Global Information Assurance Certification Paper

Security for non-profits, very small businesses, and home
Let's bring folks into the new millenium.

Glenn Wittenberg

May 02, 2002 GSEC Practical 1.4 (Amended April 8, 2002) Option 2

Abstract:
The computer industry has changed a great deal in 20 years and we have far more security risks than when it began. People generally are not aware of all of these changes.
We are going to take a look at case studies which involve a non profit, a very small "mom and pop" business and a home user. We are then going to tie together the common points of vulnerability and see what we can do about it. The main problems that arise for these people take the the form of viruses and hacking via the internet. There is the occasional vector which involves the floppy, zip or a cd someone burned, but the majority of difficulties arise from the internet. The two biggest problems are security in the operating system and education. PC and Operating system manufacturers spend $0.00 on security unless required(1) and less on education of the end users since there is no money in it. Third party manufacturers provide products to augment the operating system security, but unless virus protection, firewalls and daily maintenance are turn-key and self maintaining, it is difficult for many people to know what to do let alone make a plan of action without education. As IT professionals, it is our job to assist and and educate endusers so we can strengthen indirectly our company security perimeters. .

Background:
Before we look at our case studies let's get a little background. When I started on computers in 1982, the disk operating system was just starting up whether it was CPM or DOS or ATARIDOS or BASIC. The internet as we know it today was not available. PC systems were expensive ($6000-7000) and couldn't do much. We watched a gamut of processors and programs go by until the day of the RBBS's. (Remote Bulletin Board Services) Our town had 12 to 14 of them at any one time. Many of us downloaded a ton of programs. Ours had fairly good operators and we did not have a major virus problem although there were a few viruses being circulated around. All of us geeks had virus checkers at home but no internet and very few infection vectors. As time went by the Internet started to come into home usage and the RBBS's faded away. When I obtained service through a local dialup ISP in the middle of 1996 you could get Windows 3.11 or Windows 95 software. We really had no major security issues at that time that I remember. At work we had viruses come in on diskettes but very seldom through the internet. Things took a major jump in 1999 as Melissa and other virus/worms made use of the Outlook and Outlook Express address book to propagate.(2) It's interesting to note that Outlook 97 did not support visual basic scripting in email, but the later versions 98, Express5 and 2000 do.(3) Now the default settings of new machines for the visual basic and active x control support for the email browser and the operating system security holes which need patching have produced major security problems we did not have before.(3) We also have many more viruses than in the days of the RBBS's because of the pervasiveness and accessability of the Internet.
However - the same people that started with PC's years ago and had no problems with viruses and security are junking the old machines and are getting newer ones and internet access. At some point the law of averages catches up with them when they least expect it.

Case Histories:
I.)Our first case deals with a non profit. Here you have no IT budget and no security. There is no virus protection, no firewall, no maintenance program, limited backup, and no training.

When you land in the middle of a virus problem, you have to act quickly and minimize the bleeding, because this group of people has few resources to expend in remedial and preventative maintenance. There is little risk assessment here because you know its already past that. Risk assessment will come later when the system is up and running again.

My wife had checked email and noted that we had received an email from pastor - at our church. The virus checker had detected something - I checked the log and determined that it was magistr A . It was late in the evening so I called the church in the morning. They asked me if I could come over and help because they were having problems with their network and they couldn't get any work done.

I arrived about 11:00 and started to evaluate the network. I already knew that magistr A was loose so I disconnected the network from the router. I still needed to determine the state of the whole network. By checking each machine I was able to determine that they had done something which is not uncommon when you have no IT staff. You have machines with antivirus programs on them but let the program updates lapse after a year because it really hasn't seemed to be of much use - so why spend the money?. Then over a period of six or eight months, the network becomes infested and you don't know you have a serious problem until the whole works crashes because of the straw that broke the camel's back - the last nasty virus.

I determined immediately that they were using a shared drive from a central machine in a star configuration peer to peer network - which was the secretary's machine. Knowing this, I disconnected the machines from each other so we couldn't get cross contamination from the viruses. Using F-PROT for dos, I did a rough disinfect starting with that unit booting from a floppy so we had no locked files from windows being active. On the shared drive alone I found magistr A, magistr B, badtrans A and B, and sircam. I had a sircam fix from Symantec(4) , so I ran that. Then I booted Norton Antivirus from Cd and cleaned things up the rest of the way. They were fortunate because magistr B hadn't moved out from the temporary files yet. I also ran Norton Windoctor and defragged the drives because this hadn't ever been done.

I also had to replace a fan in the secretary's server and remount the heat sink with new compound and clips to bring that machine up to decent operating conditions.

I then evaluated each machine in terms of hardware capability and then decided what to use for a virus checker once everything was disinfected. Most of these machines would not last long in the big business world and not at all in the gaming world. The gamit spread from a Pll- 300 down to a 486-25 running windows 98 plain on 8mb of memory!

The next step was to do a windows update on each machine to plug what security issues we could in windows. This included disabling VBS and VBS host scripting. (5)(6) There was a total of eight machines.
After evaluating antivirus programs from Macafee, Symantec and Trend Micro, I decided that the checker for the job was PC-Cillin 2000. PC-Cillin had the smallest footprint with reasonable features- which is what was needed for these machines with limited resources. After disinfecting the pastor's machine and the secretary's first, and then in order, the other machines, and making sure that the network and all of the zip backups were clean, (which they weren't) - we had a level playing field to start from. I then started to install virus protection on all of the machines, starting with the pastor's and the secretary's and then going on to all of the rest.

Considering we had limited hardware resources available, I went through with msconfig (7) on each machine to minimize the programs loaded at startup. I then installed the virus protection in the most economical manner to make the best use of the resources. I did not activate all modules - ie; realtime file protection, web trap -browser and, pop3 email protection, because some of the machines didn't have the resources to run all modules. Realtime file protection was a minimum with pop3 next for email protection.

One of the machines would not install the virus protection as it took the swap file 5 minutes to swap things out so it could load on startup and then you couldn't run anything. I uninstalled the program and then left the machine as it was for good reason. I was able to ascertain that the machine was to be replaced in 2 months.

When I finished with the machines at 2 am, I felt that we could connect back up to the router.
PC Cillin 2000 was set up to do a manual update. I left instructions on how to subscribe to the manufacturer to receive information on updates. I did this because I needed to determine when people came to work and turned their machines on and when they left and turned their machines off. I would at a later date set up the machines to do an auto update on a staggered basis to conserve bandwidth usage during the day on their DSL line.

The next day I got in touch with one of the other computer professionals in our congregation and we talked about and got the word out to the rest of the congregation to set up a meeting of all the computer geeks to determine a plan of action to build and maintain an IT pool for this facility.

We met that following saturday and looked at the existing hardware, software, and network resources to determine what we could do for security and maintenance with what we had. We then looked at what needed to be done to the existing hardware and software resources to improve security for the future. The offices were being remodeled and we were able to lay out the best networking model for the facility and juggle the resources around to advantage for security and maintenance.

We took our recommendations to the church board and they approved most of them. When you show people the “smoking gun” they can see the advantages of being secure. We put a switch in by the router instead of a hub because of the enhanced security aspects of a switch. We set up the filtering on the router as tight as we could get it and made sure that the NAT was working since we don't have a true firewall, just the NAT router and limited filtering from our ISP. This is a compromise, but none of the machines has the resources to run virus protection and personal firewall and applications at the same time.

Upgrading the machines is next with a dedicated server and a real firewall. This will happen within the next 6 months to a year depending on cash flow. .

Lastly we listed our abilities and qualifications to build an IT profile and a call back list for solving security issues and performing corrective and preventive maintenance. We have a nucleus of 5 people that can make all the difference in the world by being there at the right time. We are putting into place training for the end users and have already begin to train the individuals at the facility in key security and maintenance issues to make things go. We will continue to monitor and evaluate and implement security as an ongoing task.

So, we went from no security, no budget, no virus protection, no firewall, no maintenance, and no training To better security, limited budget, virus protection, partial firewall, scheduled maintenance, and training as needed.

Three months have gone by and we have not had an adverse incident. This is no guarantee but at least we are partially stemming the flood. The bottom line here with a limited budget and old hardware is not whether you can make the facility air tight, but what can you do to make it workable with the resources you have.

I base this on 25 years of troubleshooting electronics in the field, tied in with what I have learned from our basic security course.
This is what I did:

1.Handle an incident in a timely manner; “limit the bleeding”
2.Evaluate
3.Troubleshoot
4.Fix
5.Institute new security plan based on 2.
6.Monitor
7.Re-evaluate

The day I was working on evaluating the network and getting things to go I sketched out an outline to evaluate the system so I could decide what to do;

Non profit, outline for evaluating the system.
1. What kind of hardware infrastructure is there

A. What kind of server?
    1.Full Server
    `
        a. Operating system
            1. Security patches in place?
    2. Common machine with shared drives
        a. Operating system
            1. Windows update - security patches in place?
            2. VBS and VBS host scripting disabled?
    3. Simple peer to peer no server
        a. Operating system
            1. Windows update - security patches in place?
            2. VBS and VBS host scripting disabled?

B. What kind of router
    1. NAT and Filtering
    2. Plain router with a hub built in
    3. No router - dial up ISP

C. What kind of firewall
    1. Dedicated machine with software firewall
    2. Hardware firebox
    3. No firewall

D. How many workstations?
    1. Total number
    2. Processors
    3. Memory
    4. Operating systems
        a: Windows update - security patches in place?
        b: VBS and VBS host scripting disabled?

2. What kind of software infrastructure is there?

A. What applications are being run - including internet browser and email program?
    1. What known vulnerabilities do they have?
    2. What patches have been made - and are they current?

B. Virus protection
    1. If there is a server, is there incoming and outgoing virus protection?
        a. What does it check?
        b. Is it current?
    2. What virus protection is installed on workstations?
        a. Is there realtime file protection?
        b. Is there email protection for your email browser?
        c. Is there web protection for your internet browser?
    3. How current is it on both?

C. Firewall
    1. Do the workstations have personal firewalls on them?
    2. How current are they?

3. What is the security education level of the personnel working here.

A. What do they know about virus protection?
B. What do they know about firewalls?
C. What do they know about handling email and internet browsing?

4. How much budget is available for use for security?
5. What manpower resources are available to implement this security?
6. Based on the above information, what is the risk assessment of this facility?

7. Based on the above information, what can be done to improve security for the facility?

This is continuing process as our security which is adequate now will not be in the future.

II.) The next case study involves a very small business - a "mom and pop" setup. Small businesses with 3 or 4 employees generally have no IT or security. The owners typically have a PC which they have an IP provider to do online stuff and run the proprietary programs related to their field - in this case shoe sizing and database programs. They swap mail and files between there and home.They have no clue as to viruses, hacking or anything of the sort. The internet is a big wonderful place with all kinds of goodies.
They need protection and a plan in place.

I received an email from the our shoe proprietor, and our email protection picked it up right away as Magistr.B.
I called him up in the morning and noted that he probably had a virus. He said that his antivirus program hadn't found anything but I could check if I wanted to. I arrived there about 11:30 armed with CD's and floppies and determined right away that this was not going to be a push over.

This machine was severely infected. I found 25 magistr viruses among the files that weren't locked and 10 more among the files that were locked. I then ran FPROT from a boot floppy to catch some of the others. When I was done with that I ran Norton Antivirus from a CD.
When the machine was finally cleaned up, I did a windows update (security and operating system updates from microsoft; www.windowsupdate.microsoft.com) and installed a new virus checker. Remember the first case scenario where the virus checker updates had expired. Bingo! Same thing here.

Again, I used PC -Cillin 2000 as he only had 64mb of ram under windows ME. I recommended a memory upgrade to at least 192mb and this was done the next week.

Although he only had a dialup connection, it was still time for some education. I gave him some history and showed how things had changed in almost 20 years. I set the virus checker up for manual update so whenever he was out to the internet checking email, he could check on updates. I also showed him how to subscribe to a manufacturer's web site and get notices as to when a new virus and signature updates came out.

I then told him about how the TCP-IP works and the need for a firewall to shut off the rest of the unused 65000 ports since we only use some of them do - ie; port 80 for browsing 25 for mail 443 for ssl, etc.(8) We went out to www.zonelabs.com and got zonealarm and installed and configured it for his particular business.(9) We checked that with the "Shields Up" utility at www.grc.com.(10) We held an impromptu class on security. It was not a very busy day for him and I tried to fill him in on a little history and simple things he could do to make his internet and local security better. We disabled visual basic and visual basic scripting. (4) (5). I also covered any disks, cd's or zips he might bring before he used the and provided him with information on weekly maintenance procedures which would keep windows happy.

We downloaded ad-aware 5.2 (available from www.lavasoftusa.com freeware) and ran that only to find 25 pieces of spyware that were infesting the cookies and temp files and of course the registry so they could run resident. . We soon got rid of these resource suckers. Although these are not direct security leaks, they allow certain internet entities to build a user profile to target you with emails and product info by sending back info to the "home site" when you are on the internet. (11) (12) I have seen machines with 25 - 30 of them act slow and strangely on the internet because of the fight between the spyware for resources. Before you check your machine with ad-aware press CTRL ALT DEL and look at the dialog box that shows running programs , you will see that none of the spyware shows up in the program listings.

One thing I recommended for his business which I have recommended for others. When you have your entire business on one computer, it is a good idea to keep it secure and off the internet. It is easy and cheap insurance to buy a machine just for email and internet and keep the two separate. That way you cannot compromise your business machine.

So we went from no security, no virus protection, no budget, no training, no firewall, no hope to better security, virus protection, limited budget, training, firewall, and confidence that this battle could be won on a continual basis.

Here is the outline I drew up for his system;
Very small business, outline for evaluating the system;

1. What kind of hardware infrastructure is there?
    - A. How many workstations are there?
    - B. Are they networked at all?
        1. Are there shared drives?
    - C. Operating system
        1. Windows update - security patches in place?
        2. VBS and VBS host scripting disabled?
2. ISP provider;
    - A. Do you have a DSL line?
    - B. Do you have a cable modem?
    - C. Is it through a dial up connection?
3. What kind of software infrastructure is there?
    - A. What applications are being run- including internet browser and email

program?

1. What known vulnerabilities do they have?
2. What patches have been made - are they current?

B. What kind of virus protection is installed on the workstation(s)?

1. Is there realtime file protection?
2. Is there email protection for your email browser?
3. Is there web protection for your internet browser?

C. Firewall

1. Do(es) the workstation(s) have personal firewalls on them?
2. How current are they?

4. What is the security education level of the personnel working there?
   A. Do they know about virus protection?
   B. What do they know about firewalls?
   C. What do they know about handling email and internet browsing?
5. Is there any budget available for security?
6. Based on the above information, what is the risk assessment of this business?
7. Based on the above information, what can be done to improve the security of this facility?

III.) The third case involves a home machine, and not even the primary machine. Since this machine was not the primary machine the users were even less aware than the primary home users that they had any probllems. This machine I took home and set up in my shop since I was not under major time constraints.
This machine was badly infected and would come to the Windows 98 logo screen and hang. I booted from a floppy and ran F-prot for dos. I discovered 2 boot sector viruses (anticmos A&B)(These are left over from the dos days and why they didn't wipe out the CMOS early on I don't know) and two others starting from the registry at startup (badtrans A, magistr B) which had infected Explorer and Kernel32.dll. After disinfecting these with FPROT for dos and running a full scan in dos, I then booted from a CD with Norton Antivirus and found between them all about 30 files infected. Some of these could not be disinfected and had to be replaced.

In the end, although the machine would boot and run, it ran poorly simply due to no maintenance and I found it was faster to save the data and document files, wipe the hard drive with a low level format and then reinstall the operating system and application programs. Fortunately, I was able to save the data, document files, bookmarks, etc. When I was done I installed Macafee VirusScan (their choice)(it had no virus protection before) and Zonealarm personal firewall and did some simple educating to try to keep this from happening again.

So again, we went from no security, no virus protection, no firewall, and no training to better security, virus protection, a firewall and education.
This is what I used for the system;

Home outline for evaluating the system;
1. What kind of hardware infrastructure is there?

A. Is there a home network?
    1. What kind of router are you using?
    2. Is there a cable modem?
    3. Is there a DSL line?
B. Are there several standalone workstations?
    1. Operating system
        A. Windows update- security patches in place?
        B. VBS and VBS host scripting disabled?

2. What kind of software infrastructure is there?
    A. What applications are being run - including internet browser and email programs?
        1. What known vulnerabilities do they have?
        2. What patches have been made - and are they current?
    B. Virus protection
        1. Is there realtime file protection?
        2. Is there email protection for your email browser?
    C. Firewall
        1. Do the workstations have personal firewalls on them?
        2. How current are they?
3. Based on the above information, what is the risk assessment of this system?
4. Based on the above information, what can be done to improve security for this system?

Conclusions:

So what do these three cases have in common and what does this have to do with me and my business? After all, these guys can take care of themselves. If these guys could take care of themselves at the onset, there would be no need to help.

What they have to do with business, is that indirectly they are part of the perimeter defenses in a loose sense.

For example, how many of you have email from work forwarded to your home for your perusal? And how many of you have your work email address in more than one place? It not uncommon for educators and business people to do this. Mail can go both ways. How many times have you seen people bring in files they downloaded from the internet at home for their work machine? Or files given to them by associates with product information or research data? All of these items need to be protected against. So often the perimeter defense begins at home.

What these three had in common is easy to list. All three had no security and no plan. All three had no working virus protection, no firewall, no budget, and no training. Why and how could this happen? It isn't that these people don't care, it's that they don't know. Read on.

Having worked with PC's since 1983 I have seen what people's mindset is. You can see this from the background paragraph. People have a tendency to treat computers like any other "hard good". When a refrigerator goes bad you replace it. When the car breaks you fix it. But if your refrigerator has a broken shelf which doesn't interfere with its overall functuality, you leave it. If your car has a few quirks but it still goes, you ignore it. When

your computer isn't quite right you use it till it won't boot, and then you call support.

Before our training program was in place at work one fellow called me last year only when he had been notified by associates that he was sending viruses. I asked him if he had virus protection, and he said he had. I didn't ask when it had been updated, but proceeded to check out his machine - only to find 73 viruses of various types. Had he not been notified by his associates, he would not have done anything although the machine was running slower than usual.

When you maintain your car, it is easy to check the oil and antifreeze and air pressure. It is also easy to see how much tread is left on the tires, and replace them when needed to maintain that cushion of safety. Unfortunately, people hardly ever check their virtual tires, aka virus protection, and then don't understand when they stop with a machine that can no longer go. In the same way, people buy bug deflectors for their vehicles to keep the bugs off the windshield, but they hardly ever install firewalls on their computers to keep the hackers off.

In case 1.) with the non profit - I worked on the network when it would no longer function
This did not happen in case 2.) but would have had time gone on. The businessman bought the computer system I worked on after his old one died. He didn't know till later, that a series of viruses had caused its demise.
In case 3.), the same thing happened.
No one recognized the warning signs that could have saved them a great deal of grief had they dealt with things before everything ground to a halt.
That's why viruses like Klez-H which is a variant of the original Klez can make produce 20,000 incidents in a little over a week on machines that should be safe and secure, but apparently aren't patched and/or aren't protected.(13)

At work we consider the network and internet like a utility - you turn on a switch, you plug into the wall, and you use it. When it doesn't work you call someone to fix it.

The power company sends out information to the consumer and labels underground wiring with "BEFORE DIGGING CALL -- " - because they can be held responsible if anything happens.
But you won't see a sign on a PC saying; "CHECK YOUR OPERATING SYSTEM BEFORE GOING ON THE INTERNET" because there is no accountability. If you read the EULA you will find out that there is generally no liability.

Solutions:
So what can I do as an IT professional to help this?

First, start in the work place and use information you have gathered from the basic security course - with permission of course, and use your own life experiences and those of others (real stuff - no urban legends) and references and materials used to write this practical and present it as workplace security that has relevance in other venues -

especially the home. Try to break the mindset and complacency by giving them history and then by showing how things have changed in computer security drastically over the past several years.

When people are used to taking care of their workstations and have security standards in place at work, they will begin thinking about home - if you show them the connections between work and home. When people know what they are up against now and how little it costs to have protection, it will be much easier to open the checkbook at home and do what needs to be done.

Secondly, if you belong to a service organization, or you are part of a non profit or are involved in public service, you can bet that most of these places have computer systems and probably little support. As part of your service, you can pitch in and organize support like I did so these folks can continue to do their job in a timely fashion.

Thirdly, you can help business associates and neighbors when they run into trouble with viruses and hacking. I am putting a sheet together listing inexpensive virus checkers, firewalls, and ad-busters with the pros and cons and basic "how - tos". Many people before me have done the same thing. I believe we need to use the resources available and tailor the education for our particular locale.

The more holes we can plug through education and a little hardware and software and a few techniques - the less machines viruses and hackers will have to play with. That will make a difference. Sometimes I don't have time to help everyone and I can't take on the world.
However, I can make a difference.

Reference Resources;

1. Livingston, Brian "Feel more secure yet?" April 29, 2002.

   URL:http:www1.infoworld.com/articles/op/xml/02/04/29/020429opwinman.xml.

   (4/29/2002)
2. No Author listed. "Virus History" Cknow.com. URL:
   http://cknow.com/vtutor/vthistory.htm (5/01/2002)
3. Woody Thrower, Stan Burnett, and Gary Wahlquist "Prevent E-Mail Worms" May 12, 2000.
   URL:http://securityresponse.symantec.com/avcenter/security/Content/2000 05 12.html. (4/25/2002)
4. Symantec. "W32.Sircam.Worm@mm Removal Tool" URL:

   http://securityresponse.symantec.com/avcenter/venc/data/w32.sircam.worm@mm.

   removal.tool.html
5. No Author listed " Safe Computing Guide" subparagraph "Disable the

Windows Scripting Host Functionality"
URL:http://www.antivirus.com/vinfo/safe computing/
(4/28/2002)
6. No Author listed "Disable Windows Scripting Host" May 12,2000.

URL:http://securityresponse.symantec.com/avcenter/security/Content/2000 05 12 ivdWSH.html (4/25/2002)
7. No Author listed. "How to troubleshoot using the msconfig utility with Windows98(q281965)"
URL:http://support.microsoft.com/default.aspx?scid=kb;EN-US;q281965 (1/09/2002)
8. No Author listed "portref.zip" full port list with references URL: http://www.wilders.org/download.htm(11/06/2001)
9. Zonelabs. "Zonealarm Pro User Manual PDF" URL: http://www.zonelabs/pdf/zap_manual.pdf (11/06/2001)
10. Gibson Research Corporation. "Shields Up" URL:https://grc.comx/ne.dll?bh0bkxd2
11. No Author listed "Lavasoft FAQ" URL: http://www.lavasoft.nu/faq.html (11/06/2001)
12. Bob Brand "Spyware" URL: http://www.thebee.com/bweb/iinfo200.htm (11/06/2001)
13 Robert Lemos " 'Klez' viaiant strikes unprotected PC users" April 28, 2002. URL: http://zdnet.com.com/2100-1105-891218.html. (5/01/2002)

Last Updated: July 26th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event