# CYBER MANAGEMENT ISSUES

- The namespaces and numbering system that provide the infrastructure for both public and private telecommunications are managed by private industry.
- The practice of technology as field of professional discipline is quite young to other fields. Software Artilects do not have a guild or apprenticeship systems to do artilects of physical facilities.
- Technology consultants are not required to learn their trade through a series of peer-administrated exams as do medical consultants. Buyer beware is the rule of the day.
- The field of technology practice has therefore, not unexpectedly, yielded a field of technology malpractice.
- Technology malpractice investigations are motivated by suspicion of management neglect of security issues.
- Cyber Security management often begins with research into both technology capabilities and system requirements.
- It is dependent on the capability of an organization to buy, build, or outsource technology components, and so supply chain management is a critical requirement for success in technology practice.
- Often cyber security management will attempt to delegate security functions to areas of cyberspace management that are most closely associated with the assets to be protected.

# Fiduciary Responsibility

- Operation is a generic term in many technology and system-based organizations to refer to the staff that maintains and monitors business process.
- In heavily technology-supported businesses, technology operations and businesses process are intractably intertwined.
- Even where two separate departments maintain and monitor the technology-enabled processes and business-level processes independently, the operations department is supported by screens and programs that are information-rich views of the same technology whose byte-flow and electronic circuits are monitored by the information technology department.
- For example, the technology department may configure employees to use the systems while the business department will be responsible for configuring customer users.
- Operations, or “ops”, as it is colloquially called, also generally include technology service support organizations like desktop software installation and help desk.
- In large systems-oriented organizations, large databases of personally identifiable information (PII) and information repositories of trade secrets are handled according to preset routine, in the same perfunctory fashion as systems containing cafeteria menus are handled.
- However, in secure organization, the access control settings and monitoring processes for the sensitive information are more rigorous that the technologies and procedures implemented to support the menus.

- Cyber operations in any sizable enterprise is typically a round-the-clock endeavor.
- Even where global marketplace do not demand active support, automated system processes may be required to devote considerable computer resources in off-hours to crunch members to produce data for start of-day consumption.
- Security incident identification and response procedures are a routine part of operational process, even those that do not consider themselves responsible for security.

# Cyber Security Policy Issues Concerning Fiduciary Responsibility

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.1.1 | Senior management shall appoint a Chief Information Security Officer to bear the Responsibility of cyber security management. | The role of a Chief Information Security Officer is intended to provide leadership and coordination for the organization's information security strategy, policy, and operations. | If security advocates are placed high enough in management to be peers of Chiefs in other areas such as the Chief Legal Officer and Chief Financial Officer, the need for security in organizational process and procedure should get sufficient management attention to be successful. A culture of security is not created by the appointment of an individual. Where upper management appreciates the needs for security, it can be done in a variety of matrix management structures. Where they do not, such an appointment will place the individual in a position of responsibility without authority. |
| 6.4.1.2 | An organization appointed by senior management with appropriate budget and authority shall establish a program to authorize and document changes to critical digital assets, to detect changes as they occur, and to compare the detected changes to the authorization. | Many organizations approve changes, but do not confirm that only approved changes are implemented. This policy calls for change control to the extent that every detected change is verified as authorized or not authorized. | This policy requires that a level of detail be kept for every planned change that would allow an independent observer to verify that the change was correct. As many planned changed require considerable talent just to execute, it puts too much of burden on ops to compare a plan to an actual change. If plans cannot be specified to a level of detail necessary to verify change authorization, then the detail is likely not to be sufficient for informed approval either. This policy would add benefit to both processes. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.1.3 | Lack of tested technology business recovery plan for critical services shall be considered negligence for critical consumer services. | This policy would require that technology hosting providers and software services vendors maintain alternate computing facilities that may be configured to be used in the event of a main system failure, and also to test the failover from the main site to the alternate site. | Where consumers and businesses are encouraged to reply on vendors to operate technology processes that are business or mission critical, those services shall be supported as per technology industry standards. Unless business recovery processes are part of a service contract, customers of technology service providers should not expect them to be incorporated into services. To stay in business, a technology vendor need only offer the service, not maintain the integrity of user data. As described by Louis Black, not having a technology recovery plan is like inventing fire and not keeping a torch lit in case the main fire went out. Services that are completely lost would have to be reinvented. |
| 6.4.1.4 | Wherever access control has been configured to protect cyberspace assets, the identity and organizational role of each user granted access shall be tracked to ensure that the access is revoked when the purpose of granting access is no longer valid. | This requirement is referred to as “identity management.” It usually involves setting up a database of identity information, usually modeled on human resources and contractor data repositories, and using the database as an integral part of user authorization workflow and automated systems audit. | This policy should ensure that access to sensitive information is not mistakenly granted to individuals who do not need it and that it is removed from individuals who no longer need it. Requiring users to be registered and be individually authorized may delay access to information needed to perform critical functions. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.1.5 | Process control systems that control hazardous processes and/or materials shall be very highly restricted. | Many automated systems control operations in which mistakes have safety implications (e.g., chemical mixing processes or heavy manufacturing equipment). Accidental or intentional changes in the programs that control such systems could have devastating results on the health of individuals in the proximity of such systems. | The fewer people that have access to these systems, the less likely it is that they will be controlled by anyone with malicious intent. Process control anomalies happen for reasons other than cyber security attacks, and when they do, it is better to have open access to the process control systems in order to allow any individual capable to redirect the process. |
| 6.4.1.6 | An organization appointed by senior management with appropriate budget and authority shall ensure that appropriate cyber security awareness and training have been provided to all appropriate personnel on an accepted time interval. | Organizational cyber security programs cannot be fully executed by security staff because everyone in the organization who handles information may have the ability to impact information attributes such as confidentiality, integrity, and availability. | It may not be obvious to a staff member how their behavior enhances or detracts from the cyber security program. Security training makes their responsibilities with respect to security clear and makes them accountable for their role in the security program. For businesses with ICSs, appropriate ICS awareness and training should be required. Many individuals have no ability to adversely affect information security and such widespread training programs are thus a waste of resources. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.1.7 | National governments shall ensure that sensitive information held by vendors be given the same protection it would be given by the government agency contracting with that vendor. | This is a common standard for commercial organizations which cannot pass along responsibility for regulatory compliance simply because technology services are outsourced. | This policy would hold government agencies responsible for safeguarding information, regardless of whether it has been handed to vendors or not. Governments must ensure that service providers they enlist protect information at government-established standards. This could include PII (such as names or personal identification numbers such as U.S. Social Security Numbers) or intellectual property on government programs or projects (such as weapons development or acquisition). This policy would require not only sufficient protection of this information but also notification to the government if there was a security breech in the environment containing this information. |
| 6.4.1.8 | National governments shall measure their own security using performance-based measures. | This policy would measure organizations against specific procedural and technical steps, such as success against periodic penetration testing and the time delays to patch major vulnerabilities, rather than just paperwork-only reviews. | Often, governments measure their security only by writing and reading reports (e.g., the Federal Information Security Management Act [FISMA] in the United States). A more realistic and effective measure would be to use stronger performance-based measures such as how difficult an organization is to hack into; how long their patch cycle takes; or response to specific stimuli. Many nations may not have the necessary infrastructure to scale up periodic penetration testing, exercises, or other means to give a standard measure of performance. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.1.9 | The nation's executive branch shall consider assembling a committee of cyber security experts from a variety of industries to advise on cyber security policy and assess cyber security programs. Such groups can also be established at other levels (especially department/ ministerial). | This policy would encourage a nation's executive branch to reach beyond a small circle of current advisors and seek<br>out assistance on cyber security strategy<br>issues. Examples in the United States include the National Security Telecommunications Advisory Committee (NSTAC) and National Infrastructure Advisory Council (NIAC). | As the field of cyber security is very wide, lessons learned in its practice from a variety of domains will strengthen the ability of the administration to deal with the widest variety of issues going forward. Too often, cyber security experts leave government service but are willing to continue to serve on a voluntary basis.<br>There must be very strong provisions to ensure such advisory groups do not become closed cabals of industry-government corruption or encourage anti-competitive behavior. |
| 6.4.1.10 | National governments shall codify a national cyber security strategy that includes public and private sector components, and involve coordination with key stakeholders. The strategy can include overlooked areas such as security for industrial control systems. | A national strategy lays out guidance from the national executive and should include policies, priorities, measurement, compliance, and access to funding. It can lay out priorities for research and development, defense, and stakeholder engagement. | A national strategy makes clear the national priorities and helps steer and encourage all national efforts.<br>A poorly thought-out strategy can lead all efforts in a mistaken direction, overlooking possibly disastrous vulnerabilities or threats. It can also lead to inconsistent regulatory requirements. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.1.11 | Nations shall have an organization and senior leaders with enough influence and resources to drive the nation to improve its cyber security. This leader should also generally have budget authority and direct access, when needed, to the national executive. | A senior leader (such as a “cyber czar”) with sufficient staff in countries is often key to making progress for cyber security. | Bureaucracies are resistant to change so a senior leader with the power to coordinate, convince, and coerce change is often essential.<br>A senior leader outside of normal bureaucracies can often confuse chains of command. If one organization and one leader are seen to be the center, that may lessen the feeling of responsibility for other leaders and departments especially if they lose resources to the new czar. |

