Global Information Assurance Certification Paper

Small Business Security Considerations

GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4c - Option 1
Jody J. Hietpas
February 10, 2005

Summary

There are many challenges facing small business owners. While the security of their computers may be near the last things on their minds, it could end up being one of the biggest problems. A security breach, or even a bad virus infection, can cause a large strain on the already tight resources a small operation has at its disposal. A proper plan for the maintenance, protection and disaster recovery of computer systems should be considered an insurance policy against problems. It can't stop bad things from happening, but it will help the small business owner deal with the outcome.

This paper will cover the reasons information security should be important to small businesses, some of the challenges they face, and some direction on how they may want to approach their security.

Why is this important to you?

As a small business owner, or even a sole proprietor, you may not think that information security is necessary for you. There are, after all, much bigger and more valuable targets out there in the world. There are also several good reasons small business need to worry about "that security stuff," and little of it has anything to do with your business.

Most of the attacks coming from the Internet these days come from automated worm programs that broadcast themselves around the world with no particular target[1]. Just having a computer connected to the Internet puts you at risk. The average time an unprotected Microsoft Windows XP computer can stay connected to the Internet before it is infected is around 20 minutes[2]. Even pointing your web browser at the wrong site can cause a surprising amount of software to be installed on your computer without your permission[3]. Email borne viruses and network propagating worms don't care if you are a multinational corporation or a single person working out of your spare bedroom.

What do the creators of all of this junk want with your computer? Well, it depends. Sometimes they just want access to the machine itself and your Internet connection. Combine the power of your computer with that of 10,000 others, and it makes a handy platform for attacks against third parties or to relay spam to the rest of the world[4]. Other times, they are looking for your data by hijacking the connection between you and your on-line banking service. They can collect your user name and password information and use it to transfer money directly out of your accounts.

As larger companies are raising their defenses to fend off the "evil hackers", it is the smaller companies who leave themselves open to attack[5]. The smaller, less protected companies provide much easier targets for people looking to do some damage. The payoff may not be as great, but neither is the risk of getting

caught, or the difficulty in getting in.

If you want to know why information security should be important to your business, answer these questions. Could your business survive if you were compromised in some way? Would your customers tolerate it if a virus on your laptop started sending copies of itself to everyone in your address book? Would your reputation suffer if sensitive information were leaked to a competitor? What would you do if your computers became unusable because of a virus outbreak?

Small companies are being hit by virus attacks, forcing them to spend time and money cleaning up after them. Some estimates say that one in three small businesses were hit by last year's MyDoom virus[1]. Taking steps to protect your business from intrusions is an insurance policy against problems.

Challenges

The challenges involved in securing your small business' information are the same ones facing every other aspect of your business. It comes down to time, money and expertise.

Taking time out from running your business to maintain your computers can seem like a diversion. There are usually enough other things you need to be doing, without having to spend time playing with your computers.

Money is another scarce commodity to a small business that must be spent as wisely as possible. When profit margins can be thin to non-existent, it is hard to justify spending money on security when the benefit is not easily defined.

Lack of experience in handling computer systems can be the biggest obstacle to running clean and safe systems. It is difficult to keep up with the vulnerabilities involved in using a computer on the Internet without knowing what you need to do to stay safe, how to do it, or why you should care about it in the first place. Lack of experience includes lack of awareness of the problems that exist. Technology itself can't protect your systems and data. It is also important for people to understand how to properly use that technology.

Solutions

The challenges can look difficult to overcome, however there is some good news. There are solutions to the problems that can keep you out of trouble, and plenty of people to help you when you need it.

Raise awareness

First things first, you can't fight what you don't know about. Security awareness is not a technical subject. It is about understanding what the consequences of your actions could be. End users are considered a large risk to a business due

to either naivete or malice[6].

Whatever the problems are that your own people can cause, there are some things you should do to mitigate them.

If you have more than one employee, you need to have written policies in place. Employees cannot know what is expected of them if there are no guidelines to follow. Written policies should include acceptable use of company equipment and networks, how passwords should be formatted and what action will be taken against people violating the policy. Depending on the size of the organization, you may need some legal advice on this, as parts of it could involve terminating employees or contacting law enforcement.

With the policies in place, you need to present them to the end-users. The training should be in a group class setting, or it could be web-based[8] if an in-house class is not feasible. The sessions should include reasons why they should care aside from the consequences of violating policy. Short policy reminders and tips on safe handling of email and web browsing sent to your employees periodically will also help them keep the security concepts fresh in their minds.

Assess your risk

The practice of security is all about mitigating risk. Problems can never be completely eliminated, but proper planning can reduce the effects of them. A thorough risk assessment for your business will let you know where your problem areas are, how likely they are to occur, and what the expected loss would be if it happened. This will help you concentrate your time and money on the areas where they are most needed.

Risk assessments are based on gathering an analyzing information about the physical and electronic layout of your systems. It is usually a multi-step process including gathering inventory, determining vulnerabilities, evaluating alternatives, deciding what to implement and monitoring the new system[7].

You can start by doing a site survey to make a list of the equipment you use. Your computers, PDA's, cell phones and anything else you use to run your business should be included. You should then have a map containing everything you use to store customer or financial information, or communicate with people.

Now, look at how each piece is used. Where is your important business information? For most people, there is data scattered everywhere. Most of what you need is probably on computers in your office, while contact information could be on a PDA or cell phone. Everything you use is important to your business.

Assign a value to each of your assets. How much would it cost you to replace a

piece of equipment? Try to determine what direct damage would be caused by the loss or theft of each of these systems. You also need to take indirect losses, such as missed business opportunities or loss of your reputation.

Next, consider how all of these pieces connect to each other, and the rest of the world. How are you connected to the Internet? Do you use your laptop or PDA on wireless hot spots in public places? All of these connections need to be evaluated as a method of attack. Even your cell phone can be compromised if it has Bluetooth capability and is not set up correctly[11].

Determine how likely it is that you will have an attack or a loss of each asset. Some attacks are too difficult, too costly, or have too small a payoff to make it worth the attacker's time. While it is possible for someone to grab your address book off of your cell phone, it will probably never actually happen to you, as it must be done from a very short range unless special, usually conspicuous, equipment is used. You are, however, guaranteed to have infected computers all over the Internet attempt to send the latest worm to you.

Finally, you should have some idea of what your priorities are. The most valuable assets need the most protection. Balance that against the problems that you are more likely to have, and you should have a good idea of what needs to be done first.

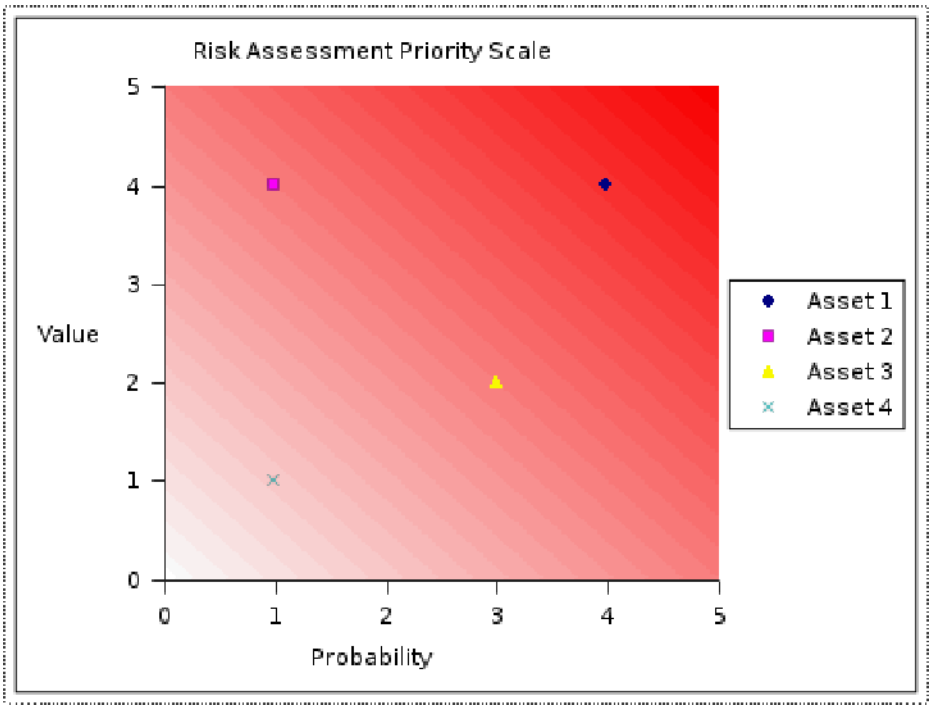

Figure 1.
Risk Assessment Priority Scale

For each asset you identified in your site survey, assign it a value on a zero to five scale, with five being the most valuable. Next, rate the probability of each of

those assets being compromised on the same zero to five scale. Adding the two numbers together will give you a total score for the risk associated with that asset. From Figure 1 above, you should see that "Asset 1" is in the most need of attention. It has a value of 4, and a probability of compromise of 4, giving you a total risk of 8. That, compared to the others, is the biggest problem. The numbers themselves don't mean anything. They are just there so you can compare all of your risks to set your priorities.

Minimum protection

There are a few steps you should take as a bare minimum to protect your business. You have probably heard them before, but I mention them here for completeness.

- Use anti-virus software, and keep it updated. Too many people still forget the second part of that statement. Anti-virus software works by recognizing known patterns in the files on your computer. Since new viruses/worms/trojans are being written all of the time, you need to keep your definition files up-to-date. All of the major anti-virus software vendors have systems that will do this for you automatically after you set them up.

- Use a firewall. In the older days of dial-up connections to the Internet, this was not a requirement. The widespread adoption of high-speed connections, such as DSL or Cable Modem, has made a hardware or software firewall mandatory. These connections are always on, connecting you to the world, and the world to you. A firewall will help filter out what you don't want on your systems.

- Keep your operating systems and software up-to-date. Just as new viruses are always being created, new vulnerabilities are constantly being found in the software that runs your business. This part can get tricky. Recent versions of Microsoft Windows have an automated tool that can keep the operating system updated, but most of the other software you run has to be handled manually. This is a tedious process, which is why it seldom gets done properly.

- Use strong passwords on your computers and external accounts. A strong password has at least 8 to 10 characters, consisting of upper and lower case letters and numbers. By default, Windows computers do not require a password to start them up. This should be changed, along with setting the screen saver to lock your computer when you leave it alone for too long. External accounts include email and web sites that require a login. The trick here is to pick a password that can not be guessed by anyone else, but that you can still remember. It doesn't work if you write it on a sticky note and leave it on you monitor, or under your keyboard.

- Practice safe email and web browsing habits. Email viruses tend to spread fast before the anti-virus companies can publish an update to look for it, so you need to stay on your guard. Don't open any email attachments that you weren't expecting, even if you know the person who sent it to you. Don't click on links in email messages, especially if it says that you need to verify your bank account information. These are "phishing" emails that try to get you to enter your personal data into a fake web site, allowing people to steal money directly from your bank account.

These five items are the most basic, but also the most effective way to protect your business. For small operations, it is not expensive. Only the anti-virus software and firewall should cost any money. The rest of the suggestions involve a change in the way you think about your interaction with the world. If you are a sole proprietor with a single computer, it may be enough to keep you in business.

Next Steps

The last section covers only the basics of what you can do to protect yourself from being compromised. Companies with a few more people will want to add to their defenses.

Mitigate or Transfer Risk

There are some risks that just can't be avoided, either because they are too difficult or too expensive to defend against. You can mitigate some of those risks by taking backups of all of your critical data regularly. They should be tested to make sure they work[1], and copies of them stored off-site. You can also buy insurance to transfer some of your financial risk to someone else. Data loss insurance is usually not covered by a normal policy, but can be purchased inexpensively to protect your business from extremely unlikely events.

Remote Access

If your people travel at all, or work off-site, they will probably need to connect back to the office to get email and move documents back and fourth. This used to happen through a slow dial-up connection directly from the remote computer through the phone lines to a modem in your office. It worked, but it was slow, expensive for long distances, and not always very reliable. Now that you can find a high-speed connection to the Internet at most hotels and coffee shops, it is much more convenient to connect through one of these networks. There are a few ways to do this without causing too many problems for your business.

Virtual Private Networks (VPNs) are set up to do just that. They encrypt all of the traffic between the user's computer and your network, so that it can not be intercepted. Most of these systems work with a protocol called IPSec, which is a set of protocols that describe how to set up the encrypted connection between

two computers. It can work in either "client-to-site" or "site-to-site" mode. Client-to-site is used to connect one computer, like a traveling laptop, back to the office network. A "site-to-site" link can be set up to connect two networks together over the Internet. It is a very powerful system, but it is also very complex, and can be defeated if it is not set up properly[14]. Some non-IPSec VPN packages also exist, including OpenVPN, which is based on an SSL/TLS system. This is the same system that allows a web browser to connect to a secure web site, but they have used it to provide a full VPN setup that is much easier to configure than IPSec.

Another way is to use a service called GoToMyPC. They allow you to interact with your PC at the office from almost any computer in the world. The service handles the encryption from end to end so you can run programs and transfer files as if you were sitting at your desk. There are no proven attacks against their system itself, but since it lets you connect from anywhere in the world, so can anyone else who can steal or guess your user name and password.

Be careful when using a publicly accessible computer, as you don't know who may have been tampering with it. A couple of years ago, a man in New York installed key logging software on computers at a number Kinko's stores in Manhattan[13]. This software would keep a record of everything typed into it by anyone else who used it. He would then go back to the same machines and take that information with him. Using these computers, he was able to steal the user names and passwords to online banking and other services from hundreds of people. He used this information to open people's bank accounts and transfer money into accounts he had set up. He was caught when he connected to a victim's computer through GoToMyPC while the victim was using it. Notice that he didn't have to break into GoToMyPC, or any of the banking web sites that he accessed. All he needed was to steal the account information and log into them.

Another thing to be careful of when traveling is outright theft of your laptop. The information stored there may be worth much more than the few thousand dollars it would take to replace the hardware[15]. You should be in the habit of knowing where it is at all times when you are traveling. Modern operating systems, such as Windows XP Professional or the Unix variants, can also encrypt entire sections of the hard drive, making it much more difficult for someone to access any data stored there.

Wireless Networking

Wireless networking (Wi-Fi) has become very popular in the last few years. It is easy to set up, the price of the equipment has dropped, and it doesn't require you to run cables around the office. The problem is that it is much harder to secure than a regular wired network, because an attacker doesn't need physical access. They can be half a mile away, and you would never know they were there. Wireless networks can be secured, it just takes some planning and work to get it done properly.

Most consumer grade wireless routers have default settings that leave them wide open to eavesdropping by anyone within a few hundred feet. Older equipment supported only WEP (Wired Equivalent Privacy) which is known to be easily breakable[12]. Newer routers that use WPA (Wi-Fi Protected Access) or the 802.11i standard are much more secure when they are properly configured, as they have been re-designed to overcome the problems inherent in WEP.

Depending on the size of your business, you can buy equipment that can handle many more connections than the consumer models, and have more options for separating the wireless network from the wired one. They also have stronger authentication controls to make sure that only your users are connecting to your network. One common way of providing a much stronger defense for your wireless network is to completely isolate it from the wired network. You would then require a VPN connection to access the resources of the wired part of the network.

If you are using a wireless network that you don't have control of, like a hot spot at a coffee shop, you should be taking some steps to reduce the amount of information you are giving to everyone around you. Remember that your network card is now a radio transmitter that can be received by anyone in range. If you are connecting to your office to check your email, you should be using a VPN or some other encryption to keep your data safe from prying eyes. If you don't have those resources available, and you are just surfing around, you can get a connection through a company called HotSpotVPN[16]. They have a service set up to allow you to open an IPSec VPN connection to their office, so all of the traffic from your computer to the Internet is encrypted. It doesn't get you complete end to end security, but it does offer a secure connection out of the public wireless network.

The Importance of People

No amount of technology can protect your business without knowledgeable people to plan, install, operate and monitor it. Most of these systems are very complex, and it takes experienced people to make everything run properly. You and your employees will need training and time to do their jobs effectively.

All employees should have security training relative to their position in the company. Basic security awareness should be taught to anyone with access to a computer, as they are often your first line of defense against new viruses that haven't yet been caught by the anti-virus software. Managers need an overview of network security so they can understand why they are being asked to spend money on it.

Support people need more in-depth training so they can understand how to build and maintain the network securely, instead of just putting it together. If the security of a system is considered while it is still being planned, it will save

money and time later, when problems are discovered. They also need to know how to monitor the system after it is running. Unless you know how the systems normally run, you can't tell if something abnormal happens.

Once your people are properly trained, they will need some time to do their jobs. The security landscape can change quickly. The people who are responsible for the security of your systems need to have some time set aside every day to read the latest news on what is happening around the world. This way, they can quickly learn what is happening to other companies, before it happens to yours. They can also forward information about any new viruses or other concerns to the rest of your staff, so everyone can watch for trouble.

No amount of technology can replace a competent staff. They are the ones who set the system up, watch it to make sure it is healthy, and handle any problems that occur.

Get Help

If your business is only a few people, it is unlikely that you have anyone with that level of technical skills on staff. You may have people who do the "computer stuff" in addition to their normal jobs, but having a full-time security expert on the payroll may not make sense to you. Maybe it's time to call someone in. Outsourcing your security and systems management allows you to have competent, dedicated security professionals around when you need them. It is not the best solution in all cases, but it can help you focus on your business, instead of the tools you need to run it.

Managed Security Service Providers (MSSPs) can be a good resource to helping you through the technical and procedural work needed to get your systems in shape[9]. They can assist in the creation of policies, perform risk assessments and help with planning and installation of new equipment or services. Sometimes these consultants are also hardware or software resellers, so they can purchase hardware and software at a lower price than you can. Depending on their capabilities, they can also be contracted to monitor firewall and Intrusion Detection System logs and respond to incidents on a 24x7 basis.

There are situations where contracting the security of your business is not the best thing for you[10]. They are, after all, a separate company. This can leave you with less control over what happens with your network. If you have in-house staff in charge of the day-to-day operations, there can be a communication problem between them and your MSSP. They will also handle your security in a way that is most efficient for them, even if it is not the way you have done it in the past. Finally, you are tying your business to their financial viability. If their business fails, you will need to replace them quickly.

If you decide to look for a service provider, there are a few things you should keep in mind when choosing one[1]. Review their references, to get a picture of how they worked with other clients. Find out how long they have been in

business, and if they have complaints filed with the Better Business Bureau, or the local Chamber of Commerce. If they will be working with some of your own in-house staff, determine who will be responsible for what to avoid finger pointing if something should go wrong. You will be dependent on these people, and they will know what the weaknesses are in your business. Do everything you can to establish a trust with them. Try to find a provider that "fits" with your business, and will work with the specific issues of your company, instead of treating you like just another client.

Overall, for very small businesses, contracting out security services may be the best way to go, simply because you can't afford a full-time staff member with the knowledge and experience that you need to protect your business.

Conclusion

Applying information security practices in a small business setting is not easy. They have too much important information to be treated as a normal home Internet user, but they lack the resources of a larger company. The challenges of finding the time and money to purchase software and equipment, and having the experience to set everything up properly are difficult to overcome. By analyzing the risks to your company, and contracting help from the outside if needed, you can maintain a very secure environment to grow your business.

References:
1. Woody, Carol and Clinton, Larry Common Sense Guide to Cyber Security for Small Businesses, March 2004, http://www.isalliance.org/resources/papers/31665_ISA_Small%20Bus%20Guide%20_LO-RES_web.pdf

2. Granneman, Scott "Infected in Twenty Minutes", Security Focus, August 19 2004, http://www.securityfocus.com/columnists/262

3. Liston, Tom "Follow the Bouncing Malware", ISC Handlers' Diary, July 23 2004, http://isc.sans.org/diary.php?date=2004-07-23

4. Granneman, Scott "Fighting the army of byte-eating zombies", The Register, October 8, 2004, http://www.theregister.co.uk/2004/10/08/fueling_the_fire/

5. Thomson, Ian "Hackers strike at 'soft target' small firms", vnunet.com, November 15 2004, http://www.vnunet.com/news/1159408

6. Sturgeon, Will "Security: It's 'wise up' or 'sack all your staff' time", Silicon.com, August 9, 2004, http://software.silicon.com/security/0,39024655,39123001,00.htm

7. Paul, Brooke "Risk-Assessment Strategies", Network Computing, October 30, 2000, http://www.networkcomputing.com/1121/1121f3.html

8. NIST Computer Security Resource Center "Awareness Materials/Activities", Last updated December 22, 2004, http://csrc.nist.gov/ATE/materials.html#web

9. Zhen, Jian "The pros and cons of MSSPs Part 1: 10 reasons to outsource security", Computerworld, December 9, 2004, http://www.computerworld.com/securitytopics/security/story/0,10801,98093,00.html

10. Zhen, Jian "MSSPs Part 2: Reasons to be wary", Computerworld, December 9, 2004, http://www.computerworld.com/securitytopics/security/story/0,10801,98114,00.html

11. Kotadia, Munir "Nokia: Bluetooth flaw gnaws at phone security", ZDNet UK, February 10, 2004, http://www.zdnet.com.au/news/security/0,2000061744,39116044,00.htm

12. Ossmann, Michael "WEP: Dead Again, Part 1", SecurityFocus, December 14, 2004, http://www.securityfocus.com/infocus/1814

13. Poulsen, Kevin "Guilty plea in Kinko's keystroke caper", The Register, July 19, 2003, http://www.theregister.co.uk/2003/07/19/guilty_plea_in_kinkos_keystroke/

14. Belani, Rohyt and Mookhey, K. K. "Penetration Testing IPsec VPNs", SecurityFocus, February 9, 2005, http://www.securityfocus.com/infocus/1821

15. Gartenberg, Michael "How Much Is Your Data Worth?", Computerworld, September 22, 2003, http://www.computerworld.com/securitytopics/security/story/0,10801,85135,00.html

16. Haskin, David "HotSpotVPN Provides Easy, Inexpensive Hotspot Security", InternetWeek, March 11, 2004, http://www.internetweek.com/breakingNews/showArticle.jhtml?articleID=18312072

Last Updated: May 26th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event