet the criteria. Another example is network access. InfoSec defines device requirements, including anti-malware, operating system, and various settings. Cisco IT is preparing to use Identity Services Engine (ISE) to automate policy enforcement. For example, an employee’s device will receive full access to the network only if it meets all requirements. Otherwise access will be limited or blocked.

In 2005, we partnered with SANS, the world’s largest source for information security training and security certification, to make generalized versions of many Cisco security policies available as templates on the SANS Security Policy Resource website. Customers can use these templates as a starting point for their own security policies.

Technology

We use Cisco and third-party technology to protect data and systems throughout the attack continuum, as shown in Table 3.

Table 3. Cisco Security Technologies Used Throughout the Attack Continuum

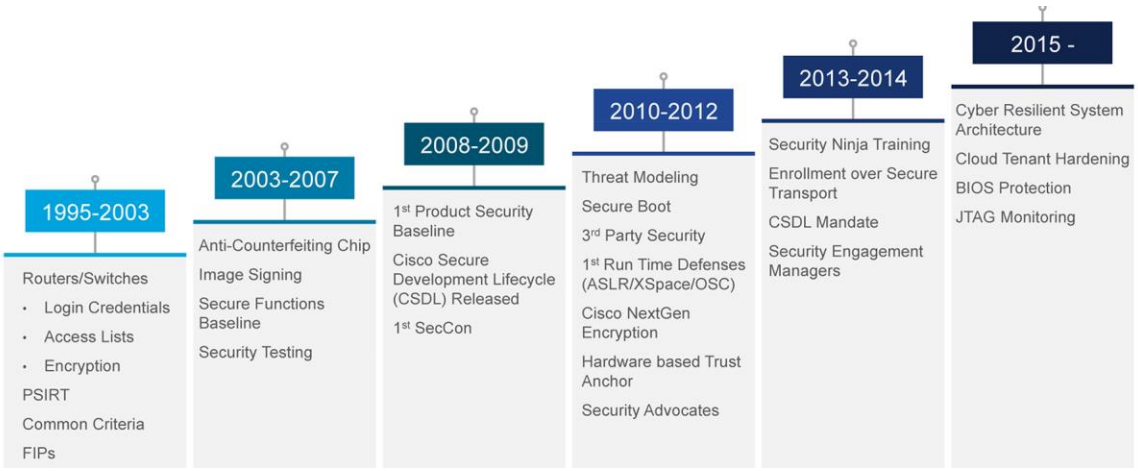
Strategy	Our Technology
BEFORE AN ATTACK: ENFORCE POLICIES AND CONTROLS	
Malware protection	Cisco Web Security Appliance (WSA)[1] Cisco Email Security Appliance (ESA)[2] Cisco Advanced Malware Protection (AMP) Cisco Intrusion Prevention System (IPS)
Policy, compliance, and device management	Cisco Identity Services Engine Cisco ASA Adaptive Security Appliances Cisco Application Centric Infrastructure Cisco Prime Infrastructure
Vulnerability management	Qualys Third-party code analysis tools Third-party vulnerability management tools
Data loss prevention	Third party
Web application security	Third party
DURING AN ATTACK: IDENTIFY AND BLOCK	
Collection and detection	Cisco Intrusion Prevention System Cisco FireSIGHT® Management Center Cisco AMP ThreatGrid Appliance Cisco Lancope
Mitigation	Cisco ISE for policy enforcement Security Group Tagging Cisco Application-Centric Infrastructure
Threat Intelligence, which WSA and ESA use to block malicious websites and email	Talos Security Intelligence and Research Group SenderBase®, the world’s largest email and web traffic monitoring network
AFTER AN ATTACK: ANALYZE AND REMEDIATE	
Reporting and incident handling	Cisco Lancope analytics with NetFlow data
Forensics and analysis	Cisco AMP ThreatGrid Appliance Cisco FireSIGHT Management Center

[1] WSA blocks 1.2 million of 75 million web transactions daily.
[2] ESA blocks 94 percent of incoming email at the edge.

Secure, Trustworthy Products and Infrastructure

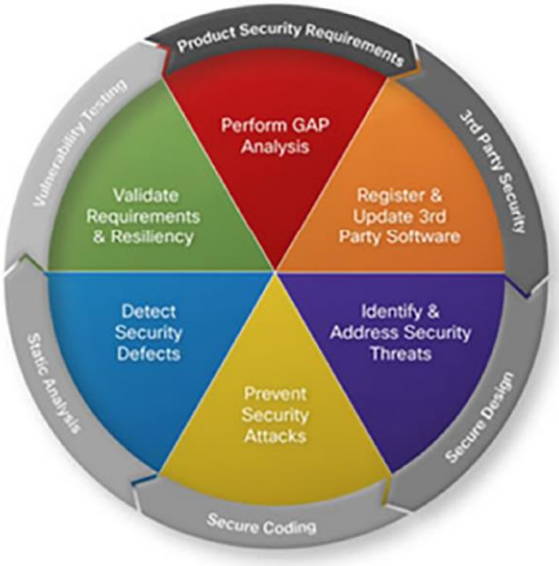
The foundation of a secure enterprise is secure and trustworthy products and infrastructure. “This requires IT organizations to procure the entire technology stack [infrastructure, compute, storage, applications] from vendors that follow processes to make sure their solutions are trustworthy,” says Steve Martino, Cisco’s chief information security officer. Cisco has been building secure technology into the products we design for our customers and our own company since 1995 (Figure 1).

Figure 1. Journey to Built-In Security



To further reduce vulnerabilities and improve resiliency, we adopted the Secure Development Lifecycle (SDL) process in 2008. SDL is a mandatory, repeatable, and measurable process for developing secure, resilient, and trustworthy products (Figure 2). SDL requires that security be a primary design consideration. It satisfies Cisco Product Development Methodology (PDM) and ISO 9000 compliance requirements, and works with Agile as well as Waterfall development. The result of SDL is that our product portfolio and global infrastructure are built on a bedrock of foundational security technologies such as boot protections and runtime defenses.

Figure 2. Cisco Secure Development Lifecycle



Results

We measure the success of our security operations using the following metrics.

On-time Closure of Security Vulnerabilities

Cisco IT and InfoSec agree on service-level agreements (SLAs) for closing security vulnerabilities. The target time depends on the severity of the vulnerability. “In the first year after adopting USM, we reduced vulnerabilities by 65 percent,” says Martino. “On-time closure of security vulnerabilities rose from 15 percent to 84 percent.”

Annual Loss Expected and Realized

Annual Loss Expected (ALE) from security incidents is based on industry research. We compare ALE to our own Annual Loss Realized (ALR), including labor, hardware, software, machine remediation, data loss, and brand reputation. Our financial goal is to achieve Realized Losses that are below Expected Losses. Our business goal is to establish clear metrics for how well are protecting Cisco and earn the trust of our customers and partners.

Critical Controls

In 2014 and 2015, we measured how well our internal processes and controls scored against the Center for Internet Security (CIS) Critical Controls. CIS has defined 20 categories of controls, including malware defense, wireless access control, continuous vulnerability assessment and remediation, and inventory of authorized and unauthorized software. Measuring critical controls shows the strength of our security posture at a given time and helps us identify gaps. In 2016, we plan to adopt version 6.0 of the controls, which provides a repeatable, consistent scoring method.

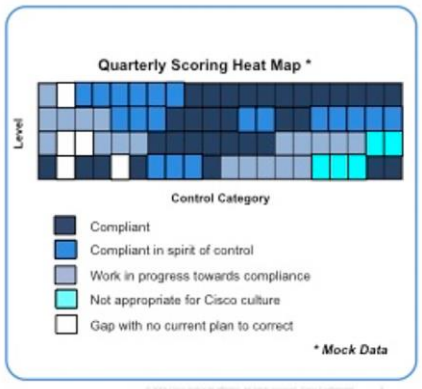
Each category of control has four levels of achievement, shown on the vertical axis of Figure 3:

- Level 1: Quick wins
- Level 2: Improved visibility and attribution
- Level 3: Configuration and hygiene
- Level 4: Advanced

Our Critical Controls grid has 80 boxes (20 controls x 4 levels). Our goal in 2016 is to mark each box with one of five ratings: compliant, largely compliant, in progress, not appropriate for Cisco culture, or gap with no plan to correct. (Examples of controls not appropriate for Cisco’s culture include disabling USBs and whitelisting endpoint applications.) InfoSec assigns the scores with input from Cisco IT’s Service Security Primes and PSAs.

