Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line

Steven R. Chabinsky*

THE PROBLEM

The Internet seems to offer the promise of everything to everyone. For global and local business, it lowers costs while increasing innovation, invention, effectiveness, and efficiencies. For wealthy and poor economies alike, the Internet greatly expands markets for products and services. For peoples free and repressed, it provides an inlet and an outlet of expression. For large and small communities, whether living in urban centers or outlying regions, the Internet enables control over critical power, transportation, water, and sewerage systems.

Lest we forget, for sophisticated criminals, terrorists, warmongers, and spies, the Internet also offers the chance of a lifetime to cheat, steal, and strike from afar with little money, covered tracks, and enormous real world impact. While the ability to use the same technology for positive or destructive ends is neither new nor momentous, it is necessary to consider whether the rapid adoption of the Internet has provided so considerable an asymmetric advantage to our adversaries that it can change the course of American history. In this regard, when we consider the intent and capabilities of our enemies, we cannot underestimate them or, as the 9/11 Commission found in a different context, suffer from failures in imagination, policy, capabilities, or management.

Thus our future remains uncertain. Based on our increasing reliance on networks to drive our economy and support our health, welfare, communications, and security, certain questions loom large. For example, can our enemies control whether, how, and when our systems operate and our vital services get delivered? Are our personal and business records, corporate intellectual property, and state secrets routinely exposed or imperceptibly altered?[1]

Unfortunately, the answers to these questions not only remain unknown, they perhaps are unknowable. Therefore, it is difficult to provide our nation's government leaders, corporate executives, shareholders, and citizens with reasonable assurance that our computer systems have not been

---

* Deputy Assistant Director, Federal Bureau of Investigation.

1. Especially worrisome are the cyber attacks that would hijack systems with false information in order to discredit the systems or do lasting physical damage. At a corporate level, attacks of this kind have the potential to create liabilities and losses large enough to bankrupt most companies. At a national level, such attacks directed at critical infrastructure industries have the potential to cause thousands of deaths and hundreds of billions of dollars worth of damage. *See* U.S. Cyber Consequences Unit (US-CCU), http://www.usccu.us/#Key_Features_ of_the_US-CCU's_Research (an independent, nonprofit research institute).

penetrated, that our software has not been adulterated, and that our hardware does not contain implants. Similarly, it is difficult to state with confidence that over time our mission-critical data and systems – which underlie our economic prosperity, national security, and public health – will remain accurate and available when needed.[2]

We do know that cyberexploitation is occurring at an unprecedented rate by a growing array of state and nonstate actors against a wide range of targets,[3] and that the threat will continue to grow as our society becomes increasingly reliant on information systems.[4] For these reasons, just over four months into his Presidency, Barack Obama announced that "our digital infrastructure – the networks and computers we depend on every day – will

---

2. A glimpse into the full scope of this problem is reflected in the SANS Institute's expert consensus ranking of the top ten cyber threats:

1. Increasingly Sophisticated Web Site Attacks That Exploit Browser Vulnerabilities – Especially on "Trusted" Web Sites.
2. Increasing Sophistication and Effectiveness in Botnets.
3. Cyber Espionage Efforts by Well Resourced Organizations Looking to Extract Large Amounts of Data – Particularly Using Targeted Phishing.
4. Mobile Phone Threats, Especially Against iPhones and Android-Based Phones; Plus VOIP.
5. Insider Attacks.
6. Advanced Identity Theft from Persistent Bots.
7. Increasingly Malicious Spyware.
8. Web Application Security Exploits.
9. Increasingly Sophisticated Social Engineering Including Blending Phishing with VOIP and Event Phishing.
10. Supply Chain Attacks Infecting Consumer Devices (USB Thumb Drives, GPS Systems, Photo Frames, etc.) Distributed by Trusted Organizations.

See SANS Institute, Top Ten Cyber Security Menaces of 2008, http://www.sans.org/press/top10menaces08.php.

3. The full dimension of the cybersecurity problem includes not only risks to the confidentiality, integrity, and availability of sensitive data, but also substantial risks to the command and control of important physical assets such as electric power grids, water supply, and other critical infrastructure. *See, e.g.*, DEPARTMENT OF HOMELAND SECURITY, PRIMER CONTROL SYSTEMS CYBER SECURITY FRAMEWORK AND TECHNICAL METRICS (2009), *available at* http://www.us-cert.gov/controlsystems/pdf/Metrics_primer_v9_7-13-09_FINAL.pdf. "Electronic control systems that operate much of the Nation's critical infrastructure are increasingly connected to public networks, including the Internet. Consequently, control systems and the associated critical infrastructure are at greater risk than before from externally initiated cyber attacks." *Id.* at 1.