# Risk Management

- Risk management applies to any kind of risk. Typically, a risk management officer or division will focus on credit risk, market risk, and operations risk.
- Technology risk is a subset of operations risk, and cyber security risk is typically viewed as a subset of technology risk.
- The human element in operation is considered more of a risk than the technology risk because despite all of the software flaws in computers, they are still typically more reliable than people at performing a job repeatedly and consistently.
- Even for systems under development, it is far more common for software engineers to sabotage a system or a project by intentionally exercising the authority in their own job function than to thwart security measures
- There are not many guidelines on how to perform cyberspace risk assessments, but there has been substantial work performed under the heading of information security risk assessment.
- Where information is considered as an asset, information security risk determines the potential loss due to damage to information. Damage to information is typically portrayed as loss or degradation of information confidentiality, integrity, or availability, though some have suggested that information security attributes be extended to encompass attributes that refer more directly to its value, such as utility and possession.
- Although there are many economic analysis methods available to a cyber security manager making risk assessment decisions, in its most basic form, the cost of a security measure is compared to the expected loss avoidance, and if it costs less to implement, the measure is recommended to be implemented

- It is important to distinguish risk assessment as a management tool from either risk management or security management.
- After risk assessments are done, decisions are made based on the results. Where strategy is involved in the security decision-making process and the outcomes of those strategies are monitored, this is risk management.
- Where the programs, processes, and projects are created to act on risk management decisions, this is security management.
- Risk management results in objectives and guidance for security management. As such, risk management is at the heart of many debates on security policy issues.
- These debates include discussion of cyber security strategy, policy, and implementation, and include risk assessment, risk decisions, concepts for mitigation such as transfer, as well as measuring effectiveness and monitoring evolution.
- Organizations in the critical infrastructure sectors are typically held to a higher standard of risk management, with systemically critical organizations being held to the highest standards of maintaining best security practices.
- This includes systems and networks whether they are connected to the Internet, or are completely privately operated networks for a limited number of identified parties, or proprietary networks within one organization, or industrial control systems which may have very limited network capabilities.
- Cyber security policy issues in risk management include organizational responsibility to understand and evaluate cyber security risk, segregation of duties utilized in risk and security management, and the government’s role in assuring risk management practices for the critical infrastructure upon which communities depend for both cyber and physical services.

# Cyber Security Policy Issues Concerning Risk Management

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.2.1 | Organizations (whether public or private) shall be held responsible for defending themselves against “normal” cyber attacks, which are attacks which standard security practice would be able to stop. | Organizations (whether government agencies, companies, or nonprofits) must protect themselves from typical attacks. Organizations that are more critical have higher levels of responsibility. | This policy ties needed levels of protection to criticality, with responsibility assigned to those who hold the risk. Organizations in the critical infrastructure sectors will be held to a higher standard of defense, with systemically critical organizations being held to the highest standards of all of maintaining sound security practices. This includes systems and networks whether they are connected to the Internet, are private or proprietary networks or automated control systems.<br><br>Attackers have been increasing their sophistication and many organizations are now outclassed and unable to defend themselves without significant increases in funding and resources.<br>If there was an agreed-upon set of cyber security standards, then critical infrastructure owners and government agencies could be held accountable for implementing them.<br><br>Despite the ubiquity of cyber security standards, accepted practices in the application of cyber security risk assessment processes are not domain specific, and so still leave all major implementation decisions to subjective judgment of impact by system owner/ operators (e.g., draft NIST 800-37r1). There is no reason to assume this exercise would have a different outcome.<br><br>In many security standards, “best practices” remain in the state where subjective owner/operator opinions dictate implementation requirements; it will be easy for targets of this policy to avoid its legislative intent. For example, recently, this practice led some energy system owner/operators to declare that none of their infrastructure was critical. It is not possible to establish via policy standards that do not currently exist. These types of requirements are best left to domain-specific regulators. This policy would raise the bar of the minimum amount of cyber security that those who operate critical infrastructure upon which the Nation depends must implement, and provide the basis for holding them accountable for implementing a standard level of cyber security. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.2.2 | All cyberspace systems shall undergo risk assessment. | Information security risk assessment strategies have been in place since the early days of the Internet. They are designed to ensure that threats are considered when deciding on control procedures, and that common vulnerabilities are identified and addressed. | This policy requires that every information system used by an organization is analyzed for security flaws.<br>Risk assessments follow checklist approaches to security assessment, and new and innovative technologies and threats are often missed.<br>Moreover, the fact that a risk assessment was done does not necessarily mean that vulnerabilities were fixed. These factors combine to provide the criticism that risk assessments commonly provide a false sense of security. |
| 6.4.2.3 | An organization appointed by and reporting to senior management shall have appropriate budget and authority to identify what mission critical digital assets, whether in applications, devices, and/or networks, are cyber vulnerable. | This policy places responsibility for conducting organization-wide cyber security risk assessment with senior management. | Without an inventory of assets to be protected, and the charter to conduct security risk assessments, security management is unguided and likely to be the equivalent of security theater.<br>Cyber vulnerabilities should be identified by experienced professionals, and so the identification process does not require attention at the senior management level. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.2.4 | An organization appointed by senior management shall provide appropriate budget and authority to establish and maintain a cyber security program to secure digital assets throughout their corresponding systems life cycle. | This policy places responsibility for managing an organization-wide cyber security program with senior management. | Though risk assessment and vulnerability reduction processes may be in place, without an overarching security program, there is no verification or validation that security goals are achieved.<br>As all cyber security processes are supported by the information technology program, the security program need not be separate, and in fact may be more effective if integrated within technology processes. |
| 6.4.2.5 | An organization appointed by senior management with appropriate budget and authority shall identify how to monitor the security of these assets during the installation, maintenance, upgrade, and change-out to assure a cyber secure system. | This policy places responsibility for managing an organization-wide cyber security operations and incident response with senior management. | Where there are joint resources assigned to incident response, those responsible for supporting critical system transaction processing will always claim the lion's share of technology resources. This often leaves inadequate resources dedicated to security response.<br>As in the case of security program management, all cyber security processes are supported by the information technology program, the security operations area need not be separate, and in fact may be more effective if integrated within technology processes. If resources are not adequate to provide security, technology managers should be held accountable as they are for any other system deliverable. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.2.6 | National governments should encourage a market for cyber security risk management. | This policy would provide economic incentives to establish a market for cyber security risk management. | Cyber security risk management is not currently economically viable. Entrepreneurs with ideas for cyber security risk management businesses should be encouraged.<br>If poorly implemented, the government might crowd out private sector solutions or be too technology- or vendor-specific. Subsidies based on government definitions of cyber security risk management would detract from creating solutions that make sense to an emerging cyberspace marketplace.<br>These could include ways to allow companies to transfer cyber security risk through insurance or catastrophe bonds, as they do for other kinds of hazards.<br>This policy does not go far enough to ensure that private operators of critical infrastructure perform risk management activities. These should not just be encouraged but mandated, and this would create the necessary marketplace to comply with the mandates. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.2.7 | Government shall create a security metrics, or “dashboard,” reporting system whose scope is the systems and networks operated by the Government. | This policy would require that systems and networks supported by the standards setting arm of the government be monitored and measured according to established standards. | The standards setting arm of the government requires accurate information about the state of security in the systems and networks which follow their standards. Requiring this information allows them to receive feedback.<br>This activity is already supported by the standards setting arm of the government (in the United States, the Department of Commerce, which includes NIST), and government systems are already uniformly subject to security management requirements (e.g., FISMA), which require management monitoring, and a “dashboard” policy is redundant.<br>This policy would require first an inventory of systems supporting the government as a whole, and so would create transparency for its dependency on systems security. |
| 6.4.2.8 | New standards shall be established to calculate return on investment in information security, and these shall acknowledge benefits that emerge from control over assets. | Return on security investment is currently calculated based on loss avoidance, and loss avoidance calculations use probability of attack as a critical input. The benefits of security in the absence of threat are not quantified. | Return on investment risk analysis loss probabilities are based on historical data and loss avoidance, but there is no historical data on which to base probability judgments for cyber security.<br>Therefore, new types of calculations are required to accurately reflect the soundness of security investment.<br>Security investment is just one aspect of technology management and should be justified on the basis of the benefits it provides. No special treatment is required to ensure that benefits are considered. |

# Professional Certification

- The process of certifying information security professionals is a growing and dynamic field. There are literally thousands of certifications available, ranging from hands-on examinations of product-specific knowledge, to subject area certification, to broad information security certifications.
- None of the popular cyber security certifications carry any form of liability or bonding beyond an expected adherence to a common code of ethics and conduct, nor are they equivalent to professional registration regimes.
- While the term “engineer” is often used in this career field (“software engineer” and “network engineer” are common examples), it is not in the same context as a registered or licensed engineer that is subject to a given government’s regulations of the profession.
- Normally, companies and organizations will train and certify their cyber security employees to some standard acceptable to the broader career field. But if internal employees are not used exclusively for cyber security operations, organizations and companies are not relieved of the responsibility for regulatory compliance when they outsource technology operations.
- Hence, they must find ways to demonstrate that the vendors with whom they have contracted are capable of meeting cyber security requirements. This requirement has spawned a plethora of checklists used by companies to determine whether the vendor security posture is capable of delivering a security operational process.

