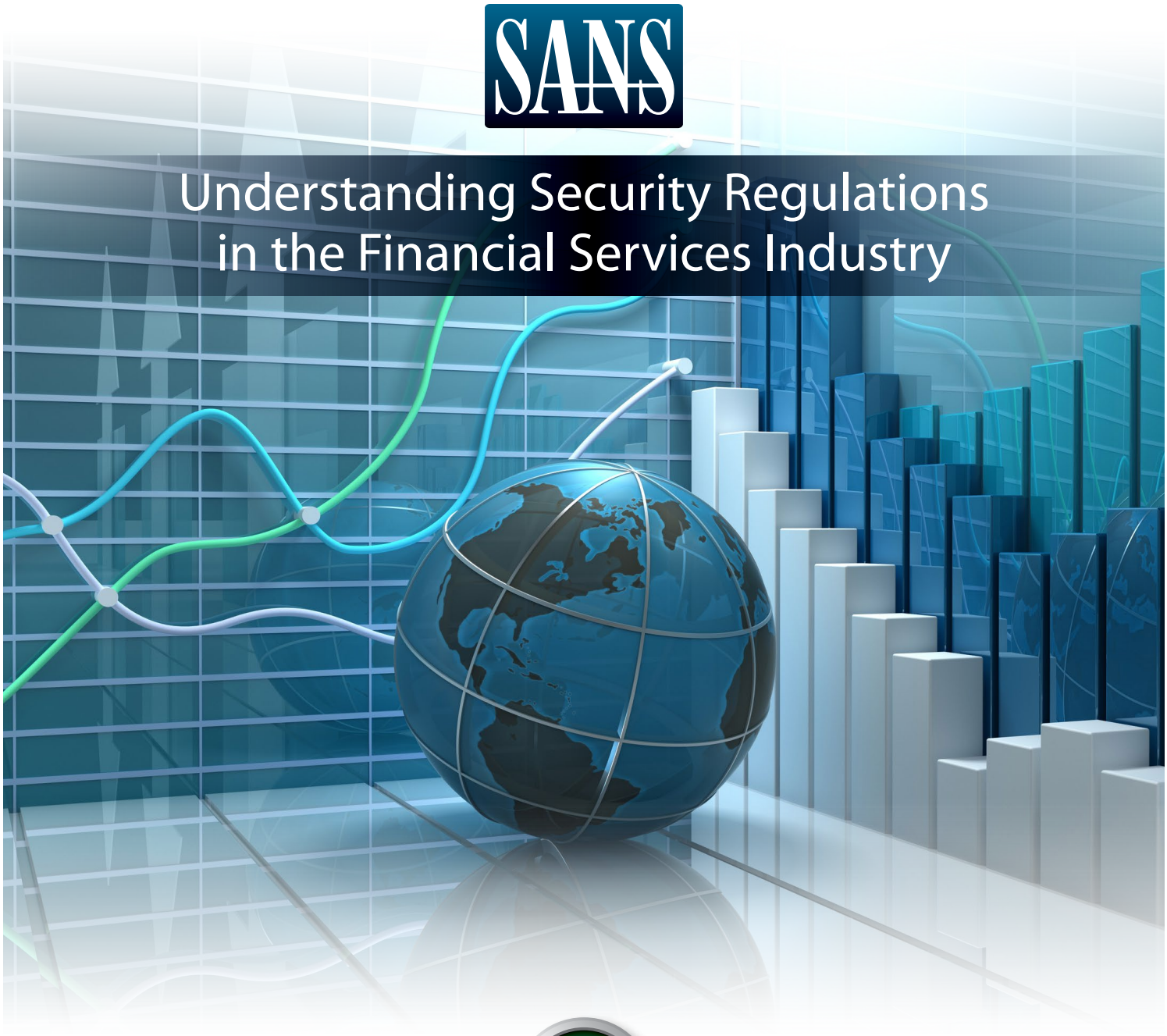
Understanding Security Regulations in the Financial Services Industry

View the associated infographic here:
https://www.sans.org/reading-room/whitepapers/analyst/infographic-financial-apps-risk-37042



Understanding Security Regulations in the Financial Services Industry

Written by David Hoelzer

June 2016

Sponsored by
Veracode

The world of financial services and banking regulation is labyrinthine, to say the least. The myriad laws and regulatory rules financial institutions must comply with can seem quite complex when viewed as discrete requirements, but from the application security point of view, all of these requirements are focused on protecting consumer information and accounts.

Compliance requires that risk assessments account for the personally identifiable information (PII) being processed, stored and accessed within the applications. Assessments must then generate reasonable controls to mitigate risks, along with documented policies and procedures, training of developers handling consumer PII, and validation of application security and detection capabilities.

Looking at risk from the point of view of the consumer allows security and risk management teams to better inform the operations group of how regulators view the organization. This is a critical connection to make because, obviously, no financial services organization wants to receive a CID[1], NORA[2] or PARR[3] for failing to protect consumer accounts and data.

Financial organizations recognize that compliance does not necessarily mean better security.[8] Because compliance can be time-consuming and expensive, some financial services organizations go to great lengths to avoid certain products and services to exempt themselves from additional regulatory requirements.

But holding back on new applications because of compliance procedures is not a good business strategy. Neither is carefully crafting the narrative to avoid regulation.

Interpreting Regulations

Virtually all financial services companies and financial institutions are subject to the Gramm-Leach-Bliley Act (GLBA),[4] while the Dodd-Frank Wall Street Reform and Consumer Protection Act provides the measure of what is "reasonable and appropriate" for protecting consumer data in financial systems.[5] The Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau (CFPB) oversee the enforcement of these regulations.

The Sarbanes-Oxley Act (SOX)[6] is a regulation that applies more to protecting investor information and systems. SOX is somewhat vague about what it means to protect information assets, but GLBA is quite specific, requiring information security training, specific policies, scanning and other activities. For those processing financial transactions, the Payment Card Industry Data Security Standard (PCI DSS) for financial services applies only to financial services companies processing payment cards. Only the portion of the business that is actually processing those cards falls under PCI.[7]

Grappling with more stringent compliance criteria, while initially requiring more effort, typically yields simplified compliance processes across all applications and more robust operations. After all, the point of the regulation is not to hamper operations but to simply require good practices!

The key to this simplification is boiling down the multiple regulatory guidelines into a

[1] Civil Investigative Demand
[2] Notice and Opportunity to Respond and Advise
[3] Potential Action and Request for Response
[4] www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act
[5] www.ftc.gov/enforcement/statutes/dodd-frank-wall-street-reform-and-consumer-protection-act-titles-x-and-xiv
[6] www.soxlaw.com
[7] www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss
[8] www.sans.org/reading-room/whitepapers/privacy/gramm-leach-bliley-act-g-l-b-practices-network-security-682

formula that can prove compliance while also actually reducing risk. See Table 1.

