Interested in learning more about security?

SANS Institute InfoSec Reading Room

Why Small Businesses Need to Secure Their Computers (and How to Do it!)

I'm here to talk to you about computer security - and I don't mean just locking it up in a closet! I'm talking about making sure that the information you keep on your computer(s) is safe, that the only people who see that information are your employees, and making sure that the information is available when they need it. I'm also talking about making sure that no one (make that no hacker) is using your computer to do things that you don't know about. Things that might make you legally liable for someone else's actions....

Why Small Businesses Need to Secure Their Computers (and How to Do it!)

A speech to be given to local small business people

I'm here to talk to you about computer security – and I don't mean just locking it up in a closet! I'm talking about making sure that the information you keep on your computer(s) is safe, that the only people who see that information are your employees, and making sure that the information is available when they need it. I'm also talking about making sure that no one (make that no hacker) is using your computer to do things that you don't know about. Things that might make you legally liable for someone *else's* actions.

When the Internet first became publicly available, and for several years thereafter, I used to tell people that, "If someone's trying to hack into your computer over a slow 56k modem, you've got bigger problems to deal with." I still believe that today, but the problem is the meaning of the phrase "to hack into your computer". What I mean by that is, if someone is trying to *steal large amounts of your information* from your computer over a (by today's standards) slow 56k modem, then you do indeed have serious security problems – not just computer security problems.

But *any* computer connected to the Internet today is a security risk. The speed of your Internet connection does not matter—the *fact* of the connection is enough to put the computer at risk. The speed of the computer makes no difference—if it's good enough to surf the Internet, it's good enough for hackers to break into. And it does not matter what software is running on the computer—*all* popular software titles are vulnerable to misuse and attack.

Let's distinguish between different types of "hacks", or attacks, on your computers. Some of the most common kinds of attacks are:

Hacking: To most people, hacking is a catch-all term for any kind of attack, but to computer people, it means, "Gaining unauthorized access to a computer system". A *hacker* is the person who does the hacking. Think of him or her as a cyber-*trespasser*.

Espionage: Stealing your information. This is *hacking into* your computer. This attacks the *confidentiality* of your information; that is, how can you be sure that the only people who have seen your information are the people you've authorized?

Defacement: Changing a Web site (or any other information stored on a computer) without the owner's permission. This is also *hacking into* your computer. Some defacements are very minor and can barely be seen; some are major changes to the Web site like putting up insults, racial epithets, obscene materials, or other things that you probably don't want associated with your company. This attacks the *integrity* of your data; that is, how do you know that the information is accurate? How do you know that someone hasn't changed a phone number, or an address, or the balance due on an invoice?

Denial of Service (DoS): In its simplest form, a DoS attack prevents you from getting to your information – therefore *denying* you of the *service* your information provides. Depending on how you've been attacked, this may or may not involve hacking. There are many forms of DoS

attacks, from deliberately causing your computers to crash to deliberately preventing anyone from getting to your Web site. This is an attack on the *availability* of your data. Even though the hacker may not have your data, they have prevented *you* from having your data, too, which can be just as bad.

Distributed Denial of Service (DDoS): DDoS is a very widespread type of DoS attack. The classic DDoS attack is one where the hacker has *your* computer run a program that you don't know about that helps in a DoS attack against another computer. (Typically, the hacker has also gotten many other computer to participate, also without their users' knowledge.) In this case, the hacker isn't interested in your information; they're interested in using your *computer* for their own purposes. This may also involve hacking – certainly, *your* computer has been hacked, hasn't it? This is also an availability attack, but not against your data. DDoS attacks the availability of your *computer* – after all, if your computer is busy doing something for someone else, it isn't busy doing *your* work. And, it's also an attack against someone *else's* data.

How bad is the problem?

Everyone's heard stories about the Pentagon's computers being hacked into. What you should know is that the Pentagon maintains two types of system (as far as security goes): classified and unclassified. The difference is that the unclassified computers don't (or shouldn't, anyway) hold any classified information. The Pentagon confirms that in calendar year 2000, there were 215 successful hacks into their unclassified computers. That's an average rate of someone successfully hacking into the Pentagon's computers *almost every business day of the year*. (The good news is that they say they are unaware of any successful hacks into their classified systems.)

Other recent hacks:

- The respected SANS Institute's (www.sans.org) Web site was hacked into and defaced in July of 2001. (SANS is a private organization dedicated to educating the technical community on how to secure their systems.)
- In May of 2001, the White House Web site (www.whitehouse.gov) was taken off the Internet by a successful DDoS attack. And in July and August of 2001, the first Code Red worm was trying to DDoS the White House.
- Several Microsoft Web sites were also successfully attacked with DoS attacks at various times in 2001.

The University of California at San Diego recently released a study in which researchers estimate that there are over 4,000 successful DoS attacks against somebody *every week*[1].

Why you—the small business person—need to be concerned

Myth #1: "Oh, my data is not all that valuable to anyone else." That *may* be true, but it's probably not. How much is your client list or a copy of your latest bid worth? Probably not much to one of your clients. To one of your competitors, though, they are likely worth quite a bit.

[1] Lemos, "Study: Sites attacked 4,000 times a week".

Of course, if you're in any of the healthcare or financial professions (or even just in an affiliated field, like insurance), then there are many state and federal regulations regarding what information you must keep private, and what steps you must take to take to make sure the information stays private[2,3].

But, what if the person attacking you is *not* trying to steal your information? Suppose they are trying to just erase it *without* stealing it? Suppose all they are looking for is the private telephone number of your best client? Suppose you are running a remote control program like PC Anywhere, and the attacker uses *it* to do his dastardly deeds? Or, suppose that the hacker doesn't want anything to do with your information – he wants your computer to do his bidding, like spreading the Code Red worm?

Myth #2: "My computer (or my connection) is too slow for anyone to care". Keep dreaming! If you have a regular modem, your connection is indeed slow by today's standards. But it's not too slow that a hacker couldn't use your computer for things you don't know about—like spreading the Code Red worm or any other DDoS attack. And, of course, if you have a high speed connection (cable modem, DSL, satellite, ISDN, etc), then you have a connection that usually isn't turned off, and isn't too slow for anything.

Myth #3: "I must be secure; I'd know if anything were doing on my computer." Really? *How* would you know? Especially if the hacker took care to make sure that whatever he/she is doing doesn't show up on your screen?

And, let's suppose you *would* know if something is happening on your own computer—like it's suddenly running slower, or you've suddenly lost a couple of gigabytes of storage space. Would you know the same thing about *every single computer* in your business? Most business people, of any size business, would not.

Let's try a test. Press Ctrl-Alt-Del on your computer. This will bring up a list of programs that are running on your computer right now (Windows NT and 2000 users will have to hit the "Task List" button after pressing Ctrl-Alt-Del). Do you know what every single one of those things does? Are you sure that none of them are malicious? And, suppose the hackers thought of Ctrl-Alt-Del, and made sure that whatever programs they're running on your computer don't show up in the list?

"Why do I care?"

You certainly care about the reputation of your business. If, for example, someone changed (or "defaced") your Web page without your knowledge, that may reflect poorly on your business and your reputation (how poorly depends on what the hacker did to your Web site). You certainly don't want to let it get around that you don't keep your clients' information confidential.

You care that your information is available to you—that your computer hasn't crashed because someone thought it would be fun. Think about what business function provided by your computers that your business couldn't survive without. For some businesses, it's their

[2] "Protecting the Privacy of Patients' Health Information."
[3] "Gramm-Leach-Bliley Summary of Provisions". Title V – Privacy.

accounting database; for others, it might be their contact list or their materials tracking system. If your computers and that critical information they hold weren't available to you, then your business would likely suffer the consequences.

Also, not securing your Internet-connected computers might be construed – legally – as negligence. Think "Due Diligence" – if your lack of action causes harm to someone else, it's possible that you and your business could be held liable[4]. Currently, there is very little case law on this particular subject. You probably *don't* want to be the test case.

You're convinced

Alright, let's say I've convinced you of the need to secure your computers. But, the Pentagon, the White House and Microsoft, who have a lot of time, money, and other resources to throw at the problem, are still getting hacked. So what can you, the small business person do? As it turns out, quite a lot! And, almost everything listed below is either free or pretty close to it.

Backups

You've heard all of your friends and relatives who know anything about computers tell you to back up your data. You've heard the horror stories about people who've lost months of work because their computer crashed and their thesis (annual report/great American novel/tax return/whatever) can't be recovered. You've read or heard or seen the news about someone picking up a computer virus and it wiped out all of their information.

All of these stories are inevitably followed by something like, "and they didn't have a backup!" What's a backup? A backup is copy of your data, usually stored somewhere other than on your computer, that you can refer to if something ever happens to your computer and its original copy of the data.

Because part of the idea in backing up is to physically take the backup copy somewhere else, most devices for backing up data use some kind of removable device to hold your data. One popular type of backup device is called a *tape backup unit*, or tape drive. A tape drive puts your data on a tape that resembles a standard music cassette tape, which you can then take with you and put in a safe place. Another popular backup device is called a *Zip drive*. A Zip drive looks like a regular floppy drive, except that its disks hold almost 175 times as much as a regular floppy disk. This makes a Zip drive ideal for backing up your important project data, your customer or accounting database, or any other discrete set of data.

You may not consider backups to be part of computer security, but they definitely are. There are lots of ways to make hacking into your system more difficult, or to detect viruses before (and after) they strike, and there are lots of ways to *attempt* to recover data that's been lost through malicious means. But, there is absolutely no better way to ensure the *availability* of your data after an attack, and the *integrity* of your data if you think it's been compromised, than a good backup.

(Of course, there's no better way to compromise the *confidentiality* of your data if you don't physically secure the backups, as well!)

[4] Effross, Section II, Subsection C, "Malpractice/ Negligence" and Section III, Subsection A, "Duty of Due Care".

Patching your systems

All of you hearing this speech have, I'm sure, extensively used some version of Microsoft Windows. Therefore, you must all be aware of the dreaded "Blue Screen of Death"(BSOD), when your screen turns entirely blue, and white printing on top of the blue screen announces (in a very cryptic fashion) that you have just lost whatever you were working on. By far, most BSODs are caused by errors in the software, called *bugs*. Of course, not all bugs cause BSODs - some bugs cause your computer to be vulnerable to people who would attack it.

Most software companies (including all of the big names in the industry) spend a lot of time and effort fixing these bugs when they find out about them. These fixes (called patches) are usually available free on the company's Web site. But, many people do not apply the patches – witness the efforts by the Federal government over the last several weeks to get as many people as possible to patch against the Code Red worm. An unpatched computer is then vulnerable to attacks. What this means in a practical sense is that an unpatched computer could be hacked using a bug discovered two years ago – a bug that was fixed in a patch released 18 months ago!

At the very least, you should patch your operating system (which is probably some flavor of Windows) and any software you use with the Internet, like your Web browser (probably Internet Explorer or Netscape Navigator) and your email program (probably Outlook, Outlook Express, Netscape Mail, or Eudora). You should also check for new patches *at least* once per month. You can find those patches on the software manufacturers' Web sites, many of which are listed in the Appendix.

Anti-Viruses

Every couple of months, it seems, the evening news is talking about the latest computer virus that's going to come along and put you out of business. There have been several in the recent past – Melissa and ILOVEYOU, and just recently, SirCam and Code Red. New viruses are being released (some might say "inflicted upon us") all the time – some estimates range as high as 10 to 15 new viruses *per day*.[5]

A computer virus, in one sense, is like any other computer program: someone has written it to perform a specific task. The main difference between regular programs and viruses, though, is that viruses often are intended to do things to your computer that you don't want them to do – like erasing your files, crashing your computer, making your computer run slower, or in some way making your information and/or computer unavailable to you. Also, unlike regular programs, viruses *replicate,* or duplicate themselves, and try to spread to other computers.

What can you, the average user, do to protect yourself against viruses? Why, practice safe computing, of course! First, purchase and install an anti-virus program if you don't already have one. (For a list of popular anti-virus manufacturers and their Web sites, please see the Appendix.) Since most viruses these days are spread by email[6], be very careful about your incoming email. Make a habit of deleting emails that come from sources you don't know (*without* opening them first). Be especially careful of email attachments that *do* come from

[5] "Internet Security for the Web" 9
[6] "Home Network Security" Section III, Subsection B, Paragraph 9.

people you know, even if you are expecting to receive them. Save all incoming attachments to your hard drive and scan them for viruses *before* opening them.

Many viruses still spread on floppy disks. Be sure to scan any floppy disk that you put in your computer with an anti-virus program.

Anti-virus programs also do more than find just viruses. They also find other kinds of malicious software that are not technically viruses. "Trojan horses" are programs that appear to do one thing while actually doing another—think of a Solitaire game downloaded from the Internet that does indeed play cards but *also* does something else, completely different, that you don't know about. "Worms" act like viruses, but they infect entire systems rather than individual files. The recently famous Code Red was actually a worm.

Of course, if you bought an anti-virus program, or one came installed on your computer when you bought it, the anti-virus program will be able to protect you against viruses, right? The answer is: sort of. The program should protect you against all of the viruses that were known about *when it shipped from the factory*. Unfortunately, the program has no way of knowing about viruses that came out after it was shipped.

The manufacturers of anti-virus software spend a lot of resources keeping up with all of the new viruses, and coming out with cures for them as fast as possible. They're pretty good about it, too; most of the viruses have cures before they can cause trouble. All of the manufacturers release updates to their anti-virus programs on a regular basis, so that the anti-virus program on your computer *can* know about the viruses that came out after you got your anti-virus program. What *you* have to do is go the manufacturer's Web site and get the latest update, and keep going there at least one a month for new updates. (Anti-virus update Web sites are also listed in the Appendix.)

Firewalls

Many of the hacks we discussed earlier are possible because the underlying structure of the Internet is public knowledge[7], and hackers use that public knowledge to figure out ways to slither in between the cracks in that structure. One way to keep out all but the best hackers is to use what's called a *firewall*. Firewalls help seal the cracks and keep out a lot of less knowledgeable hackers.

A firewall is placed between the Internet and your computer or network. It examines all of the data flowing in and out and decides whether or not to allow that data to flow past. It makes these decisions based on a set of rules, or instructions, that tell it what is and what is not allowed to flow past.. Most firewall manufacturers install a set of rules at the factory (called the default rule set) that is good enough for most everyone. In other words, you probably won't have to fool with it to get it working right; it will probably work just fine right out of the box.

A firewall not only keeps unauthorized people *out*, it also keeps your data *in*. Many Web sites gather information about you and your computer when you visit the sites. Because of the high degree of automation in today's Web sites and the integration of Internet functions in almost every piece of software, you may be sending more information than you know (or want) to

[7] "Official Internet Protocol Standards."

different places on the Internet. Many firewalls have the capability to stop this information from leaving your computer (or your network, depending on what type of firewall you have).

A firewall can be either a piece of hardware or a software program. Hardware based small business firewalls are usually about the size and shape of a cigar box. You plug one side into your Internet connection, plug the other side into your computer or network, follow the setup wizard's instructions, and you're ready to go.

Of course, purchasing a hardware firewall involves spending money, and none of the small business people I know (myself included) like to do that. And, a hardware firewall requires some setup and some knowledge of networks, which most small business people lack. So, for those who are uncomfortable with a hardware firewall, you can use a software based firewall. A software firewall is a program that you load on your computer like any other program. Several decent firewalls are available free of charge for home use, like Zone Labs' ZoneAlarm, Tiny Software's Tiny Personal Firewall, and Sygate Technology's Sygate Personal Firewall. (As always, Web sites are in the Appendix)

Modems and modem-based software

Did you see the 1983 movie *WarGames* with Matthew Broderick? The one where he hacked into the Pentagon's computers and almost started World War III? Remember how he did that? He used a *modem*—a device that hooks your computer up to a standard telephone line.

These days, modems are mainly used for connecting to the Internet. But, many small businesses also use modems for communicating with their vendors and employees who work from home. And, unless you are unusually security-conscious, chances are that there is little or no security on your modem software.

The problem here is that hackers know this, too. They know that if they can find out what the telephone number of your modem is, they may have an easy point of entry into your system. The easiest solution to this security problem is also the most obvious—turn off the modem when you're not using it. If the modem is inside the computer, you can unplug it from the wall when you're not using it. Problem solved. If you're in a situation where turning off the modems is inconvenient or just not possible, then you need a real computer security specialist to make sure that your modems are used only by those who are authorized.

Passwords

How many of you reading this have your passwords written down on a slip of paper? Is that slip of paper under your keyboard, in your wallet, in your desk drawer, or taped to your monitor? Is the password derived from your name, your spouse's name, one of your kids', parents', siblings' or pets' names, your home or work address, or your telephone number? Is it, perhaps, "password"? 12345? 54321? Are you now wondering how I figured out your password?

Passwords are usually one of the weakest links in any security scheme because most people choose passwords that can easily be figured out. They use the name of the month, or the make of their car, or the name of the street where they live. These kinds of words are called *dictionary words*, and when used as passwords, they can be cracked in minutes. Adding a nonsense character or two to the beginning or end of a word is, unfortunately, *not* a solution, because the

hackers are wise to tricks like this. (I thought my own password was secure. A password cracking program called LC3[8] cracked my password in less than 2 minutes. It didn't take me even that long to change my password to something more secure.)

So, change those passwords regularly! Don't use dictionary words as passwords. Instead, use a whole phrase, or even better, just the first letter from every word in the phrase (or the last letter, or the first letter from the first word, second letter from the second word, etc). Mix capitals and lower case letters, put some numbers and nonsense characters into it (like !@#*&), and now you've got a nice, strong password. Can it be cracked? Given enough time, any password can be cracked. But, believe me, it won't take only 2 minutes.

Encryption

For the *seriously* paranoid among us, or, more realistically, for those who place a high value on their data, let's look at *encryption*. Encryption is the process of turning regular, ordinary, everyday data into a jumble that no one could possibly understand. *Decryption* is the process of turning the jumble back into usable data. Encryption and decryption, therefore, are two different sides of the same coin.

In its simplest form, encryption is simply replacing letters of the alphabet with different letters in the same pattern. For instance, the word "telephone" would become "qbibmelkb" if encrypted by just substituting each letter with the one that comes three positions before. That is, Q comes 3 letters before T, B comes three letters before E, and so on. This is the kind of encryption your children find in breakfast cereals with "magic decoder rings".

As you can imagine, encryption schemes used to protect sensitive data are considerably more complex and far more difficult to break. Some of the best encryption schemes available today are *asymmetric*—they use one password to encrypt the data, but require a completely different password to decrypt the data. This is called *Public Key/Private Key*. One of the passwords (the "public key") is not kept secret. You let the entire world know what your public key is; anyone can then encrypt (but *not* decrypt) data that they want to send to you. Your "private key" is the one kept secret; it is the password you use to decrypt the information and put it to use. Public Key/Private Key is commonly used in email and other methods of transmitting data.

You can also encrypt the information that is on your computer. Suppose, despite your best efforts (and following all of my advice!), that a hacker does manage to break into your system. If your data is encrypted, then you at least know that any data they take is likely to be useless to them. Even the FBI has difficulty breaking the encryption of one of the most popular programs, PGP[9] (PGP stands for "Pretty Good Privacy", which it probably is if the FBI can't break it).

Testing

So, you've changed your passwords, updated your anti-virus, backed up, and encrypted your data. You've patched all of your software, turned off your modems, and installed a firewall.

[8] "About LC3"
[9] Hopper

Have you missed anything? Is there a setting you meant to make but forgot? In other words, how do you *know* if you're secure?

You probably won't be surprised to learn that there are some basic security scanners available free on the Internet. Two of the most popular free scanners are Gibson Research Corporation's ShieldsUP! and Symantec Corporation's Symantec Security Check. Both tools will give you a good idea how vulnerable you are, both before and after you work on securing your systems. And, these "hacking" tools are so easy, even an adult can use them!

For a more in-depth analysis, many computer security companies offer *penetration testing*, or trying to hack into your system. For a fee, and with your written permission, they will attempt to break into your system (*without* defacing your Web page or compromising your data) and recommend ways to close any openings they find.

Conclusion

Small businesses are connecting to the Internet like never before. Their computers, therefore, are vulnerable to hacking like never before, too. There are many things that any small business can do to help secure its own computers and prevent them from being used in attacks on others; and these things cost little or no out-of-pocket money. You, the small business person, should not only take these steps to secure your own computers (and the future of your business), but also urge all of the other business people you know to do the same.

APPENDIX

Listed below, by section, are all of the Web sites discussed above. Also listed are some that are *not* discussed above, but are relevant to the section they are listed under. For instance, there are no Web sites discussed in the section of the paper on hardware firewalls, but there are several hardware firewalls listed in the relevant section below. For all sections of the paper, there are many more Web sites that are relevant to the subjects being discussed than are possible to list here.

How bad is the problem?
SANS: www.sans.org
The White House: www.whitehouse.gov
Microsoft Corp.: www.microsoft.com

Backups
Zip drive: http://www.iomega.com/zip/index.html
Tape drive: http://www.seagate.com/products/tapesales/tapeselect/

Patching your systems
Microsoft Windows (including Internet Explorer and Outlook Express):
http://windowsupdate.microsoft.com
Microsoft Office (including Outlook): http://www.officeupdate.microsoft.com
Netscape: http://home.netscape.com/computing/download/index.html
Eudora: http://www.eudora.com/products/eudora/download/
Corel WordPerfect Office: http://www.corel.com/support/downloads/index.htm
Lotus SmartSuite: http://www.support.lotus.com/ftp.nsf/maindir

Anti-Viruses
Symantec (Norton Antivirus): www.symantec.com
    New viruses update: http://www.sarc.com/avcenter/download.html
    Product patches: http://www.symantec.com/nav/index_updates.html
Network Associates (McAfee Antivirus): www.mcafee.com
    For updates: http://www.nai.com/naicommon/download/dats/find.asp
    For new viruses update, select "DAT Only"
    For product patches AND new viruses update, select "DAT + engine"
Computer Associates (Inoculan): www.cai.com
    Virus definition file: http://support.ca.com/Download/virussig.html
    Product patches: http://support.cai.com/Download/patches/techptch.html
For other Anti-virus vendors, please see: http://www.cert.org/other_sources/viruses.html#VI

(Continued next page)

Firewalls:
Selected Hardware Firewalls:
Linksys Cable/DSL router: http://www.linksys.com/products/product.asp?prid=20&grid=5
3COM OfficeConnect® Internet Firewall 25
http://www.3com.com/products/en_US/detail.jsp?tab=features&pathtype=purchase&sku=3C16770-US
SonicWall: http://www.sonicwall.com/products/access.asp

Selected Software Firewalls:
ZoneAlarm: http://www.zonealarm.com/
Tiny Personal Firewall: http://www.tinysoftware.com/pwall.php
Sygate Personal Firewall 4.0: http://www.sygate.com/free/spf_download.htm

Passwords:
@stake's LC3: http://www.atstake.com/research/lc3/
Windows Security Guide's Random Password Generator:
http://www.winguides.com/security/password.php

Encryption:
PGP: http://www.pgp.com/products/freeware/default.asp
International PGP Web page: www.pgpi.com

Testing:
Gibson Research Corporation's ShieldsUP! https://grc.com/x/ne.dll?bh0bkyd2
Symantec Security Check:
http://security.norton.com/default.asp?productid=sarc&langid=us&venid=sym

List of References

All hyperlinks were valid and publicly accessible on the date of submission.

1. Lemos, Robert. “Study: Sites attacked 4,000 times a week”. May 22, 2001. C-Net News.com. Accessed August 11, 2001. <http://news.cnet.com/news/0-1003-200-6006924.html?tag=st.ne.1003.saslnk.saseml>
2. “Protecting the Privacy of Patients' Health Information.” July 6, 2001. U.S. Department of Health and Human Services. Accessed August 4, 2001. <http://www.hhs.gov/news/press/2001pres/01fsprivacy.html>
3. “Gramm-Leach-Bliley Summary of Provisions”. U.S. Senate Banking Committee. Accessed August 4, 2001. <http://www.senate.gov/~banking/conf/grmleach.htm>
4. Effross, Walter A., “Statement of Walter Effross Before the U.S. House of Representatives Committee on Science, Subcommittee on Technology” March 9, 1999. United States House of Representatives Committee on Science. Accessed August 7, 2001. <http://www.house.gov/science/effross_030999.htm>
5. “ Internet Security for the Web: Protecting Enterprise Networks from Malicious and Inappropriate Web-based Content.” July 2000. Symantec Corp. Accessed August 2, 2001. <http://enterprisesecurity.symantec.com/PDF/ITSECWP.pdf>
6. “Home Network Security”. CERT Coordination Center. Last updated August 6, 2001. Section III, Subsection B, Paragraph 9. Carnegie Mellon University Software Engineering Institute CERT. Accessed August 11, 2001. <http://www.cert.org/tech_tips/home_networks.html>
7. University of Southern California, School of Engineering, Information Sciences Institute. “Official Internet Protocol Standards.” Results as of August 4, 2001. Accessed August 4, 2001. <http://www.rfc-editor.org/rfcxx00.html>
8. “About LC3”. @stake. Accessed August 5, 2001. <http://www.atstake.com/research/lc3/>
9. Hopper, D. Ian. “FBI Using High-Tech Gadgets”. Yahoo! Technology News. Posted July 28, 2001. The Associated Press. Accessed August 10, 2001. <http://dailynews.yahoo.com/h/ap/20010728/tc/fbi

Last Updated: May 26th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Madrid 2017	Madrid, ES	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GAUS	May 30, 2017 - Jun 04, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CAUS	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DCUS	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TXUS	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Milan 2017	Milan, IT	Jun 12, 2017 - Jun 17, 2017	Live Event
SEC555: SIEM-Tactical Analytics	San Diego, CAUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NCUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, NL	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, COUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MNUS	Jun 19, 2017 - Jun 24, 2017	Live Event
DFIR Summit & Training 2017	Austin, TXUS	Jun 22, 2017 - Jun 29, 2017	Live Event
SANS Paris 2017	Paris, FR	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, AU	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MDUS	Jun 26, 2017 - Jul 01, 2017	Live Event
SEC564:Red Team Ops	San Diego, CAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, AU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Stockholm 2017	OnlineSE	May 29, 2017 - Jun 03, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced