Interested in learning more about security?

SANS Institute InfoSec Reading Room

Electronic Medical Records: Success Requires an Information Security Culture

Pro or con, the increased use of electronic medical records (EMR) is revolutionizing the world of healthcare. What both sides of the EMR issue do agree upon is solid information security practices are a necessary part of this transition. Although HIPAA regulations were meant to improve healthcare security, many challenges still remain. For example, audits reveal lax security; information breaches are increasing and identity theft along with fraud are prevalent. In response to these identified problems, the real solu...

Electronic Medical Records: Success Requires an Information Security Culture

GIAC (GSEC) Gold Certification

Author: Thomas L. Roberts, troberts@amplex.net
Advisor: Robert VandenBrink, rvandenbrink@metafore.ca

Accepted: December 14, 2012
(Date your final draft is accepted by your advisor)

Abstract

Pro or con, the increased use of electronic medical records (EMR) is revolutionizing the world of healthcare. What both sides of the EMR issue *do* agree upon is solid information security practices are a necessary part of this transition.

Although HIPAA regulations were meant to improve healthcare security, many challenges still remain. For example, audits reveal lax security; information breaches are increasing and identity theft along with fraud are prevalent.

In response to these identified problems, the real solution requires a security culture to be in place with a holistic back-to-basics safety approach of the entire data lifecycle. These include upper management buy-in, policies & procedures, risk management and protection of sensitive data to be part of the daily routine.

1.Introduction

The increased use of electronic medical records (EMR's) is certainly impacting the world of healthcare. Some claim EMR transition is necessary for efficiency of healthcare processes while others claim electronic records signals the final end of personal privacy. Regardless, the transition to EMRs will continue and the healthcare industry must learn to adapt accordingly. (Shoniregun).

I chose this timely topic to seek best practices and solid guidance for a secure EMR implementation. Although I have many years' experience with information security, large-scale electronic healthcare security is a new and exciting adventure opportunity.

Not surprisingly, there are large amounts of information available regarding the adoption of EMRs. What is surprising is expert debate of polar opposite viewpoints regarding the exact approach for a secure and successful EMR implementation. Some healthcare organizations have been reluctant with EHR adoption and there are also reports of poor satisfaction with existing EHR installations. (Dolan).

After poring over massive amounts of research data about EMRs for an extended period, I finally arrived at the best answer. There really is no magic bullet.

The only possible way to implement a successful EMR requires a viable, engaged, dynamic and on-going security culture. The culture also requires constant attention, care and feeding to maintain the process. Finally for the security culture to be successful, it must be a high priority at all levels of the organization to provide the necessary resources and training.

Thomas L. Roberts, troberts@amplex.net

1.2 Disclaimer

The information contained in this guide is not intended to serve as legal advice nor should it substitute for legal counsel. It is meant an introduction to the subject and should warrant additional investigation from the reader.

The guide is not exhaustive, and readers are encouraged to seek additional detailed technical guidance to supplement the information contained herein.

2. HIPAA & Enforcement

The Health Insurance Portability and Accountability Act (HIPAA) enacted by the U.S. Congress in 1996 was revolutionary legislation and provided sets of privacy and security rules. It remains the first landmark healthcare national regulation with primary goals to initiate privacy and security culture in healthcare.

For simplification purposes, HIPAA contains two important foundations. The HIPAA Privacy Rule identifies Protected Health Information (PHI.) and identifies protections. The HIPAA Security Rule defines access and processing standards of PHI in electronic form, also known as ePHI.

Protection of ePHI is accomplished by applying administrative, physical and technical safeguards. To ensure compliance of the safeguards, the Department of Health and Human Services (HHS) is designated to perform on-site periodic audits of healthcare facilities. Although HIPAA regulations are well-intended, they are technical and there are reports of misunderstandings. They also identify protections that need to be in place but falls short of providing a step-by-step guide of *exactly* what needs to be accomplished.

After HIPAA implementation, enforcement problems were later identified. In December 2011, the Senate Judiciary Subcommittee on Privacy, Technology, and Law held a hearing to discuss significant HIPAA enforcement issues.

Subcommittee Chairman Al Frankin claimed that existing HIPAA enforcement was unsatisfactory and only a small number of complaints were actually prosecuted. To back this up, he provided the following:

- Since 2003, the HHS received 22,500 complaints regarding HIPAA violations.

- Of these complaints, the Office of Civil Rights (OCR) imposed one fine and reached a settlement with six others.

The committee also identified that the original HIPAA Privacy and Security Rules needed to be amended to include real enforcement and measurable audits. They also went on to champion the benefits wide spread adoption of EHRs but also identified that more needs to be done to protect those records. (Grunberger).

3. HITECH & Meaningful Use

The Health Information for Economic and Clinical Health Act (HITECH) was released as part of the American Recovery and Reinvestment Act of 2009. Not only does this act build upon existing HIPAA security initiatives, it also provides incentives for the healthcare industry to adopt an information security culture. HITECH is also the first example of national breach notification legislation. In addition, HITECH provides financial incentives for healthcare facilities to transition towards a secure EMR infrastructure by the 2014. (Thompson).

Thomas L. Roberts, troberts@amplex.net

In an effort gain interest in adoption of EHRs, HITECH also includes incentives named Meaningful Use. Although these initiatives will have dramatic effects on the healthcare industry, in depth analysis of Meaningful Use is outside the scope of this article. For discussions points, here are some important takeaways:

- Meaningful Use will require collection, processing and managing of patient data in an electronic format. A short list includes identification of smoking habits, demographic collection and prescribing medications electronically.

- Meeting the criteria successfully for each stage will provide a clinician up to $44,000 through Medicare and $63,750 for Medicaid over a five year period. Not surprisingly, fair distribution of monetary incentives creates additional challenges. (Pittman).

- One primary goal of the HITECH initiatives is for patients to have secure access and control of their own personal health records. (Shoniregun).

- A security risk analysis is required with the promise of more audits by the Department of Health and Human Services to prove compliance. In other words, a security culture needs to be defined, engaged and in action.

  The important of solid safety practices along with a security culture in EHRs cannot be overstated. Lucy Thompson, the author of Data Breach and Encryption Handbook puts it this way: “While advocates of EHR cite numerous benefits to patients- including better quality of patient case, improved outcomes, lower costs, and increased efficiencies for the healthcare

community- the challenge of securing systems such as these are major because security is only good as the weakest link, and these interconnected systems present a variety of weak links that provide vulnerable points that hackers may be able to penetrate." (Thompson).

4. Brief: EHR Adoptions

Although some healthcare institutions have implemented EHRs, the reality is many still use manual processes. Currently only 8 to 10% percent of hospitals and 17% of physicians in the United States have a basic EMR system. According to a survey by the Markle Foundation, 83% of doctors transmit patient information by paper or fax. (Steinbrook).

Not surprisingly, many physicians report problems transitioning to an EHR. They cite that the technology involved not only disrupts their familiar methodology but also shifts their focus away from proper medical treatment of the patient. (Quinn).

This reluctance to adopt EHR's also impedes the benefits a present security culture could provide during the transition to electronic health records.

5. Brief: HITECH Audits

Although government regulations are pushing for the adoption of EHRs, the challenge of maintaining the privacy of data continues to grow. In fact the Office of the Inspector General (OIG) says security and integrity of EHRs is a top 10 management challenge of the U.S. Department of Health and Human Services. (Savitz.)

In early 2011, the OIG also identified a lack of information security controls and documented multiple security concerns during routine hospital audits.

The audit included seven hospitals from California, Georgia, Illinois, Massachusetts, Missouri, New York and Texas. Some of the identified problems were as follows:

- 151 major vulnerabilities such as unencrypted wireless connections, easy passwords and a taped over lock on a data storage room access door.

- 124 identified from above list are high-impact resulting in high priced losses, injury and death.

- Personal classified data could have been accessed from employees and outsiders at some of the hospitals and was confirmed at one of the hospitals audited.

In addition, the Office of the Inspector General also stated that the rise of EHRs is putting patient privacy at risk, especially in regards to the security and integrity of these electronic systems. (Savitz).

Deven McGraw, Directory of the Health Privacy Project at the Center for Democracy & Technology said this report is a "wake up call to the healthcare industry" and "shines a spotlight on the need to light a fire under both the regulators and the health care industry that this is a serious issue." (Clune).

The results of the HITECH audits also identify the need for a security culture

in healthcare.

6. Breaches

One of the most serious information security challenges that need to be addressed for EHR implementation is the alarming breach statistics related to healthcare. According to a Ponemon Institute, the healthcare industry is not only the most breached industry but also the fastest growing. (Ponemon).

In December 2012, The Ponemon Institute released the Third Annual Benchmark Study on Patient Privacy & Data Security. Some of the results are truly alarming:

- 94% of the healthcare organizations surveyed reported at least one breach during the past two years.

