Response to Request for Information

April 5, 2013

U.S. Department of Commerce
National Institute of Standards and Technology
Developing a Framework to Improve Critical Infrastructure Cybersecurity

Submitted by:
Digital Management Inc.
6550 Rock Spring Drive, 7th Floor
Bethesda MD 20817
Phone: 240-223-4800
Fax: 240-223-4888
www.DMInc.com

Submitted to:
U.S. Department of Commerce
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899
Email: cyberframework@nist.gov

Table of Contents

Table of Exhibits

1 Introduction

1.1 DMI Overview

Digital Management, Inc. (DMI) is a leading information technology (IT) solutions and business strategy consulting firm with a global reputation as a thought-leader in mobile solutions and next-generation cybersecurity solutions. We are a member of the Board of Directors for the Trusted Computing Group (TCG), an international standards body dedicated to developing, defining, and promoting open, vendor-neutral, and global industry standards supportive of a hardware-based root of trust for interoperable trusted computing platforms. DMI is co-chair of the TCG Trusted Platform Work Group and Mobile Solutions Work Group, co-chair of the TCG Embedded Systems Work Group, and co-chair of the TCG Software Stack (TSS) Work Group.

DMI provides security strategy, architecture, and solution services to the Department of Defense (DoD), the Air Force, and some of the largest technology companies in the world. Our clients rely on us for advanced security solutions being deployed on millions of devices around the globe. DMI is committed to implementing industry best practices and standards for process improvement, security, and quality management. DMI's certifications are listed in **Exhibit 1**.

Exhibit 1. DMI Certifications

Certification	Level	External Audit Date	Authority
CMMI-DEV®	Level 3	November 2012	Software Quality Center (SQC)
CMMI-SVC®	Level 3	December 2012	Software Quality Center (SQC)
ISO 9001:2008	Certified	April 2012	ABS Quality Evaluations (ABS QE)
ISO 27001:2005	Certified	April 2011	ABS Quality Evaluations (ABS QE)
ISO 20000-1:2011	Certified	January 2013	SRI Quality System Registrar

1.2 Foundational Components of a Sound Cyber Ecosystem Framework

DMI firmly believes that, as a country, we cannot accept that our devices and networks are indefensible. DMI has the tools and skills required to protect our computing devices and networks; it is a matter of following through with smart, prioritized, foundational investment and implementation.

To adequately defend our nation, we need a cohesive, comprehensive foundation of trust in our devices and in the information shared between those devices. Systems and networks fail as a result of local vulnerabilities exploited by an attacker, such as vulnerabilities found on individual devices. Any future cybersecurity framework should therefore encourage development of an ecosystem that depends upon the trustworthiness of the local devices that comprise that ecosystem, and then encourages trust to be built into those local devices. This concept of trust is the very foundation for a secure future cyber ecosystem. Trust is inclusive of authentication, for you cannot trust something you cannot properly identify. If we can identify and trust the devices we use, we can trust the information they present and the source it comes from. Without trust,

Device Trust versus User Trust

Historical precedent implies that proper user authentication is the basis for a sound ecosystem, but that premise ignores the fact that malware doesn't infect humans, it infects device software. Therefore, in any network connection or online business transaction, it is the device itself that needs authentication first, before any user authentication can be taken seriously. In today's networked world of untrusted devices, malware can make any device lie about the validity of the device itself or the user operating it. We need to advance to a place where a device itself can be trusted, the software running on it can be verified, and the user can be authenticated and trusted. This order of precedence is a foundational tenet for a sound cyber ecosystem.

there can be no effective, scalable solution for authentication, interoperability, or automation.

We must embed and utilize trust at the hardware level. With current software solutions, our enterprise devices and networks are left susceptible to software-based viruses and malware, and software will likely always be vulnerable to attack. With hardware-based security we can know with certainty that devices and systems are performing as expected because hardware is not susceptible to spoofing and manipulation the same way software is.

Through a combination of standards-based, hardware-based trust anchors ("Roots of Trust"), and software and security protocols and processes that rely on those trust anchors to function, we can prove a computer or device is operating as expected, and deny access when it is not. This is the concept of device and system integrity, a concept we wholeheartedly believe is the foundation for a secure cyber ecosystem. These principles are embodied in the trusted computing standards developed by the TCG.

2 Response to Questions

2.1 Current Risk Management Practices

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

Any organization that commits to securing itself does not have to look hard to find expert guidance to appropriately manage its risk. The greatest challenges are usually money, time, resources, or competing policies and interests. The private businesses that own and operate most of the U.S. critical infrastructure are money-earning ventures focused primarily on profitability and are either unable or unwilling to sacrifice significant bottom line results for the greater good. Some of these companies make very large profits, yet still do not commit to or invest in security as much as they could.

Further, lack of coordination (both in the public sector, which provides guidance to critical infrastructure, and in and among U.S industry as a whole) results in inefficient use of already scarce time, energy, and money. The NIST Framework is a promising first step in providing a united vision, roadmap, and guiding principles for coordinated cybersecurity efforts.

Finally, each critical infrastructure industry has its own unique cybersecurity challenges as described below.

- **Healthcare needs budget and resources (i.e., people).** Healthcare companies have historically had small IT departments and sparse cybersecurity resources. Today, they have become more compliance-focused with Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health (HITECH) requirements but are still not mature from a comprehensive risk approach perspective, especially with regards to the healthcare-related "Internet of things"; for example, Internet-connected medical devices and wireless tablets used in patient care and medical administration. One of the primary business risks to the healthcare industry is availability. It is critical for doctors to be able to have ready access to medical information and patient records to make quick decisions to save lives. Failure to have such access increases risk to the patient, the doctor, and the medical institution. This leads companies to make technical decisions that provide easier and easier access to data. For example, paramedics now take pictures with a tablet to send to doctors over Dropbox so the paramedics can be given

instructions to best treat, move, or transport a patient in the field, which helps save lives. Unfortunately, it does not necessarily introduce sufficient technology to protect the privacy of that exchange; however, in a resource scarce environment where investments are driven by risk-based business decisions, saving a life is a higher priority to a hospital's business than the risk of having to pay a fine for non-compliance, a security breach, or an inadvertent disclosure.

Of all industries, healthcare could best be served with additional guidelines and incentives to better secure data and the growing number of Internet-connected devices, as well as more interoperable solutions to securely share with other healthcare systems. Proper incentives may drive budget decisions needed to implement relevant security controls and monitor and respond to incidents.

- **Financial Services needs support for mid-sized and small organizations.** The large financial institutions are leaders in risk management, and their increased cybersecurity maturity over the years has forced criminals to focus on compromising customers directly, mainly through capturing user credentials that enable theft via direct access to customer accounts.

  Today, large banks are learning a lot about defending against distributed denial of service (DDOS) attacks, and recognize that like securing their online banking infrastructures a dozen years ago, addressing DDOS attacks cannot be accomplished through a cheap or quick fix. DDOS mitigation is complex and requires planning and trial and error. It involves not just network saturation, but application-level targeting as well. Large banks are starting to make the needed investments to address this class of attacks.

  The real problem in this sector is that smaller financial institutions do not have the budgets or experience to protect themselves. While procedures, processes, and guidance exist, and the information sharing structure in place is one of the best across industries (through FS-ISAC), smaller entities simply have fewer resources to fully implement and use the tools available.

- **Energy, Water, Gas, and Oil Sectors need innovation and modernization by Operational Technology (OT) vendors.** North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards are in place to ensure computer automation systems and communication networks, which are essential to the reliable supply of electric power to the nation, are reasonably protected against attacks from a range of credible threat sources. However, NERC CIP compliance is only one sector tool, merely a "minimum standards" checklist, similar to Federal Information Security Management Act (FISMA) or PCI DSS, to ensure companies are doing something instead of nothing. The NERC CIP guidelines are not comprehensive—they do not focus on overall risks. Of the 3,200+ energy companies in the country, these guidelines only apply to the small percent that are energy generators or transmission companies and are actually audited for NERC CIP compliance. Further, NERC CIP guidelines are very prescriptive, which makes it challenging to do what is necessary or appropriate for a given environment. One size does not fit all. Even with a clean audit of all compliance areas, an organization still is not assured of security, for compliance does not equal security. This is demonstrated in the long list of PCI DSS-certified merchants and card processors breached in the last six years, and Federal agencies compromised with FISMA-compliant systems.

The largest problem for these sectors is the significant gap in built-in security solutions in Operational Technology (OT) vendors' products. Historically, control system vendors have pushed back on introducing security enhancements into their systems by, for example, voiding warranties or denying further technical support if a company adds an anti-virus program to its platform. We believe NERC, Federal Energy Regulatory Commission (FERC), and major Independently Owned Utilities (IOUs) acknowledge the current situation is providing insufficient security, want to implement improvements, and know what improvements are necessary. Vendors will have to make significant investments to modernize their systems, introduce secure architectures, and evaluate and test their components on legacy systems—that is, systems they did not previously anticipate their products having to support. With only a small handful of vendors supporting the entire international energy sector, we need to provide incentives or subsidies to encourage the OT vendors to make the necessary modernization investments. The same holds true for water, gas, and oil control systems vendors.

Additionally, energy market trading applications have become a new challenge for this sector. These large, complex applications direct very sensitive instructions to the largest machine in the world: the North American power grid. While Financial Market trading systems have been tested regularly for more than ten years to prove a robust level of security, Energy Market Trading systems have not. Standards and guidance to better protect those critical applications is needed.

- **Chemical companies need education, budget, and resources.** Plant control systems suffer from some of the same issues noted above, but the biggest risk to chemical companies is loss of intellectual property. Lessons from energy, oil, gas, or any large manufacturing industry must be better understood and applied in this sector. A lack of financial and other resources is a significant challenge. *Telecommunications Companies (Telcos) need freedom and compensation to block in the cloud and share threats with customers*. Telcos understand the threats and can protect themselves. They also can and are willing to protect their customers when paid to do so. Telcos oversee the backbone of the Internet and can identify the presence of DDOS, or worm propagation, and other network-based threats before they impact a large number of targets. However, as regulated entities, they cannot share this information broadly to help others protect themselves. When the Telcos have had the means to block threats in the cloud, they have also shown a willingness and ability to work together with other Telcos to dissipate a worm infection or DDOS attack. Unfortunately, this type of coordination is a rare occurrence, primarily because there are few to no financial incentives to repeatedly coordinate blocks. Telcos believe their unique capabilities to identify and address threats in the cloud are profit-generating business assets, not simply tools for the greater good.

  Telcos could be the key to Internet security; better than anyone else, they can help identify and mitigate DDOS against our banks, they can watch who is accessing our power systems, and they can trace the exfiltration of data from companies back to the source. They know when known bad actors are present on the Internet backbone, and they can monitor the resulting behavior. Currently, there are valid privacy, civil liberties, and local and international laws to prevent the Telcos from doing so. However, these laws need to be reassessed to strike a balance between the rights they were intended to protect, and the security needed to protect our citizens from new threats that have emerged since those original protections were put in place.

- **Defense Industrial Base (DIB) is doing best, but mid-sized and small companies need support.** Large aerospace companies are leaders in defense against current advanced threats. They understand the concept of security intelligence analysis, tracking the adversary and learning their tactics, and focusing more on the behaviors of intrusions than on implementing layers of security vendor tools. Large DIB companies are also mentoring companies from many other industries who have recently suffered from presumed nation state intrusions. Only the top dozen or so DIB companies have sophisticated capabilities. Unfortunately, there are still hundreds to thousands of smaller defense contractors who are also targets, many of which partner with the larger companies. Adversaries know these small companies do not have the budget or experience to protect themselves, and they know how to use these companies as conduits to the larger ones. The knowledge is out there for medium and small companies to learn and implement protections; they just do not have the resources to do so.
- **IT Sector needs education.** Like that of the chemical industry, stealing of intellectual property is the biggest threat to the long-term economic viability of IT sector companies. Some of the largest companies in the sector understand advanced persistent threats and recognize they are being attacked and infiltrated; however, most do not. Many IT companies do not believe their data is being stolen because they cannot "see" it being taken, and of those that do understand the threat impact, most do not have the budget or resources to sufficiently protect themselves.

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

First, we need to define and socialize the difference between risk and security. We do a lot of things to feel "secure" that do not reduce our risks. Many of the "check-box" security frameworks used today make us feel more secure, but we have seen that they have not really reduced cyber risks to the degree we would expect, as is evidenced by "certified" organizations continually being compromised. We know one size does not fit all for security, but what we need to understand is what aspects are transferable and what is unique to each company. For instance, guidance like the SANS 20 Critical Controls applies to everyone, but how an organization implements those controls will be different [CSIS, 2013].

Business risk is about confidentiality, integrity, or availability (CIA). The controls to protect from each of these are different, and how an organization monitors and responds to attacks against each of these areas is different. The threat actors might be the same, and their entry methods might be the same, but the goal of the intrusion might be different, and ultimate exploits might be unique. An adversary can use a spear phishing email to compromise an endpoint in order to steal user credentials that provide access to a database, from which the adversary then exfiltrates data. The adversary could also delete or corrupt that data, or use that data to gain the necessary knowledge to access yet another data source.

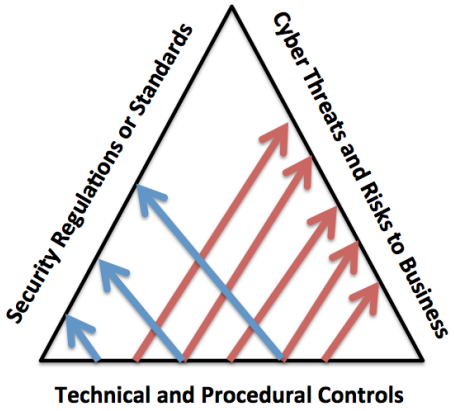
Most industries have blended risks and priorities such as protecting intellectual property while providing for sufficient availability of applications serving their customers or manufacturing plants. A loss or threat to either of those could impact business. The challenge in a unified framework is properly incorporating risk modeling that is focused on the value of an asset—the value of data, of a business process, of loss of future revenue, etc. We recommend articulating a risk-based approach that establishes the value, likelihood, and impact of security events, and developing standards that call out controls for each of the three (CIA), incorporating the risk-

based approach to best prioritize those controls. For a commercial business, it does not make economic sense to spend $100 for controls to protect $10 worth of business impact; a risk-based approach would support these sound decisions. Outside of the most mature organizations in finance or DIB, many companies are not quantifying risk effectively and in that manner. Instead, companies spend money on security protections based on trends or fear bred in the media, not on what would affect their businesses. The formalization of and education on how to quantify risk would be universal to all industries.

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

Our organization is not subject to significant regulatory requirements; however, we do maintain ISO 20000 and ISO 27001 certifications. We consider these business discriminators that most mature systems integrators must maintain. They are also a requirement to bid on specific types of work. It is therefore a risk to our business to lose our certifications. There are some business controls specifically implemented to support our compliance, but we do not use compliance as the benchmark for the entire program. We face a number of broad cyber threats and risks, which are the primary focus of our security program, as illustrated in **Exhibit 2**.

Exhibit 2. Two Drivers of Business Controls

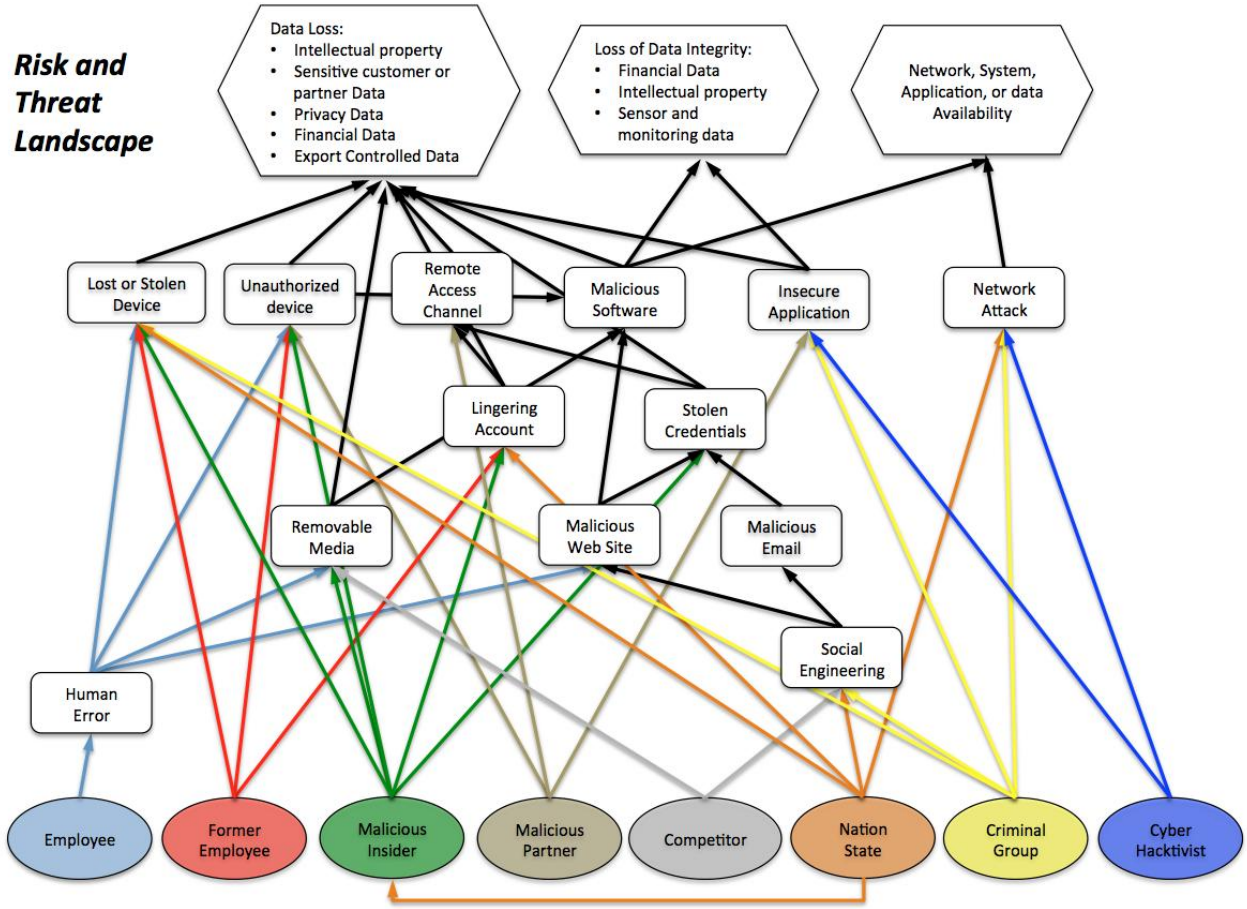


Internally we have established a Management Review Board (MRB), consisting of executives from all parts of our business, which reviews all risks and assigns business relevance to determine whether we mitigate, transfer, or accept a given risk. It is not the responsibility of the Chief Information Security Officer (CISO) to determine the risk or how to manage it; the CISO just presents the risk and the likelihood and the impact, and suggests how that risk might be mitigated, transferred, or accepted. The MRB determines the path. This approach ensures decision-making separation between technical experts and business strategists to ensure a balanced and optimally risk-informed decision.

New risks are identified by constantly monitoring the current and looming threat landscape, considering which threats are most prevalent today and which are most prevalent in our industry. What feeds this process is information sharing among our peers, and access to the best sources of security industry news from around the world. We also regularly assess current threat actor capabilities. Finally, on a quarterly basis, we map all this combined threat environment information to what events could impact our business.

Our business is information based, so our impacts relate to protecting data. **Exhibit 3** identifies our data risks at the top, and the threat actors at the bottom. The threat vectors are in the middle, linking the actors to the impact.

Exhibit 3. Business Model for Linking Actors to Impacts



We review and update this view quarterly based on newly learned attack methods or threat actors. We also include risks based on new threats we have experienced first-hand. These threats are then cataloged into a risk register where we determine and track the probability and impact of the threat if left unmitigated, describe technical and procedural controls to mitigate the threat, and list the probability of and impact to the mitigated threat for ongoing tracking. The risk register is more granular than the graphic above. For instance, things like DDOS and Ransomware are sub-categorized under Network Attack and Malicious software. Each risk is also mapped to ISO 27001 areas, showing how risks and technical controls link to ISO 27001 process requirements. Risks are categorized by frequency, the security challenges faced by the business and our industry, and by potential threats that could impact our business. Measures of probability and impact are assigned to develop an overall risk rating for each risk. That risk rating is what drives prioritization in addressing, managing, and remediating security risks within our organization.

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

Unfortunately, most organizations locate the cybersecurity risk management function in their IT departments, buried deep under the Chief Information Officer (CIO) function. The right place to locate this function is as a peer to the CIO and part of the management process. In our organization, the CIO and CISO are peers reporting to the Chief Executive Officer (CEO). The cybersecurity and risk management role needs to be part of the C-suite, close to the Chief Operating Officer (COO)/CEO, to ensure cyber threats are articulated to business leaders "in their language" on a regular basis to inform business decisions that directly impact business risk.

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

Most organizations have separate metrics and procedures for each, and rightly so. But what they do not do is correlate the two, considering cyber risks as part of overall business risks. This is likely because cybersecurity risks are viewed as an "IT-only" risk area. Because the IT function is not usually "business aware," cyber risk calculations are therefore not based on overall business impact. Rather, risk calculations mistakenly become more about keeping IT systems running and stable, not accounting for or reflecting a security prioritization that escalates those systems supporting the most critical business functions or holding the most sensitive data.

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

It should be integrated as we describe above, but most organizations do not incorporate cybersecurity risk into their overarching enterprise risk management practices. Instead they incorporate cybersecurity risk into the IT risk function. Most companies mistakenly view cybersecurity as a means to protect an IT infrastructure, when they should be viewing cybersecurity measures as a way to protect the overall business from risks stemming from having an IT infrastructure.

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

Everything builds from knowing what you have to protect, where it is located, how valuable it is, and for what period of time it has value. Usually organizations are using out-of-date or unrelated frameworks. ISO 27001 has not been updated since 2005; FIMSA is being updated, but keeps in legacy controls. Using Six Sigma or Information Technology Infrastructure Library (ITIL) provides process efficiencies and performance improvements, but does not improve security. Many organizations simply use what they are familiar with, and though these are relevant in measuring the improvements of your security model, they themselves are not the security management model. Further, many organizations focus on the newest and most exciting threats, instead of hardening their security foundations in asset management, configuration management, and vulnerability management.

The SANS 20 Critical Controls is the best model that covers all areas [CSIS, 2013]. Australia also has a Top 35 Mitigation Strategies model, which is similar to SANS and is equally sound [Strategies, 2013]. Organizations would benefit from implementing the SANS 20 Critical Controls or the Australian Top 35 Mitigation Strategies. Australia published that four of their 35 mitigations have been found to stop 85% of threats [Strategies, 2013].

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

These are very well known, and depend on the industry. However, many of the requirements are relatively high level, and not necessarily effective at improving real security. Being compliant does not mean achieving sufficient security.

All industries have to comply with state breach disclosure laws (though they are different for 47 states). If a company has offices in the European Union (EU), it is also subject to the Data Privacy Directive. A large multinational financial institution, for example, has more than 160 national and international regulations to follow from GLBA, SEC, FDIC, OCC FFIEC, to BASEL, and other foreign country specific requirements. The Federal Government is subject to FISMA or DoD Information Assurance Certification and Accreditation Process (DIACAP); Merchants and Card processors are required to follow PCI DSS; Energy Power generators and transmitters have NERC CIP compliance requirements to follow; Healthcare has HIPAA/ HITECH privacy requirements to follow; and educational organizations are subject to Family Educational Rights and Privacy Act (FERPA) privacy requirements.

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

Energy and communications are critical to all businesses; water and transportation affect employees directly and therefore indirectly affect businesses. The financial critical infrastructure affects everyone.

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

Usually organizations measure the wrong things, like number of events or number of vulnerabilities. The best metrics are immediately actionable; for example, 10 of something is okay, but 11 requires you to pick up the phone. Several metrics of greatest importance to our organization are: percent of endpoint operating systems up-to-date, percent of endpoints with correct and up-to-date security software, uptime of security sensors on the network, hours of security-related downtime, and percent of security technology in place and functioning.

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

We are not subject to requirements applicable to this question.

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

Standards and standards organizations should provide frameworks to ensure the scope of security measures are adequately covered, but should not provide prescriptive direction as to how to secure specific areas or industries. Area- or industry-specific guidance should be developed by the particular area or industry; how it should be implemented should be left for each company to determine.

Additionally, it is extremely important that all standards development efforts are inclusive of many industry perspectives, and are vendor-neutral in their recommendations. Vendor-neutral standards developed by numerous entities increase interoperability, improve security automation, and serve the public good by providing variety in solutions, all while continuing to fuel free enterprise and innovation.

2.2 Use of Frameworks, Standards, Guidelines, and Best Practices

What additional approaches already exist?

Existing standards and publications we think are most relevant include the Trusted Computing Group's (TCG) standards for the Trusted Platform Module (TPM), PC Client, Trusted Network Connect (TNC), and Architecture; SANS Security Controls; several NIST documents including Special Publication (SP) 800-147, SP 800-155, and the draft SP 800-164; Security Content Automation Protocol (SCAP) specifications and related emerging information sharing protocols; and Internet Engineering Task Force (IETF) standards such as Transport Layer Security (TLS) and IP Security Protocol (IPSEC). Each of these approaches provides a standardized solution set to a subset of the overarching cybersecurity problem.

For example, as previously described, foundational tenets for a sound cybersecurity defense include device identity and integrity grounded in a hardware root-of-trust (HROT). The TPM 2.0 HROT standard published by the TCG covers establishing a secure hardware foundation for a wide range of devices from servers to PCs to laptops to tablets and smartphones to embedded systems. Network access by trusted (as well as legacy, untrusted devices) can be controlled effectively using the TCG's TNC standard. NIST guidelines for e Basic Input/Output System (BIOS) integrity and BIOS integrity measurement closely align with TCG specifications. By combining the use of these standards and guidelines, an enterprise can develop into a Trusted Enterprise, wherein trusted devices that are known and measured are provided network access to enterprise resources, and untrusted devices (that may contain malware or have malicious intent) can be quarantined and prevented from causing widespread harm to the enterprise. This approach represents a shift in network and security architecture that is increasingly gaining ground as enterprises recognize the need for a HROT to prevent software-based cyber attacks.

Which of these approaches apply across sectors?

For the most part, they all do.

Which organizations use these approaches?

Any organization seeking to improve its security seeks out industry standards and guidance, where available. However, the degree to which guidance is referenced and implemented is dependent upon an organization's commitment to risk management, its understanding of the relationship between IT risk and business risk, and the budget and resources available to address those risks.

The unfortunate reality is that most organizations implement standards and industry guidance only in reaction to new regulation that requires compliance with those standards and guidance. Corporations do what is necessary to comply with industry regulations and what will best protect their bottom line, either through cost savings or revenue generation. To date, regulation has been woefully behind the cyber threat curve, making adoption of many of the standards identified above limited to those who see an opportunity to address real business risk or opportunity.

Predominantly, the larger Defense Industrial Base (DIB) companies have taken the biggest proactive role in adopting cybersecurity-related standards and guidance. As the cyber threat continues to increasingly impact the business bottom line across industries, we expect growing adoption of more effective cybersecurity practices in the commercial sector.

In Federal Civilian Government, adoption of standards is driven largely by compliance requirements. However, the level of implementation is directly proportional to the ability of any given agency to afford it. Unfunded mandates are less effective than funded ones.

In the Department of Defense, the Intelligence Community, and certain agencies within the Department of Homeland Security, mission needs can at times drive adoption of emerging standards and technologies ahead of compliance requirements, but still, there is a predominant dependence on compliance as the primary motivator for action. And here, again, unfunded requirements can go unimplemented.

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

Approaches are limited when any one participating group has too influential a say in what is included in the approach. Many standards bodies are led by and comprised of vendors; without a sufficient number of opinions and viewpoints, vendors can influence the inclusion of requirements that are specifically associated with the products those vendors sell. In those cases, organizations attempting to utilize standards-based approaches sometimes apply the default technical controls and monitor the default events based on capabilities provided in specific compliant vendor products, regardless of whether those controls or events are relevant to the particular business or sector, and regardless of the intention of the approach with respect to addressing the most relevant threats.

On the other hand, vendors play an important role in standards work. Only by involving vendors in the development of standards and guidelines do real products that meet the standards and provide the intended solutions get designed, manufactured, and released to the market. Therefore, it is challenging but important to strike the right balance and mix of participants in developing best-in-class approaches for industry problems.

Generally speaking, industry standards come about when multiple vendors want to grow their collective businesses and interoperate with each other, instead of having proprietary solutions as a means to do so. Objective risk management recommendations from industry organizations must be balanced with prescriptive enough input from technology vendors to drive interoperability and consistent security capabilities across products.

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

Education and adoption. The biggest barriers to a successful cyber defense are (a) our collective ignorance as to the best way forward and (b) the mandate to move uniformly in that direction. Much of the technology exists, or is implementable within 24 months. The know-how exists, but the will to implement it does not.

A reasonable question would be: Why does the will not exist? Four primary reasons: (1) Lack of a perceived threat that outweighs the cost to address the threat; (2) Lack of a mandate to address the threat; (3) Lack of knowledge about how to address the threat effectively (which goes back to the education issue); and (4) Lack of funding to implement new requirements—mandated or otherwise.

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

Most of the approaches we have mentioned provide general guidance that could apply across sectors. Some of the approaches are already geared to a specific sector or could benefit from sector-specific customizations. For instance, PCI DSS is specific to the financial sector, and NERC CIP is specific to the energy sector. Risk management frameworks, maturity models, and privacy guidance are universal approaches, although privacy is more applicable to certain industries like healthcare, finance, and education.

Existing TCG standards are not sector-specific. The energy sector could, for example, consider adding trust anchors into energy delivery systems based on TCG technologies, then develop specific profiles to identify how the standards apply to the energy sector.

The development of reports that provide guidance to identify and manage advanced threats, like those disclosed by the 2013 Mandiant report on APT1, would apply to all sectors [Mandiant, 2013].

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

Each industry understands its threats and risk posture best. Sectors would benefit most from the development of industry specific guidance by the companies in those particular industries. Again, however, it is important to get industry standards input from the companies in the industry as well as the companies that service that industry and be mindful to address the challenges in the most effective manner. It is easy to let technology vendors lead the way if their inputs are not properly balanced with industry participant needs and opinions. For example, PCI DSS requires application firewalls and Security Information and Event Management (SIEM) tools, not necessarily because they are the best way to protect payment applications, but because vendors on the board for PCI DSS influenced the standard to be friendly to the sale of their products.

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

Sector-specific consortia should assess and prioritize their needs, then fund standards activities to coordinate their needs with standards bodies and companies that produce products in that sector. This creates an effective approach for addressing sector-specific challenges that is less biased towards any individual technology or product.

What other outreach efforts would be helpful?

Security experts and business decision-makers usually only look within their industry for guidance, where in fact, there are a number of good approaches in other industries that are not being considered. For example, what manufacturing companies do to keep their plants operational applies to what hospitals could do to help keep their systems available for doctors. Regulations applicable to financial companies could also apply to energy or other industries. Implementing better mechanisms to support cross-industry news and information sharing, including events and working sessions to promote better discussion, would show tremendous benefit.

2.3 Specific Industry Practices

Are these practices widely used throughout critical infrastructure and industry?

Not all practices apply to all industries. Further, how well they are implemented is primarily a function of the commitment of the company, and the maturity of the security and risk management program and staff. The use of standard procedures and practices varies by industry; those with a greater privacy focus manage encryption and role-based access better, while those who have significant availability requirements usually have better monitoring and incident management practices.

There are also competing priorities that make practices difficult to apply widely in some cases. For example, Energy companies typically apply separation of IT (i.e., business) and Operational Technology (OT) (i.e., SCADA) networks as a best practice, but, as the smart grid is expanded, these two network types are becoming more and more connected. In this particular case, the controls to secure each of the two types of networks are not always transferable. Further, there are conflicting interests and priorities between the energy companies that have primary influence over the IT networks and the OT vendors that have primary influence over the OT networks. These conflicts have not yet worked themselves out, and therefore pose a challenge to adopting best practices as the networks converge.

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

ISO standards have, to some extent, "internationalized" some of the most common practices. The 27001 areas, for example, address some critical infrastructure practices with respect to separation of IT and OT networks.

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

Separation of business and operational (i.e., plant) systems for resiliency practices are more suited to energy, manufacturing, and communications, whereas practices related to privacy and use of encryption are more suitable to healthcare and financial industries. The rest apply to all, and all are important for a comprehensive security program.

We consider asset identification and management and incident handling the most lacking practices across the board. Companies are generally good at monitoring and detecting commodity threats, but are less savvy at knowing what assets they have or how to respond to a specific threat.

The understanding of Advanced Persistent Threats (APTs), as described in the Mandiant report referenced above, and practices and techniques to identify and mitigate APTs also apply to all sectors [Mandiant, 2013]. There is a great divide in the security industry between those who have dealt with APTs and understand it, and those who have not and do not. All critical infrastructure industries are being targeted, even if they do not know it. There needs to be more and better guidance as to relevant security monitoring, and practical and effective security response procedures to mitigate those threats. These techniques are very mature in the DIB and need to be expanded to other critical infrastructure industries.

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

See the answer to the question immediately above.

Which of these practices pose the most significant implementation challenge?

Separation of business and operations, and the control of privacy, are the most complex challenges. IT and OT are gradually becoming more and more integrated and nearly all control systems are now connected to IP networks, exposing those networks to much greater cyber threat. With different factions managing each of the two sides, security's role in this gradual integration is muddied and not prioritized. Communication is not always positive and productive between the two sides.

Concerning privacy practices, many security professionals do not understand privacy; they consider it the same as confidentiality. There is a need for better education and socialization on privacy practices. Right now only the International Association of Privacy Professionals (IAPP) is doing worldwide training on the topic, and even then, it is mostly about cybersecurity controls to protect privacy. Complicating matters, with 47 different state breach disclosure laws, it is very challenging for a legal department to determine the requirements in the event of a privacy breach in a large company, other than those that fall under HIPAA and GLBA, which supersede state laws. Organizations spend a lot of time staying compliant in the aftermath of a breach, which directly steals resources from optimally addressing the breach itself.

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

Privacy is a challenge because there is no "privacy standard," but rather standards pertaining to the protection and appropriate use of data. "Appropriate use" is based on regulation or specific consent requirements of the data owner. Making the issue more complex, international companies must also abide by EU privacy laws, which are stricter than those in the U.S. Very few U.S. organizations are certified "Safe Harbor" to house EU privacy-protected data.

Separation between IT and operations is a decades-old practice based on experience; it has not been sufficiently modernized or standardized within the industry.

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

Not usually. Typically an organization will look for standards to help solve a problem or define a process. Unless you are within an industry, or have a business purpose, that requires certification against a standard, a company often does not consider or use that standard. Further, many organizations simply are not aware of existing standards. Better and broader education of the variety and usefulness of standards and guidelines would be helpful across critical infrastructure.

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

Not usually, except companies with mature risk management programs. Most security programs are reactive. If something new escalates, like the recent DDOS risks in the financial industry, companies scramble to find solutions and resources that understand and can address the problem. Unfortunately, in that reactive situation organizations are at the mercy of security vendors who tend to sell expensive solutions that are not completely effective because the solutions do not address the source of the problem—a lack of processes and procedures to proactively mitigate and manage threats. Only once those processes and procedures are in place should companies identify and invest in proper technology to support them.

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

These risks are greatest for international companies. In the U.S., there is no expectation of privacy for an employee's use of a corporate asset or network. However there are protections required for the passing and storage of specific employee privacy data. In the EU, the requirements are more strict and severe. In either case, this issue is applicable when monitoring network traffic to identify an intrusion that inadvertently uncovers personal employee or customer data. Organizations have a responsibility to protect customer Personally Identifiable Information (PII) to the appropriate level when responding to a threat.

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

Privacy is a large concern. The U.S. considers privacy as protecting individuals from harm (i.e., identity theft), while the EU considers privacy as protection from discrimination, which could lead to harm. In the U.S., name, date of birth, Social Security Number (SSN), and healthcare data are considered under privacy protections. The EU considers far more data elements including what you read, what group(s) you belong to, where you live, etc. The more data that requires protection, the more difficult it is to implement the proper protections that still allow access to the data quickly and efficiently for network threat analysis.

Individual country laws also dictate what data can pass in and out of a country, and how data, even SPAM, is controlled. For instance, in Germany, an organization cannot implement SPAM filters to prevent SPAM from getting to a German employee's mailbox without the employee's consent to do so. The blockage of SPAM is viewed the same as preventing the physical mail from being delivered. Other countries do not allow companies to restrict access to categories of web sites (e.g., pornography or gaming). Still other countries do not allow certain classes of data generated in that country from leaving that country (similar to U.S. export control laws). The gathering of data for ediscovery to support litigation becomes very complicated on a multi-national network.

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

The regulations are well defined, but the technical and procedural controls to enforce and manage them are not well understood. This is a gap that would benefit from a standards framework. Today, industries are each implementing controls differently and independently, and what is acceptable to healthcare might be different than what auditors deem acceptable in the financial industry. Better standards across industries may lead to more and improved broad-scale technology solutions that would then be available at lower cost if they could be sold to a broader market.

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

The following are recommendations for additional core practices that should be considered for inclusion in the Framework.

- **Greater guidance and education on secure application development and application security:** Recommendations include user education and training on security and privacy processes and procedures (including modern threats utilizing social networking, use of strong

passwords, etc.); a framework for security and privacy of mobile devices and non-computing devices ("Internet of things"); physical and environmental security; and guidance for how to test the effectiveness of controls, not just the presence and appropriateness of those controls.

- **Separation of business from operational systems:** Businesses are driven to actions that reduce costs or increase profit. In this regard, separation of business from operational systems is generally perceived to be a decision that drives costs up because separation of business and Supervisory Control and Data Acquisition (SCADA) is inconsistent with how business is typically done. In a recent Automation.com article, Scott Wooldridge explains that we must assume companies will always seek to merge business and SCADA networks. From that initial assumption, he proceeds to lay out basic security practices that might improve the security of the network as a whole and security of the SCADA components in particular [Wooldridge, 2013].

  The cost of physical network infrastructure for customers is a driver for companies in the business of supplying network hardware. There is a great deal of interest in Software Defined Networking (SDN) for this reason. As SDN enters more general deployment in the enterprise, there will be increasing reliance on SDN capabilities to create virtual separation between business and operational networks. Even so, clear business requirements for interconnectivity of business and operational networks today forces acceptance of connection between the two in the enterprise.

- **Use of encryption and key management:** A brief market survey report published by Venafi is relevant to this topic [Venafi, 2011]. Key relevant findings from the survey of 471 enterprise respondents are listed below:

  - 51% stated they had experienced either stolen or unaccounted for digital certificates, or that they were uncertain if their organizations had lost, stolen, or unaccounted for digital certificates in general
  - 54% stated they had experienced either stolen or unaccounted for encryption keys, or that they were uncertain if their organizations had lost, stolen or unaccounted for encryption keys in general
  - 46% of organizations are managing at least 1,000 digital encryption certificates; 20% are managing more than 10,000
  - 83% of organizations are managing technologies from at least two different CAs; 18% are dealing with more than five
  - 88% of organizations have multiple administrators managing encryption keys; 22% have more than 10
  - 42% of organizations manage encryption technologies from at least four vendors; 8% are dealing with more than 10

  These results lead us to the recommendation that the use of encryption should be controlled with a robust key management infrastructure.

- **Identification and authorization of users accessing systems:** The primary vehicle for user identification is the user ID/password. The second most widely deployed authentication technology is the key fob one time password generator, similar to the market leading RSA

SecurID product. The use of two-factor authentication for system access should be strongly encouraged for as wide a variety of systems as possible, in particular for any systems of critical importance.

- **Asset identification and management:** Asset identification and management have traditionally been driven by cost control considerations. These systems are often implemented by bar code stickers affixed to the asset, and have no related automation or machine readable management function. A built-in, machine readable identity for computing devices, augmented with a built-in management interface for device ID collection and reporting, would be beneficial in not only asset management but in digital device identity for network authentication purposes.
- **Security engineering practices:** In many cases, security engineering practices are in place within groups that develop security software within technology product organizations, but those same security engineering practices are not in place within those same companies for their other software development groups. Security design walk-throughs and other similar security engineering practices for both hardware and software products are not as strong across the IT security vendor industry as they should be.

3 Concluding Remarks

DMI is a firm believer that standards-based security solutions are paramount to tackling today's cybersecurity problems. A comprehensive Framework that points industry to existing best-in-class standards and approaches, such as those developed by the Trusted Computing Group and others mentioned above, and identifies areas where additional methods and guidelines should be developed to fill existing gaps, is crucial to our collective ability to better defend against today's and tomorrow's threats.

Further, to make prioritized, sound security investments in standards-based solutions, we must look beyond simply meeting compliance requirements. We must acknowledge the critical role proper business risk assessments should play in driving organizations' decisions with regard to implementation of cybersecurity controls and practices.

4 Bibliography

CSIS: 20 Critical Security Controls Version 4.1. (2013). Retrieved from http://www.sans.org/critical-security-controls/.

Mandiant. APT1: Exposing One of China's Cyber Espionage Units. (2013). Retrieved from: http://intelreport.mandiant.com/

Strategies to Mitigate Targeted Cyber Intrustions. Austrailian Government, Department of Defense, Intelligence and Security. (2013). Retrieved from http://www.dsd.gov.au/infosec/top-mitigations/top35mitigationstrategies-list.htm

Venafi, Inc. 2011 Enterprise Encryption Key and Digital Certificate Management Market Outlook. (2011). Retrieved from: http://www.venafi.com/wp-content/uploads/2011/10/2011-Enterprise-Key-and-Certificate-Management-Market-Survey-Outlook-Venafi.pdf

Wooldridge, S. SCADA/Business Network Separation: Securing an Integrated SCADA System. Automation.com. (2013. Retrieved from http://www.automation.com/library/articles-white-papers/hmi-and-scada-software-technologies/scadabusiness-network-separation-securing-an-integrated-scada-system