Global Information Assurance Certification Paper

Improving Risk Estimation Accuracy

Lawrence W. Brennan
GSEC 1.3

Abstract
The traditional definition of risk is that risk is the product of threat and vulnerability. This model of risk is appropriate for assets where applicable threat data can be well predicted from historical events. There is a lack of intelligence information available to help us identify risks. In Information Technology and in critical systems, threat changes from day to day, even moment to moment. Historical data is not a valid indicator of our current state of threat in these areas. Threats previously unidentified are just some of the threats we cannot account for in the traditional risk models. In this paper, I present a risk model that offers better prioritization for what assets to protect and a better understanding of system interdependencies. There are not enough personnel, time and money to protect all of our assets, so we need a methodology to help us make decisions for what to protect. In this paper, I propose a model for determining what IS critical to your IT and critical systems, and a methodology for prioritizing protective measures.

Body
For years, authors, speakers and other pundits have extolled the virtuous formula that risk is the product of threat and vulnerability. Another way to represent this is:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability}$$
Or
$$R=(T)\,(V)^{i}$$

This model of risk assumes that we have knowledge of our vulnerabilities and our threats. Everyday, new vulnerabilities to systems come across my desk in the form of emails from a variety of reputable sources. With each newly identified vulnerability, there are people out there writing malicious code to exploit those vulnerabilities, and those who have not patched their systems. R=(T) (V) also assumes that we will have knowledge of threat. Again, historical data alone will not suffice, as threats are erratic. We need a better method of determining our risk because of the ever-changing landscape on the digital battlefield.

Traditional risk model analysis:
The Single Loss Expectancy (SLE) model is the simplest of the risk assessment models. When this model is applied to a particular asset, it yields a dollar amount that indicates the value lost if this asset were to be destroyed. It is obvious that the roots of this model stem from the accounting field. The SLE is the sort of valuation that a firms accounting department would want to create to help determine asset valuation during the annual audit for example. The concept of

risk is expressed in terms of the value of property would be lost if something tragic were to happen involving this asset.

This model of risk falls dreadfully short accurately describing risk. This model is used to express the results in a financial impact analysis[ii]. The type of losses illustrated using this method are massive catastrophic losses. Threat is typically defined as an event such as a flood, tornado, computer virus outbreak, those kinds of low probability events yet highly damaging that really catches your attention. The chance of the event occurring is a probability that the event has happened, in other words, the sky has fallen and here's the result. There is no time constraint. The event will likely happen over some defined period of time. There exists a probability that describes the frequency of such an event, or the likelihood that the event will occur. The vulnerability is usually defined as a weakness that is exploited in some very negative way by the threat. Here is an example:

> You have a server that runs the order processing database center for your firm. The value of the order processing server, including the data is $1 million dollars. If the building that houses the data center processing system was flooded, you could lose $1 million worth of software and hardware. Since we are looking at this in terms of "after the fact," the event has already happened, at least in the hypothetical example we are portraying. Thus, the probability of this event is 100%, since it has already happened. The formula looks like this:
>
> (Value of the lost asset) (probability) = SLE
> ($1,000,000) (100%) = $1,000,000

As a method for determining what to protect and when, this model is insufficient. As a method for raising awareness of the value of an overlooked system, this method has some merit. As a tool for determining the value of a system, this model attempts to provide a dollar amount, but there is no attempt at valuing the interdependencies that would be adversely impacted across the enterprise if the order processing database center were not functioning. For example, if your ordering system were not functioning, one would expect that many other systems that depended on that system functioning would sit idle. The simplicity of this model is the main detractor from being recommended for wide use. The role this model plays is

The Annualized Loss Expectancy Model[iii] (ALE) of risk comes closer to painting an accurate picture of risk, by adding the probability of an event happening over a single year's time. The ALE is still rooted in the same quagmire of inefficacy as is the SLE for many of the same reasons. Again, we are looking merely at the financial value of the asset. This limited view of risk is made only a little better by

addressing the probability of a particular catastrophic event in terms of how likely is this catastrophe to happen over a year. First, we need to calculate the Single Loss Expectancy to determine this value. Then we obtain the product of the Single Loss Expectancy and the value of the asset to produce the Annualized Loss Expectancy. The formula looks like this:

Single Loss Expectancy	x	Annualized Rate of Occurrence	=	Annualized Loss Expectancy

Or

(SLE)(ARO) = ALE

Looking back at the order processing database center, we can say that it floods on the piece of land occupied by the order processing database center once every 10 years. If no mitigation steps were taken to reduce the risk of a flood, then the loss expected from a flood at this facility is $1,000,000. The total loss of the order processing database center, and the probability each year of a flood is one out of 10, or 10%. It would look like this:

($1,000,000 (100%)) (10%) = ALE

Or

($1,000,000(1.0)) (.1) = ALE

This tells us is there is a chance of the event happening, so we have a predictive element that the Single Loss Expectancy model lacks. The threat data is in the form of the probability of a flood occurring, which is about once in ten years. The downfall of this model is that the threat information is entirely based on historical data. This model does not account for changes in threat. In this case, threat could be changed by events beyond your control, such as the installation of a flow regulating just upstream of your facility, thus reducing the threat of a flood occurring. Conversely, if for miles upstream of the facility, levies were constructed, then the flood waters would have nowhere to dissipate, and consequently, have a greater impact on your property in terms of flood severity, duration and in frequency[iv]. So, threat can increase or decrease, and this model has no way of taking this into account, we are dependent upon historical data, leaving quite a bit to be desired as a determination of risk.[v]

The Cumulative Loss Model[vi] (CLE) approaches risk from the standpoint of a single system. It takes into account all of the bad things that are likely to happen to this system over the next year. Going back to the order processing database center illustration again, you would look at each threat, the probability of each threat against this asset, and then derive an expected loss. We would look at our order processing database center, and look at all of the threats to this center that we have seen over the past several years. Examples include floods, tornadoes, and malicious code outbreak, sabotage and back up failure. We can then take all of the threats, and compute the annual rate of each threat occurring. The formula would look a lot like this:

(Probability of flood) + (probability of tornado) + (probability of computer virus) + (probability of sabotage) + (probability of back up failure) (value of order processing database center) = Cumulative loss

Or

(.1) + (.05) + (.136) + (.11) + (.03) ($1,000,000) = $426,000

This demonstrates the total amount of threat that we can predict from historical data. The risk is certainly more accurate than either of the previous models. It builds upon each improvement in an attempt to better quantify risk, but the weakness is still the model's reliance upon historical data.

Each of the preceding models is merely an enhancement on the previous model, and in effect, is just more of the same. In each of the above models, there is an assumption that we will know the threat is coming, we know the frequency of the threat and we can quantify this threat. We cannot be sure that there exists a threat at any given moment, but we can determine how important our assets are critical business functions. Instead of squandering our time discerning the likelihood of a threat, we need to come at this problem from another direction. We need to determine how critical a system is to your operations, and from there make decisions on what to protect, what to mitigate, and where to accept risk. The Iowa Risk Model© I propose is a radical departure from the Loss Expectancy based models.

The Iowa Risk Model©

The Iowa Risk Model©[vii] is superior to all of the previous risk models because we do not chase the elusive threat variable. Instead, we look at systems, and how dependent we are upon these systems. We also view systems, assets and resources as services. I will explain the service concept later. There are two immediate variables involved in determining risk; criticality and vulnerability.

Webster's Dictionary Online defines criticality as "the quality, state, or degree of being of the highest importance."[viii] Essentially, criticality is how dependant you are upon a given system or service or what kind of hardship would you experience if that system or service was not functioning. Systems and services can have varying degrees of criticality, because criticality is a continuous variable. Criticality is relatively static. Depending on the time, certain systems can be more critical than others. For example, systems controlling and contributing to the Tropical Prediction Center (TPC) in Florida is much more critical during the hurricane season than in December. To account for this, we need to average the criticality across the year and assign that asset the averaged criticality value. Averaging works well for assts such as the TPC, but not so well for college stadiums. Jack Trice Stadium in Ames Iowa will have a large attendance every other Saturday during football season, but for the rest of the year, go largely unused. If we were to assign an average based on attendance over time, that score would be inaccurate. Likewise, if you had an IT system that was used only

occasionally, but was very important at those times when it was used, this (Use / Time) approach would not bestow an accurate value. This is an example where risk assessment requires artistry in addition to the mathematics.

The probability that any two systems or services having the exact same criticality is minutely small. In fact, as a property of a continuous variable, the probability of any two systems having the exact same criticality is (1 - Infinity), since there are an infinite number of points between any two integers. This becomes fairly important as we set out to compare which systems are more important than others. Occasionally have to decide between two systems that appear to be equal in importance. Breaking this tie is a decision usually reserved for senior management. If there is not a process in place to deal with ties, then it comes down to who is stronger at the table. Needless to say, it is a good idea to have a process in place for breaking ties.

Vulnerability is defined as how susceptible a particular system or service is to disruption. Vulnerability is the second factor in determining risk. By looking at both criticality and vulnerability can we get an accurate sense of our risk, and to help us decide how we are going to deal with the risk.

One feature that makes the Iowa Risk Model© a major departure from the traditional models of risk, is that we view each asset in terms of services. What is important about each asset is not that it exists, not that it has value in the accountant's ledger, but that it DOES something that we want it to do. The thing that the asset does is what determines its value, our dependency on that asset and the role it plays in the service it provides. We can say that any asset can be accurately evaluated by the service it provides. By definition, every asset plays a role in providing some service that we value, or it is not an asset. For example, an electrical substation has value not necessarily because it is a series of step-down transformers, wires and other transmission equipment. It has value because of the thing it does, which is playing a role in delivering electricity to a community. The same can be said of a fire station. It has value because it provides a service that we rely upon. We hopefully do not call upon firefighters frequently, but when you do call upon them, you sure want that service to be there!

When evaluating an asset's criticality, we have to ask three questions:

1. What does this thing do and what service does this asset provide?
2. What other services does this asset depend upon to do this thing that it does?
3. What other services and processes depends on the thing that this asset does?

These three questions begin our process for determining the criticality of a particular asset and determining interdependencies, thus demonstrating more accurately our risk assessment. What does an asset do? A majority of the assets that we have examined in Iowa depend upon services rendered from another asset and service. John Donne in Devotions Upon Emergent Occasions wrote that " No man is an island, entire of itself; every man is a piece of the continent, a part of the main."[ix] Just as no man is an island, no service is an island. Every service depends upon inputs from other services and assets. By the same token, there are other services that depend upon the service produced by the asset you are evaluating, and those assets depend upon other services-the pattern is obvious.

When answering these three questions we have to understand the substitutability of the service that this asset provides. In other words, if this one service that we depend on is not available, what else can we use in its place? For example, Iowa is widely regarded as a food producing state.[x] If the State of Iowa stopped producing pork products, what will people eat in place of pork for meats? The obvious substitutes for pork would be chicken, beef and lamb. So we can say that pork production is a highly substitutable service. An example of a low substitutable service is petroleum fuels. If gasoline were no longer available in your area, you can't simply fill our vehicles with some other kind of fuel and expect them to run. Petroleum fuel production and distribution is a low substitutable service. If you know the answers to the substitutability questions, you will be well ahead of the curve in determining the criticality of an asset and the service it provides.

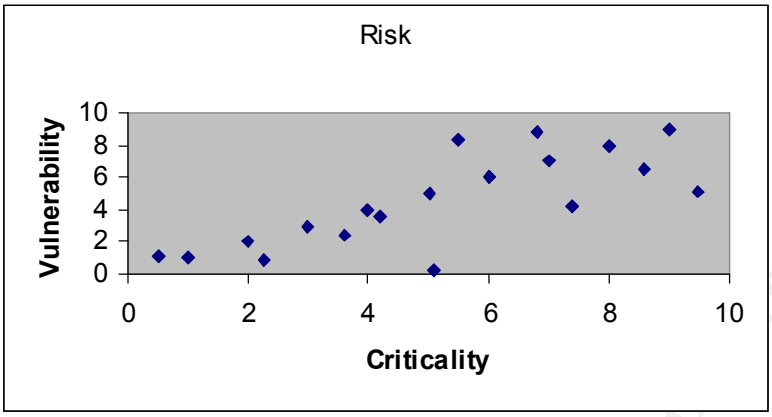
As stated earlier, vulnerability is how susceptibility a service is to disruption. To examine vulnerability, measures have to be developed that not only take into account what can immediately disrupt this service, and how easily can dependant services upon which you rely be disrupted. For example, a server farm relies heavily upon the flow of electricity. If that flow were to stop, the server farm will hopefully switch over to battery back up or an onsite generator. How easily can the electrical service be disrupted? Though I have discredited historical data as indicators of future occurrences of threat, vulnerability is one area where historical data can be a good indicator of the future.

We have created a list of measures for both criticality and vulnerability in Iowa. For each type of asset, you will have different types of factors that the feed into criticality and vulnerability. However, the more general factors of criticality consist of questions, such as how many processes depend upon this service, and how many people depend upon this service,

Visualizing Risk

We now have the criticality data and the vulnerability data for many of our assets, now what? We plot a scatter diagram with criticality on one axis and vulnerability

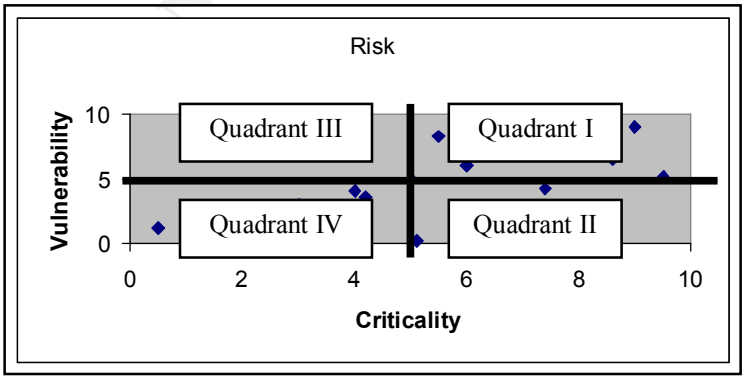
on the other axis. We refer to this as the Peters Function, named for Kenneth G Peters, Captain, United States Air Force and Chief Information Security Officer for Iowa State Government, and Dr. Justin Peters, Chairman, Iowa State University Mathematics Department. Both of these gentlemen created this concept separately and concurrently, so it is named after both men. Fortunately for us, they have the same last name. The scatter diagram looks like this:



The scale of one to ten is arbitrary, in order illustrate the Iowa Risk Model©. What we have is a scatter plot, where each asset lies in terms of its criticality and vulnerability. Each asset has a criticality and vulnerability score, and then plotted per those scores. The bottom left tends to be populated with assets that are neither particularly critical nor particularly vulnerable. The top right contains our assets that are very critical and very vulnerable.

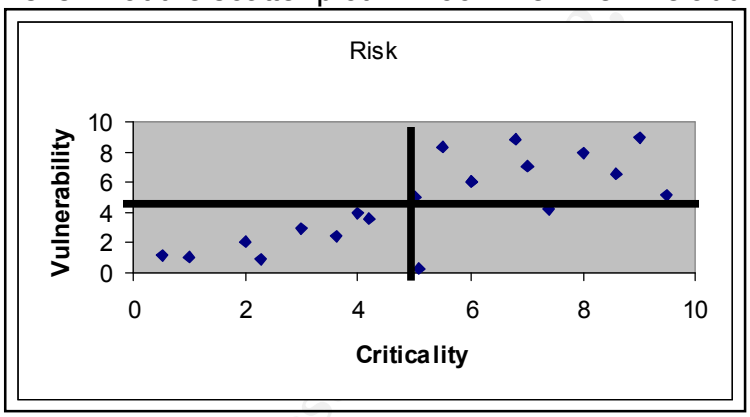
> One note worth making here, is that this does not account for assets where the vulnerability can be quickly, easily and inexpensively reduced, often referred to as low hanging fruit. Those sorts of changes should be done even though that asset may be low in both vulnerability and criticality.

In Iowa, we have divided the scatter plot into quadrants to help us better understand the criticality and vulnerability of each asset relative to other assets.



- Quadrant I contains highly critical and highly vulnerable assets. These are the ones that you really need to focus on, as they are very important and very susceptible to disruption. These are the assets the asset holder will undoubtedly spend a majority of their time combing over mitigation and risk acceptance studies.
- Quadrant II contains assets that are generally highly critical, but not very vulnerable. Action here is only necessary if you believe that you can further reduce the vulnerability.
- Quadrant III contains the assets that are of low critical and highly vulnerable. These assets are the kind of assets where you would typically address mitigation reports only if the costs are low, since these assets are not terribly critical.
- Quadrant IV contains assets that are neither particularly critical, nor particularly vulnerable. This is the last grouping of assets that will be addressed for mitigation and risk acceptance. Generally, assets in this group will be used as a reference point against which the other assets are compared. This is necessary to help round out the model.

This is what the scatter plot will look like when we add the quadrant lines.



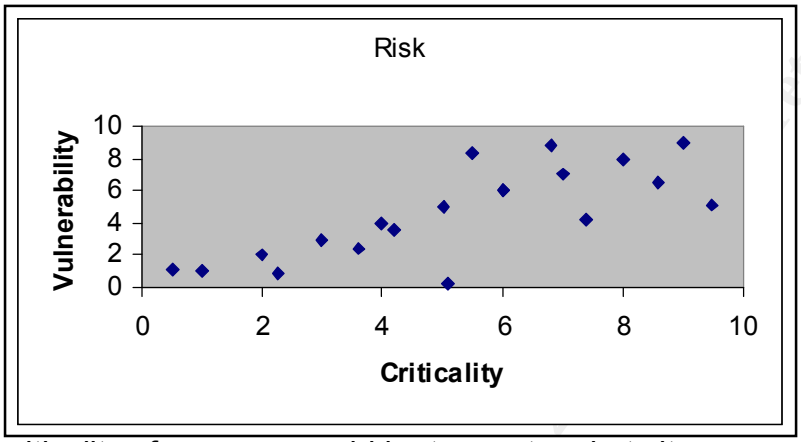
There is no hard and fast rule for where to place the lines. You can place them on statistically significant distribution points, but we haven't done that yet. Lines can be placed so as to have a list of top ten critical assets, or your top ten vulnerable assets. Senior management will generally make this decision. This is a tool to help you better understand your risk.

Changes in Criticality and Vulnerability

Vulnerability is probably the easiest factor to mitigate. For example, it is pretty easy to add concrete barriers to the entry of a facility, an identification card system for all you have access to the facility and video cameras and locks on doors. These are simple steps to take that can drastically reduce your vulnerability. As a result, we tend to say that vulnerability is more elastic[xi] than criticality. One problem that arises from reducing vulnerability is the concept of deflection. For example, that there is a small town with 10 houses. There have

been some burglaries lately, and some people want to reduce their vulnerability to being burglarized. Five of the homes add deadbolts to their doors, making it harder for criminals to gain entry into a home. This works well for those who have the dead bolts, but it is also likely to deflect those break-in attempts to the houses that have not reduced their vulnerability. Deflection is a problem one must consider carefully when choosing to mitigate vulnerability.

Criticality is more difficult to mitigate. The types of actions you can take to reduce criticality include redundancy and development of new systems. For this reason, we tend to say that criticality is less elastic, due to the difficulty of making changes to assets that can reduce criticality. An example of mitigating the



criticality of a server would be to create a hot site somewhere else. That server depends on electricity, so to mitigate the criticality of the electrical generation and transmission system; we implement auxiliary generation and interruptible power supplies.

Conclusion

Traditional assessment models fall short of accurately determine risk for critical systems and services. It is through determination of the service an asset provides and its criticality and vulnerability, that we have an accurate picture of risk. The Iowa Risk Model© provides such detailed and accurate information on criticality and vulnerability. With the Iowa Risk Model©, if you obtain threat information you can apply this model of risk, and decide which assets to protect, and which ones to accept the risk. There are not enough resources to protect everything all of the time, so we have to manage our risk. Part of this management is deciding which assets we will mitigate by reducing vulnerabilities, which assets will we reduce criticality, and which ones do we simply accept the risk, and move on. Other models of risk rely upon historical data for determining risk, and I believe that I have shown how this falls short of accurately estimating the risk to assets and systems. The Peters Function defines risk as the product of criticality and vulnerability. This model is a tool to aid in making those decisions. Though this model offers a convincing argument for determining which asset is most critical and vulnerable, the final decision on how to manage risk

resides with the decision makers. This model is merely one tool to aid in making decisions on which assets and systems to protect.

References

[i] Homeland Security Planning team, State of Iowa, October 2001. Critical Asset Assessment Model, unpublished.

[ii] Handbook of Information Security Management, Micki Krause and Harold F. Tipton http://www.detectiondesintrus.com/Documents/HISM/230-232.html

[iii] Handbook of Information Security Management, Micki Krause and Harold F. Tipton http://www.detectiondesintrus.com/Documents/HISM/230-232.html

[iv] University of Newcastle Department of Civil Engineering, Flood Risk Estimation course

http://www.ncl.ac.uk/hydroinformatics/profdev/pdn828.htm

[v] Federal Emergency Management Agency Risk Assessments http://www.fema.gov/mit/planning_toc3.htm

[vi] Handbook of Information Security Management, Micki Krause and Harold F. Tipton http://www.detectiondesintrus.com/Documents/HISM/230-232.html

[vii vii] Homeland Security Planning team, State of Iowa, October 2001. Critical Asset Assessment Model, unpublished. State of Iowa Homeland Security web site http://www.iowahomelandsecurity.org/security.htm and Iowa Homeland Security Critical Asset Protection Plan, Office of the Iowa Homeland Security Advisor, Emergency Management Division, Department of Public Defense, Unpublished

[viii] Webster's Online Dictionary http://www.dictionary.com/search?q=criticality

[ix] John Donne (1573-1631) *Devotions Upon Emergent Occasions,* 1624 http://www.incompetech.com/authors/donne/bell.html

[x] A Profile of Pork Production in Iowa http://www.extension.iastate.edu/ipic/reports/00swinereports/asl-671.pdf

[xi] Amos Web Economic GLOSS arama (sic)

http://amosweb.com/cgi-bin/gls_dsp.pl?term=elasticity

Security in Computing, Second Edition, Charles P. Pfleeger, Prentice Hall

Last Updated: May 29th, 2017

Upcoming Training

SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
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
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
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 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 Columbia, MD 2017	Columbia, MD	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 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
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
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 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