- The average price for a breach increased from $2.1 million in 2010 to 2.4 million in 2012.

- Over half of surveyed organizations have little confidence that they prevent, let alone detect a breach.

- 5000 Medicare physician identifiers and nearly 300,000 Medicare beneficiary numbers have been compromised.

- 46% of data breaches were caused by stolen or lost computing devices.

- Mistakes by insiders are the primary reason for breaches. Breaches caused by 3rd party relationships are also very common. These also hurt the reputation of the primary organization.

- 73% of organizations do not have enough resources or trained personnel to prevent and detect information security breaches.

- Security and privacy are not fiscal priorities in healthcare. This increases risk of organization reputation, patient data and the bottom line operating costs. (Ponemon).

  In an interview, Larry Ponemon MD, chairman and founder of Ponemon Institute had this to say about healthcare breaches – "Things aren't getting any better – they're getting worse in some respects… Almost every hospital [surveyed] suffered one data breach, and 45% suffered more than five over the past two years." In addition, experts believe the actual number of data breaches is much larger than being reported. (Nordqvist).

6.1 Cause of Breaches

Although not a complete list, the following are some of the most reported breach causes:

- Employee negligence: This appears to be the most common cause of a breach. It is also important to note that this category continues to increase in expense.

- Unencrypted loss of portable media: These items include USB drives, backup external hard drives, smart phones, and CD and DVD disks. Although full hard drive encryption may offer "safe harbor" protection regarding breach notification, unencrypted portable media devices do not offer the same protection.

- Third party: These breaches are also very expensive and unfortunately very common. Often breaches caused by 3rd parties can lead to loss of reputation for the primary organization via bad publicity.

- Stolen laptops and portable media: Although problematic for many organizations, these items stolen or misplaced from healthcare organizations often contain electronic protected health information (ePHI), which is subject to breach notification requirements. (Ponemon).

6.1.1 Driver for Breaches: Identity Theft & Fraud

So why are the reports of healthcare breaches increasing? One answer is to understand that historically criminals follow the money.

The "street value" of health information is 50 times greater than other types of

identifying data. (Ponemon.) PHI health records contain a wealth of personal identifying information (PII) that not only requires protection but is also very desirable to data thieves to commit fraud. In fact there is an existing black market for this type of valuable information. (Shaw.) According to Rebecca Saltiel Busch, the author of Healthcare Fraud, "The use of PHI is the cornerstone to committing fraud in healthcare. With respect to fraud, view PHI as money." (pg. 113).

In addition, Ponemon Institute did report in 2012 that over half of the healthcare organizations they surveyed reported medical identity theft. (Nordqvist).

Stolen identities are often used for receiving medical treatment, surgery or drugs. These identities can also be used for monetary reasons, such as submitting false insurance claims. ("Medical Identity Theft," n.d).

Possibly this is the motive that led a Howard University surgical employee to sell person medical information for over a year in 2010 and 2011. This unfortunate incident identifies the necessity to not only protect sensitive data from outside attackers but also monitor activity from inside authorized users. (McElhatton).

In addition it appears that celebrities are at risk of exposure regarding their medical treatments. In Los Angeles in 2008, the UCLA Medical Center was cited for selling information to the tabloids for performer Britney Spears and the late actress Farah Fawcett. (Clune). It is unfortunate that some entities under the guise of journalism would pay for PHI of a celebrity.

In fact, Farah Fawcett herself was directly involved in a sting operation regarding her PHI while in care at the UCLA Medical Center. The goal of the sting was to prove an inside employee leaked her personal information to the Enquirer. In an interview shortly after this story broke, she described how she

was deprived of privacy because of her celebrity and was not allowed the choice to share her medical treatments and condition with selected friends and family. Until this happened, she wanted to keep the information private. (Ornstein).

Another report also claims that after celebrity Michael Jackson was deceased, his medical records were improperly accessed at Ronald Regan UCLA Medical Center.

As another example of unauthorized access of medical records, it was also reported that Michael Jackson's death certificate at the Los Angeles County Coroner's Office was viewed more the 300 times. This involved at least 6 staff members and the certificate was printed before it was made public. According to a high-ranking official, the only the lead investigator of the investigation had the authorization to access the document. (Hennessy-Fiske).

These previous examples not only identify that there are monetary threats regarding their personal medical information but also may be susceptible to unauthorized medical record access driven by popularity and curiosity.

