ACM US Public Policy Council

June 18, 2011

The Honorable Mary Bono Mack, Chairman
Subcommittee on Commerce, Manufacturing and Trade
House of Representatives
2125 Rayburn Office Building
Washington, DC 20515–6115

Dear Representative Mack:

Enclosed are my responses to your questions-for-record of June 6, 2011, following the May 4th hearing on "The Threat of Data Theft to American Consumers."

Thank you again for the opportunity to testify on this important topic. I would like to reiterate both my personal interest and willingness to provide further support on this issue, and that of the USACM Council. Should you have any questions or need additional information, please contact me or Cameron Wilson, our Director of Public Policy, at 202-659-9711 or at Cameron.wilson@acm.org.

Regards,

Eugene H. Spafford, Ph.D.
Chair, U.S. Public Policy Council
Association for Computing Machinery

cc: The Honorable G.K. Butterfield, Ranking Member
Subcommittee on Commerce, Manufacturing and Trade

Encl.

ABOUT ACM and USACM

With 100,000+ members, the Association for Computing Machinery (ACM) is the world's largest educational and scientific computing society, uniting computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. The ACM U.S. Public Policy Council (USACM) serves as the focal point for ACM's interaction with U.S. government organizations, the computing community, and the U.S. public in all matters of U.S. public policy related to information technology.

1828 L Street, NW Suite 800
Washington, DC 20036

USACM.acm.org

202 659 9711 *tel*
202 667 1066 *fax*

1) Is it possible that all companies could be the victim of a criminal breach regardless of security measures?

No set of security measures can guarantee that there will be no criminal breach. Even if an organization does not have its computers connected to the Internet it is possible for a corrupt insider to expose some of the data, or for a physical theft of storage media to occur. These kinds of exposures happen even in the most tightly controlled environments, such as the U.S. defense community and law enforcement (e.g., the Wikileaks exposures, and espionage by Aldrich Ames and Robert Hanssen).

Strong security measures can be instituted to protect against malicious insiders, against theft of media and equipment, against eavesdropping of communication, and other non-software threats. Security measures can also be put in place to provide extra protection for on-line storage of data. Policies, training and technology can also be deployed to minimize the risks of user errors that may result in a breach.

However, there is a significant cost associated with some of these methods, especially if multiple defenses are layered to provide greater assurance. The more safeguards that are deployed, the greater the cost to put them in place and maintain them, and (often) the greater the burden placed on legitimate operations. There are no good metrics for security or risk to know how many safeguards are "enough" and where the weakest points might be. Thus, most organizations have some residual risks and potential exposures.

Nearly all software in use today has flaws and design weaknesses that may be exploited to gain unauthorized access. Vendors have not been held accountable for poor-quality code or lack of security features, and clients are often at the mercy of whatever is provided to them because of the terms of sale and licenses. They are further restricted by Federal laws such as the DMCA (Digital Millennium Copyright Act, PL 105–304), that make it illegal to use reverse engineering to determine what may be in licensed code — Federal law thus protects poor design and dangerous (even malicious) practices by vendors. These factors help ensure that most existing systems have flaws — discovered and yet to be discovered — and new systems will also likely be flawed, and thus vulnerable.

Accidental breaches are not uncommon, and organizations may be subject to exposure in this way, too.

It is because of all these residual risks that I presented, in my original testimony on May 4, USACM's 24 Privacy Principles. All of these principles, if embraced, will reduce the exposure and damage caused by any breach that does happen, and many will help reduce the likelihood of a breach.

2) Is it safer or less safe for companies to move personal information to cloud computing storage versus storing it on proprietary servers?

This question has multiple answers. "Cloud" has many different forms: there are different modes of deployment (public, community, private, hybrid) and different models service (IaaS, PaaS, SaaS; respectively, infrastructure, platform and software "as a service). "Safe" can also be construed in different ways — is the permanent loss of data from a disaster more or less safe than exposure of some of the data from a criminal breach? Furthermore, many cloud providers use proprietary technologies (hardware and software) to host their storage offerings, so that aspect is not necessarily meaningful.

Considering the answer to question #1, note that protection and safety are ongoing efforts that have a continual and often substantial cost and labor component. Maintenance of the physical system and its security, software patches, defensive measures, personnel screening, and other issues need to be continually monitored and upgraded. For many organizations of all sizes, there is neither the expertise nor budget available to do these things on an ongoing basis. In these cases, outsourcing some of the storage and operations to a cloud service could be an improvement over in-house operation. However, for organizations with greater resources, it may be more reasonable to maintain internal systems with local operation and supervision (which could include a private cloud).

Cloud systems also introduce some new vulnerabilities. A cloud is a huge, tempting target. Vendors use software (usually called hypervisors) to manage resources and give each customer the illusion of having private resources. This software is another point to be attacked; the fact that malicious actors can become customers of the same cloud makes it easier. The relative weight of cloud-caused advantages and vulnerabilities is difficult to assess, and no doubt situation specific. Neither approach can make a decisive argument for being more secure.

Whatever factors may be involved, it is also important to note that the security of any storage depends greatly on the provider. If a cloud provider does not have adequate physical and logical security, the data resident on that storage will be at risk. It is also necessary to properly secure the communications between the clients and servers to prevent eavesdropping, and to institute appropriate safeguards at the clients to prevent breaches. A recent study by the Ponemon Institute indicated that most cloud providers believe it is the responsibility of the client to provide data security, while clients believe it is the responsibility of the cloud provider. This mismatch suggests that neither side may currently be providing the level of protection that is really needed.

Using cloud storage requires caution and a careful examination of the risks. In-house data storage can be secured by a variety of known technical approaches, such as air gaps (not connecting systems to any networks), firewalls, and data diodes (systems that only allow one-way communications). These and similar measures can reliably prevent or control outside access, but they are not applicable to any remote storage. The need for remote data protection forces significant reliance on cryptography.

Modern cryptography provides some protection, but is not a panacea as it is widely abused and misunderstood, resulting in substantial vulnerabilities. First, the keys to the ciphers are high value targets. Clouds are accessed over networks (most often the Internet) and the keys are therefore network-accessible, and thus subject to both technical attacks and social engineering attacks against operators. Second, user accounts that have access to the data may be subverted, negating all storage-level protections. Third, applications and hardware may be subverted (including supply chain attacks) to provide access to unencrypted data at both the client and server.

There are other avenues of exposure and breach beyond the access to storage. For example, some business partners may create specialized data sharing portals to support B2B (business to business) activities. If one of those partners has poor security practices, the B2B portal may serve as an avenue of penetration to a much more secure partner. Storage of data in a cloud system may enhance security by allowing sharing while obviating the need for a portal. However, if there is a mix of portals and cloud storage, weaknesses in the portal may enable attacks against the cloud storage.

Another factor to consider is the physical, legal locale of the storage. Data that is stored on systems may be discoverable (or deleted, altered or disclosed) based on legal proceedings local to that cloud provider. The client also needs to worry about bankruptcy or financial judgments against the cloud provider that may result in the storage being sold or confiscated. In cases such as this, it is possible that the information on the disks could be sold or revealed as a side effect. In these instances, having strong encryption of the data with the cloud provider having no access to the keys may provide some protection, but as noted above, encryption may not be sufficient. Large organizations already confront these issues when choosing data center sites, and cloud vendors may offer some control for those who demand it. The real problem is that in conventional systems these concerns are more visible; the very ease of setting up cloud-based systems makes this and many other real difficulties simple to overlook.

Last of all, security is something that must be managed in an ongoing fashion. Thus, movement of data to a cloud storage location may be safer now, but as time goes on might be degraded if the cloud provider fails to adequately invest in, and maintain, appropriate defenses.

3) You testified you support legislation that would apply to all entities that collect personal information, including government. Do you think the government is ahead, equal, or behind the private sector in data security practices? Is there a difference between the different levels of government? How do the data security practices of universities and other non-profits compare to the public and private sectors?

"Government" may mean everything from a town of 300 to the National Security Agency. The resources of these entities are very different, as are the data, applications, and threats. Thus, it is possible to say that "government" is both behind and ahead of the private sector, depending on the definition of "government."

More specifically, protection of data is a function of many factors, including authority, budget, available resources, personnel, training, and risk. Most smaller governmental units do not have adequate resources or awareness of the threats and risks. As such, their systems are usually poorly protected. The same is true of some Federal agencies. Mid-sized governmental units (larger cities, most states, many Federal agencies such as NASA, FCC, etc.) may have better security, on average, than the median commercial entity, depending on their clientele and resources. Larger governmental units with high-level awareness of risk (largest cities, some states, national laboratories, Federal agencies such as NSA, FBI, etc.) are likely to have better security than most commercial entities.

NGOs and universities have different data protection needs than some public agencies. They also require a different level of access to resources. Thus, some smaller non-profits and educational institutions may have minimal security in place, and most of that is focused on only a portion of their mission. Other organizations that are frequent targets of attack, and universities with a strong local presence in computing, are likely to have stronger defenses in place. Some of these defenses are as good as those of a major Federal agency or large city.

There is no single, best answer to this question because there are no standards or metrics for security. Organizations often do not have a firm grasp of the risk to their operations and data, and even if they do, they are unable to tell when they have invested "enough" in defenses. Thus, they often do not deploy adequate resources to counter widespread and common threats. Standards and metrics for cyber security is one area sorely in need of more research and study.