The sample critical controls map shown in Figure 3 provides an easy-to-read picture of our security posture for our Board of Directors and customers. The map also helps us agree on which investments are most important.

Figure 3. Quarterly Scoring on 20 Critical Controls



Number of Cases

The CSIRT daily dashboard shows the number of threats stopped by our security solutions, such as the number of DNS probes stopped at the firewall. The Computer Security Incident Response Team (CSIRT) big-data analytics system creates the dashboard. “By analyzing the number of threats averted, we can see which security solutions provide the most value,” Guel says. “This influences our investments.”

> “By analyzing the number of threats averted, we can see which security solutions provide the most value. This influences our investments.”
>
> — Michele Guel, Chief Security Architect, Cisco

Time to Detect / Time to Contain Incidents

Another way we gauge the effectiveness of our security measures is by tracking the time to detect (TTD) and time to contain (TTC) security incidents. In April 2015, the median TTD was 6 hours and median TTC was 168 hours. As of February 2016, we are well on our way to a median TTC of 24 hours.

We label an event as an “incident” only if security is compromised because of malware, unauthorized access, or improper usage. When our systems block events, we do not count them as incidents. “We block millions of potential security events daily,” Martino says. “Omitting these blocked events from our measurements allows us to focus on managing those threats that do get past our frontline defenses.”

Tracking TTD and TTC against baselines allow us to:

- Tune instrumentation and incident-detection capabilities
- Partner with vendors to improve performance
- Continually improve our containment capabilities, such as attribution and quarantine

Next Steps

The threat landscape continues to evolve rapidly. Protecting our data and systems requires a holistic approach, with pervasive security and ongoing vigilance. “We will continue to innovate—using people, process, policy, and technology—to keep up with the ever-changing business and threat landscape,” Martino says. “We have built a strong foundation to lead Cisco’s security efforts with confidence and a mindset of continuous improvement.”

Plans include:

- Integrating security into our DevOps and continuous delivery strategy
- Scaling our security architecture to keep pace with the growth of the Internet of Things
- Increasing visibility and control of third-party cloud usage, as described in our paper about Securing Third-party Cloud Applications

Lessons Learned

Cisco IT and InfoSec offer the following suggestions to organizations that want to operationalize security:

- Carefully select your policies. It’s easier to manage and enforce 10 policies than 30. If your policies are not easy to understand and follow, users might look for ways around them.
- Consider starting with the policy templates on the SANS Security Policy Resource website. These are generalized versions of Cisco policies.

- Give IT service owners visibility into their security posture by publishing security metrics on a regular basis.
- Develop a security-conscious culture by creating online training programs. Keep modules short. A good target is 10 minutes or less. Associate security with a face by inviting your security experts to create and record the content. Look for ways to motivate employees to complete the training.
- Consider funding strategic security initiatives in addition to tactical projects. Our chief information officer and chief information security officer jointly sponsor a program called the Pervasive Security Accelerator. Among the programs it funds are Security Service Primes and USMs.

For More Information

Cisco received awards for Best Security Company and Best Security Organization at the 2016 RSA Conference. For more detail, visit http://blogs.cisco.com/security/cisco-security-leadership-at-2016-rsa-conference.

For information about managing cybersecurity risk, visit our Trust and Transparency Center.

For more detail about the Secure Development Lifecycle, visit www.cisco.com/web/about/security/cspo/csdl/.

Cisco 2016 Annual Security Report

To read additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit

Note

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described. Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties; therefore, this disclaimer may not apply to you.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**