The alarming breach statistics along with increased attention by criminals of healthcare data identifies the compelling need for a security culture to be in place. So how does one get started?

7. Getting Started With A Security Culture

To be effective, a holistic security approach that converges, law, organization policy, professional ethics is the only possible way to mitigate or eliminate threats in healthcare organizations (Shoniregun). To accomplish these objectives, it is necessary for a security culture to in place. Below are items to consider with an information security culture in healthcare.

Upper Management Buy-in

This item tops the list and for good reason. This is the most important item necessary for security culture success. In addition to providing the necessary resources, this provides the momentum to follow through with security initiatives. Getting upper management support can be very difficult but so very important to obtain.

One way to get upper management buy-in is to identify that healthcare information security breaches may be inevitable. For example, Seattle Children's Hospital sold a culture of security to upper management by telling them to expect breaches, fines and bad publicity. This strategy appears to have worked. Cris Ewell, Chief Information Security Officer at Seattle Children's Hospital had this to say about the beginning of their security culture:

"It's bigger than privacy and security … it's about involving everyone in the organization at the highest level down to the help desk level [people] who are inputting calls into the system." (McNickle).

He also went on to say that a security culture change occurred when he designated an incident response team to expect breaches. "It's not a matter of if, but when." McNickle).

To get started with selling upper management support for a security culture, the following tips may prove to be very useful:

- Adopt a business perspective of the healthcare organization; understand the initiatives and how the business operates.

- Find a way to educate upper management regarding risks and promote the cost-benefit justifications of directly addressing them with action.

- Set metrics that show information security are providing value to the organization.

- Provide news stories about healthcare breaches, show the damage they cause why it is important to try and prevent this from occurring. Due diligence will go a long way even if a breach does occur.

Although there is no tried and true method to sell a security culture to upper management, it certainly will not be handed to you. It is important to have a strategy of how to earn the culture.

Policies & Procedures

After getting an upper management security culture buy-in; this is the first action item. A key component of a security culture is for users to understand what behaviors are expected and how to securely provide healthcare services. These actions are accomplished by defining policy and procedures. These help guide and organization towards a security culture and addresses responsibility and how everyone fits it. It is also very important that these are not only communicated well throughout the enterprise but well understood. (Cole).

In addition, here are key tips to getting started with policies and procedures:

- Create a group to develop the understandable policies for the organization. Include human resources, legal, facilities management, information technology and other healthcare business areas.

- The policies need to be specific to the healthcare organization and templates can be useful as a starting point. Make sure privacy and security policies relate to each other. Taylor these policies to make sure protected health information (PHI) is protected in all areas.

- Policies need to be easy to read and understandable. Employees at all skill levels need to understand exactly what needs to be accomplished. As mentioned in the SANS Security Essentials training, a good test of policies is to share them with sample employees and have them explain them back to you to meet the intended objectives.

- Policies need to be fair and reasonable to accomplish necessary tasks. This requires a balance of safety, compliance and convenience to be reviewed. If they are too difficult, then they are too difficult to accomplish the goals. Another problem is if policies are too difficult, employees may try to find ways around them.

- Involve legal and compliance areas to make sure policies meet the necessary compliance objectives.

Thomas L. Roberts, troberts@amplex.net

- Security and privacy policies need to be enforced. This includes all levels of the healthcare organization including upper management. HIPAA along with other laws and regulations require sanction policies including enforcement documentation.

- Make sure everyone in the organization are aware that security policies. These policies should also details regarding third party healthcare relationships and expected use mobile computing devices. (Nordqvist).

- To properly communicate policies and procedures, it is also important to implement security awareness training. This greatly helps promote the expected behaviors and address gaps in employee understanding of technical risks. (Ponemon).

Risk Management

Having a well-defined security risk management process is also very important. This is where the threats and vulnerabilities are examined on a periodic basis, changes implemented, and monitoring the results. The key elements are to examine the confidentiality, integrity and availability of all EHR systems throughout the entire electronic lifecycle for effectiveness. ("Guide to Privacy, " n.d.). Success with risk management also requires these processes to be on-going and repeated often.

The high level requirements of a security risk management process are:

- Review existing security of protected health information.

- Identify threats and vulnerabilities

- Access risks for likelihood and impact

- Mitigate security risks

- Monitor results.

Because healthcare presents unique challenges regarding risk practices, expert advice can be very useful. The Office of the National Coordinator for Health Information Technology has useful tools and advice on their website at: www.HealthIT.gov

Another useful resource available is a handbook by *The American Society for Healthcare Risk Management / American Health Lawyers Association – Enterprise Risk Management Handbook for Healthcare Entities – 2nd Edition* that is a complete guide for creating and maintaining a viable healthcare risk management process.

More information can be found at:
http://www.ashrm.org/ashrm/online_store/ahla_toolkit/ashrm-ahla-handbook2013.shtml

Thomas L. Roberts, troberts@amplex.net

Protection of Sensitive Data

Not only do healthcare regulations demand this is, patients also expect that their personal data with be properly managed. As healthcare transitions to EHR's data flows, data at rest, data communications, mobile devices, and access to data needs to be reviewed as part of the risk management process. The following items are important to review regarding data protection:

Access to healthcare data needs to be authorized and audited on a regular basis. Regulations require healthcare personnel only have least privilege access. That means only enough access to complete job responsibilities, no more.

Encryption needs to be in place for data at rest (such as hard drives, portable media and other devices) especially if they contain protected health information. Keep in mind that a safe encryption practice includes proper key management to help prevent security breaches. (Thompson.) If fact, properly installed enterprise encryption will avoid the necessity of reporting an information security breach if the device contains protected sensitive information. It is also important to securely erase all computing and media devices at the end of the data cycle. (Cole).

Encryption for communications is necessary. Implement Virtual Private Networks (VPN's) where necessary and also configure strong available encryption protocols (such as IPSEC, 3DES, and AES) for communications. (Cole).

Mobile devices need to be included in security policies, especially if the healthcare facility allows end users to bring their own mobile devices. Ongoing risk management processes should include these devices. This includes a process to

securely remote erase these devices when reported stolen to prevent sensitive data loss. (“Guide to Privacy,” n.d.)

Solid provisioning and de-provisioning of system access containing ePHI should be verified for compliance and monitored. (Cole).

8. Conclusion

Although the previous list contains very important items, it really is just a starting point of creating a viable information security culture in healthcare.

The complexity of implementing an EHR is immense and by no means trivial. There is no single technology solution or best practices guideline that will achieve compliance. The real value of a security culture will be apparent when the synergy of everyone in the organization working towards a common goal of safety. It is really the only possible way to avoid the many identified security threats facing healthcare organizations. (Amatayakul).

The need for a security culture to reach the desired goal of EHRs is imperative to reach the desired results. An individual’s health data is much more than a combination bits and bytes, it contains a personal journey map of identity and health related information throughout a lifetime. As discussed previously in this paper, this information is so very worth protecting and is very valuable to criminals that would use this information for identity theft and monetary pursuits. The risks of EHRs is so apparent and pervasive, the only real chance is instill a security culture in healthcare.

The ultimate success of a healthcare security culture will occur when solid

information security practices are as second nature as disinfection. ("10 Best Practices," 2010.)

10. References

Amatayakul, Margret K. (2009). Electronic health records. (4th ed.). Chicago: American Heath Information Management Association.

Busch, Rebecca Saltiel. (2012). Healthcare fraud. Hoboken: John Wiley & Sons, Inc.

Clune, Sarah. (2011, May 17). Report: Push for electronic medical records overlooks security gaps. PBS Newshour URL. Retrieved from http://www.pbs.org/newshour/rundown/2011/05/report-push-for-electronic-medical-records-overlooks-security-gaps.html

Shaw, Thomas J. (2011). Information security and privacy. Chicago: ABA Publishing.

Shoniregun, Charles A., Dube, Kudakwashe, Mtenzi, Fredrick. (2010). Electronic healthcare information security, Advances in information security. New York: Springer Science Business Media.

Thompson, Lucy. (2012). Data breach and encryption handbook. Chicago: ABA Publishing.

Thomas L. Roberts, troberts@amplex.net

McElhatton, Jim. (2012, May 17). Howard university worker accused of selling health records. Authorities charge employee with disclosing patients' information. The Washington Times. Retrieved from http://www.washingtontimes.com/news/2012/may/15/worker-accused-of-selling-health-records/

Ponemon Institute LLC. (2012, December). Third annual benchmark study on patient privacy & data security. Traverse City, MI.