Table 1. Protecting Consumer Apps with Regulations

Regulation and Mandate	Security Requirements Summarized	Specific Controls
GLBA Safeguards Rule[9] *"…financial institutions must protect the consumer information they collect."*	Designate responsible party. Identify applications hosting or transacting customer information. Assess risks to customer information. Design, monitor and test assessment program. Hold service providers to same standards. Continue to evaluate and adjust programs.	Establish and maintain an inventory of systems and applications containing and processing critical information. Establish regular periodic scanning so that future activities remain fact-based. Scan applications regularly for vulnerabilities. Establish criteria for the prioritization of vulnerabilities and remediation activities. Pay special attention to internally or custom-developed applications with dynamic and static analysis. Establish secure coding as a culture, and provide qualified training on secure coding. Establish and document a secure development life-cycle approach that fits your business and developers. Combine functional testing and security testing of applications: Assess for operational bugs and coding errors. Establish and enforce secure coding practices such as pair programming and code review. Establish and enforce segregated development, testing and production environments. Conduct periodic threat modeling activities for all critical applications. Outcomes should inform information security monitoring and fraud detection activities. Perform regular application penetration testing, and inform the regular vulnerability scanning process to provide ongoing regression testing of applications. Establish and maintain policies and procedures. Continuously improve your visibility, assessment and security programs. Periodically audit the controls structure, seeking to validate the effectiveness of the risk management activities listed above and of the controls themselves.
Dodd-Frank[10] *"To promote the financial stability of the United States by improving accountability and transparency in the financial system."* [11]	Sets the baseline for what is "reasonable and appropriate" security around consumer financial data. You must be ready to prove your security controls and document them. This includes time to detect, respond and report breaches impacting sensitive data. Size and maturity of the organization is a consideration in what is reasonable.	
SOX[12] *"To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes."*[13]	Sections 302 and 404 indirectly charge information systems to support accounting and oversight for the accuracy of reporting. Advice for achieving this is augmented by other frameworks such as COBIT[14] and the CIS Critical Security Controls.[15]	
PCI DSS[16] *"Maintaining payment security is required for all entities that store, process or transmit cardholder data."* [17]	Protect cardholder data Manage vulnerabilities Provide strong access controls Monitor and test Maintain policy	

[9] www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying
[10] www.ftc.gov/enforcement/statutes/dodd-frank-wall-street-reform-and-consumer-protection-act-titles-x-and-xiv
[11] www.gpo.gov/fdsys/pkg/PLAW-111publ203/html/PLAW-111publ203.htm
[12] www.soxlaw.com
[13] www.sec.gov/about/laws/soa2002.pdf
[14] www.isaca.org/cobit
[15] https://benchmarks.cisecurity.org/downloads/compliance/
[16] www.pcisecuritystandards.org/pci_security/
[17] www.pcisecuritystandards.org/pci_security/maintaining_payment_security

Bake in security rather than bolting it on. Know what data you have, where it is and how it's changing. Identifying inadequately addressed risks is not helpful unless it leads to effective controls to mitigate them. Periodic audits must be performed to verify that the controls are, in fact, effective.

Due Care

Enforcement agencies now recognize that perfection is not possible. Enforcement attorneys typically retain technical experts to assist them in determining potential liability and possible negligence. In the past, hiring experts was considered "due care."[18] Now, experts are being asked whether the actions of the institution were "reasonable and appropriate." What, precisely, does this mean? Let's examine the question in two ways.

Bake in security rather than bolting it on.

What is reasonable? If a thorough vulnerability scan is run against any sizable organization on any day of the year, there will be vulnerabilities. The question is whether the organization, based on its size and age, acted in a reasonable way. A large, well-established business would be hard-pressed to claim that six months or more is a reasonable patching time frame. At the same time, it likely is not reasonable for any size organization to remediate a serious vulnerability in only minutes or hours.

What is appropriate? The question to ask when a breach happens is, "Was the organization defending itself in a reasonable and appropriate way?" What does this mean? "Appropriate" requires careful consideration of whether the possible protections were based on the sensitivity of what was bring protected, and the size and maturity of the organization.

The following real-life example involving a small payment products organization offers a measure of what is reasonable and appropriate.

[18] For a thorough discussion of due care, particularly with regard to liability, see http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1553&context=law_and_economics

No Harm, No Foul? Good News/Bad News

The consent order entered into by the CFPB and Dwolla, a small organization offering financial services in the form of payment products, provides insight into reasonable and appropriate measures taken to protect consumer data.[19] Dwolla was ordered to pay a $100,000 civil fine, retrain its staff in security of sensitive data, improve its financial systems, and stop making false claims. Specifically, according to the enforcement action, Dwolla misrepresented its data and application security practices by "falsely claiming its data security practices 'exceed' or 'surpass' industry security standards: Contrary to its claims, Dwolla failed to employ reasonable and appropriate measures to protect data obtained from consumers from unauthorized access." Dwolla was also fined for "falsely claiming its 'information is securely encrypted and stored': Dwolla did not encrypt some sensitive consumer personal information, and released applications to the public before testing whether they were secure."

