Global Information Assurance Certification Paper

The Political Campaign Headquarters is generally a short term rental of an office suite. Depending on the scope of the campaign, the physical size of the office can range from several hundred to several thousand square feet of office space. Networking infrastructure may not exist at all. If it does exist, you may be looking at flaws in security from the first day your campaign operations manager gets the key to the building. Some subleased facilities have CAT-5 cabling in place. The possibility exists for significant security flaws, including an entire organization running their office LAN on the same wires. In the not so distant past, I was asked to perform data migration and data-base related services for a litigation that was being run from a war room. The office space was sub-leased from a law firm. There was network cable in the walls, and the sublessors had access to that network. Fortunately, the attorney who directed the litigation knew not to use the existing cable which led right into another law firms' main server!

Political campaign strategy is something any opponent would want to challenge. No one wants their strategy and planning to be thwarted by opponents who seemingly can anticipate every move due to their ability to eavesdrop electronically.

The most notorious case of political espionage may be the 1972 Watergate break-in which ultimately led to the resignation of then President Richard Nixon. For more information on this series of events, please refer to the following link:

http://www.washingtonpost.com/wp-srv/national/longterm/watergate/chronology.htm

The above link is useful for getting a better idea of the timeline of Watergate. The seeds of a sitting Presidents' downfall took only a few years to come to fruition. This all happened before the immediacy we all take for granted now.

Political espionage or other forms of dirty tricks did not end with the Watergate break-in. Politics at the national level is not a game for the weak of heart or mind. It could be argued that every presidential election is a war.If this has any truth to it, we can expect intelligence and reconnaissance operations to be an ongoing, if not very public part of the campaign process. Where the line is going to be drawn has everything to do with the law and respect for the law. If we tolerate break-in's and theft of any kind in the name of getting information to aid a campaign, we are watering down the democratic process. Unfortunately, there are continuing examples of the less than honest in political campaigning. A recent example involves the mayoral run-off election of December 2003 in the city of San Francisco, California.[1] Please refer to at the following link:

http://www.sfexaminer.com/templates/story.cfm/displaystory=1&storyname=120103n_gore

In an article published in the Washington Post recently, Republican staffers have been found to have been downloading thousands of computer files from U.S. Senate Democratic offices.[2] Though it does not involve a political *campaign* security issue, it does involve serious security issues pertaining to political organizations. The contents of some of these memo's have helped Republicans deter-

1. *See* J.K. Dineen and Adriel Hampton: *Cyber War over Gore Newsom Event* San Francisco Examiner, Monday Dec. 1, 2003
2. *See* Helen Dewar: *GOP Aides Implicated In Memo Downloads* Washington Post, Friday March 5, 2004

mine Democratic strategy, especially in the area of judicial nomination. Please refer to the following link:

http://www.washingtonpost.com/wp-dyn/articles/A31803-2004Mar4.html

As the internet and networking become more important and integral parts of campaign strategy, from fund raising to getting the message out, the network will also become a focal point. This could be a potential weakness that could slow down or even sabotage a campaign. In each campaign, it is important to schedule early strategy sessions that outline network and data security issues.This is essential for the integrity of the campaign process. An election is a sometimes chaotic event, and there are some wonderfully tight and contested political contests. We need to always try to keep a level playing field. One way we can do this is by protecting the information of each candidate in a manner that stands the test of *confidentiality, integrity* and *availability*. We will look again at CIA and its importance.

Before you are even handed the keys to the strip-mall or local office park temporary headquarters, have a "Best Practices" draft in place to address some of the following issues:

1. Define a core group of workers who have have the highest level of access on the network.
    a. Campaign manager, press liaison(s), scheduler(s), logistics personnel, systems administration, contracted consultants and strategists.
2. Define a second tier of workers who have lower level access on the network.
    a. Volunteers who are working at the headquarters on a regularly scheduled basis, contracted assistants and temporary office help.
3. Define a third tier of staff that have only the most basic privileges on the network.
    a. General office help of a per diem or volunteer status.
4. Policy needs to address volunteers and how work is carried on and off site.

Imagine being in the middle of a crucial deadline and your staff is almost completely made up of individuals you have little or no history with. This is a dynamic that can come into play in a war-room or campaign headquarters setting. Disks and drives, computers in fact, are alot smaller these days and are very easy to hide in a coat pocket or briefcase. Do you have a log of all your equipment?

