Standards Today

A Journal of News, Ideas and Analysis

A publication of CONSORTIUM INFO.ORG

GesmerUpdegrove LLP

June – July 2009 Vol. VIII, No. 4

RISING TO THE CHALLENGE OF CYBERSECURITY

Standards Today is a free bi-monthly electronic Journal sponsored by the Boston law firm of Gesmer Updegrove LLP. The current issue of ***Standards Today*** and a subscription form may be found at www.consortiuminfo.org/bulletins. Questions or comments about the articles in this issue or about ConsortiumInfo.org may be directed to Andrew Updegrove at updegrove@consortiuminfo.org, or by telephone at 617/350-7800. To learn more about Gesmer Updegrove's standards and open source practice, visit http://www.gesmer.com/practice_areas/consortium.php, or contact Andrew Updegrove.

areas of on-line vulnerability as well. In this interview, PCI SSC General Manager Bob Russo explains how his organization came into being, what it does, and why it matters.

RAMBUS UPDATE:

Silicon design company Rambus has sometimes lost, but always appealed, in the myriad private suits and public investigations brought against it – until now. The question is, what changed?

STANDARDS BLOG:

The U.S. federal agencies are already heavy users of open source software, despite the fact that there has never been a unified voice in Washington advocating for the uptake of free and open source software. This month, a new organization was launched to fill that void.

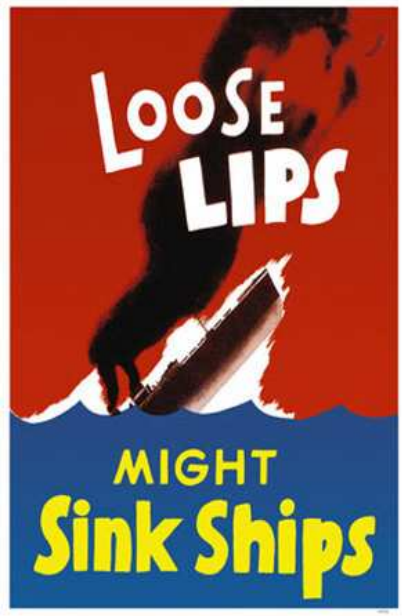
CONSIDER THIS:

Throughout the ages, monks, artists and graphic designers have lovingly illuminated and designed published works of all kinds. With electronic books finally taking hold, will the arts of the book be abandoned forever, or will a new generation of artists be allowed the bandwidth needed to enrich our future reading experience?

rove LLP. The current issue of ***Standards Today*** and a subscription form may be found at www.consortiuminfo.org/bulletins. Questions or comments about the articles in this issue or about ConsortiumInfo.org may be directed to Andrew Updegrove at updegrove@consortiuminfo.org, or by telephone at 617/350-7800. To learn more about Gesmer Updegrove's standards and open source practice, visit http://www.gesmer.com/practice_areas/consortium.php, or contact Andrew Updegrove.

EDITOR'S NOTE:

Security – Then and Now



U.S. Department of War Information Office Poster 1942

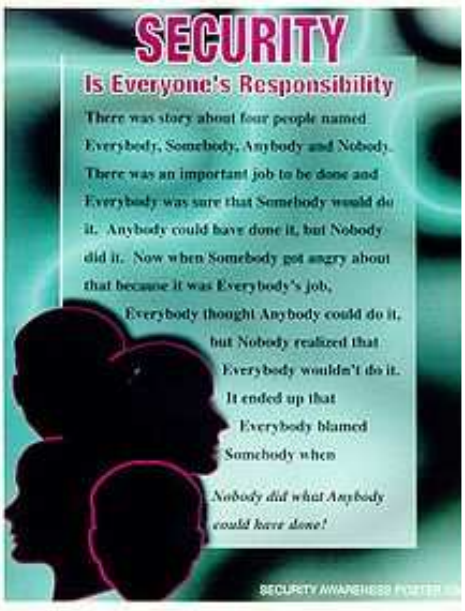
Security has always been a concern of government, doubtless from time immemorial, and especially in time of war. But until recently, ensuring security presented a much less difficult challenge – one that could be met with locks, guards, and ciphers against all but the most determined attackers.

Today, of course, that's all changed, and cybersecurity now demands attention in both the public and private sectors on a constant basis. With the danger of cyberattack becoming ever harder to ignore, the U.S. government has finally become alarmed, and is turning its attention to protecting both its own agencies as well as society at large from assaults launched by everyone from criminal hackers to rogue nations.

No surprise, then, that I am dedicating this issue of ***Standards Today*** to cybersecurity - yet another standards-dependent challenge that the Obama administration has pledged to address.

This issue is the fifth in a series I've written on such topics since the U.S. election, reflecting the heightened importance of standards and the standards development infrastructure to accomplishing key government initiatives (the prior issues were A Standards Agenda for the Obama Administration, The Electronic Health Records Standards Challenge, IT Policy and the Road to Open Government, and Standards and the Smart Grid).

In my ***Editorial*** this issue, I highlight how willing we are to deploy new technologies first, and only worry later about the risks that too often accompany them. In the ***Feature Article***, I offer a broad survey of the cybersecurity standards landscape, providing an overview of the challenges that our headlong rush into the virtual world has laid out our gates, the types of standards needed to address them, the organizations that are developing them, and the federal government's first steps in confronting its duty to protect itself, and society, from cyberattackers of all kinds.



U.S. Dept. of Commerce/Office of Security Awareness poster 2009

In this month's ***Interview***, the PCI Security Standards Council's Bob Russo provides a detailed look into the operation of a unique organization. PCI SSC is dedicated to enabling the kind of unique, end-to-end, standards-based risk management infrastructure that is necessary to protect the private information of credit card and debit card users everywhere. It provides an important example of the type of holistic, collaborative approach that will be needed to address many other complex security challenges, in areas such as electronic health records, open government, and more.

Next, I provide an update on a situation that I have covered many times over the past five years, involving a chip designer called Rambus, and a standards development organization named JEDEC. Rambus has sometimes lost, but never failed to appeal, in the past in the multiple private suits and public investigations that have been launched against it – until now. In this, my latest ***Rambus Update***, I report on a recent settlement entered into between Rambus and the European Commission, and offer some thoughts on what might have motivated its uncharacteristic decision.

In my ***Standards Blog*** selection for this month, I describe an organization that was publicly launched a few weeks ago to promote the use of free and open source software by the U.S. federal government. That organization, appropriately enough, is called ***Open Source for America***, and I'm pleased to have been asked to serve on its Board of Advisors.

I close this issue, as usual, with a ***Consider This*** essay, this time mourning the lack of interest (so far) on the part of software designers, electronic publishers, and yes, standards developers, to embrace on line the Arts of the Book that have graced handwritten and printed texts for a full millennium. Hopefully, this will be only a temporary condition.

By way of disclosure, I should (and am proud to) note that I have served as legal counsel and/or have served on the Boards of Directors of the following standards organizations featured in this issue: ***American National Standards Institute***, ***Information Card Foundation***, ***Organization for the Advancement of Structured Information Systems (OASIS)***, ***OpenID Foundation***, ***PCI Security Standards Council***, and ***Messaging Anti-Abuse Working Group***. Any characterizations of these worthy groups included in this issue are mine alone, and should not be construed to have been authorized or made on behalf of any of these organizations.

As always, I hope you enjoy this issue. But whether you do or don't, it's always good to hear from you. You can reach me at andrew.updegrove@gesmer.com.

Andrew Updegrove
Editor and Publisher
2005 ANSI President's
Award for Journalism

The complete series of Consortium Standards Bulletins can be accessed on-line at http://www.consortiuminfor.org/bulletins/ It can also be found in libraries around the world as part of the EBSCO Publishing bibliographic and research databases.

EDITORIAL:

Technology's Reach and Security's Grasp

Andrew Updegrove

Modern society harbors many bad habits. One is its penchant for enthusiastically embracing the benefits of new technologies before considering their less desirable side effects. Whether we look at the development of automobiles (first) and safety features (much later), or industrialization (first) and environmental protection (much, much later), the story is always much the same: we reach for the candy before we grasp the reality of the cavities. Only after the problems become too great to ignore do we investigate the unintended consequences, realize how difficult and expensive they are to address, and grudgingly start to rein in our appetites and exercise a bit of prudent self-discipline.

Perhaps we should not be surprised, then, that the U.S. government is only now becoming alarmed over the vulnerability to which we have become exposed as a result of our whole-hearted embrace of the Internet. With the operations of government, defense, finance, commerce, power distribution, communications, transportation, and just about everything else now dependent on the healthy operation of the Internet, that alarm is well-justified. And with the creation and storage now of virtually all data in digital, rather than physical form, exposure of our financial as well as our most intimate personal and health information is only a hack away as well.

With the creation and storage today of virtually all data in digital, rather than physical form, exposure of our financial as well as our most intimate personal and health information is only a hack away

In some ways, finding ourselves at such a pass is not so surprising, largely because in the past we have been able to create security barriers when and as needed, and allocate the costs of security failures in a workable manner that has been acceptable to those directly involved. Think of the evolution of the credit card industry, for example, in which the individual card owner whose card is stolen is effectively immune from financial liability for the card's misuse. Instead, the commercial entities that benefit from the existence of the cards accept that risk and absorb it into their cost structures. From an economic point of view, this is a rational response, and so it might seem that that the Internet simply replicates old risks in new settings that can still be adequately managed in a traditional way.

But no. As recent retail security breaches have shown, far too much information can be exposed via a single successful assault to rely upon reallocation of risk to manage the impact. The same is true in many other domains. Whether it be managing a national air traffic control system, processing billions of financial

transactions a day, or operating a unified national "Smart Grid," the stakes are simply too high to rely on damage control. Instead, we must prevent the breaches entirely, by building the firewalls higher and stronger. We have no choice but to learn how to repel the rapidly increasing horde of cyberbarbarians gathering outside our digital gates.

We need to grasp that a digital 9/11 event is already within the reach of too many – and act to protect ourselves against the consequences

Somewhat paradoxically, one key to the security solution can be found in standards. Paradoxically, in that we think of security in the given case as being based upon doing things uniquely rather than all in the same way. But in fact, security has always been based on standardized approaches (think of standard locks with unique keys, and single algorithms that generate and then interpret multitudes of scrambled messages). So also it is that the only feasible manner in which security can be achieved in a networked world is through the use of standardized approaches and tools – in this case, a multitude of them, both technical and procedural. The former makes security possible in the first instance, while the latter allows it to be maintained reliably as the network is upgraded on a constant basis.

Happily, there are many formal standards development organizations and consortia actively engaged in supporting existing security standards, and developing new ones. They range from protocols, to federated identity tools, to biometric identification standards, to holistic suites of standards, auditing requirements and certification programs created to maintain end-to-end security within complex commercial environments, such as the payment card industry. But much more work remains to be done to implement reliable security across many crucial domains.

The advent of the Obama administration offers a unique opportunity to close the gap between technology's reach and our grasp of the risk that must be managed. Today, there is a confluence of opportunity made possible by the technological sophistication of the Obama team, the launch of simultaneous initiatives to rapidly implement new technologies to address significant national objectives, and the funding needed to tackle these enormous jobs. In each case, whether it be making the transition to Web-based open government, deploying electronic health records for all citizens, or putting in place a new interactive power grid, implementing effective security protections will be crucial to success. Otherwise, the new benefits we gain may be outweighed by the new risks that we will assume.

In other words: there is no choice for the Obama administration – and Congress - but to make achieving a new level of data security a national imperative. We are already farther down the road of risk than we should be. If we fail to act, the consequences may not be gradual and reversible, as with pollution, but sudden and disastrous, perhaps as the result of the acts of a rogue state taking down the financial markets, or an international terrorist organization bent on crashing the air traffic control system at rush hour.

Is that an alarmist statement? Hardly. We have already seen the personal information of millions of individual citizens exposed through single data breaches, presumably by rings of foreign criminals, as well as government Web sites taken down by persons (or nations) still unknown. Before it is too late, we need to grasp that a digital 9/11 event is already within the reach of too many – and act to protect ourselves against the consequences.

Sign up for a free subscription to ***Standards Today*** at

http://www.consortiuminfo.org/subscribe/2.php?addentry=1

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, 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.

[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.

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 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

---

[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.

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 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:

[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

- 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 attention is paid to avoiding that result. Change management standards and processes guard against the inadvertent weakening of defenses by mandating how

[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

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

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

[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

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 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.

---

[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

- **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 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

[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

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, 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

[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

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:

  - ***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]

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

- **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:

---

[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

- ***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 authentication. In addition to standards, the Alliance develops business and deployment guidelines and best practices for managing

[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/

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

---

[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

[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

- ***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-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

[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/

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 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.,

[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

[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.

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 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

[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

> 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]

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.

---

[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

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.

I N T E R V I E W :

Enabling an Ecosystem of Security: An Interview with PCI SSC's Bob Russo

Andrew Updegrove

As anyone who follows the news is aware, data breaches involving credit and debit card information have been very much in the public eye. In the cases that have received the most publicity, information relating to over 45 million cards was compromised by the breach of retailer TJ Maxx, and when malware was installed on a server of card transaction processor Heartland Payment Systems, the number of cards compromised may have exceeded 100 million. And indeed, with millions of retail outlets taking payments via credit and debit cards, the points of opportunity for hackers to access card data in batches large and small are inevitably great. The only way to prevent such breaches is for retailers, and those upstream from them (e.g., banks, processors and card issuers), to exercise great care and constant vigilance to guard against intrusion.

But what practices are most effective, and how much security is enough? These are difficult questions, given that the answer must address the vulnerabilities of a network that includes an almost infinite number of data entry devices, a global communications network administered by many different companies, processing and database software from multiple vendors, transaction processing service companies, card issuing banks throughout the world and multiple payment card brands. Achieving security in a manner that is consistent is also vital, so that merchants are not subject to radically different requirements imposed by each payment card brand with whom they do business. Clearly, then, there is a need for a central, collaborative organization that can set the bar for security for each primary area of vulnerability in the payment card ecosystem, define best practices, certify compliance efforts, and strive for consistency, all while remaining aware of the realities of the marketplace, and costs of compliance. In other words, a standards organization.

In order to achieve such a consistent, effective security environment, five of the major payment brands (American Express, Discover Financial, JCB, MasterCard Worldwide and Visa) came together in 2006 to rationalize and standardize their evolving, individual programs and to collaborate to develop new standards as needed to address new cybersecurity threats. The organization they created is

called the PCI (for payment card industry) Security Standards Council, or PCI SSC. Today, more than 500 stakeholders in the global payment card ecosystem (merchants, banks, government and others) have joined the effort as Participating Organizations.

Not long after its launch, PCI SSC hired Bob Russo as its first General Manager. Russo came to the job with 25 years of security industry experience, in the course of which he had been a founder or senior management member of many service, software development and compliance companies. As General Manager of the Council, Russo is responsible for executing the Council's policies and achieving its goals. More specifically, he oversees the Council's training, testing and certification programs, supports the certification process, coordinates research and analysis, solicits feedback from the vendor and merchant communities, and drives recruitment of stakeholders as Participating Organizations in the Council.

In this detailed interview, Bob Russo explains how PCI SSC came into existence, the industry challenges it was formed to address, the unique infrastructure that it has helped create, and how the Council is helping the payment card ecosystem to work together to safeguard payment card and personal information. What he has to share is useful to provide insight into the challenges of protecting such information from fraud. More broadly, though, the standards that the Council develops and the infrastructure that it supports provide an example of the type of comprehensive, global risk management regime that can be emulated in many other settings where equivalent amounts of personal information will become vulnerable to breach and misuse, from open government to electronic health records. Unless similar or equivalent organizations come into existence in these areas, the consequences may be regrettable.

Unless similar or equivalent organizations come into existence in these areas, the consequences may be regrettable

Disclosure: The author and his law firm, Gesmer Updegrove LLP, have represented PCI SSC since its formation.

Part I: Why, When and How

AU: *How did PCI SSC come into existence?*

BR: The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection.

The Council was formed in September 2006 by the five major payment card brands, our founding members American Express, Discover, JCB, MasterCard, and Visa. These original members of the Council agreed to work together to develop and recognize one set of data security standards to protect their customers systems and the consumer's data that resides within them.

Prior to the formation of the Council, retailers and other merchants had expressed frustration at the challenges of securing card data in a way that was recognized universally by all the payment card brands they did business with. Organizations involved in the payment process also highlighted their desire for a mechanism to contribute to the card data security agenda and enable them to provide some input into the security standards they would be using. Hence, on the back of strong industry feedback, the Council was formed.

AU: *What are the special challenges that maintaining payment card security faces?*

BR: There will never be a silver bullet! Data, in one form or another, must always be stored and therefore must constantly be protected. Networks today are so complex, it is a constant job to make sure whatever little tweaks are made in one area by one group do not affect other areas. The only way to insure this is through constant testing, monitoring and vigilance.

There will never be a silver bullet! Data, in one form or another, must always be stored and therefore must constantly be protected

AU: *The payment card ecosystem has many stakeholders besides payment card brands and payment card users. Who are the other players in the payment card chain, and what role do they play in ensuring security?*

BR: Along with input from the five founding members, the Council is able to enjoy a wide range of contributions and insight from our Participating Organization membership which is comprised of over 500 leading global players in retail, hospitality, financial services, technology, government and academia.

These represent some of the key players in the payment card chain, from card accepting retailers, their acquiring banks or processor service providers, through to consumers' card issuing banks, technology solution providers that service various parts of the payment chain, and associations that represent various constituents within these broad groups.

This Participating Organization group, along with the Council's approved Qualified Security Assessor community, numbering 168 people/companies, is able to provide the Council with real world insight and experience of deploying security standards in the field and the challenges and threat vectors security standards must combat. This Participating Organization group represents the people who are responsible for securely handling and defending consumer's data against attack and therefore are a valuable resource in feeding front line threat information into the Council.

From this participating organization group a smaller group of 21 representatives are seated as the Board of Advisors every two years through an open election and appointment process. Two thirds of the Board of Advisors are elected, with a further third appointed to ensure adequate geographical and industry representation. These organizations are the mouthpiece of their respective industries and ensure that the Council is able to partner with industry at a very detailed and actionable level in the standards setting process. This Board of Advisors is a critical enabler in

our mission to secure businesses payment processes and consumers cardholder data globally.

Our current Board of Advisors is comprised of leaders in their respective industries such as Wal-mart, Microsoft, McDonalds, British Airways and APACS. The Board has worked tirelessly with the Council over the past two years to highlight areas of need in the market and devise educational resources such as the recently launched "Prioritized Approach" to the PCI DSS *[Ed: This is the Council's core standard, the PCI Data Security Standard]*, a resource that helps organizations starting out on their card data security journey to work with a risk based approach to compliance and start their process at the point that will reduce the impact on consumers and their business should a compromise occur. The Board of Advisors nomination and election process is underway this spring to seat the next Board and we welcome the Committees involvement in this process.

PCI Security Standards Council's QSA qualification requirements are exacting and detailed, involving both the security companies and their individual employees

AU: *Who else plays an important role in the payment card security ecosystem?*

BR: The Council's various certified security assessors and scanning vendors are organizations focused on security services and provide valuable consultancy, assessment services and technology solutions to organizations of all shapes and sizes that are focused on securing their payment card data. This is an important group at the front line of helping their customers secure payment card data.

- ***Qualified Security Assessor (QSA) companies:*** Qualified Security Assessors are employees of these organizations who have been certified by the Council to validate an entity's adherence to the PCI DSS. The Council has qualified over 100 companies and trained and certified over 1500 assessors.

- ***Payment Application Qualified Security Assessor (PA-QSA):*** These are organizations that have been qualified by the Council. Payment Application Qualified Security Assessors are employees of these organizations who have been certified by the Council to validate an entity's adherence to the PCI PA-DSS.

- ***Approved Scanning Vendors (ASVs)***: These are organizations that validate adherence to certain DSS requirements by performing vulnerability scans of Internet facing environments of merchants and service providers. The Council has approved over 130 ASVs.

Because the quality of PCI DSS validation assessments can have a tremendous impact on the consistent and proper application of security measures and controls, the PCI Security Standards Council's QSA qualification requirements are exacting and detailed, involving both the security companies and their individual employees.

As an aspect of the Council's auspices that interacts with stakeholders frequently, these organizations come under great public scrutiny. In order to maintain the

highest level of standards in assessment following QSA training, the Council has launched a quality assurance program for QSAs and ASVs. The program was designed to provide QSAs and ASVs with a set of requirements that helps ensure they provide consistent, quality validation and assessment services to merchants and service providers.

The PCI SSC developed the quality assurance program as a direct result of feedback from the Council's Participating Organizations and assessment community and is intended to promote consistent interpretation of the PCI standards and ensure quality is maintained among all vendors. Participation in the program is required for the Council's registered QSAs and ASVs, in order for them to retain the ability to conduct PCI assessments.

[The] information that may be contained in the magnetic strip on the back of the payment card… [is] is the information that cyber criminals want to steal to create counterfeit cards. The proverbial keys to the kingdom

In addition, these key stakeholders share the redacted data of their assessments and provide a unique window for the Council to observe current challenges and trends within specific aspects of the DSS, and allow a feedback opportunity to understand the real world challenges of PCI implementation.

AU: *How are these other types of stakeholders represented in PCI SSC?*

BR: For those others not specifically included in our Participating Organization, QSA and ASV communities, the Council offers an education program that includes printed materials, online resources, webinars and face to face training sessions.

The Council's newly launched Standards Training program is designed to help merchants and service providers improve preparation for on site assessment, understand what is involved in creating their own internal assessment capability, and establish an internal program to help sustain PCI DSS security practices and compliance. This new course was introduced directly as a result of stakeholder feedback to the Council.

AU: *What are the principle standards that PCI SSC has developed to date?*

BR: The Council's standards – the tools it makes available for use by public and private sector entities to secure payment card data – are designed to protect specific parts of the payments process. The Council is constantly looking for new standards to secure, and maintains a dialogue with its Board of Advisors and other industry stakeholders to bring new resources to the market to increase the security of consumers payment card data. I'd like to give a brief overview of some of these tools.

PCI Data Security Standard (PCI DSS): The PCI Data Security Standard is a set of 12 requirements that cover 6 principles to secure payment card data. At the heart of this standard is the requirement that organizations do not store sensitive information that may be contained in the magnetic strip on the back of

the payment card. This is the information that cyber criminals want to steal to create counterfeit cards. The proverbial keys to the kingdom. The fundamental principle of the PCI DSS is that organizations must not store sensitive data from the back of the card. Where information on the front of the card is stored, it must be rendered unreadable. This means that it must be truncated, hashed or rendered in some way unreadable.

Along with these fundamentals, the requirements range from securing networks and perimeters, maintaining up to date security patches and anti virus software, down to things like developing and maintaining an incident response plan and processes for your organization to follow in the event of a breach.

Forrester estimates that the TJX breach will cost TJX $1.35 billion in breach related costs including legal fees, call center costs, regulatory fines, etc.

The Payment Application Data Security Standard (PA-DSS): The Council developed this standard after feedback from our membership indicated that software applications represented a point of weakness in the payment chain. Payment applications might, for example, be touch screen applications you see used in a restaurant or convenience stores. Some of these payment applications may be unknowingly storing sensitive payment card data therefore undermining an organizations effort to comply with the PCI DSS. The Council introduced a process where payment applications are tested in Council approved laboratories to check that they are secure, not storing payment data, and will help, not hinder, an organizations efforts to comply with PA-DSS. The Council maintains a list of approved payment applications that have been tested in and approved by Council laboratories, on our website for merchants to cross reference the status of their own applications and to make informed purchasing decisions.

The PIN Entry Device Security Requirements: The PIN Entry Device security requirements have the same underlying principle as PA-DSS. They are designed to enable organizations to protect consumers' cardholder data and ensure that PED devices are not unwittingly storing payment card information, or jeopardizing organizations PCI DSS compliance efforts. As a PIN Entry device is a physical object, these requirements cover not just ensuring that a device does not store sensitive data, but also that it is tamperproof and should it be compromised, any contents of the device will self destruct.

The Council maintains a list of approved devices that have been tested in and approved by Council laboratories, on our website for merchants to cross reference the status of their own devices and to make informed purchasing decisions. The Council is currently working to expand the scope of this program to include different device types including unattended payment terminals such as ticket kiosks and self service machines.

Lifecycle of the Standards: Development and review of the PCI DSS is a continuous process that follows the Council's published PCI DSS Lifecycle process. This document (Exhibit A to the PCI DSS) outlines the PCI DSS development and evolution process. Because compliance with the PCI DSS is required of millions of

merchants, banks and other stakeholders around the world by PCI SSC's members, changes to the PCI DSS must be carefully considered, and those affected must be given advance notice of any new requirements that will be imposed upon them. The upgrading of the PCI DSS therefore operates on a two-year lifecycle process that incorporates five phases:

- Stage 1 market implementation of previous version/revisions
- Stage 2 feedback begins
- Stage 3 feedback review and decision-making
- Stage 4 new version/revision and final review
- Stage 5 discuss new version/ revision

The Council is currently in the implementation phase of PCI DSS 1.2. The next formal feedback period will start in July 2009, with the goal of launching the next version/revision of the PCI DSS in October 2010.

The last open review period culminated in the discussion of the new standard -- PCI DSS 1.2 -- at our annual community meetings in Orlando, Florida in September 2008 and in Brussels, Belgium, in October 2008. In addition to this formal lifecycle process, part of the ongoing work of the Technical Working Group (TWG) is to regularly discuss and examine existing and new security technologies, issues and best practices with the goal of ensuring that the PCI DSS provides strong levels of security and effectiveness to stakeholders in the payment process without unfairly burdening the global marketplace.

The number and variety of potential deployments for enabling and processing credit card transaction is huge, depending on IT infrastructure, hardware and the scope of the enterprise

While a planned lifecycle process is important, it is equally important that the Council be responsive to emerging threats. As a result, we have several mechanisms for ongoing communications with Assessors, Merchants and other stakeholders to provide guidance as new threats emerge. These include:

- Errata to the DSS itself;
- Flash bulletins on emerging threats;
- A monthly newsletter to the Assessor community with the latest threat information & corresponding changes required to the assessment process;
- Regular updates to the ASV test scanning environment to reflect new threats emerging "in the wild";
- Monthly Webinars with both assessors and merchants;
- Updates to the Council's online searchable FAQ and training materials to ensure they include the latest information on the threat landscape.

AU: *Most individual standards tend to address very discrete needs. The DSS is very different in that it seeks to describe a very broad security environment in many different ways. What are these ways?*

BR: The number and variety of potential deployments for enabling and processing credit card transaction is huge, depending on IT infrastructure, hardware and the scope of the enterprise. A multinational chain retailer in Boston will have a significantly different network map than a mom and pop shop in Buenos Aires, or from a financial institution that processes transactions from millions of merchants in Hong Kong. The DSS needs to take into consideration the variety of possible deployments and provide a solid foundation of security that enables these transactions to be completed in a safe manner. So, every facet of the Standards needs to be vetted to ensure that it works in multiple payment environments, and allows for the seamless integration of payment security into the transaction process. As such, a lot of the focus is not just on securing the payment information, but separating, or removing from scope the non-payment elements of the network

AU: *How does PCI SSC relate to other domestic and international standards organizations and their work?*

BR: As a global, open industry standards body providing management of the Payment Card Industry Data Security Standard, the Council must address all the payment landscape variances in around the world. As such, we openly solicit feedback and information from national and international interests. However, security solutions or guidelines mandated by regional interests may not be effective, or implementable in other areas of the world. As such, the Council regularly examines the work of other standards organizations to address whether they can function within the scope of the Council's global purview, as part of the ongoing lifecycle of the Data Security Standards. That said, the Council must remain relevant globally to service the needs of our Participating Organizations and founding members, so we will continue to resist alignment with any geographically specific norms.

A multinational chain retailer in Boston will have a significantly different network map than a mom and pop shop in Buenos Aires,… The DSS needs to take into consideration the variety of possible deployments and provide a solid foundation of security that enables these transactions to be completed in a safe manner

Part II: The Challenges Ahead

AU: *Over the past year there have been several high-profile break-ins, resulting in the compromise of cardholder data. What types of standards-related weaknesses were exploited by hackers in gaining access to this data?*

BR: From the information we have available, the PCI Standards remain sound. We have yet to see a data breach from an organization that was in compliance with the DSS. If anything, the recent breaches have underscored a necessity for more vigilant monitoring of systems, as compliance and subsequent risk for a data breach may be only one small network change away. Compliance is a snapshot in time. The Council continues to emphasize sound security practices as a business necessity, not simply a checklist approach to achieve compliance.

AU: *Security is expensive, and the economy is poor. How does PCI SSC balance costs with the need to ensure security for those that have the burden of implementing PCI SSC standards?*

BR: I think a more important question is how can an organization afford NOT to do this. Compare the cost of achieving PCI compliance to the potential cost of a data breach to an organization. For example, a recent survey by the Ponemon Institute found that the cost of a data breach rose to $202 for each compromised record last year, an increase of 2.5% over 2007, with an average expense to an organization of $6.6 million.

Forrester estimates that the TJX breach will:

- cost TJX $1.35 billion in breach related costs including legal fees, call center costs, regulatory fines, etc.
- the cost *per breached record* was anywhere from $90 to $305 *each*
- Fines from the payment brands can be as much as $500,000 per incident

Nonetheless, the Council recognizes the challenges merchants and other entities face in this economic climate. As a result of stakeholder feedback, earlier this year we introduced a new tool for helping merchants prioritize where to focus their compliance efforts, and therefore dollars. We want to show them where they might be able to reduce the most risk, the quickest. We called this tool the Prioritized Approach to PCI DSS.

We have yet to see a data breach from an organization that was in compliance with the PCI DSS standard. If anything, the recent breaches have underscored a necessity for more vigilant monitoring of systems

The Prioritized Approach framework helps merchants identify highest risk targets, create a common language around PCI DSS implementation efforts and demonstrate progress on the compliance process to key stakeholders.

The Prioritized Approach framework was created to help merchants who are not yet fully compliant with the PCI DSS understand and reduce risk while on the road to compliance.

Comprised of six security milestones, the tool focuses on best practices for protecting against the highest risk factors and escalating threats facing cardholder data security.

We compiled the tool after considering actual data compromise events, feedback from Qualified Security Assessors (QSAs) and forensic investigators and input from the PCI SSC Board of Advisors. The framework gives practical suggestions on how to approach compliance with PCI DSS to create the most immediate impact on card data security in a merchant's environment.

In addition, the Council offers training, and additional resources designed to help organizations adopt securely protect their credit card data in a cost effective manner.

AU: *In a similar vein, how do you balance the need to react to new threats as they emerge with the need for so many banks, merchants and others to give input on standards and then implement them?*

BR: The DSS is a living document with a built in lifecycle process designed to assess the current threat landscape and incorporate any changes into future editions of the standards. This feedback loop provides a critical framework for assessing future revision, and is absolutely necessary to reflect and address emerging threats to the security of payment data.

One of the ways the Council stays current with threats and challenges in the payment landscape is through our Special Interest Groups (SIG).

SIGs are independently formed task forces that tackle specific areas of interest to their members. Each SIG is led by a member of the Council's Board of Advisors who help the groups examine the impact of different technologies and industry specific challenges on the implementation of PCI Security Standards.

The DSS is a living document with a built in lifecycle process designed to assess the current threat landscape and incorporate any changes into future editions of the standards.

SIGs are independently formed task forces that tackle specific areas of interest to their members. Each SIG is led by a member of the Council's Board of Advisors, who helps the group examine the impact of different technologies and industry specific challenges on the implementation of PCI Security Standards.

SIGs help clarify elements of the DSS that might be considered challenging, or open to interpretation for those in the payment chain seeking to secure their credit card data. SIGs will create actionable support documentation, specific instructions or recommendations in an effort to clarify how a specific technology, and the manner in which it is implemented, can affect an organization's compliance with specific requirements of the DSS. To date, four SIGs have been formed focusing on wireless, scoping, virtualization and pre-authorization. It's worth noting that these are independent groups that are formed and led by voluntary members of our Participating Organizations.

The PCI SSC Board of Advisors suggested the formation of the first series of SIGS, based on market awareness, threat mitigation and the input of our Participating Organizations (POs). In the future, POs may also suggest or propose additional groups to focus on specific requirements of the DSS.

There is no Council staff input to the groups and they are free to make whatever recommendations they deem necessary. We've just published the first deliverable by the Wireless SIG led by Doug Manchester of VeriFone. That group came up with a Wireless Guideline document to help merchants understand how to securely

implement wireless within or outside of their cardholder data environment. Through resources like SIGs we are able to ensure a variety of voices from around the payment chain are heard, and are inputting into valuable educational materials for our constituents.

In addition to work with our Board of Advisors and SIGs, the PCI SSC has commissioned PricewaterhouseCoopers PwC to review technologies such as end-to-end encryption, chip and PIN and tokenization to see what impact these technologies have on PCI compliance and whether these technologies should be made part of PCI requirements in the future. The feedback process, the SIGs and BoA structure and the PwC review, are efforts by the PCI SSC to make the standards setting process inclusive, transparent and relevant. I think we're doing a good job in this regard.

The greatest threat to payment chain security is complacency. Organizations must build in security practices into their ongoing business plans. As recent data breaches have illustrated, a checklist approach to security simply does not work

AU: *What are the greatest security threats that you see ahead?*

BR: The greatest threat to payment chain security is complacency. Organizations must build in security practices into their ongoing business plans. As recent data breaches have illustrated, a checklist approach to security simply does not work. Data security is not all about prevention; it also requires detection and monitoring.

Recent post-breach reviews by Verizon Business resulted in the discovery that:

- *Breached organizations only had 11% compliance level for Req 3 (Protect card holder data).*
- *only 5% compliance level for Req 10 (track & monitor all access to network resources and cardholder data)*

Data security is not all about prevention; it also requires detection and monitoring. If your networks are compromised, it doesn't have to follow that the data within them will be.

AU: *What are the greatest practical challenges you see ahead for PCI SSC?*

BR: The aforementioned lack of vigilance is a big problem. And the misconceived perception that the DSS cannot prevent data breaches continues to be the greatest challenge to payment card security.

AU: *What role should government play? Is there a danger that we will end up with 51 different sets of security regulations in the US alone? How should industry and governments work together to avoid such a result?*

BR: Payment card fraud is something that concerns all of us, businesses and consumers; from the pizza shop down my street to the country's largest online and bricks and mortar retailers, from a housewife who manages the weekly shopping to

the businessman who conducts trade globally. For the consumer, in spite of zero liability protection under these circumstances, having your card details stolen can be an inconvenient and stressful experience. It is also very costly for financial institutions who have to reissue cards, and for businesses that can lose customer confidence and suffer damage to their reputation.

We welcome the government's interest in the topic of payment card data protection, and the Council appreciates the government's ongoing commitment to understanding and exploring the initiatives underway to contain and reduce fraud for businesses and consumers globally. We have enjoyed input from several government related entities on our Participating Organizations and have attended and spoken at many security related government events, as well as enjoy government speakers at our own Community Meetings, so we welcome the opportunity to continue to work together to continue to reduce card data compromise.

That said, for years the United States has relied heavily on the private, rather than the public, sector to rapidly create thousands of new standards every year in virtually every branch of industry as new needs arise. The PCI Security Standards Council is just one of the hundreds of "consortia" that have been founded for such a purpose.

We welcome the government's interest in the topic of payment card data protection, and the Council appreciates the government's ongoing commitment to…contain and reduce fraud

The PCI Security Standards Council is not yet three years old. Yet we have come a long way in raising awareness of the issue of securing consumers payment card data among businesses globally, along with providing a forum for collaboration amongst those in the payment chain to create a robust set of universally recognized security standards for the industry. We believe, in partnership with our Participating Organizations, we are doing a good job.

AU: *Are there other standards-related goals that need to be addressed that lie outside PCI SSC's charter that need to be addressed, and if so, by whom?*

BR: Unfortunately we don't know what we don't know. I'm sure there are, but I am so laser focused on our mission (and in conjunction with our global partners…i.e. EPC and all of the other areas of the world) we are constantly evaluating other issues that come up in other parts of the globe.

Part III: Lessons Learned

AU: *PCI SSC is generating solutions that will be relevant to an increasing number of other national and global networks that must safeguard consumer data. Electronic Health Records provide one example of data that will need to be stored and accessible to many types of parties (hospitals, doctors, insurers, and so on). Implementing Open Government goals provides another. What aspects of the PCI SSC approach are likely to provide useful models in these other situations?*

BR: The PCI Data Security Standards are built from the strongest, most fundamental best practices available to secure a specific type of (payment) data. However, we have always maintained that the principles and practices inherent within the DSS can help organizations properly segment their networks and protect any type of sensitive data you may be required to handle.

In fact, in a recent report, titled, "PCI Unleashed: Embracing PCI As A Next-Generation Security Architecture," (May 22, 2009) Forrester Research senior analyst, John Kindervag suggest that PCI should be the foundation for organizational security. From the report:

[T]he principles and practices inherent within the DSS can help organizations properly segment their networks and protect any type of sensitive data you may be required to handle

PCI: Used by millions of companies, it:

- Has been vetted
- Has established support communities actually
- Has a highly trained workforce (more or less 20,000 QSAs)
- Is easy to hire expertise around
- Non-PCI companies are looking at PCI as a best practices framework.

The conclusion he draws in the report? "PCI incentivizes good security and makes an excellent baseline framework."

AU: *What have you learned at PCI SSC that consumers or others should know that they may not be aware of?*

BR: Many consumers erroneously equate credit card fraud with identity theft, and this is simply not the case. Having your credit card number stolen is not the same as having your identity stolen. In most credit card fraud circumstances, there is zero-liability on the consumers' part. They are significantly protected from financial implications of credit card fraud. However, we recognize the issue of credit card fraud is a serious matter to businesses and financial institutions, and we are leading the charge to reduce the scope of this fraud on a global basis.

AU: *What haven't I asked you that readers should know about PCI SSC and its work?*

BR: Through the participation and input of stakeholders all over the world, and an increase focus on payment security, we are now at a point where the levels of credit card fraud are at an all time low, when measured in basis points. With the ongoing support and assistance of all in the payment chain, we hope to continue to drive this reduction, and help protect the future of payment security.

R A M B U S U P D A T E:

The EC Settlement: Rambus, Writs and the Rule of Law

Andrew Updegrove

Why did perennial litigant Rambus, Inc. settle with the European Commission?

Certainly the most watched standards-related legal conflict of the decade involves the participation of memory technology vendor Rambus, Inc. in a working group hosted by standards developer Joint Electron Device Engineering Council (JEDEC) in the early 1990s. The fame (or notoriety) of the conflict arises in part from the importance of the conduct at issue (did Rambus set a "patent trap" for implementers of the standard that emerged from the working group?), and in part from the seemingly endless string of law suits that resulted from that conduct some fifteen years ago.

Most of these suits were brought by Rambus against vendors that refused to pay royalties when they implemented the standard, but these suits almost always resulted in vigorous counterclaims against Rambus, brought by those same implementers. Investigations into Rambus's conduct were also brought by the Federal Trade Commission (FTC) in the United States, and by the European Commission in the European Union. A separate string of cases related to alleged price fixing and other improper conduct by several vendors that participated in the same JEDEC working group (these were the same companies that refused to pay royalties to Rambus). These charges ended with the vendors paying record settlement amounts to the regulators. Needless to say, neither Rambus, nor those that it sued for royalties, had much to be proud of.

In the course of these many suits, investigations and appeals, Rambus has sometimes won, and sometimes lost. But every time it lost, it fought on - sometimes through multiple levels of appeal - until it ultimately prevailed.

That is, until now. On June 11, Rambus and the European Commission announced that they had reached tentative agreement on a settlement of the investigation that the EC had opened in August of 2007. In form, the settlement agreed upon is similar to the (later overturned) restrictions levied upon Rambus by the FTC. That is, Rambus agreed to forward-looking caps on the amount of licensing royalties that it will be permitted to charge for the right to implement the JEDEC standard in question.

But why, you may ask, has Rambus finally decided to settle rather than fight on in a case that involves the same conduct that it has so vigorously defended before? That is indeed an excellent question, and I'll try and answer it as best I can in this entry.

What just happened: First, let's take a look at the facts. A press release issued by the EC when it opened its investigation stated in part as follows:

> The [Statement of Objections issued by the EC] outlines the Commission's preliminary view that Rambus engaged in intentional deceptive conduct in the context of the standard-setting process, for example by not disclosing the existence of the patents which it later claimed were relevant to the adopted standard. This type of behaviour is known as a "patent ambush". Against this background, the Commission provisionally considers that Rambus breached the EC Treaty's rules on abuse of a dominant market position (Article 82) by subsequently claiming unreasonable royalties for the use of those relevant patents. The Commission's preliminary view is that without its "patent ambush", Rambus would not have been able to charge the royalty rates it currently does.
>
> This is the first time that the Commission is dealing with a "patent ambush" under EC antitrust law, but the approach reflects well-established general case-law under Article 82 of the Treaty.

Comparatively little was heard about the EC investigation after this announcement. Meanwhile, the FTC was nearing the end of the process of losing, then winning, then ultimately losing again in its efforts to punish Rambus for what it viewed as violations of U.S. antitrust laws (you can read an overview of the FTC's efforts involving Rambus here). The FTC's road ultimately came to a dead end just this spring, when the Supreme Court refused to review the final appellate decision that had found in favor of Rambus.

The FTC's road ultimately came to a dead end just this spring, when the Supreme Court refused to review the final appellate decision that had found in favor of Rambus

Rambus seemed to then be in the clear. But two weeks ago, it announced that it had entered into a tentative settlement agreement with the EC. The EC followed with a public statement the next day, calling for public comment on the terms of the agreement (the full text of both announcements appears at the end of this blog entry). Each side confirmed the following basic facts:

- As is usual in a settlement, there is no finding of guilt or innocence
- In exchange for the EC terminating its investigation, Rambus agrees to certain restrictions on its ability to profit from certain patent claims that would be infringed by implementation of the JEDEC standard.
- Interested parties will have one month to offer comments on whether the terms of the proposed settlement are appropriate. After the comment period

closes, the EC will decide whether to make the terms of the proposed settlement legally binding on Rambus.

As expected, the two press releases characterize the dynamics of the settlement in different ways, with the EC release including this interesting statement:

> Following the Statement of Objections, Rambus proposed commitments to address the Commission's concerns. In particular, Rambus commits during five-years to put a cap on its royalty rates for products compliant with the JEDEC standards.

Certainly proposing a limit on royalties is rather different than having one imposed by legal action. So why did Rambus not take a similar tack with the FTC?

Certainly proposing a limit on royalties is rather different than having one imposed by legal action. So why did Rambus not take a similar tack with the FTC?

EC vs. FTC: For starters, perhaps they did, but settlement negotiations are confidential, and I therefore do not know what Rambus may or may not have been willing to offer the FTC at some point in time in exchange for a settlement agreement. What we can tell is that the difference in terms between the final FTC judgment (later overturned) and the terms of the tentative settlement agreed upon by the EC and Rambus is rather great. The high level terms of each are as follows:

> ***EC Settlement:*** According to the Rambus press release, for five years it will offer worldwide licenses with royalty rates not to exceed 1.5% on certain memory designs, while, "Licensees who ship less than 10% of their DRAM products in the older SDR and DDR DRAM types will enjoy a royalty holiday for those older types, subject to compliance with the terms of the license." For SDR memory controllers, the 1.5% rate will drop to 1.0% after April 2010; certain other designs will bear a 2.65% per unit royalty through the same date which will then drop to 2.0%. All royalty rates are applicable to future shipments only. According to the EC release, the settlement terms also include a "'Most-Favoured-Customer' clause which would ensure any future rate reductions would benefit the whole market.
>
> ***FTC Order:*** The February 5, 2007 FTC statement announcing the final limitations that it imposed on Rambus summarized those restrictions as follows:
>
> > [W]e find that a maximum royalty rate of .5% for DDR SDRAM, for three years from the date the Commission's Order is issued and then going to zero, is reasonable and appropriate. We also find that a corresponding .25% maximum rate for SDRAM is appropriate. Halving the DDR SDRAM rate reflects the fact that SDRAM utilizes only two of the relevant Rambus technologies, whereas DDR SDRAM uses four.

At the time of the FTC decision, ZDNet.com.uk reported that Rambus was charging a royalty of 3.5% per unit for DDR SDRAM, and that industry norms would have indicated that a 1% royalty would be the market rate in a non-monopoly setting.

While the two sets of restrictions are impossible to compare closely on an "apples to apples" basis, as the devices covered, time periods, and other details vary from one to the other, the EC restrictions are certainly less punishing than those that the FTC sought to impose. Clearly, then, the risk/reward analysis that would determine fighting versus settling with the EC may have been quite different than what Rambus faced with the FTC. But then again, maybe not, since the FTC may have offered to settle on more generous terms than it required after needing to go to the burden to taking Rambus to court.

While Rambus lost in the U.S., it has now agreed with the EC to provide licenses at reduced rates not only with respect to sales within the European Union, but throughout the world. So where the FTC failed, the EC has now succeeded, albeit on less restrictive terms

At the same time, however, it is important to focus on a single word in the EC release that might easily be missed. That word is "worldwide." In other words, while Rambus lost in the U.S., it has now agreed with the EC to provide licenses at reduced rates not only with respect to sales within the European Union, but throughout the world. So where the FTC failed, the EC has now succeeded, albeit on less restrictive terms.

Choice of law, jurisdiction and venue: In all likelihood, Rambus took a variety of factors into account in deciding whether a settlement with the EC at this time, and on these terms, was a smart move. It should be recalled, for example, that with each passing year, the Rambus patent claims grow closer to their expiration dates, and competing technologies continue to be developed. In other words, patent claims are depreciating assets, and the later in their useful life a settlement occurs, the less the patent owner gives away. Similarly, with this decision, it's own licensing efforts may be more successful, and it can spend less money in litigation with vendors if those vendors find the EC-dictated terms to be good enough.

Perhaps the most important factor to be taken into account, however, is that the competition laws in the EU are quite different from the antitrust rules and case law that apply in the United States. This distinction between the rules, laws and precedents that may apply to the same set of facts from country to country, from state to state, between federal and state courts, and even between federal courts, has often been lost on those that have cited one decision over another to support their beliefs about whether Rambus should or should not be held liable for its actions in JEDEC.

Under the English common law system that the U.S. and many other nations follow, someone cannot ordinarily be held accountable for behavior unless that behavior violates written law, as interpreted in the courts (whenever relevant cases are available). Under this legal system, it is not enough for conduct to be simply unfair

or "inequitable," even if the predominant public perception is that an actual wrong has occurred. Instead, the legal system places a higher value on protecting the individual (or, in this case, a business) from judgments that may not only come as a surprise, but may seem to have been arbitrary in the absence of a statute for reference clearly defining the type of conduct that a legislature has made illegal.

In the case of the FTC, an additional set of limitations was at play, since most of the more logical causes of action that might be asserted against Rambus (e.g., breach of contract, fraud, etc.) were not available to the FTC to assert. Instead, it needed to find a cause of action under the antitrust laws enacted in the United States. This presented a more difficult avenue to pursue, as the arguments to be made were more attenuated, and the legal precedents available to the FTC to support its position under existing cases was less clear.

As famously observed by the eminent jurist F.W. Maitland, "The forms of action we have buried, but they still rule us from their graves."

The situation recalls the system that existed in England prior to the mid 1800s, when actions not only needed to violate specific laws before they could be taken to court, but law suits and prosecutions also needed to be brought under specific formal and rather arbitrary procedures, known as "forms of action." As a result, even if a party had a legal cause of action, unless there was a recognized "form of action," the plaintiff or prosecutor could not obtain the writ needed to bring its grievance before a court.

Unfortunately, the legacy of these forms of action lives on in other variously analogous ways, such as in the concept of "jurisdiction," which determines in what locations and courts a dispute can be brought, and which courts have authority over what types of claims. This can limit the ability of a court to deliver the highly desirable result of achieving finality after each side has had a fair chance to present its case, as well as the need (or opportunity) for litigants to divide a dispute involving one set of facts into different claims brought in different courts. This has in the Rambus cases, where different states have applied different laws, and federal courts have addressed patent law to come to different conclusions. As famously observed by the eminent jurist F.W. Maitland, "The forms of action we have buried, but they still rule us from their graves."

As noted above, the FTC was not able to utilize all of the causes of action that a private litigant could have brought to bear in pursuit of victory (e.g., contract and fraud claims as well as antitrust claims). This is unfortunate, because private litigants may deem it to be in their best interests to settle a hard case where the law is nonetheless on their side, while a public agency might not. Thus, while a private party may choose to fold its hand due to ongoing legal costs as compared to the economic terms offered by its opponent, a public agency has a different motivation to soldier on, in order not only to right the wrong at hand, but to make an example of the defendant as well and to set a precedent for future courts to follow.

The Bottom Line: There are other facts that Rambus doubtless took into account as well that vary in time and geography. Both Microsoft and Intel have recently learned to their sorrow that Neelie Kroes, the Commissioner of Competition of the European Commission, has found European courts to be more supportive of her claims than the FTC has found U.S. courts to be to theirs.

A decision to fight rather than settle in the EU might therefore have seemed to Rambus to be more problematic than did its decision to take the FTC to the wall.

A decision to fight rather than settle in the EU might therefore have seemed to Rambus to be more problematic than did its decision to take the FTC to the wall. And even the prospect of granting worldwide royalty commitments might seem more palatable with a new administration in Washington that has already publicly stated that antitrust enforcement will be a higher priority than it was under the reign of its predecessor.

Whether the Obama administration will in fact aggressively pursue antitrust claims, and whether the courts will support it if it does, remains to be seen. For now, those that think that individual companies have been able to get away with too much in the marketplace can take heart in their ability to look to Europe to provide aggressive antitrust enforcement in a way that they used to be able to expect from Washington.

And what of the other half of the equation - why did the EC decide to settle on what may seem to be rather generous terms? With the FTC's experience with Rambus already known, perhaps the EC concluded that going as far as the FTC had done was likely to result in a long and drawn out battle. And, as noted by Bloomberg, Neelie Kroes' term in office will come to an end in November. She may be anxious to clean out as much of her docket as she can before she turns over the reins to someone that will be entitled to establish their own prosecutorial priorities.

At the end of the day, it is unlikely that we will ever learn exactly what all went into the decision of Rambus to kneel to Neelie after consistently fending off the FTC. But to the good, and despite the fact that a settlement does not require an actor to admit fault, if the settlement becomes final we will at last have a legal ruling in place that both bends Rambus to the will of civil authority, but also provides some measure of relief to industry from the level of royalties that Rambus has to date required its licensees to pay.

And most importantly, we will finally have an object lesson for others illustrating what may happen as a result of the type of much disputed, incessantly litigated,

and certainly regrettable activities that occurred within JEDEC so many years ago.

MEMO /09/273

Brussels, 12 June 2009

Antitrust: Commission Market Tests Commitments Proposed by Rambus Concerning Memory Chips

The European Commission has invited comments from interested parties on commitments offered by microchip designer Rambus to meet concerns that it may have infringed EC Treaty rules on abuse of a dominant position (Article 82) by claiming unreasonable royalties for the use of certain patents for "Dynamic Random Access Memory" chips (DRAMS) (see MEMO/07/330). Rambus in particular is prepared to commit to put a cap on its royalty rates for the five year duration of these commitments. The cap includes a "Most-Favoured-Customer" clause which would ensure any future rate reductions would benefit the whole market. Interested parties can submit comments within one month from the date of publication. Following the market test, the Commission may decide to adopt a decision under Article 9 (1) of Regulation 1/2003, making the commitments legally binding on Rambus.

On 30 July 2007, the European Commission adopted a Statement of Objections against Rambus, a company incorporated in Delaware, USA. This outlined the Commission's preliminary view that Rambus may have infringed Article 82 of the EC Treaty by abusing a dominant position in the market for Dynamic Random Access Memory (DRAMs). DRAMs are used to temporarily store data in products such as PCs.

JEDEC, an industry-wide standard setting organisation, developed an industry standard for DRAMs. JEDEC-compliant DRAMs represent around 95% of the market and are used in virtually all PCs. Worldwide sales of DRAM chips in 2008 exceeded 34 billion US Dollars. Rambus claims its patents cover technologies included in these JEDEC standards and is asserting these against manufacturers of DRAMS that comply with the JEDEC standard.

The Commission's preliminary view, set out in the Statement of Objections, was that Rambus engaged in intentional deceptive conduct in the context of the standard-setting process, for example by not disclosing the existence of the patents and patent applications which it later claimed were relevant to the adopted

standard. Against this background, the Commission's provisional view, as outlined in the Statement of Objections, was that Rambus was abusing its dominant position by claiming unreasonable royalties for the use of its patents against the JEDEC-compliant DRAM manufacturers at a level which, absent its conduct, it would not have been able to charge.

Following the Statement of Objections, Rambus proposed commitments to address the Commission's concerns. In particular, Rambus commits during five-years to put a cap on its royalty rates for products compliant with the JEDEC standards.

The Commission considers that an effective standard setting process should take place in a non-discriminatory, open and transparent way to ensure competition on the merits and to allow consumers to benefit from technical development and innovation. Standards bodies should be encouraged to design clear rules respecting these principles. However, in a specific case where there appear to be competition concerns, the Commission will investigate and intervene as appropriate.

As required by Article 27 (4) of Regulation 1/2003, a so-called " market test notice" with a summary of the proposed commitments has been published in the EU's Official Journal on 12 June 2009. The full version of the commitments is available on the Commission's website at:
http://ec.europa.eu/comm/competition/antitrust/cases .

Interested parties are invited to present their comments within one month of the publication in Official Journal .

Under Article 9 of Regulation 1/2003, the Commission may decide to make the commitments legally binding on Rambus. Such an Article 9 decision would find that there are no longer grounds for action by the Commission, without concluding whether or not there has been or still is an infringement of EC antitrust rules.

Rambus Reaches Tentative Settlement with European Commission

Forward-looking royalty rates established for DRAMs and memory controllers

LOS ALTOS, CALIFORNIA, UNITED STATES -**06/11/2009** - Rambus Inc. (NASDAQ:RMBS), one of the world's premier technology licensing companies specializing in high-speed memory architectures, today announced that it has reached a tentative settlement with the European Commission (the "Commission") to resolve the pending case against the Company. Under the proposed resolution, the Commission would make no finding of liability relative to JEDEC-related charges, and no fine would be assessed against Rambus. In addition, Rambus would commit to offer licenses with maximum royalty rates for certain memory types and memory controllers on a forward-going basis. European Commission antitrust procedures stipulate that a final decision must be preceded by a consultation of interested third parties on the terms of the commitments offered (the "Commitment"); this consultation was initiated today.

"Our view regarding standard-setting organizations is that the rules of such organizations must be written and clear, and that there should be consequences if such clear written rules are violated," said Thomas Lavelle, senior vice president and general counsel at Rambus. "We did nothing wrong during our participation in the JEDEC standard-setting organization, as demonstrated in multiple U.S. court victories including before the D.C. Court of Appeals. With this proposed resolution, we create a new platform where all parties can move forward by licensing our patented innovations for future use in their products rather than engaging in costly litigation."

Under the proposed resolution, Rambus will offer licenses with maximum royalty rates for five-year worldwide licenses of 1.5% for DDR2, DDR3, GDDR3 and GDDR4 SDRAM memory types. Licensees who ship less than 10% of their DRAM products in the older SDR and DDR DRAM types will enjoy a royalty holiday for those older types, subject to compliance with the terms of the license. In addition, Rambus will offer licenses with maximum royalty rates for five-year worldwide licenses of 1.5% per unit for SDR memory controllers through April 2010, dropping to 1.0% thereafter, and royalty rates of 2.65% per unit for DDR, DDR2, DDR3, GDDR3 and GDDR4 memory controllers through April 2010, then dropping to 2.0%. This commitment to license at the above rates will be valid for a period of five years from the adoption date of the Commitment decision. All royalty rates are applicable to future shipments only.

Rambus management will discuss this development during a special conference call on Friday, June 12, 2009 at 6:00 a.m. PDT. The call will be webcast and can be accessed through the Rambus website. A replay will be available following the call on Rambus' Investor Relations website or for one week at the following numbers: (888) 203-1112 or (719) 457-0820 with ID# 4179468.

The European Commission originally brought charges against Rambus in August 2007 alleging violation of European Union competition law. The Commission's investigation followed complaints set forth by certain DRAM manufacturers originating with Rambus' 1992-1995 participation in an industry standard-setting organization, the Joint Electron Device Engineering Council ("JEDEC"). Similar charges had been pursued by the Federal Trade Commission (FTC) in the United States. The FTC recently closed its investigation following a series of U.S. Court rulings underlining that the allegations of Rambus' wrongdoing were ill-founded.

About Rambus Inc

Rambus is one of the world's premier technology licensing companies specializing in the invention and design of high-speed memory architectures. Since its founding in 1990, the Company's patented innovations, breakthrough technologies and renowned integration expertise have helped industry-leading chip and system companies bring superior products to market. Rambus' technology and products solve customers' most complex chip and system-level interface challenges enabling unprecedented performance in computing, communications and consumer electronics applications. Rambus licenses both its world-class patent portfolio as well as its family of leadership and industry-standard interface products. Headquartered in Los Altos, California, Rambus has regional offices in North Carolina, India, Germany, Japan, Korea and Taiwan. Additional information is available at www.rambus.com.

A new Voice for Open Source in Government

Andrew Updegrove

I'm pleased to report this morning on the formation of a new advocacy group for the use of free and open source software in the U.S. Government. I'm also pleased to have been asked to serve on its Board of Advisors, along with other proponents of free and open source software, such as Roger Burkhard, Dawn Meyerriecks, Eben Moglen, Tim O'Reilly, Simon Phipps, Mark Shuttleworth, Michael Tiemann, Bill Vass, and Jim Zemlin.

The new organization is called Open Source for America (OSA), and you can find its Web site here. Tim O'Reilly will officially announce OSA at OSCON later today, and you can find the launch press release here, as well as pasted in at the end of this blog post for archival purposes. I'm sure that you'll also see quite a few articles blossom across the Web today relating to its announcement, but having been in on the planning, here's what it's all about.

The immediate goal of the organization will be to raise awareness about free and open source software (FOSS) in government. Or, as stated in the lede to the press release, to provide, "a unified voice for the promotion of open source software in the U.S. Federal Government arena." The full version of the OSA mission can be found in the Charter document, and reads as follow:

> The mission of OSA is to educate decision makers in the U.S. Federal government about the advantages of using free and open source software; to encourage the Federal agencies to give equal priority to procuring free and open source software in all of their procurement decisions; and generally provide an effective voice to the U.S. Federal government on behalf of the open source software community, private industry, academia, and other non-profits.

Achieving that high level goal will in some ways be a pushover, in that every Federal agency already uses open source, in most cases very extensively. As noted in the press release:

> With the U.S. Federal Government increasingly focused on utilizing and adopting technologies to better serve citizens, there is growing recognition of the freedoms that open source software and open technology solutions can provide – an open, transparent and cost-effective option – for government agencies. Gartner recently estimated by 2011 more than 25 percent of

> government vertical, domain-specific applications will either be open source, contain open source application components or be developed as community source.

But promoting the pervasive and effective use of open source software in government is still an important and worthwhile mission to support, in that the spread of open source software in the public sector has been organic and initiated at the CTO level rather than considered and favored by policy-makers for the cost containment and other benefits it can bring. While there are many organizations in existence already that promote free and open source software in the marketplace to some extent, none of them has been formed to provide a focal point for promoting FOSS to government. OSA should therefore be able to provide great value not only through its own efforts, but by providing a rallying point for coordinating and leveraging the efforts of these many organizations already in existence.

That role is important, because as in private industry, many in government are not as conversant with the advantages of free and open source software as they might be. They are also, of course, just as vulnerable to having misconceptions about FOSS as those in private industry, and perhaps more so, as a result of the efforts of lobbyists. The bottom line is that all citizens will benefit from both a cost, as well as a quality, perspective if free and open source software is given equal consideration with proprietary options whenever government procurement decisions are made.

The bottom line is that all citizens will benefit from both a cost, as well as a quality, perspective if free and open source software is given equal consideration with proprietary options whenever government procurement decisions are made

Tactically, the goals of the organization are summarized in the Charter as follows:

> The mission incorporates three goals: (1) to effectuate changes in U.S. Federal government policies and practices so that all the government may more fully benefit from and utilize free and open source software; (2) to help coordinate these communities to collaborate with the Federal government on technology requirements; and (3) to raise awareness and create understanding among federal government leaders in the executive and legislative branches about the values and implications of open source software. OSA may also participate in standards development and other activities that may support its open source mission.

From what might be called a "techno-political" perspective, and after much discussion among the founders, OSA might be thought of as being "left of center," as signaled by the introduction to the "Founding Principles" to be found in the Charter. That section begins as follows:

> 1. While respecting the right of every developer to choose the license that it believes best reflects its desires and needs, we support the four freedoms in the Free Software Definition.

For those of you not already familiar with the Four Freedoms, as originally propounded by Richard Stallman, they are:

> The freedom to run the program, for any purpose (freedom 0);
>
> The freedom to study how the program works, and adapt it to your needs (freedom 1). Access to the source code is a precondition for this;
>
> The freedom to redistribute copies so you can help your neighbor (freedom 2); and
>
> The freedom to improve the program, and release your improvements (and modified versions in general) to the public, so that the whole community benefits (freedom 3). Access to the source code is a precondition for this.

Thus, OAS does not seek to override the right of any developer and any user to select the license terms that it believes are best aligned to its own goals and philosophy, but it does support those licensing models that are intended to lead to the creation of the greatest value for the community.

OAS does not seek to override the right of any developer and any user to select the license terms that it believes are best aligned to its own goals and philosophy

The Founding Principles continue as follows:

> 2. We applaud the commitment of the Administration to make the U.S. Federal government more transparent, participatory, secure, and efficient, and urge the U.S. Federal government to pursue this goal by leveraging the advantages of free and open source software.
>
> 3. We believe that the community can drive collaborative innovation in the U.S. government space, resulting in greater efficiencies and national competitiveness.
>
> 4. We believe the decision to use software should be driven solely by the requirements of the user, and not by a mandate for a particular brand, vendor, or development model.

The timing for the initiative's launch is hardly a coincidence, in light of the stated goals of the Obama administration. As I have written about at length in the past (examples can be found here and here), President Obama's commitment to open government must be implemented at the technical as well as the policy level in order to be effective. Only through the use of both free and open source software as well as open standards can government sites become accessible to all, and provide the level of interactivity required to truly realize the vision of allowing Americans to participate in their own government.

In structure and other aspects, Open Source for America will have much in common with the ODF Alliance (although, as you will see, it already has a much more credible Web site). The similarities include free participation, a broadly

representative founding membership drawn from academia, non-profits, and for profit organizations, and the strong support of leading IT companies that have already made a firm commitment to open source software and open standards. In this case, those companies include Red Hat, Google, Oracle and Sun. The full list of over 70 founding members appears in the press release, but here is a representative sampling:

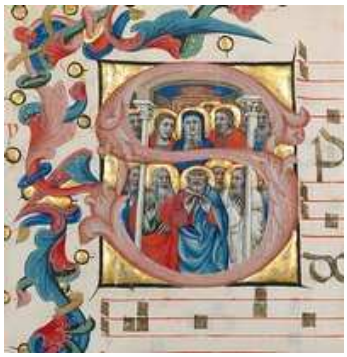
> Alfresco Software; Advanced Micro Devices, Inc.; Black Duck Software, Inc.; Canonical; CodeWeavers; CollabNet; Debian; Democracy in Action; Electronic Frontier Foundation; GNOME Foundation; ibiblio.org; Ingres Corporation; Mitch Kapor, The Linux Foundation; Mozilla; North Carolina State University Center for Open Software Engineering; Novell; Open Solutions Alliance; Open Source Initiative; Open Source Institute; O'Reilly Publishing; Oregon State University Open Source Lab; Open Source Software Institute; Institute for Software Research at UC Irvine; Software Freedom Law Center; SugarCRM; Sunlight Labs; School of Engineering, University of California, Merced; University of Southern Mississippi; Center for Open Source Investigation, Carnegie Mellon Silicon Valley; and Zimbra.

As was the case with the ODF Alliance, I expect that you will see this list grow rapidly. Membership is free and open to all, and I'd encourage you to add your, or your organization's, name to the list, as there is important work to be done. An FAQ can be found here, and the registration form here. Why not join us?

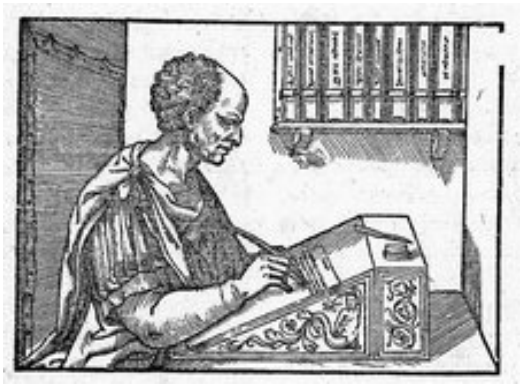
Bookmark the Standards Blog at http://www.consortiuminfo.org/newsblog/ or set up an RSS feed at: http://www.consortiuminfo.org/rss/

#59 Digitization and the (Vanishing) Arts of the Book

Andrew Updegrove



ome of the most beautiful artistic treasures created during the millennium we refer to in the Western world as the Dark Ages are books – usually of a religious nature, they were transcribed by hand in sumptuously precise calligraphy, illuminated with wonderfully colorful and imaginative borders, and graced with elegant inset illustrations that were themselves jewels of inspiration, meticulously set down with pen, brush and burnisher in inks, tempera and gold leaf on laboriously stretched and scraped sheets of parchment. When complete, these beautiful pages were bound in volumes large and small, from enormous folios that were easily read in the pulpits of candlelit cathedrals, to breviaries that nestled comfortably in the pocket of a monk's cassock. Lovingly preserved through many centuries, they are as wonderful to observe today as they were when they were fresh from the standing desks of the monks who gave them birth.



Happily, when Gutenburg reinvented movable type (first honors go to the Chinese, nearly 400 years before), the arts of the book were not lost, although as with many other crafts, artistic styles became simpler over time. Books continued to be made with fine leather bindings, though, and were often graced with the work not only of famous illustrators of the day, such as Aubrey Beardsley, Frederick Remington, and N.C. Wyeth, but of renowned artists as well. Type faces, borders and page layouts evolved under the skilful eyes and hands of artists and craftsmen who were proud to lend their talents to preserving the book as an art form. Even trade books were expected to display both clean design as well as covers that pleased and attracted the eye.

With the advent of the Internet, of course, costs of production have plummeted. Today, a design executed once can display on an infinite number of screens at no additional cost, and technology can supply a color palette hundreds of thousands of shades strong. It seems that the stage must be set for the artistic wonders of the Middle Ages to be duplicated again, not in only hundreds of books a year laboriously created across all of Europe, but in an endless number of pages crafted by the thousands of gifted individuals now able to display their talents before a waiting world at the click of a "save" key.

Except for one small detail: That hasn't happened, has it?

Indeed, fifteen years into the ever wonderful, ever widening world of the Web, we are treated to hideously cluttered home pages at news sites that seek to cram as many topics onto a single screen as are spread across the first two sections of a newspaper. Even the stylish *New Yorker*, which has lovingly preserved its original type faces and layouts in its print edition with few changes (and those of equal flair) throughout its near-century of existence, presents an on-line cover to the world that would send founding editor Harold Ross into an apoplectic fit. And this despite the fact that it is a destination site, with no need to act as a Google magnet, or any reason to fear that visitors will refuse to invest an extra click to take them another page deeper into the riches they have arrived to enjoy.

Worst of all, of course, is Google, whose Spartan presentation (calling it a style would be oxymoronic) takes the functional beyond austere to the brutally mechanistic. Try any search at the Google home page and the results will make your eyes ache. The only tiny concessions to the concept of graphic design are the corporate logo, and the pale blue divider bar spanning the top of the page. Nothing, it seems, can compare in priority to appeasing the god of fast loading speeds, or rise to the visual importance of the raw display of data.

The Google Reader is even worse – a horrible hash of grids and bars (the latter originally displayed rounded corners rather than square, but even these insignificant extravagances were eliminated in a redesign intended to shave picoseconds off of the time Reader page takes to display). Compared to the tactile pleasure of reading a well-designed book, newspaper or magazine, staring at any Google page is a spiritually deadening exercise that encourages you to flee back to the printed page as quickly as possible, thinking dark, Ludditical thoughts all the way. One can't help wondering why the marketing side of the Google house has never considered the cost to stickiness that sacrificing style for speed can exact.

Now, of course, we also have a brave new world of eReaders, with the Kindle holding pride of place among them (at least for now). Created by a book site (Amazon) expressly for the readers of books, one would have hoped that here might be found an electronic monastery within which the arts of the book might find refuge, and continue to flourish during these dark ages of digital design.

Perhaps they may yet, but for now, the situation appears bleak. The latest issue of the *New Yorker* included not so much a review as a defenestration of the Kindle's aesthetics (or lack thereof – not that the page where it displays at the *New Yorker* has the right to throw any stylistic stones). The article begins by pronouncing the Kindle screen's background color to be not just gray, but "a greenish, sickly gray. A postmortem gray" (some readers apparently find the Kindle 2's display to be even worse: "Like reading a wet newspaper," according to one dissatisfied purchaser). Nicholson Baker, the author of the *New Yorker* review continues:

> This was what they were calling e-paper? This four-by-five window onto an overcast afternoon? Where was paper white, or paper cream?...Where were sharp black letters laid out like lacquered chopsticks on a clean tablecloth?

Hardly a feast for the eyes, but at least all of the book is there to be read and appreciated, yes? Well, yes and no. According to Baker, what the Kindle is incapable of reproducing is as worrisome as what it can. The technology and standards that Amazon has taken the trouble to utilize and support are apparently not up to the challenge of displaying much more than block text, and in a limited number of fonts, at that. Baker goes on to note:

> But say you've actually found the book you're seeking at the Kindle Store. You buy it. Do you get what's described in the catalogue copy? Yes and no. You get the words, yes, and sometimes pictures, after a fashion. Photographs, charts, diagrams, foreign characters, and tables don't fare so well on the little gray screen. Page numbers are gone, so indexes sometimes don't work….
>
> When you buy the Kindle edition of Konrad Lorenz's "King Solomon's Ring," rather than the paperback version, you save three dollars and fifty-eight cents, but the fetching illustrations by Lorenz of a greylag goose and its goslings walking out from the middle of a paragraph and down the right margin are separated from the text—the marginalia has been demarginalized.

And what of the new Kindle DX, purpose built for newspaper and magazine display? Does it preserve the aesthetics of the newspaper experience, and deliver the multivarious pleasures of reading a quality paper? Sadly, no. Baker concludes that reading the news on the Kindle DX can be enjoyable, but only, "if you like reading Nexis printouts." In converting the physical page to the virtual, most of the endearing bits of the baby have, it seems, been thrown out with the bathwater:

> The Kindle *Times* ($13.99 per month) lacks most of the print edition's superb photography—and its subheads and call-outs and teasers, its spinnakered typographical elegance and variety, its browsableness, its Web-site links, its listed names of contributing reporters, and almost all captioned pie charts, diagrams, weather maps, crossword puzzles, summary sports scores, financial data, and, of course, ads, for jewels, for swimsuits, for vacationlands, and for recently bailed-out investment firms. A century and a half of evolved beauty and informational expressiveness is all but entirely rinsed away in this digital reductio.

an we guess why the visual arts have been so roundly ignored online? Bandwidth is hardly an adequate answer, given the amount of flash and video that increasingly clutter up sites of all types. Is it the fact that the Web has yet to attract graphic designers to take the hard edges off of html? If so, it would be hard to blame them, as a single Web page is so ephemeral and evanescent as to scarce warrant their attention. Or maybe it's because no one has bothered to create standards to make the display of graphic arts possible other than as amateurish, cut and paste building blocks.

Or perhaps it is that artists realize that we don't spend enough time on any given Web page to really notice a good piece of design. But what if, in fact, it's because they suspect that we simply do not place the same value on art and design in our everyday lives that we used to, as Google seems to think?

I hope that's not it, as it would be a sad day indeed when (if indeed it has not happened already!) the pleasurable practice of reading degrades finally into a utilitarian process of simple data acquisition on the fly. Reading can, after all, provide such an island of peace in the middle of our hectic lives that we should treasure all aspects of the experience, and not let the subtle appeal of well-conceived and executed page designs, attractive fonts, small, welcome embellishments, and careful color schemes pass away forever, unnoticed and unmourned, from the presentation of text.

But perhaps I am over-reacting. Perhaps we are simply transitioning through a necessary interregnum during which the basic electronic engineering work must be done to permit digital media to display (even) in elemental form, after which artists (yes, and marketing folks) will stream back into the process, and insist on leaving their creative marks upon our Web pages and our eBooks. After all (I hope), what else can they do, as the virtual continues to bully the physical out of its aggressively greedy way, and into extinction?

Is there an historical precedent for that expectation, or is it simply a vain hope that I harbor? As in so many other subjects, Thomas Jefferson may have left us a piece of fundamental wisdom that may guide us even in time like these. After the revolution, he reflected on the hard work and pragmatism demanded of the founding fathers in order to enable them to give birth to a new nation.

He summarized their sacrifices and hopes thusly: "We are soldiers, so our children can be farmers, so their children can be artists."

Perhaps in these still early days of our midwifing a brave, new digital world into existence, it is fair to grant that perhaps we must be software engineers first, so that our children can have the excitement of reinventing publishing online, so their children can be the artists that once again bring the ancient arts of the book back to the words of the future.

Read more *Consider This***...** entries at: http://www.consortiuminfo.org/blog/

Sign up for a free subscription to ***Standards Today*** at

http://www.consortiuminfo.org/subscribe/2.php?addentry=1

All images are in the public domain, and appear courtesy of the Wkimedia Commons, a project of the Wikimedia Foundation: http://commons.wikimedia.org/wiki/Main_Page