# Cyber Security Policy Issues Concerning Professional Certification

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.3.1 | Individuals in positions of responsibility with respect to cyber security shall be certified to be competent in the field. | There are several cyber security professional associations who offer certifications to members who can pass a test and provide evidence of cyber security experience.<br>This policy would require every cyber security professional to join one (sometimes even a specific one) of these organizations, pass the test, and remain a member. | It is critically important that individuals who have responsibility for security measures fully understand how their job function contributes to the overall cyber security landscape. Certifications provide the broad security background necessary to provide this view.<br>There is no consensus among cyber security experts that people who have achieved any of the available certifications are more competent to do a cyber security job than someone with equivalent experience who is not certified. This type of policy favors individuals who can afford to pay for certification tests and annual certification fees.<br>Whether or not there is any existing professional body of knowledge agreed upon to be necessary for cyber security professionals to understand is irrelevant to the fact that a certification process acknowledges the need for one and that cyber security professionals have to undergo some preliminary version of the desired test in the meantime while it is being developed. This allows the process to be established to receive the body of knowledge when it becomes available. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.3.2 | Nations shall encourage a professional cyber cadre to define and defend new job classifications for cyber security professionals. | Cyber defenders, planners, and attackers need specific high-level training for their highly specialized disciplines. The type of training required depends on industry, type of system, and role in cyber security program. | Investments in job requirement analysis will drive a more sophisticated workforce and cyber specialists. Current definitions of job classifications are just beginning to be enforced (DoD 2005). Allowing changes to the rules in progress interferes with enforcement efforts that are just beginning to take root.<br>By loosening bureaucratic rules for recruiting and retention and establishing new job classifications for cyber security professionals, programs should particularly encourage definition of critical requirements that are underdeveloped, such as cyber security for industrial control systems. |
| 6.4.3.3 | National governments shall encourage (and in many cases require) all government personnel working in cyber security to be trained and certified. For areas like industrial control system cyber security where there is not adequate training nor programs, these should be encouraged.<br>In general, nations should favor existing commercial certifications rather than develop government-only programs. | Certification and training programs—like those from SANS or industrial control system (ISC)2—establish well-known baselines and are widely available. | There is a large body of knowledge in cyber security that has been accumulated over the years, and requirements for training and certification would ensure that working professionals are accountable for applying it.<br>As there is no agreed-upon standard cyber security curriculum, widespread adoption of a specific training program and guaranteed subsequent hiring programs may have the unexpected consequence of reducing the variety of cyber security expertise within government agencies. These concerns are even more exacerbated for ICS. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.3.4 | Accreditation, training, and certification programs shall be established for all personnel working in industrial control system cyber security. | There is no standard curriculum for industrial control system cyber security nor are there any certifications or university interdisciplinary programs for cyber security of industrial control systems. | There is a large body of knowledge in cyber security that has been accumulated over the years, and requirements for accreditation would ensure that working professionals are accountable for applying it. However, the same cannot be said for industrial control systems.<br>As there is no agreed-upon standard cyber security curriculum, widespread adoption of a specific training program and guaranteed subsequent hiring programs may have the unexpected consequence of reducing the variety of cyber security expertise within government agencies. These concerns are even more exacerbated for industrial control systems. |
| 6.4.3.5 | Management shall collect data on cyber security professional hiring and use it so determine cyber security hiring effectiveness. | This is a requirement for management due diligence to ensure that plans for cyber security hiring have been successful. | This policy forces managers who recruit and hire cyber security personnel to assess the effectiveness of their efforts. These assessments should lead to continuous improvement in cyber security staffing effectiveness.<br>This type of policy should be a routine function of human resource management endeavors and should not be specific to cyber security.<br>Creating special functions for cyber security that overlap with routine management unnecessarily overburdens cyber security managers with extra paperwork. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.3.6 | National criteria for evaluating cyber security accreditation, training, and certification programs to all cyber security accreditation, training, and certification programs used by government and critical infrastructure operators shall be established, applied, and published. | It is very hard to know which vendors are capable of meeting claims that they provide adequate cyber security training.<br>This policy would create a guide for the average citizen or industrial organization to find a credible cyber security training firm. | This policy would provide much needed guidance to government agencies and critical infrastructure operators who are individually evaluating training programs. The multiple simultaneous evaluations of the same training programs is not cost-effective as it requires a technically credible government organization to identify who is credible in industrial control systems and that does not exist.<br>Publication of an "authorized" list of cyber security training programs would be a disincentive for entrepreneurs poised to enter the cyber security training market, and eventually lower both the availability and the quality of available training options. Companies would have to pay premiums to companies on the list rather than seek out innovative training approaches.<br>All hiring goals, metrics, and plans should be made public to encourage applicants—and allow public tracking of progress. |

# Supply Chain

- In the cyber security supply chain, the most visible exposure to threat is often seen as external, such as an ISP, reference data source, or cloud computing application.
- The enterprise-to-enterprise communication that is required to run a technology operation in cyberspace has surfaced many issues with respect to organizational representation of information upon which others must depend to operate in harmony.
- It has also highlighted the lack of formal accountability for the veracity and integrity of that information. However, the supply chain also includes everything that technology practitioners do to support infrastructure and applications internal to the enterprise.
- The depth and breadth of the cyberspace supply chain is difficult to quantify. It will differ depending on the type of system contemplated. It will always include some kind of software, but may also include software developers themselves.
- The types of hardware it may include range from mainframe computers to programmable chips. Almost all elements of the cyberspace supply chain have experienced known incidents of counterfeit or sabotage, and it is often hard to tell the difference, as a counterfeit part may malfunction and create unintended sabotage (DSB 2005).
- That is, another very visible but often overlooked part of an organization’s supply chain is the organization’s own IT department. This department is often not fully integrated with an enterprise, but integrates itself with a suite of technology suppliers that it assumes responsibility to operate on behalf of the business.

- Weakness in internal supply chain, such as delays in onboarding new staff, account for a lot of negative audit findings due to workarounds by staff needing to use computers to get jobs done. Given a choice between violating security policy and being cited for poor performance, performance wins every time.
- Moreover, technology managers are routinely plagued by software vendors who do not consider security requirements and usually disclaim accountability for how the software works (Rice 2008). This places a large burden on technology managers who must chose among insecure software products and integrate them into a technology infrastructure for which they are responsible for maintaining quality of service.
- This section starts with policy statements concerning software security quality that are typically encountered in the context of enterprise acquisitions. It then covers cyber security supply chain policy issues of national importance and builds on prior statements concerning Cyber Conflict in Section 6.3. These policy statements are followed by more general issues of supply chain effects on infrastructure.

## Cyber Security Policy Issues Concerning Supply Chain

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.4.1 | Software vendors shall be liable for damage resulting from code malfunctions. | End-User License Agreements are typically worded to deprive customers of any rights to liability for production malfunction. | End-User License Agreements are currently contrived to deprive end users of any rights to liability for production malfunction. Software vendors should be subject to the same standards of product liability as any other industry.<br>Software may malfunction for a variety of reasons, and many of these have nothing to do with the code. A user may install the software on a platform without the necessary resources for it to operate. Malfunction in these cases would not be the fault of the software vendor. |
| 6.4.4.2 | Software support shall not be fully automated. | This policy would require software support processes to always allow a customer to contact an individual to resolve support issues. | Software flaws are expected not just in delivered process, but also in automated support system. Any technology vendor that provides support must give customers a way to talk to a person in order at least to report support issues. For example, there are often flaws in automated support mechanisms. such as loops in customer support trouble-reporting systems that do not allow customers to submit details of their problems, or choices constrained to a list of technical problems that do not include the one experienced by the customer.<br>Software companies price software according to the level of effort it will take to support. Where the level of effort is expected to be minimal the price is cheaper, and customers get what they pay for. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.4.3 | Software security standards shall be required to legally operate e-commerce Internet sites | This policy would establish minimum security controls on all e-commerce services. | Given the risk to consumers of potential malware, impersonation, and asset theft resulting from insecure websites, no website should be able to offer consumer services without abiding by established security standards.<br>There are no established security standards that will guarantee safety from attack, and no enforcement mechanism that would provide assurance that any given website abides by them. |
| 6.4.4.4 | Nations shall use their acquisition policies to create incentives for IT companies to improve the security of their products. | National governments purchase tremendous quantities of IT equipment: hardware and software, networking equipment, desktops, automated control systems, and more. This gives nations leverage to negotiate improved security for those purchases. | If national governments, often the consumers purchasing in the largest quantities, negotiate for improved security, it will bring benefits not only to those national governments (in the form of improved security) but to companies in that nation and indeed to all consumers worldwide. If systems are more secure out-of-the-box then costs will be cheaper over their life cycle.<br>It is difficult for national bureaucracies to change procurement practices and improved security can often make systems marginally more expensive at the onset (though cheaper over the whole life cycle). |
| 6.4.4.5 | All personnel at all suppliers of cyberspace components destined for military or industrial control system use shall be screened for potential security problems. | The global supply chain makes it possible to inject malicious software and hardware into the nation's critical infrastructure. This policy would require those who handle products destined for such environments to be rated trustworthy. | Screening for security problems are a minimum requirement. A full background check or a DoD security clearance might also be required for more sensitive programs.<br>Since component makers of software, PCs and networking gear usually do not know the end user of their systems this policy would mean every maker would have to comply, which would be overly broad.<br>Screening should only be necessary when a risk assessment dictates. Blanket policies such as these are unnecessarily expensive.<br>Screening may expose employees to violations of privacy expectations, or could reveal historical information that could harm the employee's future employment potential in noncritical environments. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.4.6 | All cyber security regulations applicable to DoD networks shall be applicable to defense industrial base networks used to provide services to the department of defense. | Cyber security standards are routinely set for government agencies and this requirement extends those security requirements to companies that provide them with the products and services they use to carry out their missions. | This policy would eliminate a weak link in protection requirements around defense-related information and make it harder for espionage agents to learn about department of defense activities.<br>This policy is too inclusive as it extends to all defense contractors, not just those that provide critical services or are in possession of classified information. Moreover, not all DoD security requirements are publicly announced, and this policy would require widespread sharing of these requirements. |
| 6.4.4.7 | The DoD shall specify the organizational management structure that defense suppliers should used to manage cyber security programs. | Secure management practices are just as important as security of computers and networks. DIB companies must adhere to management structures specified by the DoD. | Specification of security management structures in DIB companies and organizations will reduce the risk of management mistakes.<br>Business leaders may feel that they should not be told how to organize their management structures, that what is important is to produce goods and services conforming to what is specified in a performance contract. |
| 6.4.4.8 | All cyberspace components destined for military use shall be made in country. | To greatly reduce the risk of embedded malicious code, devices destined for use in military applications should be manufactured domestically. | Most cyber hardware and software is produced overseas, potentially creating a security risk while also impacting the U.S. job market.<br>This policy is entirely impractical and would run up DoD IT budgets drastically. Moreover it may not even buy much protection if the designs are made outside the country, by foreign corporations or by foreign nationals working for U.S. companies.<br>All countries are subjected to the “not made here” problem when it comes to hardware and software. The United States enjoyed a unique position for decades when manufacturing was largely done domestically. However, globalized supply systems have changed the economics of production, moving manufacturing to locations where labor and materials are cheaper. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.4.9 | Cyber security suppliers shall be prohibited from sharing security intellectual property with hostile nation-states. | This is the type of policy that would add security products to the list of munitions prohibited from export to hostile nation states (State 2010). | This policy would make it easier to pinpoint cyber security intellectual property leaks by restricting information flow between sets of security companies and hostile nation-states.<br>This policy would prevent U.S. companies from protecting their global infrastructure in places where the need is greatest. |
| 6.4.4.10 | Where a third party information systems service is utilized to achieve business objectives, security requirements commensurate with the risk to business process of systemic failure of that service shall be contractually imposed and compliance monitored. | This requirement has its origins in accounting outsourcing such as payroll and benefits process, but is becoming more relevant as cloud computing services are used to perform critical business functions. Many industries are regulatory required to include this statement and resources to enforce it as an essential component of internal security programs. | Though a business may not by virtue of outsourcing transfer its regulatory requirements via contractual relationships, service contracts that include security requirements and audit clauses allow them to provide appropriate due diligence while reaping the benefits of economies of scale and specialized expertise in service delivery that are available from specialized service providers.<br>The major reason why a business contracts for information services is that it has no internal competency to perform them. Therefore, even oversight functions that seek evidence that contractual requirements are met are typically performed by staff with minimal understanding of the outsourced service who are satisfied with a checklist rather than an investigative approach. |
| 6.4.4.11 | Onboarding and other administrative processes shall be designed to facilitate rather than delay business function. | Operations management may be tempted to direct staff to bypass security procedures in order to quickly onboard a new and important client or high level employee executive | Many security procedures in large organizations are so burdensome that they inhibit productivity for authorized users.<br>Security procedures are required to ensure that and businesses should incorporate time delays into their onboarding processes rather than pressure security personnel to make quick decisions. Information security should rather benefit from the equivalent of a just-say-no campaign. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.3.12 | Cyber security access control mechanisms shall be rated for effectiveness, and this rating shall be required to be included in all cyber security sales literature. | This policy would require an authoritative agency to develop criteria to evaluate the strength of access controls such as logins and passwords. | Every system is different, so an access control that works for one may not work for another, which would render the rating meaningless.<br>In physical security, as secure specifications are developed, they are adopted in the form of local codes and ordinances, which, if demonstrably effective, may be raised to state and federal standards. The same practice should be followed for systems security. |
| 6.4.4.13 | Software vendors shall allow third parties to review code for security flaws. | Current, many ICS vendors will not allow third parties to inspect their code for security flaws which makes security disclosures very difficult at best. | Software vendors would have to expose their Intellectual Property to third parties, as access to their code would be required to comply with this policy.<br>Third party code review or penetration testing cannot be done without access to the code. The benefits of code review to users outweigh the threats to intellectual property from a small set of security testers, who could easily be screened and/or bonded. |
| 6.4.4.14 | Software security standards shall be required to legally operate –Commerce Internet sites | This policy would establish minimum security controls on all e-commerce services | Given the risk to consumers of potential malware, impersonation, and asset theft resulting from insecure websites, no website should be able to offer consumer services without abiding by established security standards.<br>There are no established security standards that will guarantee safety from attack, and no enforcement mechanism that would provide assurance that any given website abides by them. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.4.15 | Automated inventory systems in critical infrastructure such as health care shall be subject to regulatory audit. | Automation of inventory management allows “just in time” supply chain management, where inventories are kept to a minimum because suppliers can ship replacements just as the last item is removed from inventory. | Automated supply chain management systems often rely on highly vulnerable technologies such as radio frequency identification (RFID) chips embedded into labels of packages. Overreliance on these technologies as a replacement for actual inspection of inventory items could blind management to actual shortages.<br>Inventory is a critical business asset and companies have considerable vested interest in the integrity of these systems. External auditors are unlikely to add value to business process oversight for their own critical assets.<br>Although external auditors are unlikely to add value to business process oversight for their own critical asset, where not for profit companies or municipalities perform needed community services, consciousness of potential loss via theft is minimal. Inventories are not as closely watched.<br>Regulatory oversight may be beneficial in these cases. |
| 6.4.4.16 | Diagnostic laboratories used to record and correlate food sample measurements and customer complaints shall be owned and operated by domestic entities. | This is a requirement to keep all the information used to make decisions about food safety within the jurisdiction of national borders. | As cyber attack patterns grow more sophisticated, all information that contributes to consumer safety should be considered a potential cyberwar or cyber terrorist target.<br>Many food sources originate outside of the national cyberspace infrastructure and it is not feasible to transfer control of laboratory networks to firms for protectionist reasons because competing services are readily available in the country of origin. |

# Security Principles

- Over the years of security management practices, several studies have attempted to classify security technology practice into general security principles (Neumann 2004). The result is that there is a common body of knowledge of cyber security architecture patterns that, if observed in the requirements stages of technology engineering, serve to suggest well known solutions to well-known security problems.
- Security principles are generic descriptions of security features that provide solutions to cyber security problems that are both common and well understood.
- A pure technology derivation of this type of accounting principle is the principle of least privilege which dictates that users should have the minimum access they need to perform a technology task and no more. Segregation of duties applies not just to technology processes, but also to management processes. The most significant of these is the process by which security is managed.
- Managing security is a two-step process: 1) risk, 2) operation
- Once security risks have been identified, management makes decisions on whether, and if so, how to reduce security vulnerabilities. These vulnerability reduction programs should then be treated just as any other set of technology projects. Projects, by definition, are not persistent, and so any management of security measures that requires day-to-day oversight, such as user administration, is an operations rather than a risk management process.

- Where management has responsibility for risk management, and also security projects and/or operations, there is temptation to accept risk rather than spend resources to reduce vulnerabilities or verify that processes are working. On the verification side, this is obvious, and teams of auditors are normally deployed to ensure that security operations are well-managed in critical systems.
- However, on the risk management versus vulnerability reduction side, it is common to see the function assigned to the same individual. Hence, formal risk acceptance processes for security policy violations are common, even if the most senior managers in the firm have endorsed security policy.
- System security features based on tried and true security principles are not accomplished by technology alone, but by combinations of people, process, and technologies conjoined with security-aware management practices. This section includes policy statements from security principles to illustrate the issue concerning their adoption.

# Cyber Security Policy Issues Concerning Security Principles

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.5.1 | Senior management shall play a hands-on role in setting enterprise security strategy, and security strategy outcomes shall be reported at Board level. | Tone at the top is an audit term used to explain that unless senior management takes a topic seriously, no one else in the organization will. | Security management often suffers from responsibility with no authority. Moreover, too often, critical systems such as ICS are not covered under information technology security programs. Senior management need not design security strategy in order to determine what it is worth to the firm and assign appropriate resources and budget. Security management is best left to specialists. |
| 6.4.5.2 | Information shall be classified and labeled. Handling procedures for each information classification type shall be developed commensurate with the risk of misuse of information of that type. | This is an organization-wide requirement for information classification, labeling, and handling. An example is the use of the labels Top-Secret, Secret, and Unclassified. Another example is Proprietary, Confidential, and Public. In such systems, all information with the same level is protected the same way. | Information classification requires those who originate data to analyze and make decisions as to security requirements. Information classification systems are often abused by classifying information at a high level that does not need to be classified at a high level. This becomes a way to hide information from those who would otherwise have access to it. |
| 6.4.5.3 | All information shall be classified according to its content and purpose, and dissemination limited to those in roles who require it to perform designated responsibilities. | This policy is referred to as “need to know” because it results in access controls that limit information to those who need to have it to perform a given task or job function. | This policy prevents sensitive information from being shared unnecessarily and so protects individual privacy. This policy prevents information sharing by putting a burden of proof that they need to know information content on someone who requests information, when that person may not know the information content. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.5.4 | An individual who approves the disbursement of electronic assets shall never be the same as the person who distributes approved disbursements. | This type of statement is referred to as a "segregation of duties" clause. It has its roots in finance, where invoice approvals where done by an individual who checked that good were delivered before giving permission to send a check to a vendor. The policy is meant to ensure that no one individual is able to disburse electronic assets. | Today's electronic transaction systems allow large quantities of assets to be transferred with very little effort or observation, and this policy requires that two or more people must overtly collaborate in order for electronically-controlled assets to be misappropriated. It allows management to enforce accountability for asset disbursement.<br>The policy prevents individuals from executing transactions without the assistance of others, and so may create delays in the distribution of currency, goods, and services.<br>Where staff resources are scarce, this policy creates unreasonable burden on management efforts to achieve efficiency in transaction execution. |
| 6.4.5.5 | All personnel shall be screened for potential security problems. | Those who handle critical assets must be trustworthy. Screening services check for indications of a poor attitude toward security, including past convictions, outstanding warrants, and substance abuse. | Past issues with security are a good indicator f an individual's propensity to exploit a position or trust.<br>Any screening is a privacy violation. More emphasis should be placed on current job performance than background history. Information used for background checks is widely available in some countries but practically nonexistent in others. This puts individuals in countries who have no background records in an unfairly competitive position for jobs. |
| 6.4.5.6 | Identity management and authentication for<br>individuals who operate government and/or critical infrastructure systems shall be centrally controlled. | This policy would require a system that includes a database of individuals who have access to critical infrastructure, a method to authenticate those people, and a way to provide them with access into government and critical infrastructure systems. | A central function that tracks individual access to critical infrastructure would allow functions such as personnel background checks and strong access control to increase in standardization as well as take advantage of economies of scale.<br>Any large-scale government project designed to provide access to private infrastructure deprives the private property owner of the ability to manage their own assets. Such actions are evidence of totalitarian regimes, not peaceful efforts to solve community security problems.<br>The level of control provided by such a centralized authentication system would potentially itself introduce a large threat, as it may be exploited to gain widespread administrative access to critical<br>infrastructure.<br>This policy is reasonable only for IT systems. A typical ICS or mobile framework does not have a central point at which users are identified, nor a list of what functions system-wide a user should have access to. It tends to rely on IDs delivered with machines and so does not typically integrate with enterprise identity management systems. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.5.7 | Systems that maintain mission critical processes such as industrial control systems (ICS), shall utilize some form of software application whitelisting.. | A *reference monitor* is a generic term in computer security that refers to a process that intercepts requests for system resources and consults a list of authorization rules to see if the requesting subject has access to the requested object. This policy is to maintain a reference monitor to be used to identify and<br>authorize all software on critical systems.. | Among other things, this policy would allow all systems to conform to principles of least privilege. To conform to the "principle of least privilege" means that these systems will allow the minimum individual access required to perform a well-defined function. This would reduce overall infrastructure vulnerability due to a malicious utility employee.<br>This policy is reasonable only for IT systems. A typical ICS or mobile framework does not have a central point from which software is executed, much less identified, nor a list of what software a user should be able to access.<br>There is an old adage: "to a carpenter, everything looks like a nail." As systems acquire more and more software-enabled features, they are viewed as part of cyberspace. However, non-IT systems such as ICS and mobile frameworks are fundamentally different and policies such as these assume a simplicity that does not exist and with which it would be impossible to comply. |
| 6.4.5.8 | Unencrypted data other than that required to monitor business process shall never be available to Operations. | Frequently, Operations has access to all data in an organization because they are responsible for its integrity. This may lead to In advertent or intentional unauthorized data disclosure to Operations staff. | Even if all data were encrypted, there must be automated ways to decrypt it in order for it to be used, and since Operations would need a way to test those processes for integrity like any other, there is no real method of enforcing this policy.<br>Segregation of duties with respect to data access may be established with in Operations groups so that no one individual or support group would be able to see unencrypted data without collusion. |
| 6.4.5.9 | Where the same data is used by more than one department within an organization, authoritative data sources shall be established and each record shall be entered just once and shared with any other organization that requires it. | This type of policy is referred to as a "data origination and reuse" or "need to share" policy. It is usually used in large organizations that process large amounts of data and is usually meant to minimize data storage and human data entry costs. | Implementation of this policy may increase data integrity by minimizing the possibility of mistakes in cross-correlation of records between different departments in a single organization.<br>Organizational boundaries within which data may be freely shared can be difficult to determine where sensitive data is concerned. Data records often contain multiple fields with different security requirements, and these can be difficult to separate when designing data sharing strategies. Different departments may have different requirements to authenticate data sources, and the level of scrutiny provided by the originating department may not meet that requires by a consumer department. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.5.10 | Remote network access to unattended desktops shall never be allowed, even for the purposes of desktop support and maintenance. | This policy would require that desktops be technically configured to allow remote support only when express permission is granted by the desktop user. | This policy is required to maintain accountability for workstation activity. Where is it common for desktops to be commanded remotely by technology staff, the permissions assigned to the user to which the desktop is assigned may be compromised, and/or that desktop user may be able to repudiate network activity performed from the desktop.<br>This policy inhibits the flexibility of technology staff to provide normally intrusive services such as trouble-shooting in an unobtrusive manner. For ICS, shared access is sometimes an operational requirement and could be monitored by biometrics or other means.<br>This policy has the unintended consequence of not being able to make use of remote desktop technology as part of operations support procedures for critical infrastructure, where it is often necessary to provide an external specialist with access normally granted only to internal staff. |
| 6.4.5.11 | Operations shall monitor user activity to ensure that sharing of user access does not occur. | This policy would require that each user of a system be verifiably provided with a unique login identifier, that a profile of usage behavior be associated with each login, and anomalous behavior investigated. | This is a simple and effective way to detect whether users have given their passwords to others and makes it possible to pinpoint which users took what actions during investigations of system activity.<br>This policy would facilitate efficient and effective identification of account hijacking attempts.<br>Not all users should be restricted from sharing access. For example, a married couple may share the working spouse's login to their health benefits website. |
| 6.4.5.12 | Operations shall identify and report any non business use of systems resources. | As operations is responsible for maintaining business process, any cyber resources that are used outside of the proscribed operations process are not authorized. | This policy requires advance preparation of a pre-approved list of authorized use of resources. It deprives users and their management of needed flexibility to experiment with new uses of technology as well as ability to connect new devices to networks, download software, and experiment with technology services without being policed by low level staff.<br>A system cannot be secured if its purpose is not well-defined. If this policy cannot be enforced, then it will not be possible to secure the system. |

# Research and Development

- Research involves breaking new ground, bringing the latest theories and experiments together to hypothesize about a solution to a problem. The process of research is to formulate experiments that will prove or disprove such hypothesis.
- Development is about building systems for which there is some basis to believe that engineering processes using existing materials and processes will be able to be specified to meet requirements.
- Research is less immediately useful to businesses and military operations than is development. Hence, cyber security research issues often center on the efforts of academia to contribute to the growing body of knowledge in cyber security.
- Academic issues necessarily include ways to fund education of graduate students, who are expected to emerge from academic institutions as experts in cyber security technology.
- First the demographics in academia are biased toward younger, more inquisitive, less risk-adverse users, users who are early adopters of technology. These are users who cannot get fired for negligence, and resist and question attempts at education aimed at conformity to policy.
- There is also considerable turnover in this community; every year some existing students leave and new students join ongoing research projects. Finally, controls are more lax in an academic environment. As a result, there is greater risk and less control.
- Since everything is interconnected, this situation can impact other sites. If academic networks and student machines get attacked and compromised, they can be used to launch cyber attacks. Corrupted computers in academia can be used as proxies and bots. This is the environment where most cyber security research takes place.

- Moreover, cyber security research itself is limited to what current academics have identified as hot topics from funding sources. There is little, if any, references in cyber security research to systemic cyber security issues such as those found in industrial control systems.
- Most cyber security research is conducted in departments of computer science and little, if any, in engineering departments. Control theory that is studied in the engineering disciplines does not address security. Fortunately, not all businesses rely on academia to produce research.
- Many cannot wait for innovative technologies to emerge, so some have cultivated their own research institutions dedicated to studying issues of interest to the enterprise. While it is also rare that security issues are included in privately funded research endeavors, it is not completely unheard.
- Development, on the other hand, is a practical necessity in most corporate enterprises. Even where all software code is purchased and customization is outsourced, technology staff is routinely charged with meeting business requirements by engineering solutions composed of existing technology building blocks.
- Security issues in development tend to center around the process used by the development organization and whether it considers security requirements. Moreover, there are software development practices that are known to produce vulnerable code, and it is recommended that these be specifically avoided.
- Policy issues in the practice of security research and development concern government support for research initiatives, both academic and private. The policy statements in the following table begin with high-level nation-state issues, which are followed by statements reflecting concerns for academic and research quality.

# Cyber Security Policy Issues Concerning Research and Development

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.6.1 | The Nation's executive branch shall assemble a committee of cyber security experts from a variety of industries to advise on cyber security policy and assess cyber security programs. | This is a requirement for a Nation's executive branch (e.g., the U.S. President) to reach beyond his small circle of current advisors and seek out assistance on cyber security strategy issues. | The breadth and depth of cyber security issues is beyond the expertise of any one individual. National leaders should have access to the most enlightened views possible.<br>There is no need to establish a policy at this high a level. There are already multiple paths and processes by which national leaders solicit and receive advice on critical issues. Cyber security issues fall into this category. |
| 6.4.6.2 | National government shall help fund basic and applied research in cyber security risk, systems and software, in line with priorities established by the national strategy. As much as possible, such research should be collaborative, multidisciplinary, and unclassified. | This policy would provide funding for cyber security research in software, testing, computer, and network domains. It should also include multidisciplinary studies of the national security impacts (with security studies, legal and international affairs departments) as well as industrial control systems (ICS). | Research and development funding not only produces new security technology that can be applied to today's threats, but motivates graduate students to study cyber security problems, and so contributes to the brainpower that will address future cyber security threats.<br>Research and development funding from the government can sometimes crowd out problems that are considered more germane to the private sector. Moreover, if researchers are unaware of other research (such as if it being done as part of a classified project) funding can be duplicative and wasteful. |
| 6.4.6.3 | Government shall annually review all research and development investments related to cyber security. | This policy would require the production of an annual report describing how national research and development<br>funds allocated to cyber security are spent. | Without a clear research agenda for cyber security, such assessment would be a subjective exercise as opposed to an informative report. At best, it would be a simple enumeration of information easily found else where, and at worst, a witch hunt targeted at subjective evaluation of waste.<br>Other areas of research of strategic interest to the national government are supported with dedicated university affiliated research programs. Cyber Security has reached the tipping point both in importance and the level of funding to adopt a similarly coordinated strategy. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.6.4 | Private sector companies shall be given tax incentives for pursing cyber security research. | Private sector companies typically follow security standards and use existing products rather than devise their own innovative solutions. This policy is intended to motivate innovation. | This policy would increase the overall quantity of cyber security research by attracting participants to the market. Companies not currently engaged in cyber security are not likely to be attracted by a tax deduction, However, such a tax deduction may result in companies reclassifying existing research effort in related field such as customer tracking as cyber security identification mechanisms.<br>This would result is overall reductions in tax revenue without security benefit. This policy may motivate private companies to spend on cyber security research but there is no guarantee that the nation will benefit as they may not share the results of their research. |
| 6.4.6.5 | Shareholders of publicly held companies shall be given tax incentives for pursing cyber security research. | This policy is meant to increase the desirability of stock in companies that pursue security goals. | Investments in cyber security research should be judged by marketplace results, rather than simply spending which may not yield actual security benefits.<br>This policy would motivate the private sector to fund research in cyber security. It could increase their market value and also stimulate economic interest in cyber security products. |
| 6.4.6.6 | National competitions shall be established to reward student talent for and innovation in cyber security. Other competitions can also reward outstanding universities and research institutions. | Competitions with cash prizes are intended to attract talented students to the study of cyber security issues. | Implementation of this policy should create a community of students interested in joining the cyber security workforce.<br>This program might reward students for studying techniques that could be used malicious hacking, rather than defense. |
| 6.4.6.7 | Nations shall encourage awareness, education, and training for cyber defense starting with students in primary or middle schools and continuing through specific technical training for cyber defenders. | Cyber safety, cyber security and cyber ethics are currently the subject of pilot programs in the elementary and high school, this policy would move them into the mainstream curriculum. | This policy would promote critical thinking about cyber security at an early age, and by so doing influence future decision makers to incorporate ethical principles into systems of the future. Investments in training and education will drive a more sophisticated workforce and cyber specialists.<br>This policy would raise the level of cyber security nationwide. The general populace would better understand how to protect themselves in cyberspace, while professionals in information security would have a more intuitive grasp of how to secure their systems and software.<br>Education is a large-scale effort as many people deal with cyberspace and need varying levels of understanding. This means a potentially expensive and long-term effort. Moreover if awareness programs that are technology specific (“practice safe faxing kids!”),they would rapidly be out of date. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.4.6.8 | National governments shall make university scholarships available to students wishing to pursue studies in cyber security, in return for a period of government service. | This policy is intended to motivate students to study cyber security at the college level. Undergraduate college curriculums typically do not include cyber security specialization. | There are not enough knowledgeable cyber security professionals in the nation to fill the jobs expected to be required to safeguard national interests. A national scholarship program would provide a pipeline of qualified professionals.<br>Graduates of undergraduate programs will not have much cyber security expertise. Cyber Security focus usually starts at the Masters level because the amount of foundational knowledge required to practice cyber security in any given domain requires undergraduate concentration in the domain itself.<br>This policy would motivate the creation of cyber security curriculum and also motivate students to pursue cyber security work in government. It may also encourage universities to develop programs where none currently exist, such as cyber security of industrial control systems. |
| 6.4.6.9 | Academic communities shall pursue student chapters of cyber security industry associations. | Many industry associations cultivate student chapters, but the cyber security professional associations currently do not have much momentum in this direction. | Today's students are engaged in social networking. Cyber security awareness tends to discourage social networking. This type of program would bring together students working on cyber security in a cyber safe environment.<br>Cyber security professional associations have experience requirements to which students should aspire and these are freely available on websites. There is no need for more formal awareness activity of this career path. |
| 6.4.6.10 | Research and development into cyber security systems, technologies, and operations shall be pursued to the extent necessary to fill gaps between management objectives to secure cyberspace and current capabilities. | It is often the case that management would like to control a cyber environment but lacks the methods, tools, and procedures with which to enforce control. This situation puts them in a position of responsibility without authority. | This policy empowers managers who are accountable for controlling assets with the means by which to do so in the long term, even if their current capabilities are lacking.<br>Policies like this may be viewed as an open checkbook for all sorts of research related to cyber security without foreseeable benefit to the organization. |
| 6.4.6.11 | All software development shall adopt best practices for securing the software development life cycle. | This policy would require adherence to secure software coding practices as well as security testing. | Secure coding practices are known to reduce vulnerabilities in deployed technology products.<br>Innovation requires constant change in organizational strategy and process. Secure coding practices are too static to adapt to the pace of technology growth. |

# Cyber Infrastructure Issues

- This section contains illustrative examples of cyber infrastructure issues faced by private sector industries.
- The U.S. Department of Homeland Security's National Infrastructure Protection Plan (NIPP) acknowledges 18 such examples as the critical infrastructure and key resources (CIKRs) of the nation that are managed by the private sector (DHS 2009).
- Though some are more active than others, each of these sectors is required by the plan to participate in a public–private sector partnership efforts to secure the national infrastructure.
- The list of sectors include food and water systems, agriculture, health-care systems, emergency services, information technology, communications, banking and finance, energy (electrical, nuclear, gas and oil, and dams), transportation (air, highways, rail, ports, and waterways), the chemical and defense industries, postal and shipping entities, and national monuments and icons.
- Examples of information assurance policies in the illustrative domains of financial services, health care, and industrial control systems. Note that industrial control systems is not itself an industry sector, but a generic label for the type of automated equipment used in a wide variety of industry sectors.

# Banking and Finance

- The banking and finance industry encompasses a wide variety of institutions with the common focus on products and services for managing money. These institutions include banks, credit card issuers, payment processors, insurance companies, securities dealers, investment funds, clearance firms, and government-sponsored lenders.
- The industries now use e-commerce capabilities for online fund transfers, mortgage research and applications, viewing of bank statements, sales of financial advice or guidance, and subscriptions for interactive consulting. As the sector manages money using information technology, it is constantly threatened by cyber attacks. Capable and persistent cyber criminals present increasingly organized and sophisticated approaches to commit theft and fraud.
- Security has always been a concern of the banking and finance industry. The banking and finance industry is also a dept at fraud detection and response. These concerns have driven the development of many technical Internet security controls. The industry has a thoroughly documented history of dedication to various public and private forums to provide defenses against attack, enhance resiliency, and sustain public confidence in trusted banking relationships.
- The financial industry has long been plagued by the cyber security crime of identity theft. Identity theft is not actually a crime against the bank, but against its customers. Banks are affected as customers in bulk are taken in and thereafter impersonated by criminals, who gain access to bank accounts and withdraw funds.
- As banks are used to fraud, this activity has been tolerated as the cost of e-commerce. Nevertheless, the pain that bank account takeovers cause consumers has caused bank regulators to issue a requirement that banks add a second “factor” of authentication.

- second factors chosen by banks were variations on the password theme in that they are still easily appropriated, either by being guessed by someone who knows certain information about an individual, or by an intruder who invaded a consumer desktop.
- Information security practitioners consider authentication strength to increase in three levels, generally characterized as something you know, something you have, and something you are. something you know is a password. Something you have is a physical component in the possession of an individual that is used to facilitate identity verification.
- Something you are is a measurement based on physical biology, called a biometric. Examples are fingerprints and retina scans. This policy requires the second of the three levels: something you have that would not be vulnerable to such guessing and eavesdropping threats.
- The continuing threat to consumer confidence in financial institutions motivated bank regulators to issue a “red flag” rule. This rule requires a banking institution to monitor for potential critical activity on a person’s account with the goal of detecting fraud in progress and preventing account takeovers. The rule requires that both customers and regulators be notified of fraud attempts thwarted by the bank.
- The policy statements in this section therefore range from regulatory issues to consumer concerns. They are familiar to the banking and finance industry. The first few concern regulations that apply specifically to the banking and finance sector, but could more broadly apply to any company that is a party to online monetary transactions.
- The next few concern the banking and finance industry as well as any company that spends a great deal of time and money on security regulatory compliance. The remainder are examples of financial cyber security policy concerning services that banks may or may not include in their own cyber security policy to achieve cyber security goals based on their own risks assessments, and these would not be directly influenced by external standards or regulation.

# Cyber Security Policy Issues Concerning Banking and Finance

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.5.1.1 | Regulations such as privacy of personal data (GLBA), and due diligence in detection of and response to threats (FACTA) to customer accounts shall apply uniformly to all institutions that handle consumer information. | Currently these regulations impose management and audit requirements only on financial institutions and this policy would extend it to retailers and other companies that handle sensitive information on consumers. | The unequal application of regulatory standards to financial and non financial firms conducting similar lines of business is an ongoing concern, both in terms of competition and with respect to the notion that a break in the weakest link of a chain wreaks havoc upon the chain as a whole.<br>Financial institutions are the only type of organization where actual consumer assets are at risk, and hence there is no need to extend security requirements to other industries. |
| 6.5.1.2 | Bank regulatory authorities shall increase minimum regulatory capital requirements where the cyber security risk profile of a financial institution indicates systemic security issues. | Regulators routinely set minimum capital requirements that banks should have in the event that unforeseen events require them to cover losses in investments made with accountholder assets.<br>This would require them to maintain additional balances where investments were at risk due to cyber security issues. | The potential amount of money that banks may lose due to cyber security attacks has no upper bound, and this policy could require banks adequately prepare for the possibility of those events.<br>Information security risk has long been a component of technology risk, which is itself a component of operations risk. These risks have long been under scrutiny by regulators and no new regulations are required to ensure this occurs. |
| 6.5.1.3 | Financial institution regulatory authorities shall not proscribe how security controls should work, and instead emphasize that financial institutions shall accomplish goals for transaction security for every consumer. | Although regulations do not specify the technical configuration of security measures, regulatory auditors have taken a best practice approach to regulation enforcement. The result is that banks must use regulatory guidance as checklists in order to pass regulatory security inspection. | Banking regulations are detailed to the extent of micro-managing financial institution cyber security risk reduction strategies. This stifles innovation with respect to security control measures and also relieves financial institutions of responsibility for independent development of transaction security strategy adequate to control fraud and misuse of consumer and business accounts.<br>Best practices exist because organizations have been successful thwarting fraud and account misuse by implementing those strategies. Regulatory auditors who collect these strategies and audit accordingly are raising the bar for security hygiene within the industry. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.5.1.4 | Regulators shall provide clear guidance that will alleviate concerned with wireless security technology to facilitate financial transactions on mobile devices. | Consumers use just beginning to use financial services over mobile devices, and there is no special regulation that covers this communication of transactions. | Just as online banking introduced the threat of identity theft, the introduction of financial transactions over wireless media could introduce currently unknown exposure, which should be a subject of immediate concern.<br>The technology used to conduct transaction over wireless media is sufficiently similar to that used for current Internet banking transactions that no new regulatory oversight is required.<br>Regulators are not in a position to understand enough about wireless technology to proscribe safe usage. Banks should be accountable for transaction security for all transactions they support regardless of platform. |
| 6.5.1.5 | Laws that require notification to financial customers when sensitive data is exposed shall be uniform nationally, and if possible, globally. | Currently, every U.S. state has its own data breach notification laws, and many non-U.S. countries have their own laws as well. These are often inconsistent. | Banks that may have locations in only one state nevertheless have customers who are residents of other states. This required small banks to expend considerable legal resources to reconcile and regulations just to plan for the possibility of a data breach, even if one never occurs.<br>Data breach laws should be molded by the people whose privacy is at stake. As communities can only enact laws within their own jurisdiction, these laws are properly enacted at the state level. |
| 6.5.1.6 | Financial institution crime pattern analysis data including bank identification shall be made available to all consumers. | Although new reports of security breaches and identify theft are ubiquitous, legal requirements for crime reporting is confined to regulatory relationships and regulators do not share this data with the general public. | Financial institutions voluntarily share identity theft information through industry associations such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), the Anti-Phishing Working Group (APWG), the Identity Theft Assistance Corporation (ITAC) (FDIC 2004). This data is widely published and available for critical review.<br>While financial institutions may experience large-scale fraud and data breaches without informing the general public, there will be no incentive to make security a marketplace differentiator. |
| 6.5.1.7 | Consumers shall be allowed to restrict transactions that transfer balances out of their account to well-defined parameters that preclude money being transferred outside their accounts in ways that are unexpected. | Many banks provide “positive pay” services that require accountholders express preapproval to execute transactions that transfer balances out of their account. | If all banks offered such services and consumers were aware of them, a great deal of fraud could be avoided.<br>Consumers have a difficult time with even simple online transactions, and the extra security layer of express approval for wire transfers could discourage them from using the most convenient mechanisms fo accomplishing online banking. |

# Health Care

- The health-care industry encompasses a wide variety of institutions with the common focus on products and services for maintaining health. These institutions include hospitals, doctor's offices, diagnostic laboratories, medical equipment manufacturers, emergency care specialists, visiting nurses, and a host of other medical community professionals and services.
- These institutions use typical enterprise support systems such as accounting, administration, collaboration, and advertising. In addition, from the perspective of cyberspace operations, these constituents will utilize two types of mission-critical systems unique to the health-care industry: systems used to administer medical practice and systems used to administer medicine.
- By administering medical practice, we mean the tools and techniques of doctor's offices, hospitals, other care providers, pharmacies, pharmaceutical manufacturers, and insurance providers to ensure that medical facilities and supplies are available and medical staff are recruited, trained, and paid.
- By administering medicine, we mean the process of caring for human patients. We shall call these logistics systems and provider systems, respectively. Logistics and provider systems used by the health-care profession differ in both functionality and data content.
- The primary function of logistics systems is to track patients and resources through the maze of organizational workflow that has been created in order to connect patients with health-care providers, facilities, and treatments.

- The organizational workflow streams from patient home computers through workplace benefits systems, insurance agencies, diagnostic, and treatment facilities. Data content in these systems is the information required by this organizational workflow to function. It includes data that many patients consider private, and information security with respect to such information is regulated by the Health Insurance Portability and Accountability Act (HIPAA) (HIPAA 2003).
- The primary function of provider systems is to provide a patient with medical care. These include drug delivery pumps, automated sample chemical or viral analysis, diagnostic imaging tests, remotely monitored electrical implants, and a wide variety of other innovative devices.
- The information flowing through these systems may begin with the authorization from a logistics system, continue through physician prescriptions, include automated or manual analysis to identify treatment appropriate to given patient conditions, and incorporate test results and automated communication of those results to logistics systems, completing the information life cycle for a simple treatment. Moreover, a single patient likely to require any one provider system interface is likely to incur multiple records on a variety of provider systems.
- Cyber security issues unique to logistics and provider systems often focus on interoperability. Interoperability is a major goal for the health-care industry because it is seen as an enabler of fast and accurate decision making with respect to patient treatment. Where logistics systems may be rapidly combined with provider systems, patient histories may be automatically factored into expert-system-based diagnostic and prescription algorithms, enabling more accurate and effective treatments.
- The policy statements in this section therefore range from regulatory issues to life and death concerns. They should be familiar to those working in cyber security within the industry. The first few concern what cyber security professionals refer to as “hygiene” issues.

- They discuss information security standards that have been known to be effective in reducing risk of data breaches when applied consistently to enterprise data. The next few concern cyber security risks introduced by interoperability requirements or lack thereof between various types of health-care data repositories ranging from medical devices to aggregate case databases.
- The remainder concern information sharing issues and potential interrelationships between policy goals for information sharing and policy goals of privacy and integrity.

# Cyber Security Policy Issues Concerning Health Care

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.5.2.1 | All systems used by a health care company shall be operated in compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. | HIPAA specifies administrative, physical, and technical safeguards for covered entities to use to assure the confidentiality, integrity, and availability of electronic protected health information. | Information may be transferred internally within the organization via unexpected methods. Making the scope of the company HIPAA program the entire systems environment ensures that such unanticipated transfers do not result in unintentional exposure of electronic protected health information. Many company's office systems maintain information that is just as sensitive as electronic health information, for example, personally identifiable information about its own employees.<br>The HIPAA compliance program is very expensive to operate and the scope of the regulation is very clear. Narrowing the implementation strategy to administrative, physical, and technical safeguards for only the systems that store and transmit electronic protected health information allows adequate protection without unnecessary cost, which would be passed to consumers. |
| 6.5.2.2 | Cyber Security regulation with respect to health care shall impose Technology requirements for data protection based on information classification. | This requirement is motivated by privacy concerns. Although HIPAA addresses health care concerns, it does not fully cover sensitive health care data in every format in which it is currently used in all logistics and provider systems. | Any technology requirement may increase cost of service delivery, so unless there is a specific return on investment in terms of either overall health care effectiveness or cost reduction in logistics or provider systems, it does not make sense to legislate cyber security for health care data.<br>Organizations are not currently motivated to secure data. Even HIPAA regulations allow data sharing beyond patient needs given patient consent. Patients in need of health care are too preoccupied to make informed decisions on long-term use of their health data and so should be able to rely on privacy without being asked to sign it away.<br>Experience with the financial industry shows that even the most detailed technical security requirements cannot anticipate all possible security threats, and therefore cannot adequately address overall goals for security, so any low-level regulation is not likely to be effective. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.5.2.3 | Non repudation and accuracy of data shall be addressed by health care provider policy prior to confidentiality. | This policy acknowledges that there are multiple objectives for security policy and suggests that the ability to identify who modified data and whether it is correct should be the primary goal of a healthcare security program. | Healthcare resources are scarce and privacy should not be the overarching priority on how to spend security dollars, No one ever died of embarrassment, but they have died by getting the wrong prescription.<br>This policy assumes that security dollars are static. The same security control measures that protect integrity may be leveraged to ensure some measure of privacy. |
| 6.5.2.4 | Access to health care data shall be contingent upon evidence that such access is required to diagnose or treat a specific case. | Current proposals for health information data sharing do not include requirements relating to the specific purpose of data sharing. This policy would introduce the requirement. | Qualified health care providers should not be worried about justification for data access. It is enough that they be subject to audit.<br>Qualified health care providers should not be required to provide justification for data access in advance of treatment because it would slow down the healthcare delivery.<br>It is enough that they be subject to audit. All access to personal healthcare data must be justified with reference to a specific patient and condition requiring health care provider attention.<br>Access to health care data is often justified by the needs of law enforcement to develop a criminal case against victims of violence, who may not be able or willing to prosecute their attackers. Criminal investigations may also require health care providers to provide records of patient care in the course of developing cases that are not focused on the patient as victim, but as a potential suspect, witness, or other relevant relationship to the crime. Hence, all such records shall be made available to law enforcement with proper oversight and approval. |
| 6.5.2.5 | Wireless devices implanted in patients shall require strong authentication in order to operate command and control features. | There are a wide variety of medical devices with electronic circuits that accept commands that change electronic signals and medicine doses. There are not current security standards with which they are controlled. | While there is no know threat to patient health due to wireless cyber security attacks, research into the security of these devices introduces an unnecessary cost. There need to be security standards and equipment certifications for this critical equipment. As these devices allow remote command and control capabilities, any malicious individual who understand how they work may commit murder without any trace of evidence.<br>Until the security options for such devices are well understood, it is not possible to assess the risks to the patient using the devices. At minimum, remote or wireless access should not be allowed unless there is a way to audit who performed what activity performed on devices remotely. |

# Industrial Control Systems

- Despite their high reliance on automation, ICSs are not typically designed with access controls, their software is not easily updated, and they have little forensics capability, self-diagnostics, or cyber logging. While the lifetime of the equipment in an IT network typically ranges from 3 to 7 years before anticipated replacement and often does not need to be in constant operation, ICS devices may be 15 to 20 years old, perhaps older, before anticipated replacement, and run 7 × 24 × 365.
- Patching or upgrading an ICS has many pitfalls. The field device must be taken out of service which may require stopping the process being controlled. This in turn may cost many thousands of dollars and impact thousands of people. An important issue is how to protect unpatchable, unsecurable workstations such as those still running NT Service Pack 4, Windows 95, and Windows 97.
- Many of these older workstations were designed as part of plant equipment and control system packages and cannot be replaced without replacing the large mechanical or electrical systems that accompany the workstations. Additionally, many Windows patches for ICSs are not standard Microsoft patches but have been modified by the ICS supplier. Implementing a generic Microsoft patch can potentially do more harm than the virus or worm against which it was meant to defend.
- The biggest threat to industrial control systems is not necessarily the remote access necessary to maintain the operation of the field devices. An example is the Idaho National Labs Aurora demonstration that physically destroyed a diesel generator by exploiting dial-up modems.

- Another major concern is the number of people who have physical access to the controllers that may change the software on the chip sets that issue machine instructions.
- ICS security is a relatively new field and requires development of ICS-specific security verification procedures to enforce even agreed-upon policies. Even cyber security management standards are not directly applicable as they specifically address only IT management. Consequently, organizations such as the International Society of Automation (ISA) initiated an effort to develop standards for ICSs-S99-Industrial Automation and Control Systems Security.
- Some of the other organizations developing standards for ICSs include the Institute of Electrical and Electronic Engineers (IEEE), International Electrotechnical Commission (IEC), International Council on Large Electric Systems (CIGRE), North American Electric Reliability Corporation (NERC), Nuclear Energy Institute (NEI), and the U.S. Nuclear Regulatory Commission (NRC).

# Cyber Security Policy Issues Concerning Industrial Control Systems

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.5.3.1 | Systems whose misuse may cause severe damage to persons and property shall require strong authentication to operate. | This policy would require authentication to operate any system where accidents may cause damage, such as boats with wireless autopilots. | There is no reason to believe recreational vehicles will be targeted by cyber threats, and this policy would require significant cost in redesigning electronic components of these systems. Moreover, it is likely to have the unintended consequence that electronic parts from different manufacturers will be difficult to integrate.<br>The race to the electronic marketplace has created a dangerous situation wherein many devices are operated with Internet-based and/or wireless commands that can be entered by anyone knowing the manufacturer specifications. It is irresponsible of manufacturers to build capabilities into devices that allow them to be operated by anyone other than the owner.<br>There is as much probability to believe that limiting access to control systems will cause accidental damage as there is for them to be controlled by criminals who intend to cause damage. |
| 6.5.3.2 | Current cyber security threats and corresponding statutory and legal frameworks that address cyber security for critical industrial control systems shall be reviewed and reported upon annually. | This would require national agencies and other publicly funded organizations that perform cyber security threat intelligence to combine their findings annually into a consolidated report that includes laws related to cyber security. | The findings, conclusions, and recommendations resulting from such a review will be invaluable to inform future legislation.<br>Though examination of existing legislation in comparison with a changing environment is a good idea, the way this policy is worded, there is no strategic objective. Such an open-ended review may result in a waste of taxpayer dollars.<br>Annual publication of such a report is meaningless, this should not be a report process, but an expectation for government security services that the comparison should be constantly updated and available in order to ensure that controls continuously improve in the face of changing threats. |

| | Policy statement | Explanation | Reasons for controversy |
|---|---|---|---|
| 6.5.3.3 | Nations shall mandate the strength of encryption used for identification and authentication credential in critical infrastructure sectors. These extra protections shall also apply to key industrial control systems (ICS) in the critical infrastructure sectors. | Organizations in the critical infrastructure sectors deal with confidential information and the control of industrial systems. This is a requirement for security control commensurate with the amount of potential damage from their abuse. | This policy will match the high criticality of information in these sectors with concomitant protection. These kinds of information should not rely on the insecure systems of the Internet. Encryption and identification credentials are important to help establish higher assurance for these sectors. This policy is already in place for many sensitive government systems, and the industrial control systems used to manage critical infrastructure are just, if not more, vulnerable to national security threats.<br>This policy will also add cost and complexity to the already difficult to maintain SCADA, PLC, and other ICS component architecture. Additional authentication may not be easy to use, and thus may interfere with operator ability to control these devices. The way to secure these systems is to decrease, not increase complexity. |
| 6.5.3.4 | ICS design criteria shall include requirements for cyber security. | ICS designs are based on performance and safety. This policy would ensure that cyber security requirements are incorporated into designs as well. | The ability to use electronics in unintended ways is commensurate with the functionality and data storage capacity of the circuitry. The ability to use ICS in unexpected ways is at least partially dependent on the capability in these circuits. Awareness that malfunctions or intentional manipulation of the data content of ICS cyber-enabled functionality should inspire overall system designs that protect it from intentional or accident corruption.<br>Awareness that ICS malfunctions or intentional manipulation should motivate cyber malfunction detection measures that are currently missing and need to be developed to identify intentional or unintentional cyber incidents. Electronically controlled physical devices may be controlled physically as well as logically. Malfunction detection measures currently prevalent in ICS should be able to compensate for intentional or unintentional cyber functionality failures. |
| 6.5.3.5 | ICS design shall include capability for cyber forensics. | Industrial accidents happen frequently, and investigations inspect cyberspace logs and configurations if they are available. However, many PLCs, DCSs, and SCADA systems often do not identify or store the digital evidence that would be useful in such investigations. | This area is ripe for research and development to determine what specific types of cyber forensics are needed and how they would be utilized in the least noninvasive manner possible.<br>The ICS community has the knowledge-base to understand what physical parameters are required to perform a root-cause analysis of an incident. Consequently, the ICS community has developed the detailed forensics for physical parameters—temperature, pressure, level, flow, motor speed, current, voltage, etc. However, the legacy/field device portions of an ICS have minimal to no cyber forensics. Moreover, it is not clear that adequate cyber forensics exist for even newer ICSs. |