Ask yourself who is designing your network and what kind of contracts are in place that will protect your data? Who are the workers being sent to install and in some cases, maintain the functionality of my network? It is crucial to have a small working group of individuals who will be responsible for the daily maintenance of the network. Who are these people, and are they per-diem tech personnel from the local temp agency? Do any of these individuals have other agendas that might make them less than ideal workers from a security perspective? Securing a network, even a short-term network, is a process that involves ongo-

ing maintenance for that network to function effectively. One key to digital security is that the weakest link could be human, not software or hardware.

Most campaigns are volunteer driven,and low-budget affairs. They will either mushroom into prominence, or wither, some quicker than others. Many campaigns are run by very passionate volunteers. This passion is part of what makes a political campaign exciting and desirable (from a candidates perspective) because of the need for momentum to build in a fairly short period of time. In an environment such as this, there may be less focus on something as dry as computer security. This is where we are going to be finding more information battles won and lost. Individuals need to be educated, even at the volunteer level, about proper procedures for using computers, handling paperwork, destroying paperwork, securing facilities, etc. The best defense against social engineering attacks is an informed staff.[3]

Most campaign headquarters have physical security issues prior to setting up a network infrastructure. Some security issues to consider should include an inspection of all windows, doors, basement access, fire escapes and adjoining structures. Locks should be replaced and/or any malfunctioning locks should be repaired. All windows and doors should be checked for integrity. If there are fire escapes or roof access, these area's should be inspected as well. Determine if there is a need for security guards. Many office sublets have door keypads for locks. Some keypad codes haven't been changed in years. Make sure you either replace or change the keypad combination. Make it a policy to change the combination every few days. Also, it is critical to know as much as possible about the housekeeping and custodial staff. Ask questions and don't be surprised if there is an individual within one of these groups that might have the ability and desire to access your network. Make sure there are paper shredders available and write into policy proper usage. I remember working on a litigation (which will go unnamed) where the shredder box was labled "Shred Documents" and the box was often left full or near full for days on end. This is not desireable. Dumpster diving --literally going into the trash bins located in the back of the building -- is a very effective means of gaining valuable information. All precautions should be taken to prevent sensitive documents from ever making it to the dumpster in one piece.

Who is going to be keying those numbers in the door locks and computers is another critical area of social engineering that will have huge implications in the security of a campaign headquarters network. In a discussion with a principal of a large political campaign services company last week, I was told the easiest way to sabotage a campaign's network was to simply volunteer. You go in, sign up and before you know it, you have a computer with network privileges and viola! Here is where the damage can occur. Some of the damages could include generating unauthorized mass e-mailings, installing keystroke recording software, infecting with a virus or worm, creating mirror sites where archived, confidential records may be accessed at will...the list of potential damages could go on and on. The point is, know your people and make it a priority to communicate your commitment to network integrity and the security of your confidential information.

3. *See* Ed Skoudis: *Counter Hack* pg 148, Prentice Hall ©2002

Confidentiality, Integrity and Availability[4]

"Information Security has been aligned towards the accomplishment of three objectives. Confidentiality, Integrity and Availability, referred to as "C-I-A." "[5] In a busy campaign headquarters, trying to achieve the listed objectives may seem difficult on a good day and impossible on a bad day. Lets take a look at each objective and try to superimpose a set of circumstances and possible responses.

"Confidentiality is the need to ensure that information is disclosed only to those who are authorized to view it."[6] Imagine leaving the entire strategy for an upcoming televised debate at the front desk right next to the brochures that have been put on display next to the receptionist. You just might as well fax your strategic documents to your opponents and save them the bus fare. Who are those you would want to have your key information? Who are the key players on your staff? Does your staff have clear instructions on how to disseminate information? What information is not to be divulged? So let us look at the reception area example again. Generally, information is stored on servers, but can be found in all sorts of places around an office. This would include laptops, PDA's, cell phones and printers. People are assigned responsibility for this information. Who in your organization has the responsibility? Where is the data and how easy is it to get to? The confidentiality of your information is what is at stake and unless questions are asked early on, the potential for an embarrassing leak of information becomes all that much greater. A very clear chain of command is critical to ensure information is controlled. Otherwise, you can have a situation that resembles the receptionist greeting area holding key documents that have no business being there.

"Integrity is the need to ensure that information has not been changed accidentally or deliberately"[7]. Imagine a false mass emailed document that had your campaign logo, letterhead or other identifiers on the document, but whose content was wholly fabricated, unapproved and malicious in nature. Imagine that this document was emailed to millions, and in fact was read by hundreds of thousands of potential voters. Every political campaign has one crucial objective, and that is getting its message out in a clear and simple manner. Every minute spent denying a charge, or answering a question that is not relevant to the issues that you want to highlight, is a minute that has passed to the opposition. Imagine having to spend precious time managing a security crisis caused by a lack of integrity in the deliberate and damaging manipulation of data.

The Newsom Cyber-Scandal

The political games that could take place in a network environment are real and have huge implications on how information is managed. An article published in the San Francisco Examiner on Monday, December 1, 2003, states that misinformation is being propagated through networks associated with political figures. In this particular case, the political figure is the mayor of San Francisco, Gavin Newsom.

4. *See* Eric Cole et al: *SANS Secutify Essentials with CISSP CBK* pg 259, ©2003
5. *See* Eric Cole et al: *SANS Secutify Essentials with CISSP CBK* pg 259, ©2003
6. *See* Eric Cole et al: *SANS Secutify Essentials with CISSP CBK* pg 259, ©2003
7. *See* Eric Cole et al: *SANS Secutify Essentials with CISSP CBK* pg 259, ©2003

The following is excerpted from the December 1, 2003 edition of the San Francisco Examiner:

"While it is nearly impossible to determine with 100 percent accuracy who was responsible for publicizing the anti-Gore event, the originating Internet protocol address on the e-mail belongs to an organization called GavinNewsomFor and carries the same address — 216.100.140.9 — as e-mails sent from Newsom's campaign office.

After receiving an invitation to the event, The Examiner replied to verify it and on Friday received a confirmation that included the "GavinNewsomFor" Internet Protocol address.

The Newsom campaign Sunday night denied it had sent the Gore rally e-mails and suggested Gonzalez supporters may have hacked their way into the Newsom system to make it appear as if Newsom had sent them."[8]

The following questions are raised from this excerpt:

1. Where is the breach in security?
2. Who specifically orchestrated the mis-information campaign?

The breach in security in this case is not directly related to the Matt Gonzalez campaign headquarters or the computing infrastructure of the physical location. The breach in this case seems to be a misrepresentation that is in fact a somewhat crude form of social engineering. It seems someone from the office of Gavin Newsom, or someone who had access to the GavinNewsomFor TCP address 216.100.140.9 was able to misrepresent a political event that was in fact non-existent and would be embarrassing and potentially damaging to the campaign of Matt Gonzalez. In fact, according to Gonzolez for Mayor Media Director Liz Ross,[9] a press conference had to be held to address the mis-information that was broadcast through the internet. Time, money and effort had to be redirected to manage mis-information.

Time, money and effort. These are the three things a political campaign cannot afford to spend responding to fraudulent statements disseminated through networks. The new reality of running a political campaign must include the ability to keep the network integrity strong. You can count on an opponents desire to manipulate your message, and the network can prove to be a liability.

The political campaign was a runoff election for the mayoralty of San Francisco California in December of 2003 and was in fact won by Gavin Newsom.

Were votes lost due to misinformation disseminated by allies of the Newsom campaign? Were votes lost due to misinformation disseminated over networks? Was time and money spent in a re-directed manner to address the misinformation? These are hypothetical questions, and it is impossible to know how many votes were influenced by the specific mis-information propagated in this particular circumstance, however, money and time were spent in addressing this situation. Al Gore is one of the heavyweights of the Democratic Party. Anyone who publishes anything associated with his name is directly challenging the opposing candidate to address whatever issues may have been raised and mis-information notwithstanding.

8. *See* J.K. Dineen and Adriel Hampton: *Cyber War over Gore Newsom Event* San Francisco Examiner, Monday Dec. 1, 2003 http://www.sfexaminer.com/templates/story.cfm/displaystory=1&storyname=120103n_gore
9. Telephone inquiry, February 28, 2004 with Liz Ross

The following is excerpted from the December 2, 2003 edition of the San Francisco Examiner:[10]

"The electronic missives calling for a Green Party protest against former Vice President Al Gore's appearance today were almost certainly sent from a computer at the Gavin Newsom For Mayor headquarters, according to analysis by several independent information technology experts.

After initial reports of the flap, IT professionals told The Examiner they could not find any way of faking the "originating IP address" of the "Mary Green" protest e-mails. When someone uses a free Internet account, that server automatically pulls identifying information from the originating computer.

Tracing the identifying information from the original protest e-mail, network administrator Marc Dantona said, "Newsom's campaign might have some explaining to do" since it leads straight to GavinNewsom.com." "

Imagine a campaign that was put together quickly, using populist grass-roots campaign tactics. Imagine a lot of young volunteers with little or no political background and a candidate who does not have much money but is making a mark. This is the type of political campaign organization that is prone to manipulation, social engineering, network compromise and hactivism.[11] The strength of the organizational process in a campaign is an underlying trust of your fellow volunteer. This trust is also a potential weakness.

Social Engineering, or the ability to get someone to do something that benefits another person, without knowing fully the nature or intention of that individual, needs trust in order to be an effective measure. Social engineering attacks are simply attacks against human nature.[12] The most effective countermeasure, therefore, would be a heightened level of suspicion towards any query directed at a campaign staff member. I recently engaged in a bit of telephone tag with two senators' offices (I will leave them unnamed). The level of screening for my line of questioning was in my opinion less than desirable. In fact, I would have preferred that none of my questions were answered, but the *desire to be helpful* let more than one office worker to divulge information I (if I was the Senator) would not have so easily turned over. I purposefully will not divulge what was gleaned from these conversations. Human nature you see, has a tendency to be helpful. The point is simply that policy must include and in fact stress--the importance of human interactions and how this is often a first step towards reconnaissance.

This political campaign scenario is played out all over the country, and is one of the amazing aspects of living in a democracy. Our mission as network security administrators is to keep information confidential. We also need to assure the integrity of the information and render the data to those who have the privilege of using that data in an honest manner. The sometimes chaotic and brass knuckled world of political campaign work demands a close-knit community structure in place as soon as possible. The longer a campaign waits before assigning a network security officer/policy, the higher the likelihood there will be tampering.

10. *See* J.K. Dineen and Adriel Hampton: San Francisco Examiner, Tuesday Dec. 2, 2003
11. *See* Mark G. Milone *Hacktivism: Securing the National Infrasctructure* pg 385 The Business Lawyer November 2002 Volume 58 Number 1
    A definition of "hacktivism" is available at
    http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci552919,00.html
12. *See* Cyrus Peikari and Anton Chuvakin: *Security Warrior* pp199-201 ©2004 O'Reilly & Associates

Strategies for Physical Security

Considering that is was a botched burglary that brought down a presidency in 1972, not paying attention to physical security is inviting disaster. When setting the actual office up, consider which rooms would be more suitable for sensitive information. Areas with high traffic or cubicle areas should be avoided for sensitive systems. Pay attention to emergency exit routes and how they intersect. If in an emergency an area designated as an area where sensitive computers are located is now a high traffic area for an emergency, it may be necessary to reconsider where the computers designated as "sensitive" are located. It is important also to prevent any possible crime of opportunity. Leaving PDA's, CD/DVD's or other portable electronic devices laying about is asking for trouble. Consider using tracking devices for all devices. The last thing a political campaign needs is the entire strategy for an upcoming set of stump speeches out for the world (read opposition) to consider in a manner that does not have the controls in place that a policy-message centered speech would demand.

The Microsoft Security Response Center[13] has very good information available that can be used in developing a set of security regulations that can be implemented before the volunteers pour in. Key areas to consider are how sensitive information is handled. Is it readily available to the next temp receptionist who logs in, or is the data kept on a computer in a more secure area, behind a locked door, with encryption. Another point to consider is the potential for problems in high traffic areas. Computers should be bolted in some way in high traffic areas, even though all a bolt will do is slow down a thief. Portable computers and PDA's present problems as well. Consider using tracking software and encryption on those portable devices, as well as alarms. Screen saver passwords are a must. Remember to change the password from whatever the default is. I had a conversation with a schoolteacher recently who complained that the password to the grading system database was *required* to be left at default. I asked why, and the answer was "the systems administrator did not want to get bogged down in changing passwords everytime a teacher left for a new job..." Imagine being able to log into a public school's grading database and change a few of those grades around... I imagine we will be reading about this scenario in the future. "Knowing a user's password can provide an entry point to launch further attacks against the host..."[14]

Political gamesmanship is an art in a presidential election year campaign. Any local campaign for that matter, can feel the heat. Let's not forget the infamous trick used by Kevin Mitnick to obtain access to a network. On one occasion, Mitnick tossed a floppy disk down a hallway with a yellow stickie labeled "Officer Salaries..." Some unsuspecting employee could not resist inserting that disk, launching some malware and viola, Mitnick was once again inside a network he had no business being in. Keeping this example in mind, anyone who is running a campaign office will no doubt want to take a close look at the materials that are left about. Campaign offices are busy places, very public and full of life. Books, beepers, laptops, PDA's, cellphones, pagers and posters are everywhere. I can

13. *See* Ed Bott and Carl Siechert: *Microsoft Windows Security for Windows XP and Windows 2000 Inside Out* ©2003 Microsoft Press
14. *See* Steven Northcut et al.: *Inside Network Perimiter Security* pg241 ©2003 New Riders Publishing

only imagine how easy it would be to walk into a campaign office, maybe not even have to sign in, and find oneself at a computer terminal in minutes. In every case, coming up with an agenda to address physical security is imperative.

Probably the most basic inspection regimin would start with a physical resources inspection for signs of unauthorized access.[15] Was a window left open last night? Was that rear-entry that is never used left slightly ajar? Was a fire-escape ladder left completely extended to street level? Who is responsible for the inspection? Have a person or persons designated for this detail, and do a thorough background check on whoever is in this position. Also, check all locks (cabinet and computer locks) for signs of tampering. Physical audits of all movable media should be done on a regular basis. The best practice for this type of audit would be on a weekly basis.

I highly recommend the CERT website for any administrator who is putting together a network for a political campaign. The relevant information is of immense practicality. Please see http://www.cert.org for more information.

Other considerations

Major operating systems in use today are fundamentally flawed with regards to network/internet security. The "Internet" as it exists today is also flawed. It was not originally designed for the usage that now exists. The Internet was originally designed as a network resource for the university and military communities. In the 1950's and 1960's, both communities were comparatively small. Keeping up to date with the latest software, especially operating system software, is a daunting task.

Please review Security Policy at the following links:

1. http://www.odu.edu/webroot/orgs/ao/po/polnproc.nsf/files/3507.pdf/$FILE/3507.pdf [16]

The above listed link is the security policy for Old Dominion University. The policy is clear, concise and readable. Of note are directives for serial numbers, locks on computers in public area and instructions for removing sensitive data to more protected areas in inclement weather and the use of water detection devices. One concern I have with this particular policy is it's age. It was written in 2000. Security Policy is something that needs to be updated frequently to address changes in technology.

2. http://www.it.ufl.edu/policies/security/ [17]

This is the current security policy for the University of Florida. It is very well organized, up to date and covers the main areas we need to address. After an introduction paragraph, specific instructions are provided defining security managers and their responsibilities. This is followed by instructions on unmanaged and managed hosts, the establishment of policies and procedures for physical security, audits, host and network security and training and security awareness. This document is a very good example of a well thought out policy that has been

15. *See* http://www.cert.org/security-improvement/practices/p098.html ©2000 Carnegie Mellon University. CERT®
16. *See* http://www.odu.edu/webroot/orgs/ao/po/polnproc.nsf/files/3507.pdf/$FILE/3507.pdf © 2000 Old Dominion University.
17. *See* http://www.it.ufl.edu/policies/security/outlines/unit-policy-outline.html © 2004, UF Office of Information Technology

reviewed by a cross section of people involved with the university including administrators, legal and human resources. “Specificity is one of the most important aspects of good policy. One of the best ways to avoid unenforeable policy is to reduce the ambiguity.”[18]

Given how busy political organizations are, it would be a stretch to expect a major security policy statement to be drafted for every campaign. Running for councilman/woman in a small town probably won’t need a major security document produced. In a larger campaign, the need will be there. On a national level, policy should be standard, however, getting straightforward answers on whether they exist I have found difficult. There are many resources available that can help make for a smooth transition from general concerns to a functional concrete policy. The above listed security policy links are just a couple of examples of how to put together a set of practices that will work.

No matter how busy, it is not unfair to expect that your data has integrity. You need to feel assured that what is being sent out from your network is unaltered, and that your information is controlled and confidential. The basis of Confidentiality, Integrity and Assurance is the cornerstone of any network, big or small.

Political organizations will focus more on the realities of network based compromises to their candidate(s) message as each incident becomes part of the political landscape. I believe the systems administrations team for a political campaign will become an integral component of any organized campaign. Indeed, some recent presidential campaigns placed a huge focus on internet based strategies for everything. This includes meeting up with other supporters, fundraising and the organization of events. The internet is a perfect medium for any start-up political group and campaigning can be made much easier by using the versatility of the medium to inform and educate potential voters.

The glaring weaknesses of the network will always demand constant monitoring and searching for methods to achieve that elusive balance of flexibility, strength and security. It is only through security within the network environment that we can trust the candidates message. As was found out in late December of 2003, in the heat of a run-off election, someone was about to get a message out to the people of San Francisco. This message was a blatant misrepresentation of who the author was, where an event was being held, and for what purpose. This is exactly the sort of malicious activity we must protect against. For if we do not, the medium will become irrelevant to propagating a free flow of ideas, ideals and ultimately the representatives of our freedom.

The cost of malicious and illegal activities is rising every month, with headlines such as below in newspapers on an almost daily basis.

COMPUTER VIRUSES, WORMS SET COSTLY INTERNET RECORD[19]
By Tim Lemke
THE WASHINGTON TIMES

February was the worst month ever for cyber-security as a record number of computer viruses and worms attacked the Internet, flooding in-boxes with unwant-

18. *See* Steven Northcut et al.: *Inside Network Perimiter Security* pg119 ©2003 New Riders Publishing
19. *See* Tim Lemke: The Washington Post, Sunday Feb 29, 2004

ed e-mail, crippling Web sites and costing businesses up to $83 billion worldwide.

It is precisely this condition that requires those of us in the field of network security to constantly keep our information updated and keep a questioning eye on all information that is on our network.

In closing, I look forward to an exciting 2004 Presidential election season. The broad depth of democracy can be found in all the heated debates, the political talk-show circuit, the major media outlets CNN Fox ect...but most importantly, the small groups of citizens who are working for their candidates in offices in small towns all around the country. They are the grassroots, no matter what their affiliation is, and they deserve honesty, integrity and assurance in all the activities associated with the campaigns they are aligned with.

Presidential aspirants are politicians (generally) with much experience. They are not systems administrators, network technicians or programmers. They only want their computers to serve them and the ideas they want to put forth to the public. Presidential aspirants are often men and women who have careers in public service. How we, as information technologists, inform and educate these policy makers is of vital importance. We have the opportunity to make information security a priority in the ongoing political dialogue. We can only do this through a very strong committment to confidentiality, integrity and availability.

My hope is that this paper will stimulate additional discussion on this timely and crucial subject. I have no doubt that issues pertaining to network security will arise in various campaigns now underway across the country.

References

J.K. Dineen and Adriel Hampton: *Cyber War over Gore Newsom Event* San Francisco Examiner, Monday Dec. 1, 2003

Helen Dewar: *GOP Aides Implicated In Memo Downloads* Washington Post, Friday March 5, 2004

Ed Skoudis: *Counter Hack* Prentice Hall ©2002

Eric Cole et al: *SANS Secutify Essentials with CISSP CBK* ©2003

J.K. Dineen and Adriel Hampton: San Francisco Examiner, Tuesday Dec. 2, 2003

Mark G. Milone *Hacktivism: Securing the National Infrasctructure* The Business Lawyer November 2002

Ed Bott and Carl Siechert: Microsoft Windows Security for Windows XP and Windows 2000 Inside Out ©2003

Steven Northcut et al.: *Inside Network Perimiter Security* ©2003 New Riders Publishing

http://www.cert.org/security-improvement/practices/p098.html ©2000 Carnegie Mellon University. CERT®

http://www.cert.org/security-improvement/practices/p098.html ©2000 Carnegie Mellon University. CERT®

http://www.odu.edu/webroot/orgs/ao/po/polnproc.nsf/files/3507.pdf/$FILE/3507.pdf © 2000 Old Dominion University.

http://www.it.ufl.edu/policies/security/outlines/unit-policy-outline.html © 2004, UF Office of Information Technology

Tim Lemke: The Washington Post, Sunday Feb 29, 2004

Note: There were a number of telephone queries with individuals associated with current or recently disbanded national political campaigns who either did not respond, responded with vague answers to specific questions on network security, or responded with “I will get back to you.” I have purposely left names excluded.