




Cybersecurity: Build Trust, Visibility, and Resilience

White Paper

together we are
the human network.  CISCO

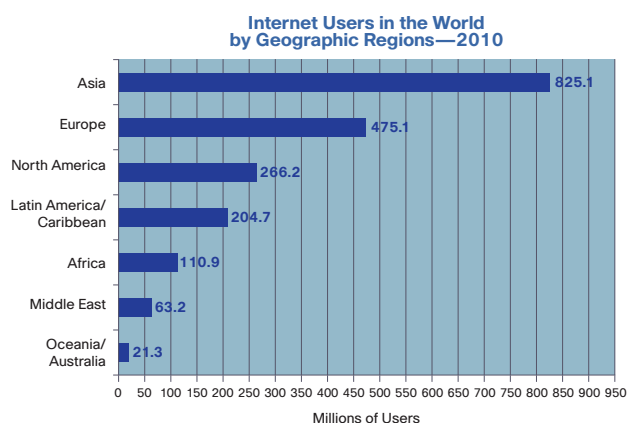
In this white paper, you will learn about security issues in today's Internet world. Organizational leaders, as well as IT staff, must understand these challenges and opportunities:

- Understanding the proliferation of risks
- Achieving a trusted network
- Creating network transparency and visibility to assess risks
- Establishing network resilience when security incidents do occur
- Working with Cisco® to address trust, visibility, and resilience in the network

Introduction

The global adoption of IP has changed the way citizens, businesses, and governments interact. Today, there is no more prevalent a communications platform than the Internet. Over the past 10 years, worldwide Internet growth has increased over 400 percent with an estimated 29 percent of the world population, or almost 2 billion people, being Internet users. In the United States alone, estimates say that 77 percent of the population, or roughly 240 million people, are broadband Internet services users.

Figure 1. Worldwide Internet Usage



Source: Internet World Stats—www.internetworldstats.com/stats.htm
Estimated Internet users are 1,966,514,816 on June 31, 2010
Copyright © 2010, Miniwatts Marketing Group

The evolution in Internet-enabled devices and the popularity of social media are fueling information growth. The world's store of digital content has reached 487 billion gigabytes and is growing. Cisco predicts that by 2013, 90 percent of consumer Internet traffic will be video. All of these factors present network-enabled organizations with a host of challenges and opportunities. They also present opportunities for those with ill intent.

We are no longer a network-centered nation, but instead a network-dependent nation. The long-predicted "Network of Things" is happening now. Network-connected devices are integral to every modern industry, from factory floors to building heating, ventilating, and air conditioning systems. It seems that everything is becoming "IP addressable." Furthering this dependence in the U.S. is diplomatic, intelligence, military, and economic reliance on the modern IP network.

Cybersecurity Challenges and Threats

Today's network-dependent organization faces an array of challenges and threats. Information and its critical role manifest in many different ways and formats, and are subject to countless outlets for distribution and sharing. Organizations find themselves balancing several factors.

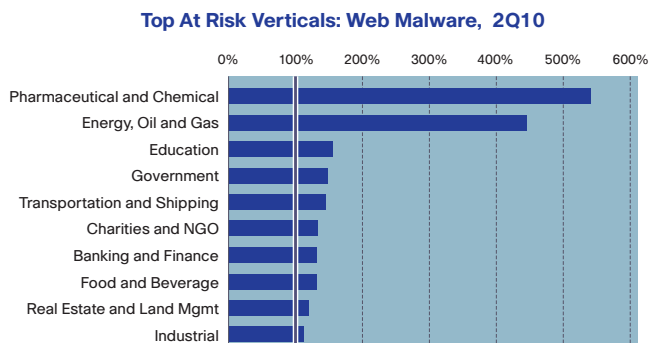
How do you properly **manage and protect** the information within the confines of an organization's best interest and regulatory environment while still taking advantage of new and disruptive technologies?

How do you **overcome the layering** of a previously consistent organizational boundary? The formerly rigid boundaries between public and private domains blur as virtualization traverses the organization and its information repositories.

How do you **address not only risks on the edges of the next technological advance but also within the core fundamentals** of information technology management? There are daily challenges behind the mundane tasks of managing a modern information technology environment.

With every challenge emerges new opportunities for malicious actors to insert themselves into the chaos. An ever-growing mixture arises among traditional cyber crime, economic and military espionage, and the shadowy concepts of cyber network discord. While modern organizations wait and assess the use of innovative technologies, cyber criminals are using technological innovation to their advantage. They exploit the gap between how quickly they can profit from vulnerabilities and the speed at which organizations deploy advanced technologies to counter the threat.

Figure 2. Malware Risk to Various Organizational Sectors



Source: Cisco ScanSafe

The uses of multi-vector attacks are growing. Cyber criminals remain intent on targeting legitimate websites, with strategically timed, multi-vector spam attacks in order to establish key loggers, back doors, and bots. Criminals plan their malware to arrive unannounced and stay resident for long periods. Regardless of your market sector, the threat is growing.

Cisco as a Natural Partner

No single company can solve the complex challenge presented by the Internet, but the inherent role of the network positions Cisco as a natural partner in developing and executing a successful cybersecurity strategy.

Cisco breaks down the complex environment surrounding cybersecurity into three considerations that require people, process, and technology.

The considerations are trust, visibility, and resilience. The network is pervasive across these focus areas and is critical to managing risk and improving your organization’s security posture.

Trust in Network Security

The word “trust” is often overused in cybersecurity discussions, yet it describes a foundation that must be established. An organization must have the confidence and belief that they can identify and manage their information technology assets. While trust seems like a simple function, it is often a fundamental challenge.

- Can you trust who and what is connected to your network?
- Can you trust the configuration of the devices attached to your network?
- Can you trust that you are not exposed to unnecessary risks?

These basic processes and functions form a foundation that can be trusted yet constantly verified. Cisco sees three steps in achieving this fundamental level of trust:

- **Asset Discovery and Management:** Validating user and device identity at the system point of entry and maintaining a state of trust
- **Configuration Management and Remediation:** Identifying misconfigurations and vulnerabilities so that corrective actions can occur to assure policy compliance and risk reduction
- **Architectural Optimization:** Design and feature application combined with best practices to create a threat-resistant and risk-tolerant infrastructure

Network trust requires simple and basic activities that organizations must perform well in order to establish a trusted foundation from which to build.

Network Visibility and Transparency

Transparency promotes trust and, Cisco believes that visibility is crucial to transparency. Visibility into the enterprise network helps enable the prevention and detection of threats and unnecessary risks.

The Internet-connected world represents a global threat that must be monitored and understood. Cisco uses its global network presence and technologies, such as Cisco Sensor Base™, as important components in understanding and keeping pace with constantly changing threat sources and mechanisms. Keeping pace requires the ability to quickly detect and mitigate these learned threats. However, as more complex threats evolve, organizations must identify suspicious behaviors and patterns and quickly remove the uncertainty surrounding the observed behavior. This requires the use of capabilities already inherent in the enterprise network for understanding information flows and identifying applications. To create an organizational risk overview, IT staff must take the critical step of assessing the known threats, vectors and signatures, and network behavior; available accounting and auditing sources should also take part in this part of the security process. Crucial to achieving this network visibility are:

- **Global Threat Analysis:** Using the global network as a sensor to collect and analyze information that IT can use to reduce the risk of compromise
- **Network Intelligence:** Utilization of enterprise network technologies to remove uncertainty and understand behaviors of internal information flows
- **Situational Awareness:** The systematic approach to supporting enterprise security decisions

Resilience

In today's environment, keeping pace is not an option but a necessity. However, no organization or enterprise is impervious to intrusions. Once a security breach occurs, your environment must quickly respond so that the scale of the threat is mitigated, the effects on operations and daily business are minimized, and that the organization can learn from the event. One of the many guarantees of connection to the public Internet is that your network will be threatened. It is important to assess your organization's abilities across these three areas:

- **Positive Network Control:** Using controls to manage traffic and maintain connectivity during a network intrusion
- **Threat Mitigation:** Limiting the consequence and scale of a threat, attack, or breach in an agile manner
- **Incident Handling and Forensics:** Quickly compiling relevant data to understand the methods that exploited your system and to assess how another breach can be avoided in the future

Summary

In conclusion, the Internet population, network-connected devices, and threats equal to, and perhaps exceed, our dependence on the modern network. In order to continue prospering from the use of this technology, the all organizations must address this challenge. Cisco is a natural partner in any enterprise cybersecurity strategy, because the network platform plays an important role in this environment. For your organization to keep pace with the dynamic environment, you must learn to use the network to achieve trust, gain visibility, and provide resiliency in your enterprise.



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.