Grunberger, Rachel. (2011, December 22. Senate hearings focus on lack of HIPAA enforcement, final HITECH rule. Inside Privacy. Retrieved from

http://www.insideprivacy.com/senate-hearings-focus-on-lack-of-hipaa-enforcement-final-hitech-rule/

Savitz, Eric. (2012, December 7). Why healthcare data breaches are a c-suite concern. Forbes. Retrieved from

http://www.forbes.com/sites/ciocentral/2012/12/07/why-healthcare-data-breaches-are-a-c-suite-concern/

McNickle, Michelle. (2012, December 6). Patient data breaches: Future looks grim. Information Week Healthcare. Retrieved from

Thomas L. Roberts, troberts@amplex.net

http://www.informationweek.com/healthcare/security-privacy/patient-data-breaches-future-looks-grim/240143949

Nordqvist, Christian. (2012, December 7). Data breaches – a growing problem in healthcare organizations. Medical News Today. Retrieved from:

http://www.medicalnewstoday.com/articles/253717.php

Cole, Eric. (2006). Security best practices. Secure Anchor. Retrieved by

http://www.securityhaven.com/docs/Security_Best_Practices.pdf

Ornstein, Charles. (2009, May 11). Farrah fawcett: "Under a microscope' and holding onto hope. Los Angeles Times. Retrieved by

http://articles.latimes.com/2009/may/11/entertainment/et-fawcett-interview11

Hennessy-Fiske. (2010, June 10). Michael jackson's medical records at UCLA were improperly accessed, source says. Los Angeles Times. Retrieved from

http://latimesblogs.latimes.com/lanow/2010/06/michael-jacksons-medical-records-at-ucla-were-improperly-accessed-source-says.html

Thomas L. Roberts, troberts@amplex.net

McNickle, Michelle. (2012, October 19. Health data breach response: Culture change needed. Information Week Healthcare. Retrieved from

http://www.informationweek.com/healthcare/security-privacy/health-data-breach-response-culture-chan/240009343

The Office of the National Coordinator for Health Information Technology. Guide to privacy and security of health information. Chapter 2 – Privacy & security and meaningful use. (Version 1.206012) Retrieved from

http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide-chapter-2.pdf

Health Info Net. (2010, November). 10 best practices for the small healthcare environment. (Version 1.0). Retrieved from

http://www.healthit.gov/sites/default/files/basic-security-for-the-small-healthcare-practice-checklists.pdf

Quinn, Frank (2012, September 12) MedCity News. EMR adoption – Why are some physicians reluctant? Retrieved by http://medcitynews.com/2012/09/emr-adoption-why-are-some-physicians-reluctant/

Thomas L. Roberts, troberts@amplex.net

Dolan, Pamela Lewis. (2012, May 7). Doctors' love-hate relationship with EHRs. American Medical News. Retrieved from http://www.ama-assn.org/amednews/2012/05/07/bisa0507.htm

Pittman, David. (2012, December 7). Most docs won't qualify for EHR 'meaningful use'. MetPage Today. Retrieved from http://www.medpagetoday.com/PracticeManagement/InformationTechnology/36327

Steinbrook M.D., Robert. (2009, March 12). Health care and the American recovery and reinvestment act. The New England Journal of Medicine. Retrieved from http://www.nejm.org/doi/full/10.1056/NEJMp0900665

Bureau of Consumer Protection – Federal Trade Commission. Medical identity theft: FAQ's for health care providers and health plans. Retrieved from http://business.ftc.gov/documents/bus75-medical-identity-theft-faq-health-care-health-plan

Last Updated: September 26th, 2017

Upcoming SANS Training

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

SANS DFIR Prague Summit & Training 2017	Prague, CZ	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS October Singapore 2017	Singapore, SG	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZUS	Oct 09, 2017 - Oct 14, 2017	Live Event
Secure DevOps Summit & Training	Denver, COUS	Oct 10, 2017 - Oct 17, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VAUS	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, JP	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS Brussels Autumn 2017	Brussels, BE	Oct 16, 2017 - Oct 21, 2017	Live Event
SANS Berlin 2017	Berlin, DE	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
GridEx IV 2017	Online,	Nov 15, 2017 - Nov 16, 2017	Live Event
SANS London November 2017	London, GB	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CAUS	Nov 27, 2017 - Dec 02, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZUS	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Khobar 2017	Khobar, SA	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, DE	Dec 04, 2017 - Dec 09, 2017	Live Event
European Security Awareness Summit & Training 2017	London, GB	Dec 04, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TXUS	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Frankfurt 2017	Frankfurt, DE	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Bangalore 2017	Bangalore, IN	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Oslo Autumn 2017	OnlineNO	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced