

April 18, 2002

Dr. Mark Luker
EDUCAUSE

Dear Mark,

On behalf of the University of California, I am offering the commentary in the attached questionnaire regarding "A National Strategy to Secure Cyberspace." Clearly this is a critical issue of concern today to the best minds in the nation. I believe that UC can contribute to our collective efforts to address these concerns.

I note that the questionnaire focuses on different segments of the national community. As you know, the University does not exist in isolation from other communities - in fact it is an integral part of most of them. Not only are we a "major enterprise" but we have industrial and governmental partners in research and education with whom we share technology and communications. Our faculty, students and staff use information technology and the Internet in their pursuits from many locations other than their primary campuses. In that light I have offered comments in a number of areas identified in the questionnaire besides the section on Higher Education.

While we certainly acknowledge the terrible immediate threat of terrorist activities, we also believe that one of the greatest potential long term threats we face is to our civil liberties. If we lose sight of our fundamental principles and freedoms in reaction to the violence directed at us, then in a real sense "the enemy" will have won.

We believe that "security by obscurity" is bad policy and not likely to minimize the threats we face. Rather, we believe that appropriate sharing of information about vulnerabilities and attacks will lead to their remediation most quickly. Legal or financial incentives might possibly help but must be implemented with caution so as to avoid unintended consequences.

Finally, it is clear that mitigation of information technology and network vulnerability will take significant research and more time than we may have. It must become a national priority with adequate funding, broad oversight, and coordinated results.

The University of California stands ready to help. We look forward to your and EDUCAUSE's leadership in this common endeavor.

Sincerely,

William H. Campbell
AVC-IR&C

A NATIONAL STRATEGY TO SECURE CYBERSPACE

QUESTIONS TO BE ADDRESSED

GOVERNMENT COMPUTER NEWS/WASHINGTON TECHNOLOGY

LEVEL 1—THE HOME USER AND SMALL BUSINESS

1. Awareness: What kind of awareness program and assistance should be available to help the home user and small businesses learn about and deal with their cybersecurity needs?

The University community relies heavily on technology that each member manages directly. We provide assistance and advice to the extent that we can but we believe technology vendors should be required to do more, particularly when vulnerabilities or new threats are exposed. We often see new reports of major “viruses” or other attacks but seldom do they include information on mitigation. There should be a straight forward way for individuals to seek and receive technical assistance, perhaps modeled after the “recall” mechanism used in other industrial sectors.

2. Assistance: What can be done to make it easier for home users and small businesses to safeguard their systems? Should Internet service providers (ISPs) perform more of the cybersecurity functions for the home user and small business?

The University depends upon commercial Internet service providers for the large majority of our network communications. Faculty and students working from home often have “permanently on” Internet connections which are prime targets for illicit intrusion.

Internet service providers should offer a range of protections so that appropriate service can be provided for the average user as well as the technically knowledgeable user. Such protections should not impede normal use or freedom of expression, of course, but should include obvious technical measures such as source address verification and link level encryption.

In addition, ISPs should be ready and willing to help respond to attacks using the tools of their trade to trace and/or contain illicit activity reported by users.

What ISPs **must avoid** is becoming involved in scanning data passing through their systems. Not only would this infringe on civil liberties but it could make the ISP vulnerable to liability for damage that they might fail to prevent. A consequence of the latter would be an overly conservative approach to preventative measures, and could result in giving police-like powers to the ISP.

3. Disclosure: What disclosure of risk should ISPs, software vendors, and hardware vendors make to home users and small businesses?

Full disclosure of reasonable risks is expected of all vendors. Most people will not be technically knowledgeable enough to assess risks on their own. Risk statements should include the possibility of unknown vulnerabilities to the operating system or applications software as well as “denial of service” and other network based risks.

Such disclosure should occur not only at the time of purchase but throughout the ownership or use period of the product(s).

4. Emerging Technology: What emerging technologies (e.g. wireless area networks for the home, wireless connectivity of the home to the Internet, broadband connectivity to the home) pose additional security risks to the home users and small business; what can be done to address those risks?

