Global Information Assurance Certification Paper

2-11-02
James Gentile
GIAC – Security Essentials Certification v1.3

Disaster Recovery

Abstract

Disaster recovery is something that has once again gained the forefront of what people are focusing on of late. This paper will define some of the major reasons why it is essential for any company to have a plan of action in place, in writing, with executive management approval in case an unforeseeable event occurs. It will also delve into the topic of risk assessments, and recommend a disaster recovery plan for a fictitious production company.

Why Prepare for a Disaster Recovery

Disaster recovery's function, among others, is to coordinate and ensure the development of recovery plans (Business Resumption Plan, BRP) following a corporate model. Each critical business units also needs to have contingency plans for delivery of services during disaster events. The BRP will be the business unit's vehicle for documenting their recovery needs, procedures, and processes. It will also form the guide to follow during the initial stages of recovery from a disaster event.

These disaster events may include:

- Terrorism
- Evacuation of a building or city
- Fire, flood, or other "traditional" disasters
- Loss of power to a building or business unit
- Disruption to the delivery of computing resources
- Physical off-site cable construction situations such as cut cable

Disaster Detection and Determination

It is important to remember that the detection of an event that could result in a disaster that could affect the processing of key information at a data center is the responsibility of whoever first discovers or receives information about an emergency.

A disaster should be declared if there is a real or potential threat (from any cause) of:

- Danger to life or health of associates,
- Destruction of, or damage to, company property

If a major disaster has occurred or for any reason there is a real or potential threat of:

- Suspected disaster
- Anticipated disaster
- Loss of communications
- Loss of critical business units
- Loss of essential computer services
- Loss of a site or denial of access to a site.
- Loss of other critical computer equipment

Disaster Recovery Planning

"Disaster recovery planning" is defined as identifying, documenting, training and testing procedures necessary to ensure the consistent and continuous operation of critical end user applications while maintaining the integrity, security and reliability of the data processed by those applications.

> Although most disaster recovery plans address only data processing related activities, a comprehensive plan will also include areas of operation outside data processing. The plan should have a broad scope if it is to effectively address the many disaster scenarios that could affect the organization. A "worst case scenario" should be the basis for developing the plan. The worst case scenario is the destruction of the main or primary facility. Because the plan is written based on this premise, less critical situations can be handled by using only the needed portions of the plan, with minor (if any) alterations required. *1*

Goals and Objectives

The key objectives of the contingency plan should be to:

- Continue critical business operations
- Minimize immediate damage and losses
- Reduce the complexity of the recovery effort
- Facilitate effective co-ordination of recovery tasks
- Identify critical lines of business and supporting functions
- Establish management succession and emergency powers
- Provide for the safety and well-being of people on the premises at the time of a disaster
- Minimize the duration of a serious disruption to operations and resources (both information processing and other resources)

Management must make a decision to undertake a project that satisfies the following objectives:

- Identify the alternatives and select the most cost effective approaches for providing backup operations capability and timely service restoration
- Develop and implement contingency plans that address both immediate and longer-term needs for the Data Center and other business facilities
- Determine vulnerability to significant service interruptions in the Data Centre and business facilities and define preventive measures that may be taken to minimize the probability and impact of interruptions
- Identify and analyze the economic, service, public image and other implications of extended service interruptions in the Data Centre and other business facilities Determine immediate, intermediate and extended term recovery needs and resource requirements[2]

Procedures, guidelines, and resource listings contained within each BRP will direct the owning business unit on what they need to do to recover their operations and what resources the support areas can be expected to deliver to them in a disaster situation.

The resource listings will include such things as:

- PC's
- Servers
- Telephones
- File cabinets
- The recovery site
- Number of desks & chairs

These listings will also contain all other pertinent office supplies that will be needed to perform critical operations. There will be listings defining the timing for delivery of critical computing resources such as: SAP, email, Internet, and other assorted computer applications and supporting resources designated as critical and scheduled to be recovered and delivered to the business unit.

There are five typical required responses to a disaster, or to a problem that could evolve into a disaster:

- Detect and determine a crisis condition
- Notify persons responsible for recovery
- Initiate the business continuity plan
- Activate the designated backup sites
- Disseminate public information

Risk Assessment

Risk assessment is identifying and quantifying the exposures that threaten an organization's assets and profitability. A risk assessment is defined as follows:

> Risk assessment is the process of identifying threats to an asset and specifying the controls that are necessary to secure that asset based on the value of the asset and the impact of its loss. A basic requirement of an effective security plan is to identify and classify all of the assets to be secured. A formal risk assessment program will help the planning and selection of protection measures used for an asset. Not all risks can be offset at a favorable cost; it is not only legitimate but prudent for management to accept certain levels of risk. Security and controls are not ends in themselves, and should always be justified by a business need to limit genuine exposure of the assets to unauthorized users. *3*

Below is a typical model that showed a lot to advance a simple set of clear guidelines on how to think about risk in the organization and risk in planning the audit. This model approached internal control from the perspective of the organization's objectives, the risks to achieving those objectives, and then the controls needed to mitigate these risks. As you can see from the diagram below it illustrates the sequence and expanded it to show the three-step approach to assessing risk.

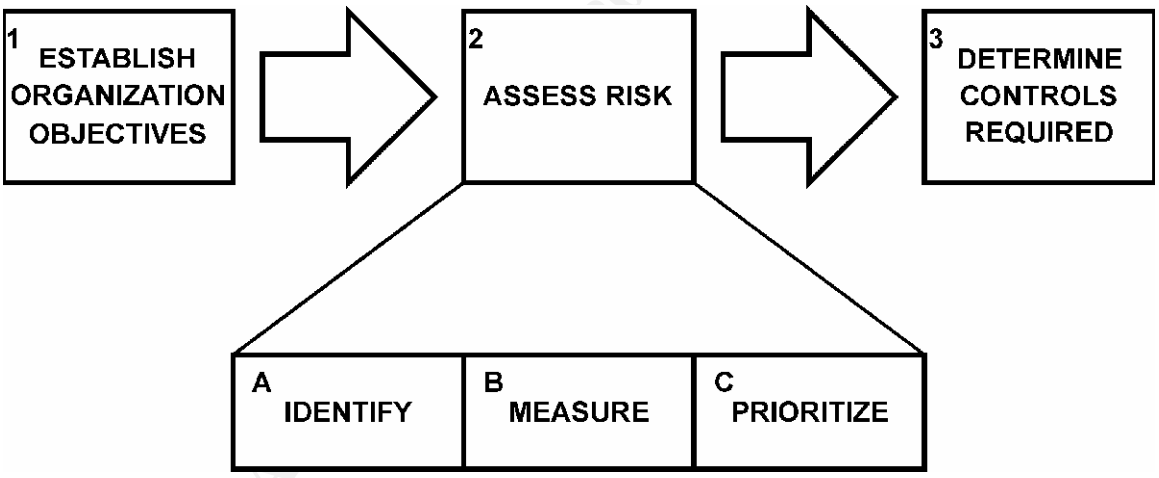

Figure 1. Corporate Risk Assessment Overview

Next, let's will review the audit risk assessment for a typical production company with approximately 1,200 employees. The analysis would normally begin with the fundamental goals and objectives defined by the company in question. The fundamental goals and objectives should always spark a brainstorm of speculation about the threats and opportunities that could affect the goals in some material or significant way. These threats and opportunities would then become the shaping force for the annual audit program as well as high-level guidance for the emphasis within each audit performed.

Identified Risks & Disaster Prevention Measures

Risk Assessment generally considers exposure to these risks:

1. Property Losses

    - Physical Damage

      This would be defined as the risk that is associated to properties consisting of either the building not being able to be occupied for excessive damage or the building being partially or completely destroyed. If a disaster does occur the company must have a temporary location that they can use until a permanent one is found.

2. Data Losses

    - Its import that all data is captured, stored and in a facility that is a safe distance from the organization site.
    - Incremental backups are preformed on a daily basis (Monday - Friday) on all user and system disks on all multi-user systems.
    - Full disk backups are performed on a weekly basis for all disks.
    - Backup procedures are documented in writing and updated on a regular basis, as changes are required. A copy of the current backup plans will be maintained in the IT office.
    - Each backup procedure will generate a log file, which can be inspected on a daily basis to determine the success of failure of the backup.
    - There is an on-line tape library on an off-campus listing each system record of the dates and types of backups performed and the number and date of the associated magnetic tape.
    - There is backup staff members assigned to perform the system backups for each system. The backup staff member should check the backup log on a daily basis to verify the backup and check the hardware and /or software for problems related to the backup procedures.
    - The backup staff member is required to make a written statement of all backups that are performed daily.
    - At random unannounced intervals and periodic scheduled intervals the backup tapes will be selected and restored to a test system in order to ensure that the backup system and process is working and correctly storing the data. These tests will be performed under supervision in a “timed test” format to simulate stress and expediency.

3. Hardware.

All computer hardware will be categorized based on the uptime requirements of the services and data that the systems provide. Hardware redundancy will be categorized based upon the provided example of uptime requirements:

- 99.9999% Uptime:
    - Hardware based RAID 5 Fibre Channel Storage
    - Mirrored DLT Auto-loading Backup Units/Arrays
    - Mirrored System Drives
    - Clustered Server Configuration
    - Redundant Power Supplies, Network Cards, and as much redundant system hardware as is fiscally reasonable. (UPS, Surge Protection, . . .)
    - Co-located backup hardware through a Managed Service Provider (MSP) in a remote location.

- 95% Uptime:
    - Hardware based RAID 5 Storage
    - Single DLT Auto-loading Backup Unit
    - Mirrored System Drives
    - Redundant power supplies
    - Redundant network cards
    - Large single UPS Power Backup

- 85% Uptime (corporate minimum standard):
    - Mirrored System Drives
    - Software based RAID 5 Storage
    - Single DLT or AIT Backup
    - Mirrored System Drives
    - Redundant power supplies
    - Redundant network cards
    - Single mid-range UPS Power Backup

Network Considerations

The IT department is responsible and accountable for making sure that the disaster recovery plans and procedures are in place. Each team will have a specific task and check list that they will be responsible for making sure that they will be able to bring the company to full operations once a disaster occurs. The following teams, roles and responsibilities would need to be described:

The Data Center Operations Team

To provide operational and technical support during recovery operations in the backup phase until normal operations are restored as well as operational and technical support for normal data processing thereafter, at the designated recovery site. Implement emergency shift rosters in order to provide 24-hour support at the recovery site. Apply normal operational procedures and recall all relevant backup media from off-site storage along with general dispatch duties.

The Networking Team

Provide alternate voice and data communications capability in the event normal telecommunication lines and equipment are disrupted by the disaster. Evaluate the requirements and selects appropriate means for the restoration of the telecommunications network at the designated backup sites. Provide network computing support and other distributed services. Implement network disaster recovery procedures during recovery and normal operational procedures thereafter; also responsible for hardware and software vendor call-outs.

The UNIX Recovery Teams

Perform actual recovery of all UNIX servers' critical client systems and applications during the backup phase, as well as ongoing support of above applications and systems after normal operations are restored in the recovery phase and thereafter at the designated backup sites. Assist with recovery and restoration of non-critical client systems and applications. Implement disaster recovery procedures during recovery and normal operational procedures thereafter.

The Database Server Recovery Teams

Responsible for recovery of database server's critical client database applications and systems during the backup phase, as well as ongoing support of above databases after normal operations are restored in the recovery phase and thereafter, at the designated backup sites. Assist with recovery and restoration of non-critical client's database applications and systems. Implement database formatting and disaster recovery procedures during recovery and normal operational procedures thereafter.

The Web Development Recovery Team

Responsible for recovery of the Web servers and access during the backup phase, as well as ongoing support and maintenance of above after normal operations are restored in the recovery phase and thereafter at the designated backup sites. This includes:

1) Installation and/or setting up of the Firewall
2) Successful recovery and initialization of a security package on the Web servers. Also responsible for implementing recovery procedures during recovery and normal an operational procedure's after recovery has been established.

The Application Server Recovery Team

Perform actual recovery of all critical client server applications and systems during the backup phase and provide ongoing support of above applications and systems after normal operations are restored in the recovery phase at the designated backup sites. Assist with recovery and restoration of non-critical client server applications and systems. Implement disaster recovery procedures during recovery and normal operational procedures thereafter.

Other Planning Considerations

Critical information gathered by each disaster recovery operation team for proper disaster recovery planning consideration includes a disaster recovery team organization charts, team interface charts, office equipment inventory, office supplies, computer hardware inventory, computer software inventory, frequency and location of software backups, critical data files, procedure manuals, off-site storage contracts, and microfiche.

Security Assessment

Introduction

Lets begin with a current assessment of current risks, polices, and procedures; which is then followed by recommendations, alternatives, and a tactical implementation plan. It is assumed that company x has over 25 network nodes; this includes both internal networks for the headquarters building and satellite offices located across the U.S. It is also assumed that Internet access and e-mail are required. Let us also assume that company x conducts field research, so remote dial-up access is required.

Current Assessment

A review of current policy and procedures

Let us assume that company x's current security strategy consists only of a dated "Security Policy" which covers the proper handling of sensitive documents and information to physical security of facilities, including authorized entry and escort procedures. However, there is a lack of a written network policy, leaving them currently relying primarily on the experience of its network and system administrators to handle network protection. We will also assume that fortunately, to date, there has not been a significant known breach in the network, a network that relies primarily on a firewall to protect it from the outside. However, there has been an outbreak of many viruses received via employee email.

Interviews with a number of people, including IT technologists and management

There are a number of issues that this company addresses as part of its security strategy. Conducting interviews on the following issues can provide insight on what issues employees think may threaten or enhance security. "This gives a good idea of the problems and issues known to the organizations." *3*

These subject areas may include:

- Audit Trails
- Network controls
- Physical security
- Application controls
- System accreditation
- Remote dialup access
- Policies and procedures
- Database access controls
- Security education and awareness
- Protection and distribution of software
- Password and authentication standards
- Centralized controls, monitors, and automated alerts

An examination of the technology currently employed

The computing center supports a diverse technology environment that is comprised of UNIX, Windows NT and Novell NetWare servers running a variety of business applications. These servers reside on a Fast-Ethernet backbone of CISCO routers and switches. Most traffic is unencrypted, and a firewall is used as the primary means of network defense.

Recognizing the global virus problem, McAfee anti-virus has just recently been deployed to nearly all workstations and servers (including the Microsoft Exchange e-mail servers where the majority of recent viruses pass through).

A risk assessment to learn new things about the environment

> The next step, a limited risk assessment of the computing environment, is meant to discover problems of which the organization is unaware. The limited risk assessment is used to measure the overall exposure of the organization to abuse." This includes more than just a review of technical applications used to provide security; it includes "physical security, organizational procedures, and the likelihood an attack can occur. *3*

An assessment is likely to uncover unauthorized access to restricted rooms and restricted network resources, and may also find operating systems and applications that are not employing the latest security patches. This may be due to weak adherence or non-enforced company access procedures or worse, the lack of a standard company policy.

A serious look at competitors and the value of inside confidential or sensitive business information may give an idea of the likelihood of attack. It is important to note that this assessment must include hackers who are simply looking for another challenge.

A review of future applications and directions

Company x will continue to research, staying at par with industry standard tools and technology to support its business operations. Although there are many new software applications, office applications are primarily used and should be sufficiently protected as they remain at pace with current network security measures (i.e. firewalls, proxies, etc) following its newly developed corporate policy. This holds true with physical security; the corporate policy should dictate that physical security must remain sufficient to protect company assets.

Scope and Assumptions

This security strategy will focus on network security. It will include servers and business applications used on the network. We will assume that the most critical network uses are for office applications and a shared research database.

Requirements Analysis

"The requirements analysis is really a checklist of issues we have discovered as part of the current assessment. Using the findings of the current and risk assessments, we can construct a set of overall requirements. " [3]

- Common authentication mechanism
- Segregate management of security to a separate department.
- Automated controls for remote and mobile users
- Network user security education
- A review of current written network security procedures and their implementation
- Virus protection

Architecture

The security strategy can be implemented into the current network infrastructure. It will require the purchase of additional equipment that is necessary to provide a safe level of security.

Recommendations

Based on the network requirements and proposed architecture three basic areas need to be initiated.

1. Computing security policy, signed by senior management
2. Network accreditation (both software and hardware)
3. Implement Virtual Private Network (VPN) technology

Receiving written approval by senior management is critical to ensure policies and consequences are enforceable, without it, the Security Strategy is not worth the paper it's written on.

Alternatives

To support the large number of mobile users, Microsoft RAS should be used in conjunction with VPN technology to allow secure dial-up and remote connections. This will enable users with proper authentication (including an electronic key) to access all of their network resources as if they were on the LAN back at their home office.
VPN technology provides significant improvements in communication security between corporate sites, both large and remote. Without VPN technology, traffic traverses the Internet unencrypted, unless done so at the source.

Costs

> A balance should be struck between the benefit of the recommendation and its cost. The estimated costs for each alternative including purchase, maintenance, training, and support, should be detailed. Wherever possible, the costs should be expressed in terms of both one-time and annual charges. *3*

The costs listed in dollars only cover hardware and software purchases. Installation costs will be given in terms of approximate man-hours. It must be noted that this is the most significant cost to any Security implementation plan.

Purpose	Product	Purchase Price	Maintenance Plan	Installation Cost	Training
VPN, RAS	Windows 2000 Professional Server	$1199 w/10 client access licenses (one time)	80 man hours a year	30 man hours	$3000 per person (one time)
VPN, RAS	MS License Pack (unlimited)	$1999 (one time)	1 hour a year	2 hours	
VPN, RAS	Dell Server	$6000 (configured)	10 man hours a year	20 man hours	

In order to effectively implement this with VPN technology it must upgrade to Windows 2000 Server. The purchase of a new more powerful server should be included as part of the upgrade.

Recommended Solutions

To implement the recommendations previously define, there must be dedicated and budgeted additional staff, equipment and resources. The following are recommended courses of action:

1. Purchase and deploy new VPN, RAS server solution listed above.
2. "Develop an accreditation process for all systems based upon system and data classification. The accreditation process should, as a minimum, define and enforce standards for authentication, access control, monitoring, and audit." *3*
3. Develop an automated solution to capture security alerts and notify appropriate personnel
4. Convene a working group to update current security policy with a section dedicated to network security policy; receive signature from senior management.
5. Receive signed approval from senior management to proceed with security strategy implementation.

Tactical Plan

The following is the order in which the recommendations should be implemented following a review of their impact and risk. The goal of this Tactical Plan is to get as much of the security strategy implemented as possible in the shortest amount of time, yet doing so in such a manner as to enable the eventual completion of all security strategy recommendations.

1. Convene a working group to update current security policy with a section dedicated to network security policy. Receive signature from senior management.
2. Receive signed approval from senior management to proceed with security strategy implementation.
3. Purchase and deploy new VPN, RAS server solution listed above.
4. Develop an automated solution to capture security alerts and notify appropriate personnel
5. "Develop an accreditation process for all systems based upon system and data classification. The accreditation process should, as a minimum, define and enforce standards for authentication, access control, monitoring, and audit." *3*

Conclusion

It is now generally recognized that business disaster recovery planning is a vital activity, and should be implemented in even the smallest of businesses. The creation of, and maintenance of such a plan, is a complex undertaking, involving a series of steps. Prior to creation of the plan itself, it is essential to consider the potential impacts of disaster and to understand the underlying risks: these are the foundations upon which a sound disaster recovery plan should be built. Following these activities the plan itself must be constructed, which in itself is no small task. This then must then be maintained, tested and audited to ensure that it remains appropriate to the needs of the organization. The example of company x relays these points in a pretty straight forward fashion, and if you consider that this is a relatively small company, you might have a good idea of how complex these plans actually are for fortune 500 companies.

References

1. Wold, Geoffrey W. "Disaster Recovery Planning Process" Disaster Recovery World© 1997, and Disaster Recovery Journal© 1997, are copyrighted by Systems Support, Inc. http://www.drj.com/new2dr/w2_003.htm

2. "Disaster Recovery Planning: Project Plan Outline" Computing & Networking Services, University of Toronto. Copyright 2000. http://www.utoronto.ca/security/drp.htm

3. Bruce, G. and Dempsey, R. Security in Distributed Computing. NJ: Prentice Hall, 1997

Weyerhaeuser in Action, January 8, 2001. http://www.weyerhaeuser.com/disaster-recovery/

Expert Advice on Disaster **Recovery** Planning, December, 1999. http://www.bankinfo.com/chat/tran61599.html

Disaster **Recovery**. Stonehouse Technologies, January, 2001.http://life.csu.edu.au/hazards/0DisasterRecovery.html

Case Studies - Bureaux, Disaster **Recovery**, Study 2, January, 2001. http://www.straitlogics.com/bureaux2.asp

McNamee, David. "Management Control Concepts: Assessing Risk Assessment" *New Perspectives on Healthcare Internal Auditing. Copyright 1996* http://www.mc2consulting.com/riskart2.htm

Family Business Experts "Risk Management: Does Your Family Business Need It?" Family Business Institure, Inc. Copyright 2000-2001. Atlanta, GA. http://www.family-business-experts.com/risk-management.html#RA

Dolislager, F. et al., "ORO Risk Assessment Guidance" The Risk Assessment Information System Website. http://risk.lsd.ornl.gov/homepage/rap_docs.shtml

Bryant, M., et al. "Risk Fields" The Risk World website. Tec-Com Inc., Copyright 2000. http://www.riskworld.com/websites/webfiles/ws00aa012.htm

Microsoft Consulting Services. "Configuring a VPN." http://www.microsoft.com/serviceproviders/whitepapers/configuring%20a%20vpn%20solution.doc

Last Updated: July 27th, 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
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 San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	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
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
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 London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
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 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
Community SANS Sacramento SEC401	Sacramento, CA	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
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event