First the bad news: There was no claim of breach. There were, however, false claims for consumer data protection that were detected and challenged by authorities. This is groundbreaking, legally. In the past, organizations could easily fall back on the claim that there was no actual harm.

In the absence of any demonstrable harm, how can there be an actual cause for a complaint? Interestingly, the same rationale is not applied when it comes to issues of physical safety. For instance, fire code violations can easily result in significant fines due to the potential for physical harm even if there hasn't been a fire. It could be that information security regulators—and possibly in the future, the legislators as well—are beginning to apply the same regulatory rigor to the safety of financial and personal information.

Now the good news: In a sense, the requirements in the consent order could be viewed as a step-by-step checklist of activities and controls that must exist as a foundation for information security. These items, in conjunction with the CIS Critical Security Controls,[20] allow management to set and expect concrete deliverables from information security overall and security of applications in particular. This is really good news for compliance-conscious organizations.

Compliance Road Map

Specific requirements for risk assessment and periodic audits should serve as metrics to assess whether proper controls are, in fact, being created and that they are actually effective.

Fact-Based Risk Assessment

For risk assessment processes to be reasonable and appropriate, they must be fact-based and the organization must reasonably act to prioritize and address identified risks. When we say "fact-based," we are saying that actions taken by the organization must be informed by actual data. For example, an organization conducts a phishing exercise and is informed that employees are easily fooled. Based on this data, the organization crafts policy and training to address the issue. Periodically, the organization would then verify that the control is effective through testing, provably remediating the issue.

[19] www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/

[20] www.cisecurity.org/critical-controls.cfm

High-level risk assessment is typically a fairly simple thing. For example, when it comes to financial organizations, it's known that bad actors will seek to perform unauthorized transactions, establish fraudulent and fungible identities, and misappropriate customer PII. Assessments must take into account these types of activities.

Lower level assessment then follows. For example, if the organization has access to source code, assessment would then focus on functional bugs such as SQL injection within the application, as well as a review of the code.

Scanning and Remediation

The first two CIS Critical Security Controls require that the organization develop and maintain an inventory of systems and networks. This inventory must include not only how many systems there are, but where they are, what they are, what data they process, and how they are configured. After this baseline information has been established and a reasonable measure of change control has also been established (CIS Control 3), vulnerability assessment and remediation begin.

Although there is certainly a place for exhaustive vulnerability scanning, it is often not terribly effective without a way to prioritize and complete repairs. An organization of even just a few thousand systems, let alone hundreds of thousands to millions, will be hard-pressed to address every single finding in a timely way. A list of systems and networks prioritized by risk impact is much more appropriate than just a list of all vulnerabilities. Logically, priority will go to systems containing and processing critical information—information that would have a measurable impact on operations if compromised or lost.[21]

This leads to establishing criteria for prioritization, and is driven by both system and network scanning activities and the inventory-critical information being processed; in other words, a fact-based approach. With the criteria established and systems identified, regular periodic or even continuous scanning should be performed. This approach would also begin to satisfy CIS Control 4.

During scanning, pay special attention to internally developed or custom developed applications. These systems are of great concern because they often process, access or control access to an organization's most critical information. To understand how to perform this testing, we must consider how application security and secure development are handled.

[21] For a financial services organization, this information will almost always be the very information that regulators want to see protected.

Secure Development

It's one thing to say that an organization has strong coding practices; it is an entirely different thing to actually implement such practices. Considering our example in the consent order, we find evidence that Dwolla said publicly and may actually have believed that it was secure and had excellent security practices. According to the stipulated order, a developer leading an application development team had no data security training whatsoever. Further, even though the organization had documented software development practices, those practices were not followed by this team. We also learn that the applications developed by this team apparently handled PII.

