RFI – April 2013

NSS Labs – NIST: Cyber Security Framework RFI

Author – Francisco Artes; Ken Baylor, PhD; Vikram Phatak

Overview

NSS Labs, Inc. is the world's leading information security research and advisory company. NSS is both an analyst firm specializing in security technologies and a testing laboratory widely recognized as the "go to" company for research, product claims validation and unbiased research. This distinction sets NSS apart from other analyst firms, which publish industry opinions based solely on surveys and questionnaires.

We deliver a unique mix of test-based research and expert analysis to provide our clients with the right information needed to make IT decisions. CIOs, CISOs, and information security professionals from many of the largest and most demanding enterprises rely on NSS. The company is located in Austin, Texas. For more information, visit www.nsslabs.com.

NSS is pleased to submit the following answers to NIST's RFI for its Cyber Security Framework initiative under Executive Order 13636. Answers provided reflect empirical data collected during testing within NSS Labs following our openly published methodologies (https://www.nsslabs.com/reports/categories/methodologies) as well as the professional experience of our analysts who have served as Chief Executive officers within large enterprise and critical infrastructure (as defined by 42 U.S.C. 5195c(e)) corporations. Additionally, generalized information has been provided based on NSS' work with its subscribers / customers who represent large cross-sections of US critical infrastructure from financial institutions to utility and natural resource services.

Table of Contents

RFI Answers

Within this document, each heading represents a major section of questioning as outlined in the Cyber Security Framework RFI, with sub-headings being used for each heading's respective question. Information provided within the RFI, normally sections of text preceding questions to supply context, have been included and are *italicized*. All answers are in normal font and text, and represent the opinion of NSS Labs.

Current Risk Management Practices

What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

Imperfect information and a lack of visibility are the primary challenges facing critical infrastructure. For example, engineers of industrial control systems do not receive interdisciplinary training on computer security and therefore base system design decisions on traditional factors such as uptime and accessibility. Further, operators of critical infrastructure are frequently unaware of the risks associated with how their systems are configured and deployed. Lastly, the attack capabilities and intentions of numerous adversaries are unknown.

Therefore the greatest challenges in improving cybersecurity practices are in rapidly developing accurate information about systems needing protection as well as visibility into current deployments and the capabilities and techniques of adversaries looking to compromise critical infrastructure. Once this basic capability is complete, a sober assessment of risks based upon data and facts can be made and a remediation plan can be developed. The rush to put forth a plan prior to obtaining accurate information runs the risk of making things worse by providing a false sense of security while alienating stakeholders who will be required to expend resources to follow guidelines and regulations that have not been proven to be necessary.

Furthermore, all regulations and frameworks should be maintained by and enforced by regulators, not regulations. These regulators should be a special category of advisors from the private sector that are members of companies that do not resell services or products.

What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

There are several key issues that private and public organizations face, in no particular order:

- The appearance or assumption of anti-trust due to working alongside competitors to help bolster security across an industry.
- An ideal that "we do things differently than everyone else" leads to an isolated mindset; often limiting key decision makers from seeing commonality with their peers outside their respective companies.
- Industry specific goals are often mistaken for uniqueness that would prohibit collaboration. For example, a pharmaceutical company recognizes that its key data to protect are those repositories of documentation, research information, and chemical composition of their drugs. Wile a computer gaming company recognizes that its key data to protect are repositories of source code, design and technical documentation, marketing plans, etc. Neither recognizes that the essence of what is being protected, the IP produced by both, is essentially the same and their combined best practices and lessons learned through failure could benefit the other.
- Corporations do not want to share their "secret sauce" in case that sauce gets used to breach them.
- Where do you balance sharing information to improve security, and keeping information confidential to maintain security?

Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?

NSS Labs has a top down approach to information security. As all of our senior officers are current and former information security professionals, as well as the majority of our operations staff, we have an actively encouraged "Security Culture". Security mindset is pervasive throughout our rank-and-file. We have a uniquely different issue in that our own employees are constantly pushing for our practices to be better, and often take initiative to test and develop these new security practices and measures.

Where do organizations locate their cybersecurity risk management program/office?

This can vary from company to company for strategic purposes. Arguably it can be stated that housing cybersecurity / risk management programs under the office of the CIO is often breaking many segregation of duties issues outlined within other compliance practices, yet is overlooked or goes unnoticed by many organizations. Cybersecurity / risk management groups should stand equal to Information Technologies (IT), as their job is to set practices and audit the compliance and implementation of those practices by IT. Having your chief security officer, or head of security in the absence of such a position, reporting to the CIO doesn't benefit the company and may create a conflict of interest.

CISO vs. CSO

Typically we see the heads of security of organizations falling into one of two titles. The first, the Chief Information Security Officer (CISO), is the more common of the two and like a Chief Information Officer (CIO) this person's focus is generally the corporate critical infrastructure. These would be items such as financial systems, email, corporate perimeter security, employee endpoint security, human resource systems, etc. The second, and potentially most valuable addition to overall cybersecurity posture within a company, is the Chief Security Officer (CSO.) This position is more akin to the Chief Technology Officer (CTO) as the focus of this officer of the company is towards the security and architecture of the IP, infrastructure, systems, etc. that the company produces as part of its market product. Whether this is developing and supporting strategy for public networks or for consumer applications and resources, this position, when used correctly, is devoid of compliance and regulatory oversight that the CISO may have, and the team supporting the CSO's objectives is often more strategic and tactical than is that of the CISO.

All of this poses the question of: "where would be the best fit for our head of security and thus our cybersecurity / risk management program?" And this should vary based on your company's operational goals. Examples:

- A technology company that is developing innovative new Internet offerings, IP, or is driven by the technology and IP they produce would benefit from the head of security reporting into the CTO who drives these initiatives. This places security inline with corporate initiatives as security for the offering to market (B2C or B2B) is taken into account during the entire development and support lifecycle of the product. Likewise, this is a more suitable situation for a CSO rather than a CISO.
- A financial organization may decide that the head of security should fall under the COO of an organization or even perhaps the CFO or general counsel. Security here must go far beyond compliance and regulatory efforts within the marketplace due to the emergency of crimeware tools and tactics that take advantage of over taxed and ill focused security teams. Again, this may be a prime example of the implementation of a CSO in addition to a CISO within the organization.
- A publicly traded organization may best benefit from the head of security reporting to the CFO due to the focus and need to maintain compliance under SOX. If the company demands broader security initiatives, and all should, this CISO reporting to the CFO is ideal and allows for the divesting of tactical security to the CSO who could report to the COO and have little involvement with compliance and regulatory matters.

In any such scenario it is best to hire key team members who have the tactical or compliance based skills most needed by the company.

How do organizations define and assess risk generally and cybersecurity risk specifically?

Due to imperfect information and poor visibility, cybersecurity is a "market for lemons". Organizations have therefore historically looked for cybersecurity to prevent an interruption of business, and in some cases prevent a loss of key intellectual property. This approach could be defined as a "catastrophic" approach to risk management. Further, due to the many unknowns, different industries have taken different approaches – often falling back to defending against the "known unknown" by taking a "kitchen sink" approach.

The ideal that many vendors and their marketing teams have presented is that with layered security, especially when a heterogeneous methodology is utilized, risks are mitigated and you are "safe" (e.g. products claiming to stop the latest zero-day (0day)). There is a perception that prior exploits, even those recorded and cataloged under the Common Vulnerability and Exposure Library (CVE), are therefore blocked. This simply isn't the case.

Research at NSS shows that even with a comprehensive layered-security model there are major correlations of failures to detect and block well-known exploits from bypassing all security products.

Companies need to understand their true threat landscape, and make decisions based off of what actually does punch through their current defenses. Watching a SIM/SIEM and hoping to find an attack that gets past your layered security is reactionary and fails to afford a corporation, especially one who's operation is critical to national defense or infrastructure, the opportunity to assess risks properly.

To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?

Unfortunately, most enterprise risk management programs do not incorporate cybersecurity risks due to a lack of hard data. Enterprises frequently spend more energy mitigating currency risk or hedging mission critical commodities than cybersecurity.

Research indicates that cybersecurity risk should not be decoupled from the other risk management programs, including physical security risk management programs.   Different departments should work together to perform training, physical security assessments, information security assessments, and determine where the boundaries are, including “flexible boundaries”. These departments can work with audit and risk management to determine the most likely risks and threats, and how to close the extant vulnerabilities, or mitigate them with various controls.

What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

PCI-DSS, SOX, FFIEC, GLBA, HIPAA, FISMA, Mass Data Breach, CA SB1386, ISO 27001/27002, and SAS 70 / SSAE 16 are some of the existing standards. They define best practices such as penetration testing, executive ownership, as well as tools such as anti virus, firewalls, intrusion prevention, web application firewalls, and even vulnerability scans. However, none of these standards are designed to measure and manage cybersecurity risk. All are designed around validation of operational compliance.

Some best practices have been abstracted from various compliance regulations. Items such as onboarding and off boarding of employees, segregation of duties, review of access controls and user accounts (e.g. “garbage collection”), etc. are all well founded and supported practices, as are those relating to authentication, authorization, and auditing. Self-auditing within organizations continues to grow as is evident by the growing market of SAAS and appliance offerings in the auditing / testing section of cybersecurity.

NSS is unique in its use of cybersecurity tools to test and measure security effectiveness of products offered throughout the gambit of cybersecurity offerings. We have added highlights from testing the security effectiveness of appliances and software ranging from SCADA to the most modern firewalls and intrusion prevention systems (IPS) in the appendix of this RFI.

What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?

They are limited and generally relate to information that must be provided to customers post a breach of security and are tied to loss of information. Financial institutions comply with FFIEC guidelines, those processing credit cards adhere to PCI (albeit in limited parts of their infrastructure) and public companies comply with SOX. Various state-level data protection laws such as California SB 1386 focus on breach notification, the SEC requires public disclosure of hack attacks in limited situations, but most companies have little regulation or standards in place.

Name	**Scope**	**Mandatory**
PCI-DSS	Credit card processing	Y
SOX	Public record finance	Y
FFIEC	Financial Institutions	Y
GLBA	Financial Institutions	Y
HIPAA	Health Records	Y
FISMA	Federal Agencies	Y
Mass Data Breach	Doing business with Mass resident	Y
Cali SB1386	Doing business with California resident	Y
ISO 27001	Information Security Management Systems	N
SAS 70/SSAE 16	Attestation framework	N

What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?

In today's market environment even corporations not recognized as critical infrastructure are integrated into the telecommunication, electrical, and electronic financial services ecosystems.

What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?

Most companies have not adopted performance goals with regards to managing cybersecurity risk. Those that do, however, follow a process whereby essential services are reviewed and optimized by cybersecurity teams. Through optimization and documentation, such processes become repeatable and this is the first move towards securing essential services and providing optimal cybersecurity. It also provides "security" a disguise; allowing it to bypass internal political barriers.

Most organizations measure success based on financial profitability. Security can, in effect, reduce costs by establishing a development framework and corporate best practices so that otherwise one-off solutions no longer necessary.

Useful metrics are hard to come by in cybersecurity. Presenting materials that show X-number of attacks occurred this month versus Y-number next month has little to do with your true security posture or effectiveness, nor does it have anything to do with the performance goals of your organization. Yet these metrics are pervasive because they lend themselves to achieving a good audit score. Ironically, it is the attacks that are not being captured in any log that are the ones an organization needs to be concerned about.

In the absence of published support of business process and goals, organizations are left to develop their own performance goals to measure the success of the cybersecurity groups, as well as risk to their companies. Risks are often reviewed in the same manner as market research with regard to impact to the bottom line on financial statements. Risk vs. Reward has been the mantra of security certification programs such as ISC^2's *CISSP* for years. With this mindset the purchase of a few million dollars worth of firewalls is weighed against the risk and cost of losing the data on systems that should fall behind firewalls and other layered security.

If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?

While NSS does not have reporting requirements as it is a private company. However, many of our senior analysts have led information security practices within Fortune 100 companies, companies with massive amounts of credit processing, financial institutes, etc. Generally speaking, auditing and compliance with regulatory agencies is either self-filed or done through a registered / approved third-party such as a major consulting firm. There is very little direct interaction with any regulatory body.

With regard to the motion picture industry, the MPAA operates a very mature security program that demands and affords direct communication with the regulatory body (the MPAA itself) for all vendors providing services to the six major motion picture studios that comprise the MPAA. The results of regulatory audits directly affect how the business and trust with IP is given to any one vendor or global corporation servicing this industry. A review is conducted on the requirements and demands of the regulatory aspects of the audit, along with the general cybersecurity operations for each vendor that voluntarily subjects to the process. The methodology matures each year due to the accumulated data. Every head of security from each of the major studios and all of the vendors provides input. This also creates a feeling of ownership and those involved with the process are more inclined to utilize the methodology and improve on it within their respective companies.

With regard to Financial Services, the industry is highly regulated. There is a great amount of bureaucracy and multiple detailed audits each year. As a result smaller banks have a 'survive the audit' mentality rather than focus on truly protecting customer data, and many initiatives are driven by compliance departments rather than security departments. Nonetheless, legislation such as GLBA has been a great benefit. The FFIEC supplementary guidance for internet authentication 2011 has also forced smaller banks to take internet fraud seriously. With larger banks there has been a strong separation between security and compliance and both are able to focus effectively on protecting customer data. While burdensome on financial institutions, the requirement to report and be audited has been very beneficial for the end customer and for confidence in the financial sector.

What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?

Historically, government compliance programs have focused on frameworks that utilize process and procedure with loose criteria in order to make them flexible. Unfortunately, that does not provide sufficient guidance for proper security. An organization might be able to check all the boxes, and still be insecure.

As noted in earlier, cybersecurity is "a market for lemons" where information is asymmetric and therefore market forces have broken down. In similar situations other industries, such as medicine and law have developed systems to address the demand for high standards that ensure public trust. While there are a number of professional certifications within the cybersecurity / information security field, the industry lacks oversight and governance which could afford the same qualifications and controls for licensing and accreditation as are established for medical doctors and attorneys. Through such measures the government could positively impact cybersecurity.

Likewise, just as the insurance industry in order to reduce risk spearheaded motor vehicle safety, fire safety, and medical best practice improvements, mandatory cybersecurity insurance would likely empower insurance companies to drive security innovation.

Use of Frameworks, Standards, Guidelines, and Best Practices

As set forth in the Executive Order, the Framework will consist of standards, guidelines, and/or best practices that promote the protection of information and information systems supporting organizational missions and business functions.

NIST seeks comments on the applicability of existing publications to address cybersecurity needs, including, but not limited to the documents developed by: international standards organizations; U.S. Government Agencies and organizations; State regulators or Public Utility Commissions; Industry and industry associations; other Governments, and non-profits and other non-government organizations. NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage. Please provide information related to the following:

What additional approaches already exist?

There are a variety of sector-specific certifications (individual technical certification and compliance acknowledgement certification) that have been developed. These groups generally compete for market dominance, while driving to grow their individual profitability. Many provide “certification” without performing actual audits or reviewing artifacts, and this provides the market place and consumer with a false sense of security.

Additionally, some sector-specific associations have formed and modeled their frameworks and methodologies after (often based upon) NIST, ISO, etc. These associations contain member companies who opt-into the programs and support the association via collecting membership dues. Entertainment, energy, and finance are examples of industries with independent governing bodies that are developing best practices, frameworks, and methodologies.

While not directly applicable, the American Medical Association, state medical boards, and similar bar associations within the legal market have establish sector-specific certification and accreditation that could be templates for cybersecurity.

Which of these approaches apply across sectors?

The documentation and application of standards such as ISO 17799 and 27001 are easily adopted across sectors. These are all basic best practices, processes, and methodologies that provide guidance and uniformity. They are very often used as the basis of cybersecurity, corporate information security policies, etc. The commonality of many of these best practices to those found inside of SOX, GLBA, HIPAA, PCI, etc. is evidence of their lasting and agnostic nature.

Which organizations use these approaches?

In the absence of specific government frameworks and standards for cybersecurity many sectors have developed their own best practices and security frameworks which are based upon best practices found within ISO, NIST, etc. A prime example would be the MPAA’s Best Practices for digital content protection and handling.

What, if any, are the limitations of using such approaches?

Most of these approaches focus on the limitation of exposure in an attempt reduce the likelihood of a security breach. There is little recognition that cyberwarfare / cybercrime is asymmetric: attackers only need to be successful once; defenses need to be effective 100% of the time. As a result, every compliance standard guarantees failure.

Further, few provide guidelines for dealing with the inevitable breach, and even fewer take into account the likelihood that the network, system, or application has already been breached (prior to the implementation of a policy.)

What, if any, modifications could make these approaches more useful?

A shift in focus from complying with general best practices to achieving specific objectives such as information gathering, with the objective of obtaining active threat intelligence as well as visibility into corporate assets and workflows is essential. This would return operational security and situational awareness to the mindset and culture of cybersecurity. Holistically security process should include information intelligence, visibility into the security flaws limitations of deployed technologies, as well as visibility into security risks based upon what the bad guys are doing.

How do these approaches take into account sector-specific needs?

By nature this approach would be sector-specific as it starts with information gathering and developing a plan accordingly. Just as a doctor diagnoses a patient before prescribing a solution, this approach allows for cybersecurity professionals to diagnose and prescribe the correct solution based upon the unique needs of the situation. Traditional compliance is akin prescribing aspirin for everything and ignoring the need to diagnose the ailment.

When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

Indeed there should be. While core competency / best practice items which are commonly shared across standards and guidelines will remain, there is a need to customize frameworks to reflect sector-specific requirements. The MPAA developed their current guidelines and testing frameworks (found at: http://www.fightfilmtheft.org/best-practice.html) by mapping best practices for their sector-specific needs to ISO, NIST, SAS, etc. Adoption and review of other similar sector-specific frameworks were utilized as well, such as those from computer gaming. This allowed for a far more efficient development and more importantly, deploying an adoption of this framework by the industry. Buy-in was streamlined due to the involvement of those that would be subject to the new frameworks and standards during their development, and the framework itself matches common workflow and practices within their industry.

What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

By acting as a neutral party, such a central organization can afford the avoidance of anti-trust concerns when sharing industry knowledge and lessons. Such a group should not simply drive a framework, but rather facilitate committees of sector-specific thought leaders who can work towards improvement and customization of standards and process. By enacting controls over companies within that sector the group would add merit to their security standards, bypassing internal political arguments over the costs associated with compliance.

What other outreach efforts would be helpful?

Sector-specific public-private organizations similar to the DOJ's Infragard and USSS Electronic Crimes Task Force would be highly beneficial. By building the relationships with their counterparts in the private sector it is far easier to share and communicate information, act during a breach, or request help.

Specific Industry Practices

In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry. NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

- *Separation of business from operational systems;*
- *Use of encryption and key management;*
- *Identification and authorization of users accessing systems;*
- *Asset identification and management;*
- *Monitoring and incident detection tools and capabilities;*
- *Incident handling policies and procedures;*
- *Mission/system resiliency practices;*
- *Security engineering practices;*
- *Privacy and civil liberties protection.*

Are these practices widely used throughout critical infrastructure and industry?

Some are more widely used than others. The separation of business from operational systems is commonly found inside of corporations, technology companies, and those who produce digital IP, and of course with regulated industries such as financial institutions and healthcare. However some critical infrastructure, such as the energy sector, still have flat networks. This has resulted in accidents and is the impetus for modern issues and current industry concern as networks are being expanded and interconnected without due care, thus bypassing the previous security methodology of air-gapped infrastructure.

Encryption, when used, is often more a process of finding the strongest levels of encryption that are scalable then anything else. More companies have issues with key exchanges, repositories, and escrowing then they do with moving sensitive information without encryption. That said, while encryption is highly adopted for data in motion, encryption of data at rest is often not implemented. Had data at rest been encrypted, the majority of breaches known today would have resulted in the attackers gaining access to unusable data.

With regard to identification and authentication of users, there has been widespread adoption of the use of central user authentication systems such as Microsoft Active Directory. But this is more often to address the issues of economy of scale with regard to administration than they are for security. As a restult, more sound practices such as two-factor authentication have not yet been widely adopted.

Asset identification and management has seen several iterations of technologies to help tackle these issues, but it always turns into the housekeeping tasks of IT. Abandoned, not executed properly, and high-costs to maintain are often cited as reasons to forgo this process. However, identification of assets is critical to understanding and formulating a sound security program.

Monitoring and incident detection tools are growing in popularity and diversity. Focus by major SIM/SIEM vendors is now on the efficiency of producing reports and live data, which shows customers are pushing harder on usability of these data aggregation systems. The development and deployment of security operations centers (SOCs) continues to grow, often fed and enabled by monitoring systems. Recent awareness by industries that their systems are compromised, not that they **may** one day be compromised, has lead to the development of new innovative technologies such as breach detection systems (BDS.)

Incident handling, policies and procedures are as of yet immature. Most companies are unaware of how to respond should an incident occur. Companies specializing in incident response have emerged to assist in navigating this often-confusing process. Government agencies have not been transparent in their engagement requirements. i.e., dollar value of loss before an AG will become involved / interested in the case. It is unclear if their decision making criteria maps to good public policy.

Probably the most used, and in some cases overly applied, aspect of security architecture is resiliency practices. From DR to BCP these practices are called for in many frameworks and compliance standards. Redundant-everything is often the mantra of large IT organizations, and the fear of a single-point of failure is often a driving force within network, DR, and BCP architecture. Vendors have responded with mature well-designed methodologies for systems to detect failure and automatically enable backup services even if devices are placed thousands of miles apart from one another. The practicing of resiliency efforts, from testing fail-over systems, to bringing online hot/warm/cold sites, and even now the use of cloud services shows an ongoing focus and ever advancing/maturing implementation of this best practice.

Conversely security engineering practices are not improving with regard to cybersecurity. Engineering staff is often not cross-trained to understand the tactics or mindset of an attacker, and systems continue to fall prey to being setup for efficiency and ease of use with no regard to data security..

Privacy and civil liberties protections are not uniform within the corporate world. Clearly where demanded through programs such as HIPAA and PCI there is should be due care and attention given to the handling, storage, and access of such PII. Beyond that, privacy varies from company to company, and business model to business model. Companies for whom people are “the product” treat privacy differently from traditional companies where people are the customers.

How do these practices relate to existing international standards and practices?

Many of these practices are covered at some degree under various international standards, whether the cybersecurity group within a company or industry knows them is another matter. Below are some examples of sector-specific and international standards and practices that are publicly available and address the topic areas of this section of the RFI:

Separation of business from operational systems:

- NERC Urgent Action Standard 1200 calls for the separation of operational and corporate networks for SCADA security.
- MPAA Supplemental and Common Guidelines (http://www.fightfilmtheft.org/best-practice.html)

Use of Encryption and key management:

- COBIT 4.1
  - DS5.8
  - DS5.10
  - DS5.11
- HIPAA/HITECH
  - 45 CFR 164.312 (a)(2)(iv)
  - 45 CFR 164.312 (e)(1)
  - 45 CFR 164.312 (e)(2)(ii)
- ISO/IEC 27001
  - A.10.6.1
  - A.10.8.3
  - A.10.8.4
  - A.10.9.2
  - A.10.9.3
  - A.12.3.1
  - A.15.1.3
  - A.15.1.4
  - Clause 4.3.3
  - A.10.7.3
  - A.12.3.2
  - A.15.1.6
- NIST SP800-53 (R3)
  - AC-18
  - IA-3
  - IA-7
  - SC-7
  - SC-8
  - SC-9
  - SC-13
  - SC-16
  - SC-23
  - SI-8
  - SC-12
  - SC-13
  - SC-17
  - SC-28
- Fedramp Sec Controls (Low)
  - NIST SP 800-53 R3 AC-1
  - NIST SP 800-53 R3 AC-18
  - NIST SP 800-53 R3 IA-7
  - NIST SP 800-53 R3 SC-1
  - NIST SP 800-53 R3 SC-7
  - NIST SP 800-53 R3 SC-13
- FedRamp Sec Controls (Moderate)
  - NIST SP 800-53 R3 AC-18
  - NIST SP 800-53 R3 AC-18 (1)
  - NIST SP 800-53 R3 AC-18 (2)
  - NIST SP 800-53 R3 IA-7

  - NIST SP 800-53 R3 SC-7
  - NIST SP 800-53 R3 SC-7 (4)
  - NIST SP 800-53 R3 SC-8
  - NIST SP 800-53 R3 SC-8 (1)
  - NIST SP 800-53 R3 SC-9
  - NIST SP 800-53 R3 SC-9 (1)
  - NIST SP 800-53 R3 SC-13
  - NIST SP 800-53 R3 SC-13 (1)
  - NIST SP 800-53 R3 SC-23
  - NIST SP 800-53 R3 SC-28
  - NIST SP 800-53 R3 SI-8
- PCI/DSS V2
  - 2.1.1
  - 3.4
  - 3.4.1
  - 4.1
  - 4.1.1
  - 4.2
- NERC/CIP
  - CIP-003-3 - R4.2

Identification and authorization of users accessing systems:

- COBIT 4.1
  - DS 5.3
  - DS 5.4
- HIPAA/HITECH
- ISO/IEC 27001
- NIST SP800-53 (R3)
- Fedramp Sec Controls (Low)
- FedRamp Sec Controls (Moderate)
- PCI/DSS V2
- NERC/CIP

Asset identification and management:

- HIPAA/HITECH
- ISO/IEC 27001
- NIST SP800-53 (R3)
- Fedramp Sec Controls (Low)
- FedRamp Sec Controls (Moderate)
- PCI/DSS V2
- NISTIR 7693 – Specification for Asset Identification

Monitoring and incident detection tools and capabilities:

- COBIT 4.1
- HIPAA/HITECH
- ISO/IEC 27001
- NIST SP800-53 (R3)
- Fedramp Sec Controls (Low)
- FedRamp Sec Controls (Moderate)
- PCI/DSS V2
- NERC/CIP

Incident handling policies and procedures:

- COBIT 4.1
- HIPAA/HITECH
- ISO/IEC 27001
- NIST SP800-53 (R3)
- Fedramp Sec Controls (Low)
- FedRamp Sec Controls (Moderate)
- PCI/DSS V2
- NERC/CIP

Mission/system resiliency practices:

- COBIT 4.1
- HIPAA/HITECH
- ISO/IEC 27001
- NIST SP800-53 (R3)
- Fedramp Sec Controls (Low)
- FedRamp Sec Controls (Moderate)
- PCI/DSS V2
- NERC/CIP
- AICPA

Security engineering practices:

- DoD 8570.01-M

Privacy and civil liberties protection:

- HIPAA/HITECH
- PCI/DSS
- GAPP
- ISO/IEC 27001
- NIST SP800-53 (R3)
- Fedramp Sec Controls (Low)
- FedRamp Sec Controls (Moderate)

Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?

The separation of business and operational networks is one that is a challenge from both the security and engineering perspective. Often such a change is driven by security, the segregation of networks and inclusion of internal firewalls, barriers, processes, and additional efforts are no small undertaking for a small to medium business let alone that of a large corporation or utility provider. The size, scope, and intricacies of the network or networks that must be separated, along with the relevant architecture to maintain critical functions, can be quite complex and require skillsets that are in short supply. Schools rarely supply engineers with adequate instruction or mastery of diverse and layered networks.

Are some of these practices not applicable for business or mission needs within particular sectors?

No, all of the related topic areas are generally considered part of "best practices" regardless of industry, regulatory governance, or standard. Most companies within the United States produce the same type of product, intellectual property. From car manufacturers the latest wonder drug in pharmaceuticals protecting critical data is paramount. Job and industry stability, economic growth models, and even the health and safety of citizens all depend on the cybersecurity efforts within these companies. All are generally private companies, some have government support and are provided information which validates headcount, initiatives / executive backing, and expenditures to provide adequate security, and others do not.

When a sector is left without feedback or guidance there is a great potential for a "it's never happened before so why should we bother" mentality with regard to new security initiatives. Due to the need to justify costs, management will often prevent changes to practices, policies, and for that matter add technology or headcount. Open communication, sharing of critical thread feeds and bi-directional intelligence reporting are critical to improving cybersecurity efforts for these and many other reasons.

Which of these practices pose the most significant implementation challenge?

Privacy and civil liberties protection is the most challenging especially in light of some business models that monetize lax privacy standards. Protecting the privacy and rights of customers is becoming a key issue with consumers and vendors alike. Due care and due process must be given to all topics under this heading. While everyone will agree that adding security to fortify privacy and ensure civil liberties is always welcome, there are other international concerns that need to be addressed within this framework. The United States differs in these key topic areas of cybersecurity when compared to the EU, Canada, and other nations. Large corporations in the United States often have offices, branches, or entire legal corporations within other countries. Data stored in the United States is not always protected, and this framework should address and apply civil liberties protection and privacy universally if such information and data is stored in the United States.

How are standards or guidelines utilized by organizations in the implementation of these practices?

They are applied universally and generally are utilized in the framing of policies and methodologies. ISO/IEC 27001 & 27002 are often used to frame executive ownership, establish common controls, and provide methodology for many aspects of a company's security practice. SAS 70 (now SSAE No. 16) is used to develop controls and add check-up and auditing to most processes. Policies are developed from process as a best practice. The repetitive utilization of some of these best practices with different standards has inculcated them into the mindset and jargon of the industry: segregation of duties, password again and retention, key escrowing, executive ownership, and segregation of critical networks from corporate networks are all examples of reused practices that are now considered to be de facto policies for many companies.

Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

Generally, no. This all depends on the type of company and what it is that they produce. Regardless, the ideal that IT standards equate to security best practices is a dangerous misconception. IT has a focus on the overall SLA they provide and their scope of responsibility is often limited to corporate infrastructure and applications such as financial, human resource, and email. Cybersecurity teams generally lack proper allocation on all fronts. Little to no research has been performed on the proper number and quality of cybersecurity human resources for any given size of a company, what systems and tools would be needed for particular risk or even what metrics should be recorded and reported to demonstrate success.

Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?

No, most organizations do not have a formal escalation process. While some large corporations have such policies and processes due to compliance regulations, the issue remains that there is often no one to escalate to outside of the company. Information can be provided to the Department of Justice or to the Department of Homeland Security, etc. but more often than not this information goes unacknowledged. Few federal resources exist to assist with a true risk / threat / action against a company. Companies are faced with moving targets with regard to dollar amounts and interest by prosecutors, there does not appear to be any one body within the government that will take a lead on investigating or collection of data, let alone any group that provides general intelligence back to companies. While organizations escalate internally, notify key officers, and in some cases customers depending on the severity of a breach or action, the government does not seem to have any program or process that such internal escalation would interact with.

What risks to privacy and civil liberties do commenters perceive in the application of these practices?

If handled properly, none.

What are the international implications of this Framework on your global business or in policymaking in other countries?

Privacy and civil liberties laws change from country to country, and international corporations are faced with challenges ranging from simple adjustments in the degree and sensitivity of monitoring breach reporting systems to being restricted to using only local citizens to perform reviews of collected data. In some cases local government may demand unmonitored access to customer information and the removal of encryption to allow monitoring of corporate communications. Companies are forced to build complexity into systems in order to retain such records in more friendly countries, and limit company confidential information on remote networks. This leads to complicated rules, laws, customs, and regulations and legal interpretations that are challenging to navigate. This is represented in the architecture of Management Systems for security infrastructure devices such as firewalls, NGFW, and IPS where vendors have had to afford companies the ability to segregate “domains” of responsibility and access to their own systems, as well as hyper granular access controls to logs, system tools, and sometimes to the devices themselves. Corporations also institute policies for the review of employee, network, email, and other data often referred to as “corporate search warrants” which are often based on the least common (e.g., most stringent) denominator of restrictions. This process will often involve the general counsel, head of human resources, and chief executive of IT.

How should any risks to privacy and civil liberties be managed?

These should be addressed up front with full disclosure with greater resources applied when civil liberties are at risk. A plain English policy and procedure should be in place, complete with oversight by an independent body. This body should audit and investigate potential breaches. Anonymous systems will be of great assistance, while corporate search warrants (overseen by due legal process albeit expedited) to gain access to specific data must be mandatory, etc. International practices and regulations need to be taken into account, and collaboration and cooperative efforts need to begin to help normalize the varying implementations and interpretations of privacy and civil liberties with regard to online data, activities, and usage of systems and public (Internet) resources.

In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?

With the wide-spread deployment of physical security systems such as video surveillance, door / premises access controls, and even integration into alarm systems the ideal of converged security cannot be ignored. These systems are vital to overall cybersecurity which often relies upon physical access controls and limitations. With video analytics facial recognition can be added to validate a keycard holder is indeed the person who should be accessing a secure area. These systems are on the corporate network, many times accessible by anyone who has gained access to the network.

As mentioned before, a shift in focus from complying with general best practices to achieving specific objectives such as information gathering, with the objective of obtaining active threat intelligence as well as visibility into corporate assets and workflows is essential. This would return operational security and situational awareness to the mindset and culture of cybersecurity. Combined with the licensing of cybersecurity professionals, this will enable the diagnosis and treatment of cybersecurity within Critical Infrastructure.

Reading List

Analyst Briefs & Topical Research

1. Cybercrime Kill Chain vs. Defense Effectiveness

https://www.nsslabs.com/reports/cybercrime-kill-chain-vs-defense-effectiveness

Cybercriminals persistently challenge the security of organizations through the rapid implementation of diverse attack methodologies, state of the art malware, and innovative evasion techniques. In response, organizations deploy and rely on multiple layers of diverse security technologies. This paper examines the attackers' kill chain and the measured effectiveness of the four major classes of protection technologies (firewall, intrusion prevention systems, endpoint protection/antivirus, browser protection). Empirical data is layered to present results on the security effectiveness of these protection technologies as measured in NSS Labs’ group tests.

(Presented at Black Hat Abu Dhabi, November 2012).

2. Modeling Evasions in Layered Security

https://www.nsslabs.com/reports/modeling-evasions-layered-security

Maltego is a program that can be used to determine the relationships and real world links between many things, and has been adapted by NSS Labs to show the relationship and correlation of unblocked exploits through a layered security stack of hardware and software tools. Utilizing the empirical data collected during NSS Labs’ tests on next generation firewalls (NGFW), intrusion prevention services (IPS), breach detection systems (BDS), endpoint security, browser security, and antivirus engines, paired with data on exploit availability of popular crimeware kits or penetration testing tools (e.g. Metasploit), NSS Labs is able to model layered defense stacks and illustrate exploits that are able to evade detection and bypass all security devices in the entire stack. NSS Labs can then simulate a client’s specific infrastructure to determine which current evasion techniques are capable of bypassing which security devices, and which exploits will be effective against which workstations and servers. For example, of the fifteen vendor-tuned IPS devices tested by NSS in 2012, eleven can be bypassed by the same exploit. There is only one combination of two layered IPS devices that would block all currently tested exploits. Through this modeling, client’s can then pinpoint and prioritize the exploits and vulnerabilities that pose the most threat to their organization.

3. The Targeted Persistent Attack (TPA) - The Misunderstood Security Threat Every Enterprise Faces

https://www.nsslabs.com/reports/analysis-brief-targeted-persistent-attack-tpa-misunderstood-security-threat-every-enterprise

In recent years, media attention — and technology vendor hype — has focused intensely on a well-publicized series of highly sophisticated, politically motivated attacks, including the Stuxnet and Flame worm outbreaks. But these attacks are unlikely to impact most enterprises significantly, and the attention paid to them has distracted many IT security practitioners from a far more serious real-world threat — one that NSS Labs has defined as the targeted persistent attack (TPA). This Analysis Brief discusses the misunderstandings surrounding APT, the real meaning of TPA to enterprise security practitioners, and possible options for effective remediation.

4. The Top 20 Best Practices to Help Reduce the Threat of Targeted Persistent Attacks (TPAs)

https://www.nsslabs.com/reports/top-20-best-practices-help-reduce-threat-targeted-persistent-attack

The companion paper to this, "*The Targeted Persistent Attack (TPA) — The Misunderstood Security Threat Every Enterprise Faces*," discussed the misunderstandings surrounding APT, defined the real meaning of TPA to enterprise security practitioners, and introduced possible options for effective remediation. This Analysis Brief details the top 20 best practices to help reduce the risk of a TPA to the enterprise.

5. Vulnerability Threat Trends - A Decade in Review, Transition on the Way

https://www.nsslabs.com/reports/vulnerability-threat-trends

After the close of 2012 NSS Labs performed a comprehensive analysis of vulnerability data to identify industry wide threats and trends covering the last 10 years. Despite massive security investments of the software industry, vulnerability disclosures have risen considerably in 2012. Several additional observations make the evolution of the year 2012 stand out significantly compared to the previous years since the peak in 2006. The parallel and massive drop of vulnerability disclosures by the two long established purchase programs iDefense VCP and TippingPoint ZDI indicate a transition in the way vulnerability and exploit information is handled in the industry. Key findings:

- Industry control systems (ICS/SCADA) saw more than six fold increase in vulnerabilities from 2010 to 2012. Identify and control access paths to ICS/SCADA systems. Prepare for attacks and related vulnerability disclosures.
- The five year long trend in decreasing vulnerability disclosures ended abruptly in 2012 with a +12% increase.
- More than 90 percent of the vulnerabilities disclosed are moderately or highly critical – and therefore relevant.
- 9 percent of vulnerabilities disclosed in 2012 are extremely critical (with CVSS score>9.9) paired with low attack/exploitation complexity.
- Microsoft and Apple operating system vulnerabilities decreased significantly from 2011 to 2012, by -56 per cent and -53 per cent respectively.

6. Defeating Advanced Malware in 2013

https://www.nsslabs.com/reports/defeating-advanced-malware-2013

On Feb 1st 2013, the Washington Post announced it had been hacked by Chinese hackers. It was the third announcement that week by a major news organization claiming compromise of corporate networks by Chinese hackers searching for confidential information. The Washington Post, New York Times and Bloomberg News had joined the ranks of US defense contractors, leading Internet and solar companies that had been penetrated by hackers using targeted persistent attacks (TPAs). In the NY Times attack, 45 pieces of custom malware were used, yet only one piece was detected by the installed leading antivirus package. Traditional security products struggle to protect against theses constantly-evolving threats. This brief examines a new breed of products utilizing "isolation technology" to combat TPAs and advanced malware.

7. What Financial CIOs Need to Know About Online Banking Fraud

https://www.nsslabs.com/reports/analysis-brief-what-financial-cios-need-know-about-online-banking-fraud

Fraudsters are focusing on targeting the customers of Financial Institutions (FIs) rather than the FI infrastructure. Online banking fraud commonly uses advanced botnet kits such as Zeus and SpyEye to perpetrate financial crimes. This advanced malware is installed on millions of PCs affecting consumers and enterprises, and results in hundreds of millions of dollars worth of online banking fraud per year.

When financial fraud occurs as a result of this malware, the burden of protecting FI customers is increasingly being placed on FIs. With the evolving legal and malware environment, FIs need to proactively take steps to educate and defend themselves. Financial CIOs may greatly reduce the likelihood of financial loss by following the advice in this paper.

8. The Future of BYOD

https://www.nsslabs.com/reports/future-byod

Enterprises are currently scrambling to deploy solutions for the growing bring your own device (BYOD) movement. However, BYOD is merely a precursor to the next two phases: bring your own cloud (BYOC) and bring your own network (BYON).

These changes will result in a very different model of user interaction with the enterprise. Rather than focusing on deploying a solution that may be already obsolete, NSS Labs recommends enterprises understand the BYOD trajectory, follow best practices, and build effective solutions that satisfy users and protect corporate intellectual property (IP).

9. The Challenges of BYOD

https://www.nsslabs.com/reports/challenges-byod

Bring your own device (BYOD) can create a revolution in workplace productivity, with users focused on value creation rather than security procedures. The benefits of BYOD are sometimes overshadowed by unforeseen complications in the execution phase. This brief covers many of the key issues and offers pragmatic advice for their mitigation. MDM capabilities and risk for smart devices are also examined.

10. Intelligence Matters: How Security Threat Intelligence Services Can Help Protect the Enterprise in an Increasingly Dangerous World

https://www.nsslabs.com/reports/intelligence-matters-how-security-threat-intelligence-services-can-help-protect-enterprise

Today's enterprise faces complex, sophisticated security threats -- from targeted persistent attacks (TPAs) to zero-day vulnerabilities -- on a scale that would have been unimaginable just a few short years ago. Recognizing and prioritizing these threats is a task that can strain even the most capable enterprise security organization to breaking point. A security threat intelligence service can serve as an invaluable supplement to in-house capabilities, but only if it is properly evaluated, selected and managed.

11. How to Protect Against the Threat of Spearphishing Attacks

https://www.nsslabs.com/reports/analysis-brief-how-protect-against-threat-spearphishing-attacks

NSS Labs' researchers have identified spearphishing as the most common targeted method sophisticated attackers use to compromise high-value targets. Where classic phishing takes a net-casting approach in its use of email, spearphishing uses social engineering techniques to create a more targeted invitation to click on a link or an attachment contained in a message. A recipient who follows the link may be invited to provide a user name and password or other personal information, or malware may be silently installed on the target's computer. The most effective defenses are user education and training that help end users avoid behaviors that enable successful phishing attacks. Technologies like antivirus tools and endpoint protection platforms (EPPs) have shown only mixed results in defending against exploits, and it is clear that a reliance on purely technological solutions is likely to be ineffective.

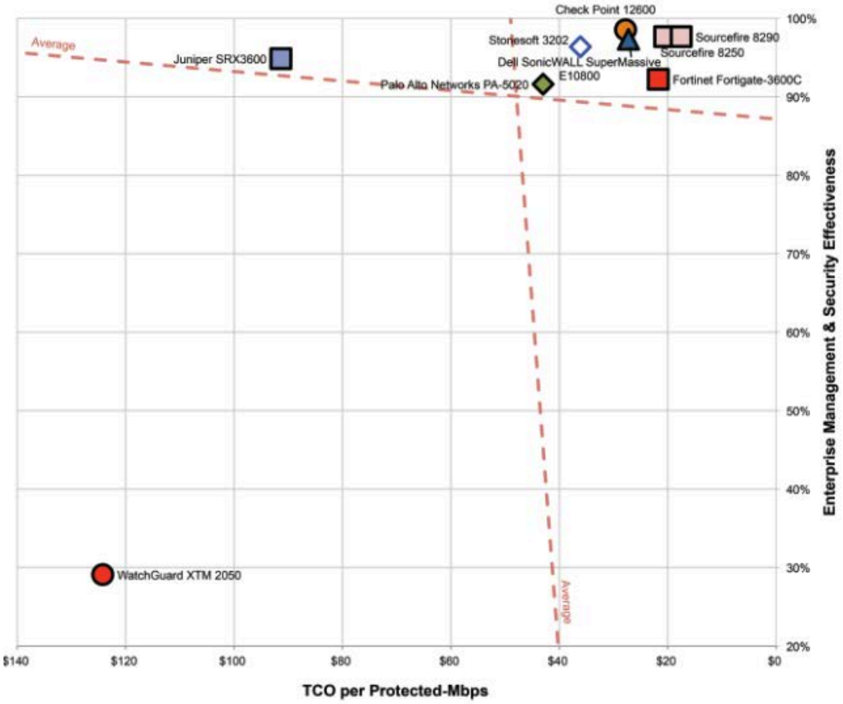
NSS Labs Security Testing Results

1. 2013 Next Generation Firewall Group Test & Comparative Analysis

https://www.nsslabs.com/reports/next-generation-firewall-comparative-analysis-2013

The 2013 Next Generation Firewall (NGFW) Comparative Analysis Reports, which evaluates nine leading NGFW products for security effectiveness, performance, enterprise management capabilities, and total cost of ownership, is the second group test for NGFW that NSS has conducted. Overall there is marked improvement from most vendors' 2012 test scores, making it clear that vendors are investing time and effort in addressing many of the overall stability, leakage, performance and security effectiveness concerns from last year.

2013 Next Generation Firewall Security Value Map™



Key Findings:

- **NGFWs' Security Effectiveness Scores Improve Significantly**: In the latest 2013 tests, 8 of the 9 products scored over 90% for security effectiveness (excluding management). This is a marked increase compared to 2012, when only half of tested vendors scored above 90% in this category. The overall scores for security effectiveness in 2013 ranged from 34.2% to 98.5% compared to 18% to 98.9% in 2012.
- **New Metric Highlights Enterprise Management Failings**: If a device cannot be managed effectively, the security effectiveness of that device is compromised. As part of this test, NSS performed in-depth technical evaluations of all the main features and capabilities of the enterprise management systems

offered by each vendor and factored it into the final score as a new and unique metric called "managed security effectiveness". Managed security effectiveness scores ranged from 29.1% to 98.5%.

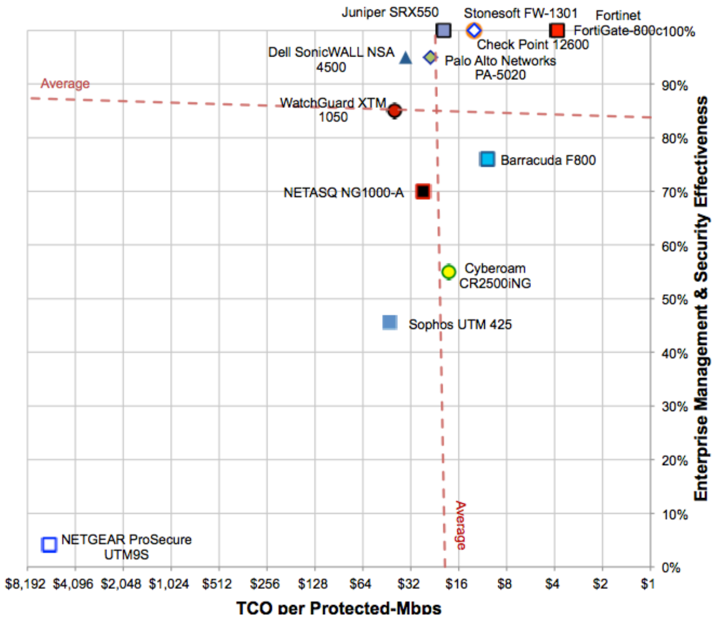
- **Check NGFWs' firmware before deployment**: Out of a total of 9 products tested, 6 vendors submitted products that required firmware updates or configuration changes to complete the NSS tests.
- **Total Cost of Ownership (TCO) Remains Fairly Stable**: While the overall range of TCO decreased in 2013 testing, prices per protected megabit per second remained fairly stable with most tested devices costing below $44 per Protected-Mbps. The overall 2013 range was $18 - $124 per Protected Mbps, down from a range of $30 - $375 in 2012 testing.
- **More Vendors Back their Performance Claims**: Only 2 of 9 products tested had throughput rates that were significantly less than their vendors' stated claims. In 2012 testing, 5 of the 8 products tested performed well below their advertised speeds.

2. 2013 Network Firewall Group Test & Comparative Analysis

https://www.nsslabs.com/reports/firewall-comparative-analysis-2013

Although firewalls are one of the most mature and stable security technologies, NSS finds that there is still much room for improvement in management capabilities, which are increasing critical for enterprise deployments. These are the final results and analysis from our 2013 Group Test for Firewall (FW), which evaluates products from 12 leading Firewall vendors. The firewall market is mature, populated with established vendors and providing limited scope for true innovation. As such, cost and capabilities, especially enterprise management and the ability to integrate with the established security and network infrastructure, are emerging as drivers for final product selection by customers.

2013 Network Firewall Security Value Map™



The 2013 Firewall Group Test revealed the following key findings:

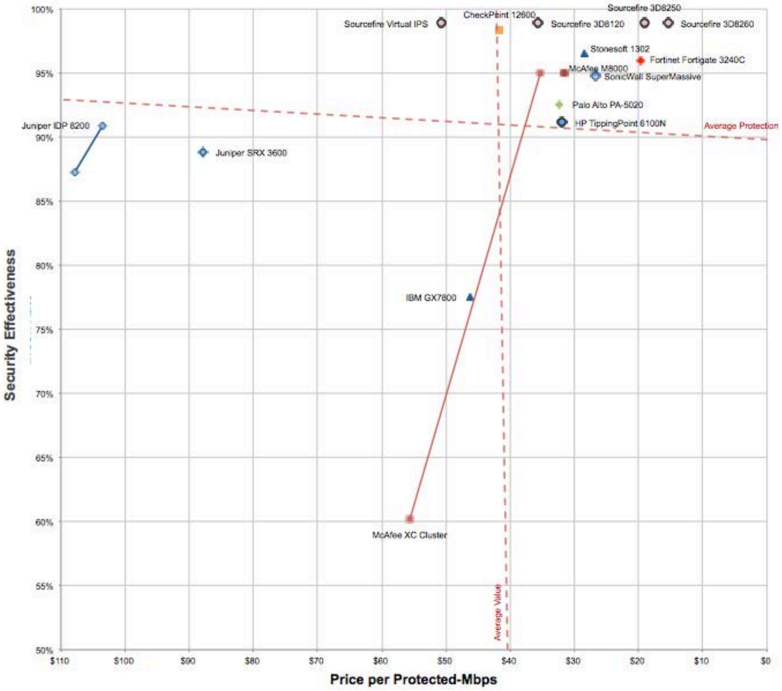
- **Enterprise management emerges as key differentiator**: Only 4 of the 12 vendors tested scored 100% for their management capabilities. This is the first Firewall SVM where management scores are weighted into a vendor's overall score a change NSS made to reflect enterprises' growing emphasis on more robust management capabilities when making firewall purchasing decisions.
- **Some firewalls continue to fail TCP Split Handshake and SYN Flood Protection tests**: While most vendors passed all security tests, two out of twelve products failed the fundamental TCP split handshake test, meaning a remote attacker could bypass these firewalls' rules and policies by posing as an internal "trusted" connection. One firewall also failed SYN flood protection tests, meaning it could prove susceptible to denial of service (DoS) attacks. With ongoing attacks by groups like LulzSec and Anonymous as well as the growing use of easily downloaded exploit tools, standard attacks such as DoS are seeing a resurgence and it's critical that all firewalls be able to block these threats.
- **Vendor claims continue to be exaggerated**: Of the 12 products tested, all performed significantly below the vendors' throughput claims – 40% below on average. Individual product rates ranged from 15% to 78% below their published throughput and buyers should consider this when evaluating the overall value of particular firewall.

3. 2012 Intrusion Prevention Systems Group Test & Comparative Analysis

https://www.nsslabs.com/reports/ips-comparative-analysis-2012

Are current IPS products worth the money? Hidden management and administration costs coupled with lower than stated performance can disguise the true value of IPS products. These are the final results and analysis from our 2012 Group Test for IPS, which evaluated 10 leading IPS vendors and 15 products. While testing shows that IPS is a competitive market with several vendors obtaining high marks for security effectiveness, it is apparent from this latest report that enterprise customers could end up paying hundreds of thousands of dollars more than they need to in larger deployments.

2012 Security Value Map for Network Intrusion Prevention™



4. 2013 Corporate End Point Protection Comparative Analysis – Phishing

https://www.nsslabs.com/reports/corporate-avepp-comparative-analysis-phishing-protection-2013

Phishing attacks are one of the most common and impactful security threats facing users today. In this test, NSS evaluates the ability of corporate endpoint products to block phishing attacks. The average phishing URL block rate for these products over the entire 12-day test period ranged from 99% to 50%. Instantaneous product block rates were generally erratic and varied by as much as 52% for specific points in time.

In the NSS Consumer EPP Phishing Comparative published January 30, 2013, it was demonstrated that few EPP products currently have anti-phishing technologies that could be considered highly effective and that inconsistent blocking over time means that block rates are frequently far less at any given moment than indicated by the average rate. This corporate test finds that only two of the tested products were able to meet or beat the protection afforded by current web browsers as reported in November 2012.

5. 2013 Corporate End Point Protection Comparative Analysis – Exploit Evasion Defenses

https://www.nsslabs.com/reports/corporate-avepp-comparative-analysis-exploit-evasion-defenses-2013

As security products improve their abilities to detect cyber threats, criminals adapt by utilizing evasion techniques in an attempt to conceal the exploits and payloads. This group test report analyzes some of the current methods used by cyber criminals to circumvent or evade detection from endpoint protection products (EPP).

NSS tested 11 enterprise level endpoint protection (EPP) products to measure their effectiveness in protecting Windows computers against exploits. All of the vulnerabilities exploited during this test were publicly available for months and in some cases years prior to the test; they have all been observed in use on the Internet.

IT professionals need to be aware of the differing levels of evasion protection available in EPP products tested. Enterprises, especially those that have implemented a bring your own device (BYOD) policy, who seek protection from attacks against desktop PCs and laptops should closely examine results from this test.

6. 2013 Corporate End Point Protection Comparative Analysis – Exploit Evasion Defenses

https://www.nsslabs.com/reports/corporate-avepp-comparative-analysis-exploit-protection-2013

Endpoint Protection Products (EPP) are designed to protect against a broad spectrum of threats. Products originally developed to detect self-replicating code (viruses and worms) have added protection against adware, spyware, rootkits, bootkits, phishing attacks, and exploits, in addition to providing firewall capabilities and more.

The ability to block exploits is one of the most significant tasks required of EPP products. When a new vulnerability is exploited, not only can malware, known or unknown, be silently installed, criminals can take over the exploited computer manually, thereby evading signatures and heuristics designed to detect malicious code. If an EPP can block an exploit, it has effectively blocked any and all malware that the exploit may attempt to execute or install. The ability to catch the payload an exploit delivers has value but provides far less protection than blocking the exploit itself.

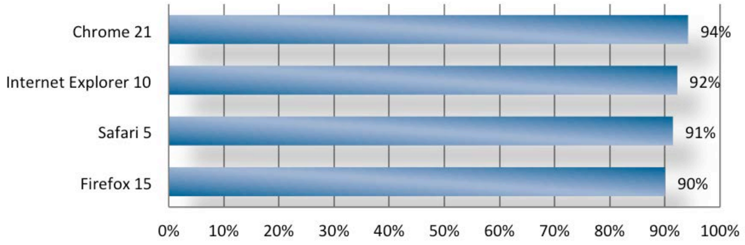
NSS tested 11 popular enterprise EPP products to measure their effectiveness in protecting Windows computers against exploits. All of the exploits used during this test have been publicly available for months (and sometimes years) prior to the test, and have also been observed in use on the Internet.

7. Browser Security Comparative Analysis: Phishing Protection

https://www.nsslabs.com/reports/browser-security-comparative-analysis-phishing-protection

The most common and impactful security threats facing users today are socially engineered malware and phishing attacks. As such, they have been the primary focus of NSS Labs continued research and testing of the security effectiveness of browsers. While drive-by downloads and clickjacking are also effective attacks that have achieved notable publicity, they represent a smaller percentage of today's threats. Drive-by downloads are commonly the result of a successful phishing attack and clickjacking attacks often lead to a phishing web page. *Note: This test was performed alongside a similar test of socially engineered malware (see: Browser Security Comparative Analysis: Socially Engineered Malware).*

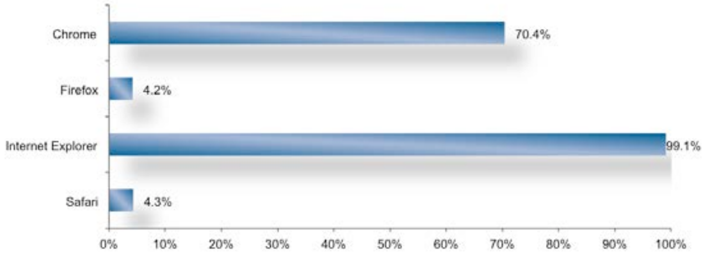
The average phishing URL catch rate for browsers over the entire 10 day test period ranged from 90 percent for Firefox (version 15) to 94 percent for Chrome (version 21). With a margin of error of about 2 percent, there is little difference in the average block rate of the browsers and one must consider other factors, such as socially engineered malware blocking capabilities, for qualitative differences in the security effectiveness of the browsers.



8. Browser Security Comparative Analysis: Socially Engineered Malware

https://www.nsslabs.com/reports/browser-security-comparative-analysis-socially-engineered-malware

The web browser is the primary vector by which malware is introduced to computers. Links in phishing emails, compromised web sites, and trojanized "free" software downloads all deliver malware via web browser downloads. The web browser is also the first line of defense against malware infection. Browsers must provide a strong layer of defense from malware, rather than defer to antimalware solutions and operating system protections. This test examines the effectiveness of the leading web browsers in blocking malware.



Overall Malware Block Rate by Browser (higher % is better)

During the testing period, Internet Explorer 10 with App Rep had a mean malware block rate of 99.1%, with App Rep adding 10.6% percent to the 88.5% URL reputation blocking achieved by the browser. Chrome with Google's Malicious Download Protection had a mean block rate of 70.4%. However, only 4.5% of the blocked malware was based upon URL reputation; Google's Malicious Download Protection provided 65.8% additional protection. Firefox and Safari, which have no download protection, were only able to block 4.2% and 4.3% of the malware respectively.

The four leading browsers were tested against over ninety-one thousand samples of real world malicious software. Major differences in the ability to block malware were observed. Data represented in this report was captured over twenty (20) days through NSS Labs' unique live testing harness, and provides insight into the built-in protection capabilities of modern browsers, including Chrome, Firefox, Internet Explorer, and Safari.

To put the numbers in perspective, for every twenty encounters with socially engineered malware, Firefox and Safari users will be protected from approximately one attack. That means nineteen out of twenty socially engineered malware attacks against Firefox and Safari users will end up testing the user's antivirus and/or operating system defenses. Chrome users will be protected from about fourteen of the twenty attacks, leaving their antivirus and operating systems responsible for protecting against six attacks, and IE10 users will generally be protected from all twenty attacks.

Page intentionally left blank.

Contact Information

NSS Labs, Inc.
206 Wild Basin Rd
Building A, Suite 200
Austin, TX 78746 USA
+1 (512) 961-5300
info@nsslabs.com
www.nsslabs.com