Most University campuses use wireless data communications as part of their network infrastructure. Today these systems are highly vulnerable to eavesdropping or worse attacks. Wireless communications must be secured with link level encryption, at a minimum. Current standards are ineffective and must be replaced with programmable encryption standards as well as efficient access management technologies.

Broadband technologies using a shared medium such as coaxial cable are also vulnerable to eavesdropping. Furthermore, since they support “always on” connections, home computers served in this way are particularly vulnerable to attack. Broadband adapters might be designed with greater intelligence so as to be able to notify the user of anomalous behavior and possibly serve as a minimal firewall when necessary.

5. Broadband Initiative: If the Federal Government acts to facilitate more rapid deployment of broadband connectivity to the home user and small business, what cyberspace security requirements should be a condition of Federal support?

True broadband connectivity will come about only when fiber optical media serves homes and small businesses. An additional advantage of this medium is its minimal vulnerability to eavesdropping.

As noted above, high bandwidth “always on” connections should be configured with edge devices that can provide at least some level of protection to as well as from locally attached computers.

LEVEL 2—MAJOR ENTERPRISES

1. Responsibility: Who in an enterprise should be responsible for IT security? How often should that person brief the CEO? What role should the Board of Directors play in over sight of IT security? Should the Board require an outside audit and, if so, how often and from whom?

Typically the Chief Information Officer (CIO) is responsible for security of information systems and communications. That officer might delegate that responsibility but should be in a position to report to the University CEO (Chancellor or President) routinely and upon demand. University Boards of Trustees or Regents should be aware of this responsibility and expect to be kept informed of both readiness and response measures. Periodic audits would help ensure that readiness measures were in place and supported.

2. Best Practices: Where should the CEO, Board and/or auditors obtain guidance on best practices or standards to use in IT security self-evaluations and IT security policy development?

This has yet to be determined but it should be broad based to avoid any particular bias or “blind spot.” A Federal agency might take a leadership role in convening a standing body with broad representation. Recommendations from such a panel should be vetted or peer reviewed to ensure the best possible results.

3. Disclosure: What information about IT security should the corporation disclose to its stockholders, to its creditors, to its auditors, to its Board.

N/C

4. Enterprise Wide IT Security Policy: Should enterprises be required by their Boards of Directors or Auditors to have a regularly updated policy statement on IT security practices? Should enterprises be required by Boards and Auditors to employ software to enforce their IT policy?

The University has IT security policies that are reviewed regularly in light of emerging concerns. However, the ability of “software to enforce ... policy” is inherently limited. It also can give a false sense of security to users who should instead remain aware of the potential risks.

5. Awareness: Should enterprises require employee participation in regular IT security awareness training? Where should enterprises obtain assistance in developing such training?

Yes.

6. Insider Threats: How can a balance be struck between preventing insiders from damaging the enterprise by misusing its IT systems, and respecting the legitimate privacy concerns of employees?

It would be a mistake to try to “lock down” every possible system in an effort to eliminate risks. A result could be serious degradation of usability and still extant vulnerabilities. Instead, a balance must be found between overly restrictive measures and mitigation of incidents that might occur.

7. Partners and Supply Chain: What IT security risks does an enterprise run from its relationships with its partners and supply chain? How can those relationships enhance or degrade IT security?

The University has partners in many sectors of this nation as well as the world. To the extent that we share technologies and communications, we also share risks and this means we should share mitigation strategies. As we enter into e-commerce relationships, the risks will become even greater.

8. *Event Reporting: What IT security events should an enterprise report and to whom?*

This needs broader discussion. In general, incidents that might affect other systems or institutions should be reported to higher level authorities. Isolated incidents can be dealt with locally.

9. *Threat and Vulnerability Information: How should an enterprise learn about and decide how to react to IT security threats and vulnerabilities? How can an enterprise evaluate the numerous software “patches” distributed to it by its IT vendors?*

One of the strengths and also weaknesses of IT is its configurability. If products were designed to isolate customization from basic function, installation of “patches” might be less burdensome.

10. *IT Vendors: To what extent should an enterprise “outsource” its IT security functions? How can IT security vendors be evaluated? How can an enterprise act to improve the security of the IT products and services it procures?*

TBD

11. *Risk Management and Insurance: How can an enterprise evaluate the appropriate level of IT security spending or the return on investment in IT security? What role can insurance play in IT security for an enterprise?*

N/C

LEVEL 3—SECTORS OF THE NATIONAL INFORMATION INFRASTRUCTURE

A. The Federal Government

1. *Best Practices and Standards: Should there be a set of IT security best practices, policies, and/or standards for various types of agencies and/or various types of functions supported by IT systems? How should they be developed, how detailed should they be, and should compliance with some of them be required by law or regulation?*

N/A

2. *Accountability, Responsibility, and Oversight: What regular auditing of Federal agencies’ IT security should be performed? By whom? To whom should it be reported? What should be done with the results? How can appropriate levels of timely remediation be best linked to such audits? How can sustain interest by senior levels of department management be best achieved?*

N/A

3. Funding: Is the IT security performance level of many Federal agencies such that many agencies will be unable to adequately remedy their performance within normal annual budgetary practices? Is a funding initiative similar to the approach used in Federal Government Y2k remediation required and, if so, how would that work?

N/A

4. Cross-Department Activity: What IT security functions should be performed at the departmental level and what should be performed centrally? How could there be greater collaboration among agencies and departments to achieve economies of scale in operating some IT security related functions?

N/A

5. Connecting Critical Functions to the Internet: How should we best address the security risks arising from critical Federal functions being performed on networks that have routers and other systems vulnerable to denial of service and other cyber attacks from the Internet?

Federal agencies are not that different from private enterprise in this regard. Both need similarly secure network technologies and robust, secure service platforms. In addition, all sectors need strong and secure digital credentials and associated authorization systems.

6. IT Security Personnel: What is the extent of the Federal Government's shortfalls in qualified IT security personnel? How can the Federal government improve its recruitment, education, in-service training, and retention of qualified IT security personnel?

N/A

7. Procurement: What role should procurement policy have in improving Federal IT security?

Federal procurement historically has had great influence on vendor products. By including reasonable requirements for security functions as part of IT procurements, vendors will be encouraged to improve their products, thus benefiting us all.

8. Awareness: How should IT security awareness training be addressed for most Federal employees?

N/A

9. Event Reporting: How can the Federal government achieve better compliance with the requirement that departments and agencies report malicious activity on their cyber networks and systems? What should be done with such reporting?

N/A

10. Warning, Analysis, Incident Response and Recovery: What system and capabilities should the Federal government have and what should individual agencies have to warn, perform analysis, and respond to IT security incidents?

N/A

11. Organization: What, if any, further organizational changes are required to improve Federal IT security?

N/A

12. National Security: Are there additional IT security programs, structures, or capabilities required especially for national security related departments or agencies?

N/A

B. The Private Sector

1. Sectors: What IT security roles should be performed by similar enterprises acting together on a sectoral level? How should such sectoral activities be organized?

N/C

2. Information Sharing: What is the role of the Information Sharing and Analysis Centers (ISACs) and how can their performance be enhanced? How can the Federal government improve IT security information sharing with the private sector concerning vulnerabilities, threats, warnings, and analysis?

There should be a way for enterprises to register a “security contact” with Federal incident response coordinators so that information can be promulgated quickly and securely.

3. Best Practices and Standards: What should be the role of best practices and standards at the sectoral level?

N/C

4. Incident Response and Recovery: What sectoral level cooperation mechanisms should exist for incident response and recovery?

As with inter-agency emergency response (police and fire, etc.) there should be coordination of activities across sectors. This exists today but only informally. A focal point for this activity in each community, broadly speaking, might prove valuable.

5. *Digital Control Systems: What unique security threats are related to digital control systems and SCADA systems and how should they be addressed?*

N/C

6. *Connecting Critical Functions to the Internet: Are there sectors that perform critical functions which could achieve greater security and reliability by operating networks unconnected to the Internet and other public switch, open systems? There will be individual sections at this point in the strategy dealing with the unique issues and plans arising in specific sectors, including:*

- *Banking and Finance*
- *Transportation*
- *Information Technology*
- *Chemical Manufacturing*
- *Energy*
- *Telecommunications*
- *General Manufacturing*

N/C

C. State and Local Government

1. *Organization: Should state governments organize IT security organizations for information sharing and incident management at a state level? If so, should such organizations include state agencies and departments? city and county agencies? critical infrastructure related private sector entities in the state? Should state and local governments have a national mechanism to partner on IT security related activities? What should be the Federal role with such organizations?*

Local responsibility for IT security will be more effective than national level responsibility.

2. *Law Enforcement and Emergency Services: In addition to other state and local government IT security requirements and activities, what unique problems and requirements do law enforcement and emergency services agencies confront and how should they be best addressed?*

Primarily lack of expertise in technology issues. It isn't clear that law enforcement can afford to hire adequate expertise. It might be worth while to identify local or regional resources that could be brought to bear when needed.

D. Higher Education

1. *Preventing attacks from Universities: How can academic freedom of inquiry be maintained while at the same time preventing the large scale computing power of universities from being hijacked for denial of service attacks and other malicious activity directed at other sites?*

Academic freedom is not constrained by requiring proper configuration of information technology. Academic freedom **would be** constrained by inappropriate eavesdropping on

communications, inappropriate requirement for identity when seeking information resources, or similar intrusive measures.

Universities are particularly vulnerable to criticism for allowing freedom of expression and intellectual pursuits, especially when such expressions or pursuits may be unpopular. However, it is critical that Universities maintain those freedoms against erosion. Perhaps Thomas Jefferson's observation that "The price of freedom is eternal vigilance" cuts both ways. Not only must we defend our freedoms, we must ensure that they are not used for unlawful or malicious purposes.

The University of California has a very comprehensive "Electronic Communications Policy" (see <http://www.ucop.edu/ucophome/policies/ec/>) that covers both network abuse and abuse of information technology. Active education of the university community and responsible enforcement of this policy should provide good protection against most potential problems.

2. Preventing attacks within Universities: What functions on a university system require high levels of IT security (e.g. medical records, research trials, patents) and how is that best achieved within the context of an academic setting?

Again, academic freedom is of great importance but strong and secure access management can protect sensitive resources without constraining such freedoms. For example, members of the university community can be issued one or more digital credentials identifying their roles or responsibilities without revealing their specific identity.

By the same token, information resources can be protected by strong access controls and other strategies such as use of encryption while information is in transit. Such technologies exist today but, for many practical reasons, are not yet fully deployed.

Most campuses have deployed firewalls both at the edge of campus networks and around the critical operational IT services to help protect against attacks. Ultimately it is again proper configuration and management of the platforms themselves that will provide the best defense.

3. Organization: How can universities best organize to address the IT security questions they face in common? Should best practices or standards be agreed on a national level? Should there be a mechanism for information sharing on threats and vulnerabilities among university CIOs and systems administrators?

Information sharing among universities already occurs but could be improved. Just as there are national bodies representing university registrars, attorneys, auditors, etc., there could be a national body representing university IT security officers. EDUCAUSE would be a good home for such a body.

"Best practices" are always a good context in which to share ideas. "Standards" are more difficult since each campus will have its own special challenges to deal with.

Information sharing regarding threats and vulnerabilities should occur at a level lower than the CIO. It is the operational managers that must learn of this information as quickly as possible. In turn, it would be their responsibility to inform their CIO following local procedures.

LEVEL 4—NATIONAL LEVEL INSTITUTIONS AND POLICIES

1. Training and Education: How should the nation deal with the lack of trained IT security personnel? What are adequate numbers of personnel with various levels of training and how do we achieve those levels? Is the H-1B visa program part of the overall solution or are there roles that must be performed by U.S. citizens?

Training is probably not the difficult problem; motivating people to go into this profession is. Without adequate compensation or recognition, only a few of the best technical minds will be drawn to this field. Thus a first step must be to recognize the critical need for personnel and reward those who choose this profession with tools and organizational support as well as direct compensation.

With regard to H-1B visas, we must distinguish between a person's origin and their interests. It should not be assumed that a person of foreign origin will not support the interests of the U.S. or that he or she might let another nation's interests supersede those of the U.S. It is only in a few special instances that U.S. citizenship should be required.

2. Highly Secure /Trustworthy Computing: In addition to addressing the vulnerabilities in currently deployed software and hardware, should greater research emphasis be placed on developing entirely new and significantly more secure approaches to operating system software, computer hardware and the interface between the two? How should such efforts be funded? How should procurement of such systems be encouraged?

Clearly some security problems lend themselves to this approach but certainly not all such problems. In addition to technology, there should be significant penalties for failure to address "the vulnerabilities in ... deployed software and hardware". Without direct incentive, there is little motivation to make the necessary improvements.

3. Securing the Mechanics of the Internet: Can the traffic control systems of the Internet (Domain Name Servers, Border Gateway Protocols) be made more secure? Can routers be made more secure by separating control functions from the general traffic channel? How can major denial of service attacks be mitigated? What problems arise in deploying more secure systems, how should they be overcome, and how should such improvements be funded?

There are many areas in which Internet technology could be improved. First, there are configuration options that would mitigate certain attacks if deployed broadly, for example ensuring that the source address of a data packet is legitimate. In addition, new logging functions could be implemented that would help trace the origin of DOS and similar attacks. Current technology only identifies how a data packet will be delivered - not the path it took to get to a given point.

It is also the case that the economic model of the Internet does not encourage concern about misconfiguration of systems. Most often there are no financial consequences to the origin of a DOS attack and no penalty for Internet backbones to carry that traffic. Instead, in some cases the financial burden falls on the victim of the attack, and that entity who has no recourse. A study of this problem by technologists and economists might result in a strong recommendation for reform.

Finally, it is also the case that access to the Internet is completely anonymous. This is a strength and also a weakness. However, just as a Library maintains anonymity for its patrons but sometimes must know who has not returned a book, it is possible to manage access to the Internet such that there is a record of “who” is using a given access platform without revealing that identity unless there is a legitimate need to know. Such a mechanism might possibly reduce abuse merely by presenting to the potential miscreant the risk of discovery.

4. Securing Emerging Systems: What types of information technologies and systems will increase in numbers and complexity in the next three to five years and how can their vulnerabilities be predicted in advance and avoided? How can enhanced security measures be widely incorporated into wireless networks and wireless internet connections? What security problems arise from significant growth in the number and functionality of wireless, internet enabled, semi-autonomous devices? What security problems arise from “ad hoc networks” that use multiple wireless connections to reach the internet?

Two particular vulnerabilities are link level eavesdropping on wireless communications and potential denial of service attacks by spectrum jamming. The first can be mitigated through use of encryption but the second is very difficult to address systemically.

In addition, wireless devices with “roaming” capability will make locating a miscreant even more difficult than it is today.

5. Privacy: What risks to privacy could arise from some approaches to achieving IT security? How can those risks be eliminated?

As mentioned above, the identity of a person connecting to the Internet could be known to a local registration system for good reasons but that system **must** be protected against illicit access in order to protect basic Internet user privacy. In addition, access to services on the Internet should not require multiple use of a single identity but should be designed to use any one of several identities that an individual might have, or merely roles, responsibilities or affiliations - so called “group identity” - instead of specific identity.

6. Interdependency: How can we determine in what ways the various critical infrastructures are dependent upon one another and what vulnerabilities in one infrastructure could pose major problems for another? How should the burdens of addressing interdependency vulnerabilities be apportioned?

N/C

7. Regulation and Market Forces: What is the role of state and federal regulation in achieving IT security? How can market forces be further stimulated to achieve improved IT security as an alternative to regulation? What role can be played by corporate disclosures policies, by internal and external auditors, by Boards of Directors, by the insurance industry, by liability law, by tax policy?

As suggested above, the economic model employed in the current Internet does not encourage adequate attention to vulnerabilities or the sources of attacks. However, governmental agencies should not undertake to regulate the Internet but should make it clear that liabilities for abuse do exist and will incur financial or other penalties. The same is true for manufacturers of information technology and systems.

8. Research: What should be the national IT security research priorities? How can those priorities best be addressed between and among corporate research departments, universities, national laboratories, and federally funded research and development centers? How should the research costs be apportioned?

First, there should be no proprietary technology that is critical to IT security. This means that private industry will have a hard time justifying the expense of development in this area. Thus it is likely to fall to the university community or federally funded labs to do the basic research needed to foster new technologies or security mechanisms.

Priority should be given to “hardening” the core Internet technologies for operational monitoring and attack mitigation. Longer term, research should be undertaken to define how to restructure complex systems to minimize the effect of a failure or intrusion in any one subcomponent, and how to enable thorough testing of subcomponents for possible vulnerabilities. Given the complexities of today’s operating systems - 10s of millions of lines of software - it is simply impossible to eliminate all possible vulnerabilities.

9. Information Sharing: What additional IT security information sharing should occur among and between federal government agencies, state and local governments, corporations, and the public? What are the barriers to such greater sharing and how can greater sharing best be achieved? How can data about attempted unauthorized penetrations and other malicious activity best be aggregated and analyzed? What system or systems should exist for issuing IT security warnings?

“Security by obscurity” is never reliable. Information sharing should be appropriate but as broad as possible. Inappropriate withholding of information should result in appropriate censure.

10. Vulnerability Remediation: What role should individuals and corporations have in identifying IT security vulnerabilities? To whom should they report such vulnerabilities? How and when should users be informed? How could vendors or large scale enterprise users distribute “patches” in such a way as to insure their rapid utilization? How should critical infrastructure operators and the government identify and remove logic bombs, Trojan horses,

and other malicious code that may have already been covertly installed on systems and networks?

Some of this was addressed above. Automating software updates, as both Apple and Microsoft have done, is a good start. In addition, software and even some hardware modules could be provided with “fingerprints” that would allow verification of their integrity automatically.

11. Certification: Should software, hardware, and IT security consultants be certified, and if so, how and by whom?

N/C

12. Continuity of Operations, Recovery, and Reconstitution: What plans, capabilities, and arrangements should exist at a national level to respond to the wide spread outage of IT systems in one or more sectors?

N/C

13. Crime: What role should the criminal justice system play in achieving IT security in government and in critical infrastructures? Are current state/local or federal criminal justice capabilities adequate? Are current legal prohibitions and penalties adequate to deter?

One strategy that does not help is something like “carnivore” that simply raises suspicion and distrust of the criminal justice system. Such technology might prove useful in some cases but it must be proven to be reliable and safe if it is to be trusted by the general public.

14. National Security: What policy and operational differences arise if the source of malicious activity in cyberspace is a nation state?

N/C

LEVEL 5—GLOBAL

1. Information Sharing: What arrangements should exist for sharing information about vulnerabilities and malicious activity among institutions in various nations?

The Internet does not recognize national borders. The comments above regarding information sharing apply internationally as well.

2. Cooperation Standards: Should there be internationally accepted standards about what malicious activity in cyberspace should be considered criminal, what the penalties should be, and what investigatory cooperation should be mutually afforded participating nations?

This will be difficult because of differences in national positions on some basic issues. However, cooperation in investigations and mitigation, where possible, should be expected.

Appendix A: Message from EDUCAUSE

April 16, 2002

Dear Colleagues:

I would like to ask you, as a member of the higher education community, to provide input on the National Strategy to Secure Cyberspace, currently being formulated by the Bush Administration. A national strategy is slated to be announced this summer by the White House.

EDUCAUSE staff have been working closely with government officials to coordinate a higher education response to the national strategy. A series of questions to solicit input is available at <http://www.qcn.com/cybersecurity/breakout3pqs.pdf> . Three questions specifically address IT security within the higher education community.

The EDUCAUSE/Internet2 Computer and Network Security Task Force will coordinate the initial task of collecting answers from the higher education community and responding to the questions posed by the White House Office of Cyberspace Security. Please visit the EDUCAUSE Web site to submit responses to the three higher education-related questions:

<http://www.educause.edu/netatedu/groups/security/security-survey.html>

Comments must be received by APRIL 19 to be included in the response that EDUCAUSE is coordinating for higher education. The task force has also received federal funding to convene a series of meetings over the next few months to help forge systematic and systemic change to improve the security of our networked resources. Questions about the work of the task force, and comments or reactions To the government's set of questions, should be directed to Rodney Petersen at rpetersen@educause.edu or 202-872-4200.

Thank you for your contribution to this important national initiative.

Mark Luker
EDUCAUSE Vice President