Organizations must establish secure coding as a culture. Security isn't something that is added in as an afterthought. Instead, part of the project initiation and specification includes conscious security design, baking in the security from the very beginning.

For this to be effective, organizations must identify qualified individuals or organizations that can provide secure development training for developers. This effort aligns with CIS Control 9, which requires skills assessments and supplemental training. Establish effective training as a springboard to a secure development life-cycle program that fits the needs of the business and the style of the developers. Ensure that this process includes both functional testing (delivering the features that are promised) and security testing (delivering reliable, safe code).

Code review must also be included, a good amount of which can be handled through automated software but can also include manual code review and pair programming approaches. As effective as these are, however, it would be good to supplement them with penetration testing exercises focused specifically on these applications.

Ultimately, the vulnerability scanning process should be leveraged so that identified issues become automated future tests. This process allows for quick and easy regression testing as a part of the vulnerability scanning process.

One final critical element for secure development is the segregation of the development, testing and production environments. All security standards that touch on secure coding require that these environments be separated. Further, the development and test environments must never use or have access to actual production data, even old data. Even the administration of these systems must be segregated, with different individuals managing and administering each of these environments.

Establish Policies and Procedures

Although this is called out in our road map as a separate activity, policy and procedure creation should be occurring throughout these processes. Considering the Dwolla consent order again, we find that the financial services organization in question "failed to adopt or implement a written data-security plan to govern the collection, maintenance, or storage of consumers' personal information."[22]

For a risk assessment activity to be considered effective, it must identify risks and the organization must then act in some way to control the risk. How the organization reacts is governed by the reasonable and appropriate standard. Not acting at all, however, cannot be appropriate when considering risks to critical systems or information.

Management is responsible for measuring overall effectiveness of these controls and the entire process through periodic auditing. This responsibility squarely aligns with the Dwolla consent order, providing a measure of assurance that an organization is approaching the problem of information security correctly.[23]

Remember the Goal

There are many more activities that can be included in an effective application information security program that mitigates risk and supports compliance mandates. Rather than attempt to be exhaustive, remember that the goal is to be effective.

Take the provided road map and investigate your own organization. Have all of these issues been addressed? Are there any deficiencies? Are your existing controls reasonable and appropriate given the data being handled, the size of the organization and the age of the enterprise? If you can't say yes to those questions, you have identified risk within your business, and now you have a tool to help address it.

[22] http://files.consumerfinance.gov/f/201603_cfpb_consent-order-dwolla-inc.pdf page 7, bullet 29

[23] http://files.consumerfinance.gov/f/201603_cfpb_consent-order-dwolla-inc.pdf page 14, bullet 25

About the Author

David Hoelzer is a SANS fellow instructor, courseware author and dean of faculty for the SANS Technology Institute. In addition to bringing the GIAC Security Expert certification to life, he has held practically every IT and security role during his career. David is a research fellow in the Center for Cybermedia Research, the Identity Theft and Financial Fraud Research Operations Center (ITFF/ROC), and the Internet Forensics Lab. Currently, David serves as the principal examiner and director of research for a New York/Las Vegas-based incident response and forensics company and is the chief information security officer for an open source security software solution provider.

Sponsor

SANS would like to thank this paper's sponsor:

VERACODE

Last Updated: August 20th, 2017

Upcoming SANS Training

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

SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MDUS	Sep 25, 2017 - Sep 30, 2017	Live Event
Data Breach Summit & Training	Chicago, ILUS	Sep 25, 2017 - Oct 02, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, DK	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, GB	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, COUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, NL	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, CZ	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Oslo Autumn 2017	Oslo, NO	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS October Singapore 2017	Singapore, SG	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS AUD507 (GSNA) @ Canberra 2017	Canberra, AU	Oct 09, 2017 - Oct 14, 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 Brussels Autumn 2017	Brussels, BE	Oct 16, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, JP	Oct 16, 2017 - Oct 28, 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 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 Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Adelaide 2017	OnlineAU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced