Standards Today
A Journal of News, Ideas and Analysis

A publication of CONSORTIUM INFO.ORG GesmerUpdegrove LLP

June–July 2009 Vol. VIII, No. 4

FEATURE ARTICLE:

Security Standards and the Internet: Keeping the Cyber Barbarians Beyond the Gates

Andrew Updegrove[1]

Abstract: *Until the advent of the Internet, security was largely based upon limiting physical access to tangible things of value, including information, which existed only in two forms: as it had been recorded on paper or other fixed media, and as it could be retained in the unaided recollection of individuals who, in turn, had gained physical access to that media. The advent of electronic databases and the Internet, combined with business models that require that many partners be given at least limited access to electronically transmitted and archived data, has dramatically altered the security landscape. As virtually all aspects of public and private life become deployed on the Internet, new standardized tools are needed – and must be implemented – to control the growing levels of risk. In this article, I survey the challenges we face to implementing effective cybersecurity, the types of standards used to provide it, the organizations that develop such standards, and the initial steps that the United States federal government is taking to implement them.*

Introduction: Prior to the advent of the digital age, ensuring security was largely accomplished though physical means. Whether the value to be preserved was goods, art, or precious metals, it could be placed behind physical walls and bars, and access restricted via guards and locks. Even intangibles, such as money, ownership in companies, and title to property were recorded in tangible form – money literally changed hands via bank notes or against presentation of paper checks. Similarly, corporate ownership interests could be transferred only through the delivery of a stock certificate (or paper stock power) on which appeared the signature of the former owner, and title to real property could only pass from one owner to another when the seller handed the new owner a signed, paper deed,

[1] The following standard setting organizations mentioned in this article are either current or past clients of the author and Gesmer Updegrove LLP, and/or the author serves, or has served, on their boards of directors: American National Standards Institute (ANSI), Information Card Foundation, Organization for the Advancement of Structured Information Systems (OASIS), OpenID Foundation, PCI Security Standards Council (PCI SSC), and Messaging Anti-Abuse Working Group. Any characterizations of these organizations included in this issue are mine alone, and should not be construed to have been authorized or made on behalf of any of the organizations named.

which in turn was acknowledged and delivered into the custody of the local Registrar of Deeds. In each case, these physical records of intangible rights could be safely stored in bank vaults, safety deposit boxes, and county record offices. Even information was physically instantiated – in paper documents or, more recently, on vinyl disks and magnetic tape. Except to the extent that the information could be transported in the unaided memory of someone who viewed the recorded data, sufficient levels of security could be provided simply through physical custody.

The evolution of security technology over the millennia was therefore largely incremental. Locks eventually supplemented human guards, and locks became more sophisticated in step with the advancement of the metallurgical arts. Stone-walled vaults with time gave way to rooms of steel. Ciphers and codes became more sophisticated, too, but the means to crack them were still limited by the unaided processing power of the human brain.

Up until the very end of the twentieth century, then, guaranteeing that valuable objects could be kept safe, and that valuable information could be protected secure from exposure or corruption, was largely a matter of investing adequate cost and care. Where the system failed, it could usually be traced to discrete acts of carelessness, specific inadequacies in policy, and betrayals of trust by usually identifiable individuals.

Similarly, the operations of commerce, government, communications, the financial markets and all the rest of the essential processes that underlie domestic and international society were under the direct control of specific individuals. Stock trades were executed on physical trading floors, military orders were usually delivered on paper, and requisitions for goods and services were transmitted by the mails or expedited delivery services. The records of all of these transactions were singular, or limited to a small number of copies, each of which was in the custody of a party to the transaction.

Since the Internet is the single backbone to which everything connects, everything is therefore potentially vulnerable, except to the extent that computer engineers can replicate the robustness of defense that walls of steel and armed guards provide in the physical world.

While objects still enjoy the protections of physical custody, the challenge of providing security has changed dramatically for virtually everything else within the last decade. Today, billions of trades in securities can occur on a single exchange in the course of any given day, and all of the records of these transactions are stored electronically. Governments are rapidly transitioning from paper to information technology for transactional and records preservation purposes, for reasons of cost and convenience. Commerce, communications, and indeed almost all other activities in modern life either already are, or on their way to being, conducted exclusively via the Internet. In the process, all of the data enabling these activities has been digitized, and all of the records generated to reflect them exist only in electronic databases that are usually linked to the Internet as well to permit new data to be added, and existing information to be accessed.

Since these transactions are accomplished via the Internet, that means that each is potentially vulnerable to exposure in transit, and that the databases at each end of the relationship are potentially exposed as well. Moreover, as the value of a network or database rises in direct proportion to the number of users that are linked to it, commercial forces inevitably drive towards more points of access (and therefore more points of vulnerability as well.

Since the Internet is the single backbone to which everything connects, everything is therefore potentially vulnerable, except to the extent that computer engineers can replicate the robustness of defense that walls of steel and armed guards provide in the physical world. Otherwise, access to medical records, financial information, state secrets, and all other information of value cannot be limited to only those that are intended to have it.

Sadly, that level of robustness is too rarely implemented in the field today. Recent, well-publicized breaches of security at major retailers have exposed the payment card data of millions of consumers, and federal agency Web sites have been brought down by attackers whose identities remain unknown. The sophistication of the criminals whose programs are constantly probing the defenses of networks continues to grow, as does the appeal of cyber attack as an offensive strategy – in no other conceivable way could a small country bring a super power to its knees, even if only temporarily.

The challenges relating to enabling cybersecurity are compounded by the fact that the pace of innovation and change has not subsided since the advent of the Internet and the Web. In the approximately fifteen years that the Internet has been in wide usage, successive advances have swept the marketplace, adding new dimensions of risk: first came the availability of cheap, wireless products, providing "drive by" access to insufficiently protected information to anyone interested in intercepting it. Next came the proliferation of wirelessly enabled mobile platforms of various types in addition to laptops: netbooks, smartphones and tablet computers, connected by telecom as well as open WiFi feeds, multiplying the number of nodes needing protection.

> *Since the Internet is the single backbone to which everything connects, everything is therefore potentially vulnerable as well*

Most recently, the popularity of "cloud" computing is spreading, moving the data itself back and forth between its owner and remote locations, such that even enterprise users may now have to interact on a constant basis with data living beyond, rather than within, the firewalls that are under their direct control. The result is that the techniques and the standards needed to address security issues can never be complete. Providing effective security will always, to some extent, be a goal that races ahead of the methodologies striving to achieve it.

The importance of information security has been legislatively addressed in various settings in the past, and these laws are finding increasing application in the cybersecurity arena as well. They include regulatory actions such as the Sarbanes-Oxley Act of 2002 (relating to financial information), and the Health Insurance Portability and Accountability Act (HIPAA), which protects the privacy of personal health care data. More recently, individual states have enacted laws mandating the reporting of data breaches to those affected.

Nevertheless, while industry and government have been aware of the dangers that can accompany the enormous benefits that the Internet can bring, too often they have been slower to perfect their defenses than to connect their (read: our) valuable information to the Web. In the United States, complacency has recently given way to well-justified alarm, and multiple public and private efforts are being launched in an effort to contain the risk. Internal and external awareness of the importance of cybersecurity has also generated a third "C Level" information technology management position: in addition to CIOs and CTOs (Chief Technology and Chief Information Officers), more and more public and private enterprises are adding CISOs, or Chief Information Security Officers, to their management teams.[2]

Each of these efforts will rely heavily on standards of many types – to establish identity, to grant or deny access, to increase convenience, and much more. In this article, I will survey many of the types of standards and related infrastructure that are required to establish and maintain effective data security, as well as the standard setting organizations (SSOs), both consortia as well formally accredited bodies, that develop and maintain them. I will close by referring to some of the initial steps being taken by the Obama administration and Congress to actively address the need to protect the nation against cyberattack.

The inability of physical security tools to protect virtual data may seem the greatest challenge. In fact, it is the desire to take advantage of the enormous benefits of accessing common information that introduces the greatest risks, and requires the most complex solutions

I Challenges of Cybersecurity

The inability of physical security tools to protect virtual data from unauthorized access may seem to present the greatest challenge to guaranteeing effective cybersecurity. In fact, it is the desire to take advantage of the enormous benefits of accessing common information that introduces the greatest risks, and requires

[2] See, for example, Aitoro, Jill, Guarding Networks, NextGov.com (June 25, 2009) *at* http://www.nextgov.com/nextgov/ng_20090625_8685.php?oref=rss in which the elevation of the importance attached to cybersecurity in government agencies is explored:

> As early as last year, CISOs [Chief Information Security Officers] complained that they, and their charge to protect government systems, just weren't getting attention and support from senior managers and politicians…. In less than a year, lack of authority is no longer a complaint. More than half - 57 percent - of CISOs say their decisions have a significant impact on the security posture of their agencies, according to a survey conducted by the International Information Systems Security Certification Consortium (ISC2) during the first quarter of 2009.

Accessed August 6, 2009. All on-line resources cited in this article were last accessed during the week of August 3, 2009.

the most complex solutions. The nature and magnitude of this challenge can be appreciated from the simple fact that the principle value that the Internet delivers is to interconnect as many people as possible, to as much information as possible.

The business models that have grown up to exploit this potential therefore drive towards maximizing the number of individuals with access to valuable data, rather than restricting it. In the first instance, business decisions are made regarding which persons should have access to which data, under what conditions, and for what purposes. The technical challenge is then not only to design software and hardware capable of implementing those decisions, but also to fraud proof the resulting system in such a way that unauthorized access can be prevented to the greatest degree possible, and rapidly discovered if defenses are nonetheless breached.

As in the physical world, perhaps the greatest challenge is to maintain the protections that technology has been able to provide. But unlike the physical world, where a daily visual inspection of a perimeter fence can disclose a hole cut through it the night before, data breaches are difficult to prevent, and hard to discover. Consequently, a back door to a network providing ongoing intrusions, or a worm on a server transmitting financial data beyond a firewall, can not only be easily installed when a poorly executed system upgrade creates a vulnerability, but almost impossible to detect as well.

Public-private sector case study: Electronic Health Records: The promise of electronic health records (EHRs) provides an apt example of both the rewards, as well as the challenges, that face information technology (IT) professionals and standards developers in designing cybersecurity solutions and tools.

In the traditional world of health records, each care provider generated and maintained her own paper records. While the methods and descriptive terms that an individual care provider might use were similar, they were not identical. Across specialties, the nomenclatures used in relation to symptoms and diagnoses would vary to some degree, as would the observational and lab test data sets relevant to diagnosing and treating the illnesses within their individual areas of expertise. Over the years, some of these records would be likely to follow from one primary care provider, while others (e.g., child hood diseases and immunizations, care given during vacations, etc.) might not. As a patient's life progressed, the stack of records would grow and grow, organized primarily only on a chronological basis, and set down in the variously legible scripts of many hands.

> *As a patient's life progressed, the stack of records would grow and grow, organized primarily only on a chronological basis, and set down in the variously legible scripts of many hands*

When one care provider needed access to another's records relating to the same patient, she, or her assistant, had to contact the other by telephone (assuming the patient could remember the other care giver's name). On receipt of the request, the overworked staff of the physician, lab or other caregiver would need to locate the file, copy it (perhaps in full), and mail it to the person requesting it, who would then need to review it in search of the needed information. In the ordinary course, this process would be slow, tedious, expensive, and subject to error, and in the case of a medical emergency, entirely impossible. But the records themselves were reasonably secure, since all information was at all times (except when in the mails) within the personal custody of a professional whose name and identity (in connection with any particular patient) was likely unknown to the world at large.

Similarly, when authorizations were needed in connection with insurance claims or referrals, the same laborious, paper-based process would need to be followed, perhaps marginally speeded by use of telecopy machines. The data itself would likely remain unavailable to researchers, since, unless the patient had already agreed to become part of a formal clinical trial or study, the information would be non-uniform, necessary permissions for disclosure would not have been obtained from the patients involved (and might no longer be possible to obtain), and all of the data would need to be tediously reentered, as uniformly as possible, using the protocols established for the particular trial.

The negative results of such a system include the length of time for information to transfer, the likelihood that some information will not be available at all when most needed, increased likelihood of errors in transcription, expensive replication of tests already conducted, lack of access to diagnoses and disease conditions already made and known, and the need to make "least risk" medicating and treatment decisions in the case of an emergency. Or, stated at a higher level, significant additional costs of care, many more misdiagnoses, and far too many avoidable adverse outcomes.

> *The public's willingness to make its personal medical information available for inclusion will be based upon their faith in the ability of the EHR system to maintain that data on a confidential basis*

All of these costs and risks are, at least theoretically, avoidable if all relevant data relating to a given patient is entered, throughout the patient's lifetime, in a single data base, in a consistent fashion, that is accessible to all of those (including researchers and descendants) that a patient may wish to give access to during (and after) her lifetime. How to accomplish this goal while preserving the confidentiality and privacy of the individual, however, is both difficult (because of the large number of individuals that will need to have access to the data) as well as important (due to the effect that such information may have on a person's insurability and employability, among other concerns).[3]

Notwithstanding these challenges and the very substantial costs of designing, implementing and maintaining a nationally-compliant, standards-based EHR system, Congress has granted the Obama administration's request for billions of dollars in support of achieving this goal. But as critics have stressed, the public's willingness to make its personal medical information available for inclusion will be

[3] Almost every other aspect of creating EHRs is difficult as well, requiring the development and use of multiple types of standards in addition to those that relate to security. For a more detailed review of EHR-related standards issues, see Updegrove, Andrew, The Electronic Health Records Standards Challenge, *Standards Today*, Vol. VIII, No. 1 (December – January 2009), at http://www.consortiuminfo.org/bulletins/dec08.php

based upon their faith in the ability of the EHR system to maintain that data on a confidential basis.

In theory, the security goals to be pursued in relation to EHRs are simple: at minimum, a patient should be entitled to know that her information will be:

- Only made available to those to whom she gives permission
- Only be used for the purposes she approves
- Kept at all times in a secure fashion
- Available to her whenever she wishes to have access

If we carry these goals over into practice, however, the situation rapidly becomes more complex. The root problem is that the greater the number and variety of individuals that should have access becomes, the trickier, more expensive and more complicated the technical means to permit them (but no one else) to gain entry becomes. For example, how should the following competing goals and objectives be balanced and resolved:

> *In theory, the security goals to be pursued in relation to EHRs are simple. In practice, the situation rapidly becomes more complex*

- ***Cost versus security:*** Many aspects of security, such as encryption and de-encryption add dramatically to the costs of maintaining security. If the goal is to reduce the costs of healthcare, how much security is cost justified?
- ***Convenience versus effectiveness:*** If security practices are too onerous, staff (and even patients) will look for ways to disable, or work around security features. Moreover, millions of care providers, insurers, benefits providers and pharmaceutical staff must work within the system, all of whom must undergo expensive training, and retain that training, in order to work efficiently and cost-effectively.
- ***Patient versus care provider:*** The patient will likely only wish to access her medical information on an occasional basis, and in much less depth. Care providers will need to access it repeatedly, and in detail. Whose convenience should be paramount? A care provider that logs on once a day to access a secure system will be willing to go through a more expensive, device-dependent (e.g., a security token), protracted log on process than many patients might, but a system that makes all of the patient's information available to the patient as well as to the care provider will only be as secure as its weakest log-on access method.
- ***Security versus ease of ubiquitous access:*** Information that is kept within an institutional, wired setting is more easily kept secure than information available on a wireless basis to all types of devices. Providing ubiquitous access on a secure basis is also more expensive. And information that can be accessed by any authorized person anywhere in the nation will be exposed to many more points of vulnerability.

Situational security solutions: EHRs provide but one example of the many significant security challenges that must be addressed, and each to some extent will require a different approach and design in order to attain adequate security. The variables and techniques for addressing them are beyond the scope of this article, but are suggested by the following highlights.

Balancing risks and rewards: How should factors such as those identified above be balanced? Optimizing factors such as convenience, cost, and security will to some extent always be a mutually exclusive goal. If each of these factors is to be accommodated on a balanced, rather than an absolute basis, we will always need to tolerate some degree of failure and compromise. Traditionally, courts have often addressed such a situation by granting judgments to compensate the few that suffer the consequences of compromise, and then assuming that the costs of such awards will be spread across the many that economically benefit from the sale of the goods or services involved. Similarly, Congress has on occasion stepped in to require that the individual losses that result from employing less than fool-proof security methods will be borne by those that benefit from the reductions in costs that such imperfect methods enable. Those costs, of course, are passed along to all of the customers of the same parties, but the incremental increase in prices will at most be small. In short, the system becomes self-insuring.

This is the system that followed from the barrage of credit card "come on" mailings that were released upon the public some years ago. When many of the offers made in those letters were activated by other than their intended recipients, Congress ruled that the card issuers must absorb the costs of the fraudulent purchases. These remedies will likely need to be tailored to the situation involved, with different solutions being provided (for example) in the case of credit card data breaches than EHR security failures.

By taking the level of realistic threat into account, security (and access) decisions can be made on a more cost-effective basis

Likelihood of breach: Some of the major factors to be taken into account in designing situational security best practices will be the nature, sensitivity, and attractiveness of the data in question. For example, the number and intensity of attacks will likely be far higher where identity theft or other financial fraud is the objective than in the case of seeking access to medical information. Consequently, credit and debit card data repositories would be expected to be more intensively targeted than EHR databases, but a subset of the data in EHRs – social security numbers, for example – would still need to be well-protected. Similarly, infrastructural and governmental data will be more likely to be targeted by terrorists and wartime opponents than consumer information. By taking the level of realistic threat into account, security (and access) decisions can be made on a more cost-effective basis.

Means of enforcement: Achieving security is a function of control as well as cost, in that implementation is time-consuming and constraining on operations. Given that implementing security is challenging within a single enterprise, how is it to be achieved across enterprises? The federal government provides one example, where some of the most complete EHR implementations in the United States have already been achieved within the Veterans Administration. Mandating an appropriately high level of security in this venue will affect thousands of facilities, but the task is lessened by the fact that they are already subject to common IT control.

A far more ambitious goal has been taken on by the Obama administration, which has pledged to create a "unified framework" of secure data exchange, within which the defense, intelligence and civil communities will employ a common strategy to protect critical federal information systems and associated infrastructure, as called for by President Obama in a speech he delivered on May 29 of this year in which he described his plans to secure the U.S. cybersecurity infrastructure. While almost all government agencies are subject to the edicts of the Executive branch, they nonetheless represent a patchwork of legacy systems even within individual agencies, and the agencies themselves are not only separately managed, but at times also aggressively competitive with each other in many ways.

Moving outside of government, the challenges become even more daunting, especially within the regulation-averse U.S. private sector. Not surprisingly, the Congress has decided that the private sector will need to be cajoled into rapidly implementing EHRs through a legislative combination of carrots and sticks: the former being near-term financial incentives for millions of caregivers to implement standards-compliant systems, and the latter comprising long-term penalties for those that fail to comply.

PCI SSC takes a holistic, environmental approach, assessing and addressing the end-to-end vulnerabilities of the payment card process and the relevant activities of each stakeholder along the way.

How can similar goals be achieved beyond the reach of regulation? Can industry itself meet the need for pervasive security where compliance must be voluntary across vast and diverse networks of stakeholders?

Private sector case study: the payment card industry: The answer, perhaps surprisingly, is yes, as demonstrated by an initiative launched in the payment card (credit and debit) industry. That initiative is the PCI Security Standards Council (PCI SSC), a collaborative effort established by five major payment card brands (American Express, Discover, JCB, MasterCard, and Visa) in 2006. Rather than focusing narrowly on individual technical standards, PCI SSC takes a holistic, environmental approach, assessing and addressing the end-to-end vulnerabilities of the payment card process and the relevant activities of each stakeholder along the way.

The result is the creation of a complex, global security infrastructure that includes not only a suite of process standards for those that collect, store, and transmit payment card data, but also technical standards for the manufacturers that develop and sell card readers and related technology, and for those that audit the compliance of industry participants with PCI SSC created security requirements. The standards themselves are supported by certification programs that attest to the compliance of merchants, IT vendors, issuing banks and the auditors themselves.

Payment card brands then decide with whom they will deal, based upon the requirements that they individually develop, relying on the PCI SSC-related certifications and compliance assertions of those with whom they deal – thereby providing the incentive for millions of participants in the payment card ecosystem to comply with appropriate security safeguards when they are in a position to affect the security of cardholder data.[4]

II Cybersecurity Standards

As is common in other IT settings, properly conceived and developed cybersecurity standards can (and should) achieve multiple goals, including enabling interoperability, lowering costs and increasing choices in IT acquisition, and increasing reliability and predictability of outcomes. Unlike the discrete standards that adequately serve many purposes in other disciplines (e.g., dimensional standards, where success can be declared when the light bulb screws into the socket, or performance standards, which permit price comparison shopping, as between two 60 watt bulbs), security, like interoperability, must be addressed on a systemic basis. But unlike the pursuit of interoperability, where islands of proprietary products can and often do continue to exist within most systems that are otherwise guided by interoperability principles, a great deal of careful design work can be defeated by the existence of a single point of weakness. Security, therefore, must be addressed systemically, thoroughly and consistently, or it is hardly worth addressing at all.

Security standards methods and goals: The range of standards required to achieve persistent security is wide, and includes not only technical standards, but design, evaluative, and process standards as well, supported by a wide variety of guides, profiles and best practice documentation. This environment of security standards and related infrastructure includes the following:

> *Security, therefore, must always be addressed systemically, thoroughly and consistently, or it is hardly worth addressing at all*

Risk management: At the highest level, security is based on a holistic plan that evaluates risks, and provides ongoing appropriate safeguards to address those threats. Risk management is both a multi-step process and an ongoing mission. It begins with identification and assessment of risks, progresses through selection of cost-effective solutions, identifies roles and responsibilities, specifies remedial actions when failures occur, and continues through specification of ongoing maintenance and (as importantly) updating requirements and processes. Both high level and detailed standards and best practices assist in the creation of such designs and plans.

Change management: Any addition or modification to a system provides the opportunity for the security of the system to be compromised, unless careful

[4] For a detailed overview of the PCI SSC standards, infrastructure and environment, see the interview that follows in this issue, titled, Enabling a Ecosystem of Security: an Interview with PCI SSC's Bob Russo, at: http://www.consortiuminfo.org/bulletins/jun09.php#interview

attention is paid to avoiding that result. Change management standards and processes guard against the inadvertent weakening of defenses by mandating how changes are requested, planned, implemented, tested, and documented in a consistent and thorough fashion.

Physical: While IT systems are vulnerable to a wide range of virtual threats, data ultimately lives on servers that are vulnerable to fire, power failure, internal failure, and physical attack. Appropriate standards are therefore needed relating to factors such as fault tolerance, location, fire prevention and containment, power maintenance, and external backup.

Availability: A closely related concept is "Availability," which seeks to ensure that data is not only never lost, compromised or corrupted, but that it can be accessed when needed as well. Standard definitions of availability permit "like to like" bidding and selection among data hosting service providers.

Because the ways of securely establishing identity are very varied, the number of standards needed to allow them to be broadly implemented is great as well

Architectural: Under traditional hardware and software development best practices, security is optimally addressed during the development stage, rather than added on the outside as a patch, or imposed as an additional layer. Such "security by design" techniques can be applied both architecturally and at the operating system level. Where a secure operating system is not provided, "secure coding" practices can also be followed at the application level. Security achieved via these methods can be constraining, however, and also makes the integration of components supplied by different vendors more difficult and expensive. As a result, standards of secure design have been increasingly supplemented by standards that provide security while increasingly interoperability. With the advent of the Internet, wireless connectivity and cloud computing, the importance of such standards, and the need to develop new ones, has greatly increased.

Identity and authentication: How does a system know that you are who you say that you are when you seek to access the system? In order to avoid unique methods of establishing identity in every instance at greater cost to the system host and inconvenience to the visitor, a variety of standards have been developed to provide common ways of allowing the user and the system to be properly introduced. Identification typically begins with a standardized method of authenticating the identity of a visitor by exchanging and verifying the data that the visitor submits. The same method provides a basis to "federate" identity in order to achieve convenience goals such as "single sign on" capabilities across sites that utilize the same standards, thereby making life easier for the user.

Federated identity typically involves additional infrastructural resources, such as trusted third parties that can host identity information and vouch for a visitor upon presentation of the appropriate identity credentials that the user has obtained from the third party. Hosts of data will want such standards to be not only technically effective, but able to guarantee a level of security acceptable to them as well. As a result, they may wish to participate only in federated identity systems where third parties must comply with appropriate process standards, and where auditors exist to certify the compliance of these third parties with the same standards, in order to verify the integrity of the trusted environment. The various constituent standards needed to enable such a trusted environment may come from multiple SSOs.

Because the ways of factually establishing identity are very varied, the number of standards needed to allow them to be broadly implemented is also great. Without seeking to provide a comprehensive list, these methods include the manual input of information (e.g., user names, passwords, and responses to automated verification questions), technological (for example, security tokens that generate unique strings of random numbers using algorithms shared with the host and identified to the token), biometric (including identification of individual fingerprints, iris patterns, and keystroke rhythms). The ability to use so many methods, each served by its own standards, encourages innovation and price competition, and makes hackers work harder to penetrate the defenses of those that use them.

Non-repudiation: In a transactional setting (e.g., at an e-commerce site), it is not sufficient to simply authenticate a visitor before allowing access beyond the firewall. In addition, the visitor will need to acknowledge the instructions they enter in a way that prevents them from later repudiating their actions in order to avoid the consequences (e.g., responsibility for paying for an order they enter). Mechanisms such as digital signatures are used in this setting to indicate the irrevocable acceptance of terms.

No security system will be perfect, and means are therefore required to verify that accessed data is intact, to discover breaches when they have occurred, and to determine the nature and source of the breach

Access: Identity information is essential not only for gaining entrance within a firewall, but also to regulate what a visitor may do, and where they may go, once they have gained initial access. Just as national security standards establish varying levels of security clearance, it will often be appropriate within a private network setting, as well as a government system, to grant varying degrees of access to data within the outside perimeter of a protected network. In order to achieve that goal, non-technical standards are first needed to define the levels of security and the attributes of those entitled to have access, and then technical standards are needed to enable such access on this differentiated basis.

Encryption: An effective security plan will likely need to employ more than one strategy, especially where it may be difficult to defend the firewall. One such strategy is to encrypt data, not only when data is being transmitted externally, but when it is stored internally as well, rather than only being received, processed and retransmitted. Encryption standards provide common ways to render data unreadable while generating unique keys to once again access the same data.

Integrity: Not all threats to security involve those with evil intent. Of equal importance is ensuring the ongoing integrity of data, which involves limiting those that have authority to add, modify and remove data, as well as when data should enter an archival state where further changes should be prohibited entirely.

Assurance: Closely related to integrity is the question of whether sufficient protection has been provided by the security regime employed that the data protected can in fact be trusted. If security is light, the integrity of data will always be more suspect.

Auditability: No security system will be perfect, and means are therefore required to verify that accessed data is intact, to discover breaches when they have occurred, and to determine the nature and source of the breach. In order to do so, every action in relation to a system must be logged, searchable, and easily accessible, as described and required by appropriate standards.

Specific standards: As might be expected, the very large number of standards that have been developed range from the broad and ambitious, to the narrow and technical, and standards of each type must be combined in order to achieve a complete solution. Given the very large number of security standards in existence, the specific standards listed under the following categories are necessarily offered by way of example only.

No security system will be perfect, and means are therefore required to verify that accessed data is intact, to discover breaches when they have occurred, and to determine the nature and source of the breach.

Systemic standards: While identified as single standards for conventional numbering purposes, tools of this type may more usefully be thought of as best practice guides, which are themselves dependent upon the implementation of a host of subordinate standards, often developed by other organizations. Two examples that have similar goals, but which are very different in approach, are:

ISO/IEC 27000-series: This family of IT security standards is the product of Subcommittee 27 of Joint Technical Committee 1 of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It includes six complete standards, with 11 additional specifications either planned or in the process of development. The series is intended to provide guidance to companies and entities of all types that rely upon IT networks. Like the ISO standards that relate to quality assurance (ISO 9000 series) and environmental protection (ISO 14000 series), this series describes certifiable best practices within an overall “Information Security Management System” (ISMS), which is described in ISO/IEC 27002. Several of the standards were originally developed by the British Standards Institute (BSI) and reissued by ISO/IEC in 2000. The ISMS addresses many of the topics noted above in its various parts:

Risk Assessment
Security Policy
Asset Management
Physical and Environmental Security
Access Control
Information Systems Acquisition, Development and Maintenance
Information Security Incident Management

Business Continuity Management
Compliance

ISO 27002 has been adopted as a national standard by 12 national standards bodies.[5]

Payment Card Industry Data Security Standard (PCI DSS): The PCI DSS was developed by PCI SSC to specifically protect payment card (credit and debit) data that is exposed by the card holder in the process of initiating, processing and completing a financial transaction. Accordingly, it applies to all entities that hold, process or pass along payment card data. Unlike the ISO/IEC 27000 series, the PCI DSS is based upon six stated principles, each of which is supported by one to three requirements. The requirements are in turn laid out in much greater detail, and address specific topics such as maintaining the security of wireless networks, when payment card data can be stored and by whom, when such data must be encrypted, and how often and by what methods security must be documented and tested. The principles and requirements are as follows:

Build and Maintain a Secure Network
Requirement 1: Install and maintain a firewall configuration to protect cardholder data
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data
Requirement 3: Protect stored cardholder data
Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program
Requirement 5: Use and regularly update anti-virus software
Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures
Requirement 7: Restrict access to cardholder data by business need-to-know
Requirement 8: Assign a unique ID to each person with computer access
Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks
Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes

[5] The ISO/IEC 27000-series of standards is available for purchase at the ISO Web site, at http://www.iso.org/iso/catalogue_detail?csnumber=41933

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

The PCI SSC security environment is currently supported by two additional PCI SSC standards, one of which establishes compliance criteria for use by vendors that design and sell Personal Identification Number (PIN) entry devices for use in connection with payment card transactions (the PED Standard). The second provides guidance to software vendors that sell tools used by payment card processors, with the goal of avoiding the designed-in necessity or opportunity of storing sensitive payment card information (the Payment Application Data Security Standard, or PA-DSS).[6]

Technical standards: A host of technical standards are needed to implement security at the machine level. The following is only a sampling of the many standards, and standards-based structures, that have been developed to address the single issue of establishing and managing on-line identity.

A host of technical standards are needed to implement security at the machine level

- **Security Assertion Markup Language** (**SAML**)**:** SAML is one of the very large, and still growing, number of standards based on the Extensible Markup Language, a specification and related set of tools that developers can use to "extend" XML's syntax and other rules for describing content in such a way that the material can be reused by other computers and applications without the need for conversion. In the case of SAML, the goal is to allow the easy exchange of data for the purposes of authentication and authorization. SAML is particularly useful for enabling "single sign on" capabilities, which (ideally) enable a user to log in once per session, and not each time they open another application or browser window. SAML serves as the basis for a variety of more targeted cybersecurity standards. It was developed and is maintained by the Organization for the Advancement of Structured Information Systems (OASIS), a consortium focused on ecommerce that hosts dozens of simultaneously active working groups.[7]

- **OpenID:** OpenID is a standard that enables a user to achieve single sign-on capabilities by establishing an on-line identity that is authenticated by a third party (called an "OpenID provider") when the user seeks to log on to a given Web site. In the case of OpenID, the identity is represented by a unique URL hosted by the OpenID provider. One advantage to the OpenID standard is that it does not rely on a single form of verifiable identity, allowing the user

[6] PCI SSC standards, supporting materials, lists of compliant products, and additional information can be accessed at the PCI SSC Web site, which can be found at https://www.pcisecuritystandards.org/

[7] An example of an XML-based standard for security purposes is the IETF's Incident Object Description Exchange Format (IODEF), which provides a framework for sharing information typically used by Computer Security Incident Response Teams (CSIRTs) investigating security incidents. IODEF supports the reporting of on-line fraud techniques such as phishing and widespread incidents involving spam. *See:* http://xml.coverpages.org/iodef.html

to employ one of a number of different alternatives, from simple (and less secure) to complex. OpenID is maintained by the OpenID Foundation, a consortium with roots in the open source community.

- **Public Key Infrastructure:** The concept of a public key is implied, but not explicit in its name: for every public key, there is also a private key, and both identity and authenticity can be established by matching up the two. In a public key infrastructure, a third party (the certificate authority, or CA) generates and maintains the keys, and issues the private key to its owner. The CA also registers the public key with a registration authority (RA), which maintains it and stands behind the "binding" of the public key, the private key, and the identity of the holder of the private key. The details of the arrangement are described in public key certificates issued by the CA. PKI standards are developed or utilized by more than a dozen standards organizations, including PKIX, the PKI working group of the Internet Engineering Task Force (IETF), and committees of the Institute of Electrical and Electronics Engineers (IEEE), the European Telecommunications Standards Institute (ETSI), and the Internet Mail Consortium (IMC).

III Security Standards Organizations

The number of SSOs and other entities engaged in the development of cybersecurity standards, or developing security solutions based upon such standards, is very great. The reasons are several, and include the fact that, as earlier noted, achieving security must be a systemic and ongoing exercise. This means that a proper risk management plan must be tailored not only to the general needs of particular industries (e.g., financial, retail, etc.), but also to specific needs and architecture of the network owner. Similarly, while many security goals, such as identity management, rely on the creation of infrastructures that in turn rely on standards, the creation and management of such infrastructures in itself must be achieved through collaborative action. The evolution of a single new threat "in the wild" (such as phishing – the ruse (for example) of leading someone via an emailed link to a Web site pretending to be that of the visitor's bank) can lead to the formation of one, or several, new SSOs. Due to the importance of security, government agencies are increasingly playing a leading role in supporting the development of security standards, in addition to being active members of SSOs.

> *The evolution of a single new threat "in the wild" (such as phishing) can lead to the formation of one, or several, new SSOs*

Government efforts: Federal and state governments are enormous consumers of IT technology, and are increasing their reliance on IT-based systems to replace paper and face-to-face processes. Under the Technology Transfer and Advancement Act of 1995, 15 U.S.C. § 3701 (TTAA), U.S. government agencies are encouraged to participate in standard setting organizations, as well as required to specify consensus-based industry standards, rather than government-unique standards, in their procurement activities whenever possible. Participation in some SSOs is also significant among state and local government IT personnel.

Despite the requirements of the TTAA, however, the increasing perception of cybersecurity risks by government, as well as the setting of ambitious security-dependent goals by successive administrations, has led Congress to authorize direct action. When Congress and the President need standards-dependent assistance, they have traditionally looked to the National Institute of Standards and Technology (NIST), an agency within the Department of Commerce. Under the Obama and George W. Bush administrations, NIST has been assigned new roles in support of legislation concerning cybersecurity, as well as major technology based initiatives that must rely heavily on the assurance of security. NIST's activities in this area are managed through the Computer Security Division of the Information Technology Laboratory.[8]

In 2002, Congress passed the Federal Information Security Management Act of 2002, 44 U.S.C., Sec. 3541, et seq. (FISMA), which is intended to "provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets." Under FISMA, NIST is charged with "developing standards, guidelines, and associated methods and techniques for providing adequate information security for all agency operations and assets, excluding national security systems." More generally, NIST is the custodian of the Federal Information Processing Standard (FIPS).[9]

Most recently, and in partnership with the Department of Defense, the Intelligence Community, and the Committee on National Security Systems, NIST released a first installment report on a multi-year initiative to build a "unified information security framework" for the entire federal government under which the same security controls would apply to military and intelligence information systems as well as those of civilian agencies. The unified framework is intended to, "produce significant cost savings through standardized risk management policies, procedures, technologies, tools and techniques."[10]

> *The SSOs that develop security standards range from formal, global organizations, to national standards bodies, to broad-based consortia, to narrowly focused alliances that exist for the sole purpose of developing a single security standard*

Private sector: As noted, there are a large number of SSOs active in the security area. They range from formal, global organizations, to national standards bodies, to broad-based consortia that host security standards working groups in support of

[8] The NIST Computer Security Division maintains a public Web site at which publications, news, and activities can be found: http://csrc.nist.gov/ The substantial number of NIST publications on cybersecurity can be accessed through this page: http://csrc.nist.gov/publications/index.html

[9] The FIPS home page can be found at: http://www.itl.nist.gov/fipspubs/

[10] NIST Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, available at: http://csrc.nist.gov/publications/PubsDrafts.html#800-53_Rev3

their overall mission, to narrowly focused alliances that exist for the sole purpose of developing and maintaining a single security standard or supporting materials. The following are examples of SSOs actively engaged in the security standards area:

Global "de jure" SSOs: ISO/IEC JTC 1 SC 27: ISO and IEC are two of the three "Big I," global standards organizations that are active in the IT area (the third is the International Telecommunication Union, or ITU). Participation in these bodies is at the national level via a nationally representative standards organization (in the United States, that organization is the American National Standards Institute, or ANSI). Joint Technical Committee 1 is the very active committee established by ISO and IEC to collaborate on IT industry standards. JTC1 Subcommittee 27, "IT Security Techniques," currently has five active working groups addressing topics such as information security management systems, cryptography, security evaluation and controls, and identity management and privacy, and maintains the 27000-series discussed earlier in this article.[11] Other security standards of significance include ISO/IEC TR-15443: Information technology - Security techniques - A framework for IT security assurance; ISO/IEC 17799: Information technology - Security techniques - Code of practice for information security management; and ISO/IEC 20000: Information technology - Service management.

National Initiatives: While most cybersecurity standards activities occur within consortia that have global memberships, SSOs whose membership is either entirely or predominantly limited to U.S. stakeholders may have working groups addressing security issues relevant to their respective industries as well. In addition, the American National Standards Institute (ANSI) hosts two panels focusing on security issues (a third, the ANSI Healthcare Information Technology Standards Panel, also addresses security issues relevant to electronic health records). These panels seek to bring together representatives of the multiple individual efforts that may be ongoing in other SSOs, as well as those of other stakeholders with an interest in the resulting standards.

- ***Identity Theft Prevention and Identity Management Standards Panel (IDSP):*** The IDSP is a cross-sector coordinating body established by ANSI and the Better Business Bureau in September of 2006. The panel coordinates the development and uptake of standards and guidelines by the private sector, government and consumers in order to limit identity theft and fraud. The panel holds workshops that highlight existing standards and identify gaps where new tools are needed, and plenary meetings to report on progress and identify topics for further attention. Workshop reports summarize results and provide recommendations. The IDSP's third plenary meeting, held this year, addressed the current state of identity theft prevention and identity management.[12]

- ***Homeland Security Standards Panel (ANSI-HSSP):*** The ANSI-HSSP is a public-private partnership established in February, 2003 that identifies relevant consensus standards where they exist, and if none are available,

[11] The home page for SC 27 is here: http://www.iso.org/iso/iso_technical_committee?commid=45306

[12] Further information about the IDSP, as well as links to its work product, may be found at: http://ansi.org/standards_activities/standards_boards_panels/idsp/overview.aspx?menuid=3

assists the Department of Homeland Security (DHS) and other stakeholders in driving the development and uptake of standards critical to homeland security. Like the IDSP, this panel hosts workshops and plenary meetings, the eight of which will be held in October of this year. The panel covers a variety of areas of identified risk on an ongoing basis, including cybersecurity.[13]

Global consortia: The IT industry (and to a lesser extent the communications technology industry) are notable for the hundreds of SSOs, usually with global memberships, that have grown up outside of the traditional national SSO/Big I standards infrastructure. These SSOs are often referred to as "consortia." Those that concern themselves with security issues fall into a number of categories:

➢ **Broad based organizations:** A number of consortia with many working groups are very active in developing security standards in support of their overall mission. They include:

OASIS currently hosts 15 technical committees developing security standards in areas such as biometric identity, digital signatures, encryption key management, and identity management

- ***Internet Engineering Task Force (IETF):*** The IETF is one of the oldest and most important consortia serving the standards needs of the Internet. Membership is at the individual level through the Internet Society (which hosts the IETF), although many members

- participate at the encouragement (and with the economic support) of their employers. The IETF currently maintains 17 Working Groups in the area of security.[14]

- ***Organization for the Advancement of Structured Information Systems (OASIS):*** OASIS was founded in 1993, and focuses on developing standards in support of eBusiness and Web services (OASIS states that it has developed more standards enabling Web services than any other organization). It is also known for providing the standards for application-specific markets. It currently hosts 15 technical committees developing and/or maintaining security standards in areas such as biometric identity, digital signatures, encryption key management, and identity management.[15]

[13] Further information about the ANSI-HSSP, as well as links to its workshops and work product, may be found at:
http://ansi.org/standards_activities/standards_boards_panels/hssp/overview.aspx?menuid=3

[14] The home page for the IETF Security Area is here: http://trac.tools.ietf.org/area/sec/trac/wiki
Links to the individual Working Groups can be found here:
http://www.ietf.org/dyn/wg/charter.html#Security%20Area

[15] OASIS Technical Committees in the security area can be found at: http://www.oasis-open.org/committees/tc_cat.php?cat=security

- **Organizations focusing specifically on security:** A variety of consortia focus only on security standards and practices, sometimes with reference to a particular area of concern, such as mobile computing. Examples include:

    - ***Trusted Computing Working Group:*** TCG was formed in 2003 by major chip, hardware and software vendors (AMD, Hewlett-Packard, IBM, Infineon, Intel, Microsoft and Sun Microsystems) to implement security features at the silicon level via incorporation of the Trusted Platform Module specification it developed. TCG promotes industry standard specifications for trusted computing, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices. TCG compliant systems are intended to facilitate authentication, data protection, network security, multiple layers of enabled security, and disaster protection.[16]

    - ***Web Application Security Consortium:*** WASC was founded in January, 2004 to, "develop, adopt, and advocate standards for web application security," in response to the risks associated with conducting business online, and the challenges of securing Web sites against possible threats. WASC objectives include: identifying the security risks to e-business and privacy on the Web; establishing consistent technical terminology relating to web security issues; establishing web application security standards of best practice for secure software development; and identifying independent security review and policy guidelines.[17]

- **Organizations focusing exclusively on one aspect of security:** A variety of organizations focus exclusively on one facet of security, and especially so in the area of federated identity. The following organizations each address that aspect of security, and are presented in the order of their founding, representing together both the increasing importance of a simple, secure Web experience, as well as the manner in which technology and industry are evolving to provide new security solutions.

    A variety of organizations focus exclusively on one facet of security, and especially so in the area of federated identity

    - ***Liberty Alliance:*** The Liberty Alliance Project was formed in 2001 to deliver and support an Internet-based federated identity standard that enables single sign-on for consumers as well as business users capable of including (for example), a person's online identity, their personal profile, personalized online configurations, buying habits and history, and shopping preferences, with the information being administered by the user to permit sharing only with organizations of their choosing. The desired outcome is to permit consumers, citizens, businesses and governments to conduct online transactions while protecting the privacy and security of identity information through universal strong

[16] Further information about TCG can be found at: http://www.trustedcomputinggroup.org/about_tcg

[17] Current WASC projects are listed at: http://www.webappsec.org/projects/

authentication. In addition to standards, the Alliance develops business and deployment guidelines and best practices for managing privacy, and provides interoperability testing and certifications programs.[18]

- ***OpenID Foundation:*** The Foundation was formed in 2005, and has roots in the open source rather than the vender community. The OpenID standard has enjoyed broad support at popular consumer and social networking sites such as Yahoo, PayPal, MySpace, and Facebook. An ecosystem of identity providers has grown up around the standard to serve the needs of individuals that wish to use the OpenID standard to make their use of the Internet more simple, efficient and safe.[19]

- ***Information Card Foundation:*** A group of major corporations (Equifax, Google, Microsoft, Novell, Oracle and PayPal) launched the Foundation in June of 2008 to support the use of the "information card" metaphor in federated identity solutions. Information cards contain user profiles and can be created either by the user, or by a trusted third party. Conceptually, information cards are the virtual equivalents of credit cards that, when "swiped" in a reader, enable a secure link between a transaction and a user's billing information hosted by a payment card company. Like OpenID, information cards provide single sign on capability, and can host additional information in order to avoid repetitive filling out of on-line forms at multiple sites.[20]

A group of major corporations (Equifax, Google, Microsoft, Microsoft, Novell, Oracle and PayPal launched the Foundation in June of 2008 to support the use of the "information card" metaphor in federated identity solutions

- ***Kantara Initiative:*** The formation of the Initiative was announced on April 20 of this year, with a mission to, "[f]oster identity community harmonization, interoperability, innovation, and broad adoption through the development of open identity specifications, operational frameworks, education programs, deployment and usage best practices for privacy-respecting, secure access to online services." More succinctly, and taking this list full circle, the promoters of the Liberty Project conceived of the Initiative as a kind of host,

[18] Specifications developed by the Alliance can be found here: http://www.projectliberty.org/liberty/specifications__1

[19] Resources serving the OpenID ecosystem can by found at the OpenID Directory: http://openiddirectory.com/

[20] Current ICF Working Groups can be found here: http://informationcard.net/foundation/working-groups

clearinghouse and hub for the multiple federated identity activities already active, and yet to be launched.[21]

- ***Organizations focusing on on-line fraud:*** A large number of consortia were launched to confront the dramatic spread of spam, "phishing" and other practices that either degraded the on-line experience, or were fraudulent. Some of these SSOs later merged or disbanded. Here are two that continue to be active:

  - ***Anti-Phishing Working Group (APWG):*** The APWG was founded in 2003, and focuses on eliminating identity theft and fraud resulting from phishing and email spoofing. The organization provides a forum to discuss phishing issues, define the scope of the phishing problem in terms of hard and soft costs, and share information and best practices for eliminating these abuses. Membership is open to qualified financial institutions, online retailers, ISPs, the law enforcement community, and solutions providers. APWG also serves as a public and industry resource for information about phishing and email fraud, and identifies and promotes technical solutions intended to protect against phishing attacks. APWG deliverables include reports and white papers.[22]

  - ***Messaging Anti-Abuse Working Group (MAAWG):*** Founded in 2004, MAAWG's particular point of focus is the various forms of messaging abuse practiced via the Internet, including messaging spam, virus attacks, and denial-of-service attacks (i.e., attacks intended to render a Webs site non-functional). MAAWG's activities center on collaboration, technology, and public policy. MAAWG produces a variety of documents, including an ISP Code of Conduct and recommendations for best practices on topics such email forwarding, authentication, and metrics.[23]

> *A large number of consortia were launched to confront the dramatic spread of spam, "phishing" and other practices that either degraded the on-line experience, or were fraudulent*

- **Organizations (or efforts) focused on a specific industry:** Some consortia (or working groups within consortia) arise from, and serve the particular needs of, discrete industries with strong security needs. Examples from the financial and credit industries include:

  - ***Financial Services Technology Consortium (FSTC): Security and Infrastructure Standing Committee:*** The FTSC sponsors collaborative technology development-pilots, proofs-of-concept, tests, and demonstrations supported by member financial institutions and technology companies. Its aim is to advance interoperable, open-

[21] The best way to capture the still-evolving work program of the Initiative is at its Dashboard page, which can be found at: http://kantarainitiative.org/confluence/dashboard.action

[22] APWG white papers, reports, and other resources can be found at: http://www.antiphishing.org/resources.html

[23] MAAWG documents can be accessed at: http://www.maawg.org/about/publishedDocuments/

standard technologies that provide critical infrastructures for the financial services industry. The consortium comprises financial institutions, technology vendors, independent research organizations, and government agencies. FSTC is unusual, in that it provides a project-oriented collaborative research and development environment where members can: compare technologies; validate the feasibility of specifications in practice; and prototype new infrastructures for financial transactions. FSTC achieves these goals by sponsoring side-by-side comparisons of emerging technical solutions in the laboratory and in actual field operations, and validating early implementations of emerging industry specifications. The Security and Infrastructure Standing Committee covers a range of issues, including federated identity, fraud, distributed software assurance, and investigating security concepts with "breakthrough" potential.[24]

- ***Mobey Forum:*** The Mobey (as in "mobile") Forum's mission is to facilitate the emergence of banking services across mobile devices, "through cross-industry collaboration, business model analysis, experience sharing, experiments and cooperation and communication with relevant external stakeholders." Its members include financial institutions, mobile operators, handset manufacturers and others interested in enabling mobile financial services such as payment, remote banking and brokerage, and in raising the awareness of mobile financial service implementations; facilitating the open provisioning of such services; identifying business considerations and working to obtain the interoperability of the technical and security requirements for the mobile finance industry; and acting as a liaison between various standardization forums in the mobile and financial industries.[25]

> *The Mobey Forum's mission is to facilitate the emergence of banking services across mobile devices*

- ***PCI Security Standards Consortium (PCI SSC):*** PCI SSC (mentioned earlier in this article, and featured in an interview that appears later in this issue) was formed in 2007 by five major payment card brands (American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc.) to create, support and promote end-to-end risk management standards for the payment card ecosystem. Its standards and certification programs address those that process, store and transmit payment card data; those that develop and sell software and hardware for the same purpose; and those that audit and certify the compliance of these

[24] The Standing Committee's activities are summarized at this page: http://www.fstc.org/scom/index.php?id=4

[25] Mobey Forum documents can be found at: http://www.mobeyforum.org/?page=mobey-documents

> same companies to PCI SSC standards. Over 600 merchants, banks, and other entities are Participating Members in PCI SSC at this time.[26]

In addition, there are many other non-profit organizations that support member security efforts through activities such as: training, research and meetings (e.g., the Information Security Forum); developing certification standards and administration of certification programs for securities professionals (i.e., the International Information Systems Security Certification Consortium, Inc., (ISC)2); advocating for online privacy protection (such as the Online Privacy Alliance, which promotes protection through self-regulatory policies); and promoting the convergence of physical and IT security standards and interoperability (e.g., the Open Security Exchange).[27]

IV The Road Ahead

Better late than never, and with the impetus of a new administration behind it, the federal government in the United States has become energized over the importance of assessing and confronting the inherent risks associated with increasing online connectivity. Fulfilling that commitment will be a daunting task, given that no resource is safer than its weakest link.

Unlike several other high profile Obama administration initiatives with strong standards dependencies (such as deploying electronic health records and a national Smart Grid), most of the standards needed to achieve effective security are already in existence. The immediate challenge of achieving reliable security will therefore depend more on making wise choices among available standards, rather than in accelerating the development of standards yet to be created. This does not mean that the task will be simple, however, because in this case, government must implement standards across its own networks, rather than simply requiring that others do so across their systems. Morever, the tests to which compliant systems will be put in the field will be much more severe, and additional standards will constantly need to be developed, selected and implemented as new threats arise in the wild.

In contrast to EHRs and the Smart Grid, government must implement standards this time across its own networks, rather than simply requiring that others do so across theirs

Happily, a level of commitment appropriate to the task was expressed by President Obama on May 29, when he announced the results of a 60 day cybersecurity policy review conducted at his request by acting senior director for Cyberspace Melissa Hathaway. In his speech, the President summarized the five key findings of the

[26] PCI SSC's core standard, the Data Security Standard (DSS) can be found at: https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml Links to its other standards and supporting documents can be found on the left side of the same page.

[27] An extensive list of list of over 500 SSOs of all types, sorted by category, is maintained by the author at ConsortiumInfo.org, at: http://www.consortiuminfo.org/links/
SSOs that are either wholly or partially dedicated to security standards can be found here: http://www.consortiuminfo.org/links/linkscats.php?ID=22

review, and the actions he proposed to take based upon that review. He described one priority area as follows:

> Third, we will strengthen the public/private partnerships that are critical to this endeavor. The vast majority of our critical information infrastructure in the United States is owned and operated by the private sector. So let me be very clear: My administration will not dictate security standards for private companies. On the contrary, we will collaborate with industry to find technology solutions that ensure our security and promote prosperity.

Such public/private partnerships will require a driving force. In the same speech, the president announced the creation of a senior cybersecurity coordinator position, to be filled by an individual of his choosing. That person would run a new White House cybersecurity office, and would also serve as a member of the National Security Staff and National Economic Council. As of this writing, that person has yet to be appointed, and on August 3, Acting Director Hathaway announced that she was resigning. While Ms. Hathaway cited personal reasons, press reports indicated that the real reason may have been turf battles capable of marginalizing the post.[28]

Congress, too, has begun to attend to cybersecurity concerns. On April 28 of this year, a bill was introduced in the Senate that would require cybersecurity protections in addition to those already required under FISMA. In its current form, the proposed bill (titled the U.S. Information and Communications Enhancement Act of 2009 (S.921)), also calls for the establishment of a National Office for Cyberspace in the White House. It would additionally require every federal agency to appoint a Chief Information Security Officer. The supplemental title to the bill recognizes the importance of both risk management as well as technical standards in establishing effective security:

There are a number of existing laws of significance that predate the emergence of current cybersecurity fears, but which will necessarily imply the need to take cybersecurity-related precautions

> A bill to amend chapter 35 of title 44, United States Code, to recognize the interconnected nature of the Internet and agency networks, improve situational awareness of Government cyberspace, enhance information security of the Federal Government, unify policies, procedures, and guidelines for securing information systems and national security systems, establish security standards for Government purchased products and services, and for other purposes.[29]

[28] See, for example, Gorman, Siobhan, Security Cyber Czar Steps Down, Wall Street Journal, August 4, 2009, at: http://www.consortiuminfo.org/links/linkscats.php?ID=22

[29] The current draft of the bill can be found *at:* http://www.opencongress.org/bill/111-s921/show

While these recent actions are attracting attention in the press, there are a number of existing laws of significance that predate the emergence of current cybersecurity fears, but which will necessarily imply the need to take cybersecurity-related precautions. They include the Health Insurance Portability and Accountability Act (HIPAA), which protects health records, the Sarbanes-Oxley Act of 2002 (SOX), which concerns the financial information and practices of public companies, and the Gramm-Leach-Biley Act of 1999 (GLBA), which protects personal financial information, among others.

How government and the private sector will interact in the area of security standards remains to be seen as a matter of detail, but from a higher level, recent history suggests that private industry will continue to lead the way in the creation of the standards, best practices and guidelines needed to address security issues, while the Obama administration will develop policies, and manage implementation, of security practices across the federal agencies. Only if the private sector lags in regulating itself by developing and implementing adequate defenses will government be likely to step in and impose legislative solutions, mostly likely in a targeted manner (e.g., to protect and/or to allocate financial responsibility for data breaches involving consumer information).

In the final analysis, the existence, and inevitable increase, in the number and nature of cybersecurity threats represents yet another inconvenient truth about the ever-emerging world we live in. But unlike climate change, the solutions needed to protect us from cyberattack can be created much more quickly, can be implemented far more cheaply, and can have immediate effect. As with climate change, public and governmental awareness has now been raised. The most important challenge ahead will be to maintain that awareness, and the will to consistently implement the evolving solutions that are, and will continue to be, urgently needed.