4. *Intelligence Community and Annual Threat Assessment: Hearing Before the Sen. Armed Serv. Comm.,* 111th Cong. 38 (2009) (statement of Dennis C. Blair, Dir. of Nat'l Intell.), *available at* http://www.dni.gov/testimonies/20090310_testimony.pdf ("As government, private sector, and personal activities continue to move to networked operations, as our digital systems add ever more capabilities, as wireless systems become even more ubiquitous, and as the design, manufacture, and service of information technology have moved overseas, the threat will continue to grow.").

be treated as they should be: as a strategic national asset," to be protected as "a national security priority."[5]

To be sure, numerous academic and professional fields have developed around cybersecurity and risk management. All is not lost. Most certainly, there is a corresponding need to guard against an overreaction to these problems that would lead to total risk avoidance at all times for all things. Yet, how many people have the data necessary to assess their vulnerabilities, the threats against them, and the harm they are facing in the event of a successful attack? Each data point is essential to establishing an accurate risk profile and, in turn, making informed decisions about how we prioritize and protect our resources. Similarly, how many directors, officers, and government leaders understand who within and outside their organization affect their risk posture? Is the systems administrator or the chief information security officer in charge? Or, as tends to be the case far too often, is the company put at risk when an employee shows up at work one morning with a thumb drive that he plugs into his desktop's USB slot?

Regrettably, we have brought these vulnerabilities upon ourselves, having first invented the Internet and then having eagerly embraced the ensuing Digital Revolution without establishing a corresponding viable security structure. This point has not been lost on FBI Director Robert Mueller, who likened our predicament to that of Ancient Rome. In 2007, Mueller said:

> There is an old saying that all roads lead to Rome. In the days of the Roman Empire, roads radiated out from the capital city, spanning more than 52,000 miles. The Romans built these roads to access the vast areas they had conquered. But, in the end, these same roads led to Rome's downfall, for they allowed the invaders to march right up to the city gates.[6]

I. FRAMING A CYBERSECURITY STRATEGY

It is difficult to develop a national strategy for a subject as vast as cybersecurity. Where do we start and, perhaps equally perplexing, how do we know when to stop and move on toward implementation? From a federal government perspective, these questions were presented not long ago to the National Cyber Study Group (NCSG). The NCSG was formed by the Office of the Director of National Intelligence and began to meet

5. Remarks by the President on Securing Our Nation's Cyber Infrastructure (May 29, 2009), *available at* http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

6. Robert S. Mueller, III, Dir., FBI, Address at Penn State Forum Speaker Series (Nov. 6, 2007), *available at* http://www.fbi.gov/pressrel/speeches/mueller110607.htm.

weekly in May of 2007.[7] Under the skillful leadership of Melissa Hathaway,[8] the NCSG developed in less than a year the cyber strategy that would later be adopted by the White House as the Comprehensive National Cybersecurity Initiative (CNCI).[9] The CNCI is contained within National Security Presidential Directive 54, which is cross-designated as Homeland Security Presidential Directive 23. That document remains classified and therefore unavailable to the public, although the White House has released an unclassified summary.[10] Nevertheless, for purposes of this article, knowing the entirety of the policy is less important than exploring the framework used to develop, monitor, and coordinate the strategy.

II. THREAT ACTORS AND THREAT VECTORS

It has been observed wisely that while no models are perfect for developing strategy, some are at least useful. The first imperfect and ultimately useless model that NCSG members considered was to break down cybersecurity strategy into the three components of computer network operations (CNO) – namely, computer network attack (CNA), computer network exploitation (CNE), and computer network defense (CND).[11] At first blush, this approach seemed reasonable. If policy makers

7. The NCSG consists of dozens of senior managers from across the government. The sheer number of high-level representatives seated at the table (and spilling over to the seats lined up against the walls) is a visible indicator of the magnitude of both the cyber problem set and the cyber solution set from within the federal executive branch alone. The NCSG includes members from the seventeen-agency intelligence community, the Executive Office of the President, and law enforcement, homeland security, military, and civilian departments and agencies.

8. Hathaway was later called upon by President Obama to serve as Acting Senior Director for Cyberspace for the National Security and Homeland Security Councils, responsible for leading the 60-day interagency review of the plans, programs, and activities underway throughout the government dedicated to cybersecurity. *See* President Obama Directs the National Security and Homeland Security Advisors To Conduct Immediate Cyber Security Review (Feb. 9, 2009), *available at* http://www.whitehouse.gov/the_press_office/AdvisorsToConductImmediateCyberSecurityReview/.

9. Despite the underlying breadth and wisdom of the strategy, it is a fair criticism to note that the CNCI name is overstated in its use of the term "comprehensive." Getting our nation's collective arms around the problem known generally as "cybersecurity" is difficult, if for no reason other than the dynamic nature of the global ecosystem known as "cyberspace." Policy makers cannot help but leave strategic gaps that are in need of continual review. Cybersecurity policy, like cybersecurity itself, is a process. There are no one-time solutions.

10. The unclassified summary of the CNCI is available at http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

11. The Department of Defense defines "Computer Network Operations" (CNO) as "[c]omprised of computer network attack, computer network defense, and related computer network exploitation enabling operations." DEP'T OF DEF., DICTIONARY OF MILITARY AND ASSOCIATED TERMS, Pub. No. JP1-02, at 96-97, *available at* http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf. "Computer Network Attack" (CNA) consists of "[a]ctions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."

could determine which departments, agencies, infrastructure owners, and thought leaders played prominently in strategic development within these three areas, surely (the logic held) they would be well on the way to organizing new solutions.

The model broke down quickly, however. It did not take long for the NCSG to realize that the definitions of CNA, CNE, and CND are muddied, without clear legal or policy distinction, and often bleeding between themselves. One person's CNE may be another person's CNA, and the other way around. After all, the same root access typically used by an intruder to conduct surveillance of a network can be used by the same intruder for the purpose of shutting down the network entirely. Meanwhile, CND has been viewed by some to consist of information security officers focused on their own targeted systems and, equally, of others who would try to neutralize the threat along its route, including at its source.[12] As a result, the skill sets, mission authorities, and actors underlying CNA, CNE, and CND are likely to be grouped together rather than distinguished from one another.[13] Hence, for purposes of strategic development, breaking the problem down along CNO divisions turns out to be a non-starter.

Moving on, one might be tempted to consider breaking down the problem (and the response) by the identity of the threat. Such an effort would quickly lead to organizing the cyber threat into three broad categories: nation states, terrorists, and criminals (the latter two would include organized groups as well as lone offenders.). The appeal of this particular breakdown is that it aligns most closely with our nation's executive branch authorities. Clearly defined departments or agencies are involved and have primacy, whether domestic or abroad, in the event of a state-sponsored act of war or espionage against our government or private sector interests, and similar distinctions emerge under both law and executive orders in the event of terrorist or criminal activity.[14] The trouble

---

Id. "Computer Network Defense" (CND) is "[a]ctions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks." *Id.* "Computer Network Exploitation" (CNE) is defined as "[e]nabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks." *Id.*

12. By way of example, military doctrine describes the term "active defense" as "[t]he employment of limited offensive action and counterattacks to deny a contested area or position to the enemy." *Id.* at 4.

13. *See, e.g.*, Adam Stump, *Vice Chairman Cites Need for Cyber Warfare Experimentation*, DEFENSE LINK, June 20, 2008, *available at* http://www.defenselink.mil/news/newsarticle.aspx?id=50273 (reporting on remarks made by Vice Chairman of the Joint Chiefs of Staff, Marine Corps Gen. James E. Cartwright, about building a military force that has both the 'defend and operate skills' and the 'exploit and attack skills.').

14. *See generally* Title 10 of the United States Code; National Security Act of 1947, Pub. L. No. 235, 61 Stat. 486 (1947) (vesting war powers in the Secretary of Defense); Title 50 of the United States Code; Exec. Order 12,333 (as amended), *United States Intelligence Activities*, 73 Fed. Reg. 45,325 (July 30, 2008); and Title 18 of the United States Code

with spending time approaching policy from the perspective of the adversary's identity, however, is that it is either meaningless or difficult to implement in practice. Our networks are almost indistinguishably vulnerable to a wide array of nation states, terrorists, and criminals (all of whom may interact with one another). Thus our network defenders are not substantially assisted by emphasizing jurisdictional or policy factors. Moreover, attributing a specific cyber event to a particular actor remains difficult by design.[15]

Ultimately, the NCSG settled on a rather elegant solution to the cybersecurity problem. Rather than first focus on CNO or threat actors, the group charted out the cyber threat vectors. It turns out that the threat vectors fall rather neatly into four broad categories: supply chain and vendor access, remote access, proximity access, and insider access.

With respect to the supply chain, it is widely accepted that the global economy has given our nation the ability to compete and purchase services in an expanded market that has driven down prices and promoted rapid invention and innovation. Unfortunately, the global supply chain also has substantially increased our vulnerability to adversarial manipulation of our software and hardware. Straight out of the box, our computers (or the architecture they ride on) can be poisoned with dormant capabilities that can be awakened by those who do not have our best interests at heart. Equally true, our technology systems can come out of the factory in pristine condition, only to be manipulated by the delivery service, the wholesaler, the retailer, the installer, the repairman, or through the downloadable firmware update or patch. Supply chain and vendor operations are very difficult to monitor and can compromise us entirely. Moreover, even without a global supply chain, these same exploits could be introduced domestically by organized crime groups, disgruntled employees, or foreign intelligence officers operating inside of our country. Hence, inevitable calls for protectionism must be considered within this larger, more difficult context. Fortunately, numerous ongoing efforts, including the CNCI's Initiative 11, have identified and are seeking to address these and related concerns.[16]

(defining law enforcement jurisdiction and federal criminal offenses).

15. For a variety of significant reasons, we have embraced interoperable standards and technologies that permit anonymity while shunning technologies that promote identification. Thus, arguably, we have made the process difficult, even though in theory one could not imagine a process that lends itself more readily to perfect attribution than does a point-to-point communication medium such as the Internet. After all, every communication that travels through cyberspace has a definite start point and end point.

16. *See, e.g.*, MARIANNE SWANSON, COMP. TECH. DIV., NIST PARTICIPATION IN THE COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE 11: SUPPLY CHAIN RISK MANAGEMENT (SCRM) (2009), *available at* http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2009-04/ispab_mswanson-nist_april2009.pdf (stating that globalization of Information Technology (IT) hardware and software products being built, delivered, maintained, and upgraded increases risk of supply chain attacks, provides adversaries with greater opportunities to manipulate IT products over the IT product lifecycle and access to U.S. government networks when product

The next avenue of attack to consider is remote access or, in common parlance, computer network intrusions or "hacking."[17] We see the most of this threat vector either because it is the greatest problem or because it is the most easily tracked. Systems Administrators typically are overwhelmed by the quantity of warnings issued by automated intrusion detection, prevention, and firewall systems, and by the additional need to study the logs associated with other technology services and applications. Indeed, the National Institute of Standards and Technology (NIST) correctly observes that our visibility into remote access security incidents is so great that an organization must prioritize its review and response efforts.[18] Hacking, together with the associated methods for obtaining remote access provided by malicious email attachments and drive-by downloads might or might not be the worst of our problems, but they certainly are the most visible. From a strategic point of view, it is important to ensure that the volume of the perceived remote threat and the resources directed against it are not considered to the exclusion of other equally pernicious threat vectors. Even if we were able to prevent all remote intrusions and remote attacks, we still would have trouble – a lot of it.

---

or service is delivered, and increases opportunities for adversaries to exploit U.S. government networks); s*ee also* Department of Homeland Security, Acquisition and Outsourcing Working Group: Mission, https://buildsecurityin.us-cert.gov/swa/acqwg.html (explaining that "[e]ach organization in the supply chain path has an influence on the security or exploitability of the software. Knowing who produced the software and being able to determine if they use security-aware practices in producing software can provide the requisite transparency for informed risk-based decisionmaking in purchasing software or contracting for software services."); Trusted Computing Group, Fact Sheet, http://www.trustedcomputinggroup.org/files/resource_files/7F38FA36-1D09-3519-ADD14CB3D28EFEA6/FACT%20SHEET%20May%202009.pdf (stating that private sector consortia include the Trusted Computing Group, "a not-for-profit organization formed to develop, define, and promote open specifications for trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals and devices").

17. As used in this article, the term "hacking" refers to the act of unlawfully accessing a computer entirely without authorization, or accessing data or functions on a computer in a manner that exceeds authorization. As a matter of U.S. federal law, the principal statute that criminalizes hacking and related cyber offenses is 18 U.S.C. §1030. For purposes of strategy, Distributed Denial of Service (DDoS) attacks are best considered within the "remote access" category, even though they do not necessarily involve "access" into a computer system.

18. As observed by the NIST, from a market standpoint, complete log analysis by any individual company may lack a sufficient return on investment to justify the effort:

> One of the challenges to the effective management of computer security logs is balancing the availability of large amounts of log information with the limited availability of organizational resources for analysis of the data. . . . Organizations could realize benefits in using the data to reduce risks, but the staff time and resources needed to perform the analyses and to manage the log information have to be taken into consideration.

NAT'L INST. OF STANDARDS AND TECH., INFO. TECH. LAB. BULL., LOG MANAGEMENT: USING COMPUTER AND NETWORK RECORDS TO IMPROVE INFORMATION SECURITY 1, 2 (2006), *available at* http://csrc.nist.gov/publications/nistbul/b-10-06.pdf.

"Proximity access" refers to the abilities our adversaries have when they are physically close to our networks but not directly inside them. The interception of wireless signals is a good example of this vector. Through common techniques such as wireless sniffing (passive electronic monitoring of information being transmitted through wireless), peer-to-peer connections (joining a wireless connection and obtaining the ability to access other computers connected to the same wireless network), and "evil-twin attacks" (the attacker poses as a legitimate wireless network in order to lure unsuspecting users), wireless connected devices and wireless access points can turn into a significant cybersecurity liability.[19] Wireless keyboards can present similar opportunities for eavesdroppers, broadcasting keystrokes through the air, even user IDs and passwords. Of course, high-tech gadgets are not needed to engage in close access operations. The term "shoulder surfing" has been used to describe the risk to private data posed by the bad guy who simply casts his eyes on an unsuspecting user's keyboard or monitor.[20]

Finally, insider access must be addressed. Current employees, contractors, and trusted business partners have a unique opportunity to do us harm because they have been provided authorized access to our physical and digital spaces. Once authorized, they can operate from within the "soft gooey center" without being challenged by the "hard outer shell" of gates and guards, intrusion prevention systems, and firewalls. Operating from the inside also provides a distinct perspective on a company's security weaknesses, including technical gaps, lapses in policy enforcement, knowledge of where the crown jewels are located, and even vacation schedules of security staff, just to name a few. Although a cyber attack is more likely to come from an outsider, research indicates that when an insider does strike, the damage may be substantially greater.[21]

The insider threat is usually recognized as including intentional employee fraud, theft of intellectual property, and information technology sabotage, whether at the hands of disgruntled employees, those seeking illicit financial gain, or those seeking business or nation state advantage.[22] In addition though, it makes practical sense to consider the insider threat as also embracing well intentioned employees whose conduct unintentionally causes or contributes to a breach. After all, whether through socially engineered emails or the exploitation of default passwords, our adversaries

---

19. *See* DEPARTMENT OF HOMELAND SECURITY, U.S. COMP. EMER. READINESS TEAM (U.S. CERT), USING WIRELESS TECHNOLOGY SECURELY 1 (2008), *available at* http://www.us-cert.gov/reading_room/Wireless-Security.pdf

20. *Id.*

21. VERIZON BUSINESS RISK TEAM, 2009 DATA BREACH INVESTIGATIONS REPORT 11 (2009), *available at* http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf ("Insider breaches (individually) continue to be much more damaging than those caused by other sources . . . .").

22. *See, e.g.*, DAWN CAPPELLI ET AL., COMMON SENSE GUIDE TO PREVENTION AND DETECTION OF INSIDER THREATS 5-6 (3d ed. 2009).

routinely take advantage of the predictable security failings of employees, and in this way defeat our expensive perimeter defenses.

III. STRATEGIC CHALLENGE: CONSIDERATION OF RISK FACTORS

Recognizing the full extent of these threat vectors is a necessary first step, but it represents only one part of the strategic equation. In order to lower the security concerns that each of these vectors poses, it is helpful to introduce the concept of risk. The classic risk formula is a useful guide in this regard: Risk = Threat x Vulnerability x Consequence.

Two basic theoretical truths emerge from this formula that are useful from a strategic perspective, regardless of whether the equation itself is susceptible to practical application or whether actual values can be provided with ease for each of the variables in a particular setting. First, lowering any of the three variable factors (threat, vulnerability, or consequence) will lower the risk.[23] Second, driving any of the three factors to zero will eliminate the risk altogether because, through multiplication, "R" will become zero if any variable is zero (this is the rationale for using multiplication in the equation rather than addition.).

These points taken together lead to the following conclusions: if any one variable can be brought to zero, all things being equal, that is the most effective security path to take; once a variable is brought to and permanently maintained at zero, it is not cost effective to pursue either of the other factors; and, if none of the variables can be brought to zero, a defense-in-depth approach – focused on lowering each of the three factors – should strongly be considered. To be sure, there is always a point where the costs of seeking to eliminate or even reduce a particular risk (or variable) will outweigh the benefits, thus leading to valid and necessary risk management considerations.[24]

A couple of examples outside the cyber context help drive home the point. First, consider the risk we all face each summer from garden variety mosquitoes. Cycling through each of the three factors, we could go after the *threat* by putting up a bug zapper to kill or repel each mosquito. Alternatively, we might allow at least some mosquitoes to live and instead focus on reducing the mosquito victim's *vulnerability* to being bitten.

---

23. The underlying assumption, which must be validated as applied to a particular scenario, is that lowering a particular variable does not have the unintended consequence of raising either of the other two variables.

24. *See, e.g.*, ROD BECKSTROM, NATIONAL CYBERSECURITY CENTER, DEPARTMENT OF HOMELAND SECURITY, A NEW MODEL FOR NETWORK VALUATION 1, 6-7 (2009), *available at* http://www.beckstrom.com/images/networks.pdf (applying Beckstrom's Law to demonstrate that "the net benefit value of a network is equal to the summation of all transaction benefits, less all transaction costs, less security costs, and less security related losses to a user," and observing: "One dollar of security investments is only a benefit when it reduces expected losses by more than a dollar.").

Wearing DEET or long-sleeve shirts and pants or sitting within a net-covered area all come to mind as valid approaches. Finally, if some mosquitoes will live, and self-defense is uncomfortable or impossible, managing the *consequence* of mosquito bites might be achieved through the application of calamine lotion. Still, a good number of people will fail to ward off the mosquitoes, decide not to wear appropriate clothing or chemicals, and not be prepared with calamine lotion. They will have treated the costs of mosquito defense as outweighing the benefits. They take their chances, itch, scratch, and recover. Would their calculus change if mosquitoes carrying dengue fever came to town? You bet it would.

Next, consider the risk involved in hiring a house-cleaning service. Perhaps you saw an advertisement and find the service affordable. Yet, there remains a nagging sense that allowing a stranger full access to your home could result in theft or damage. Using risk analysis, you would break down the problem into its three component parts and focus on ways to drive down the threat, reduce the vulnerability, and because the first two might fail, eliminate negative consequences. Reducing the threat likely could include performing a background check on the applicant, obtaining references, and seeking referrals. Surely the overall risk of theft or damage may be lowered by reducing the likelihood that the *threat* actor (the potential housekeeper) will steal or act carelessly. Alternatively, or in addition, the overall risk would be lowered by reducing the likelihood that *vulnerable* targets (household possessions) are subject to being taken or damaged. Storing as many valuables as possible in a safe might help achieve this result, as would removing them from the house. Finally, unless the homeowner can have complete confidence in the housekeeper's character and capabilities (thus reducing the threat), or is able either to remove everything fragile and of value or lock them in a safe (mitigating the vulnerability), the overall risk of theft or damage may be lowered by mitigating the *consequence* of theft or damage. For replaceable items, obtaining homeowners insurance would fit the bill, as would hiring a cleaning service that is insured and bonded. Of course, in any given situation, the value of the goods that might be broken or stolen may not justify the additional costs of hiring only known individuals from reliable cleaning services, purchasing a house safe, and obtaining homeowners insurance. If that is the case, it might make sense to accept the risk.

IV. DIAGNOSING CYBERSECURITY VECTORS AND RISK

Turning to cybersecurity, our shared challenge is to apply risk analysis to each of the four threat vectors previously discussed. Thus, anybody involved in cybersecurity strategy, law, policy, or research would do well to take the "Cybersecurity Vectors and Risk" chart printed below and attempt to complete it. Typically, each of the twelve cells requires active engagement.

CYBERSECURITY VECTORS AND RISK

	Reduce the Threat	**Reduce the Vulnerability**	**Reduce the Consequence**
Supply Chain/ Vendor Access			
Remote Access			
Proximity Access			
Insider Access			

Reducing the cybersecurity threat means focusing either on preventing or deterring the adversary from acting.[25] Preventing the adversary from acting might include law enforcement, diplomatic, intelligence, or military efforts to neutralize the individuals (kill, capture, or cajole), or their tools (deny, destroy, or disassemble). Deterring the adversary from acting could include an even wider array of options, depending on the particular adversary. Rational adversaries presumably engage in their own cost/benefit analysis,[26] which would be affected by sticks (for example, threatened law enforcement, military, diplomatic, social, or economic sanctions), carrots (perhaps economic opportunities or enhanced social standing for lawful use of offensive skills), or futility (if the threat actor successfully exploits a vulnerability but does not obtain the expected benefit).

Addressing cybersecurity vulnerabilities requires a focus on hardening the targets, whether through supply chain management, better design, information security practices, education, or other means. Absolute protection is not required. Surely, for example, it would be a great benefit if we could reduce our vulnerabilities to the point that only the most sophisticated nation states could exploit them. Not only would that reduce the number of incidents, it would also limit the field for determining attribution should we observe a security event (which itself would serve as a deterrent to those nation states whose current activities rely on anonymity and blending in with the noise of criminal activity).

---

25. From a risk management perspective, it is important to remain mindful that even when a pre-positioned adversary does not have the intent to act, systems or data may be inadvertently compromised through negligence or recklessness. For example, whether or not those distributing the vast array of malicious software currently residing throughout our networks intend to inflict harm, it is obvious that their creations have not been beta-tested to avoid unintentional disruption.

26. BECKSTROM, *supra* note 24, at 2, 9 (referring to hacker economics).

Finally, consequence management requires a focus on minimizing the harm that results when an adversary takes advantage of an existing weakness. Cyber events must be included within Incident Response and Continuity of Operations plans in order to limit losses to life, property, privacy, public health, business operations, and confidence. Efforts in this space might seek to limit the actual loss in the first instance (for example, by encrypting data or removing the most sensitive data to more secure systems), or might seek instead to "play through" the loss by having the ability to restore the situation to an acceptable state, perhaps by maintaining redundant equipment (such as alternative communications channels), data (including offsite back-ups), processes (including command and control systems), and personnel (via succession planning and the geographic distribution of leadership).[27]

Notably, there are almost always opportunities to share contributions or knowledge from one risk factor discipline for the benefit of work being done by others. For example, those who pursue our adversaries are typically exposed to their motives, intentions, tactics, and techniques, each of which is relevant to those focused on reducing vulnerabilities to exploitation or attack, or on limiting the consequences of a successful intrusion or attack. After all, an adversary's target list not only assists in prioritizing defensive efforts, but may also identify vulnerabilities of which the target was unaware, or suggest that certain consequence management efforts would be ineffective. Similarly, those who are most likely to be victimized by cyber attacks have relevant information for those seeking to reduce the threat, as well as for those planning for recovery and continuity, and vice versa.

Not all information can be shared for all purposes. There are legitimate legal, policy, and business reasons that prevent those who would enhance our nation's security from sharing all they know with one another. Still, for the reasons discussed here, identifying those impediments and seeking to resolve them must remain a priority.

CONCLUSION

Current trends towards digitization, automation, and interoperability need not be mutually exclusive of security. However, the cybersecurity challenge can only be addressed effectively by fully understanding the wide range of threat vectors. Even then, these concerns can only be efficiently resolved by seeking the best options for lowering each of the three risk factors. Policymakers, strategists, and those who operate on the front lines

27. *See, e.g.*, Research and Innovative Tech. Admin., *Plan for System Redundancies To Ensure Appropriate Incident Response Activities and Continuity of Operations During Emergency Situations*, INTELL. TRANSP. SYS., Mar. 2002, *available at* http://www.itslessons.its.dot.gov/its/benecost.nsf/Lesson?OpenForm&344A152BE286EA3A8525714200618BCD^LLCats.

of cybersecurity should carry out their direct and indirect roles in ways that help to lower the threat, vulnerability, and adverse consequences associated with supply chain and vendor access, remote access, proximity access, and insider access. Anything less leaves the advantage with our adversaries.