Legal Considerations When Creating an Incident Response Plan

Bryan Chou

Legal Considerations When Creating an Incident Response Plan

GIAC (GSEC) Gold Certification

Author: Bryan Chou, bnchou@live.com
Advisor: Adam Kliarsky
Accepted: December 16, 2016

Abstract

Creating a cybersecurity incident response plan (CSIRP) is basic requirements of any security program. CSIRPs generally follow the six phases of the incident response process (preparation, identification, containment, eradication, recovery, and lessons learned) or some derivation of those steps (Kral, 2011). Once a security event begins, the cybersecurity incident response team (CSIRT) is focused on identification, containment, eradication, and recovery.. In other words, they are trying to get operations back to normal. The preparation phase is the time to thoughtfully consider and research the legal decisions required during a security event. Legal considerations to include in the CSIRP include the pertinent laws and regulations, what to do if prosecution is a possibility, and maintaining attorney-client privilege.

1. Introduction

One of the primary responsibilities of an information security professional is to plan and prepare for a security event. Any number of events from malware on a desktop to a distributed denial of service attack can cause an interruption to a business operation. In the midst of an event, the cybersecurity incident response team must work quickly and effectively to address the threat. The CSIRT must make quick decisions and actions to minimize the impact of an event. With the average cost of a data breach reaching $4 million in 2016, organizations have a financial incentive to take the time and resources to properly prepare for a security event (Ponemon Institute, 2016). After the security event is over, the organization must often deal with the legal repercussions including legal and regulatory investigations and litigation from any harmed individuals or companies.

Certain actions or lack of action, taken during a security incident may have some legal repercussions. Most organizations must operate under different regulatory rules including PCI, HIPAA, and FISMA. Even if the organization is not under the umbrella of a regulatory body, it will fall under various laws based on the location where it operates. While the primary goal of incident response is to remediate the situation, evidence must be handled and stored properly if prosecution is desired in the future. Indications of tampering or questions regarding the integrity of the data can hinder the chance of success in prosecution. Multiple class action suits quickly follow most large data breaches. More than 140 lawsuits were filed after the Target breach (Simmons, 2015). In general, work performed by a security team is considered normal operations and not protected by attorney-client privilege. Without this privilege, any communication or work performed by the security team can be used as evidence in a legal proceeding. With proper planning, some security work performed under direction of counsel can be protected. The legal considerations discussed are focused on the United States. Some international laws and regulations are included only as they pertain to U.S. companies. Organizations outside the U.S. should research local laws and regulations when creating a CSIRP.

Bryan Chou, bnchou@live.com

2. Legal and Regulatory Bodies

The explosive growth of computers and e-commerce has raced ahead of laws and regulations. There have been numerous attempts to pass comprehensive cybersecurity legislation but "nothing of value has passed" (Sotto, 2015). Although some cybersecurity laws have been passed, "Congress is lagging on issues related to cybersecurity" (Chowdhry, 2016). Instead, a patchwork of rules issued by Congress, federal agencies, industry groups, and states has developed over time. The federal government passed the 1996 Health Insurance Portability and Accountability Act (HIPAA), 1999 Gramm-Leach-Bliley Act, and the Federal Information Security Management Act (FISMA) as part of the 2002 Homeland Security Act. Those three acts cover information security and privacy requirements for health information, financial information, and government agencies, respectively. Some government agencies have determined that certain cybersecurity issues fall under their purview. For example, the Federal Trade Commission (FTC) "has filed more than 60 lawsuits by reference to its authority under s. 5 of the FTC Act to protect consumers against unfair and deceptive practices by companies (Santarcangelo, 2016). Many states have passed their own legislation, which creates many challenges for companies that operate in multiple states. "Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private, governmental or educational entities to notify individuals of security breaches of information involving personally identifiable information" (Greenberg, 2016). Industry bodies and other non-governmental organizations provide their own regulations. The Payment Card Industry (PCI) provides detailed requirements for any organizations that handle cardholder data. There are even restrictions for U.S. companies that do business in the European Union (EU).

The CSIRP must consider these laws and regulations when written. The laws and regulations will often define sensitive or protected data and the reporting requirements in the case of a data breach. The CSIRP needs to include this information so that the CSIRT knows when notification is required. Failure to follow the prescribed process can often result in fines or other penalties. The CSIRT must know and understand the reporting

requirements and include them in the CSIRP. It should include the following information, at a minimum:

- applicable law or regulation,
- data breach trigger,
- person or organization to contact, and
- information to include in reporting requirements.

The following sections cover some of the more common laws and regulations affecting organizations. This is not an all-inclusive list. The pertinent laws and regulations will vary depending on the industry sector, types of data processed and stored, and business locations.

2.1. HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 included a provision for the Secretary of Health and Human Services (HHS) to publicize standards for the electronic exchange, privacy, and security of health information. The "Standards for Privacy of Individually Identifiable Health Information," also known as the Privacy Rule, set national standards for the protection of certain health information. The Privacy Rule addressed the use and disclosure of individual health information, entities covered by the rules, and standards for individual privacy rights (United States Department of Health and Human Services, 2003). The Privacy Rule applies to any health plans, health care clearinghouses, and health care providers, known as covered entities that transmits health information electronically. All information protected by the Privacy Rule is commonly known as protected health information or PHI which includes individually identifiable health information including past, present, or future medical condition, treatment, or payment.

A breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the PHI (Office for Civil Rights, 2013). A breach of PHI requires notification to the affected individuals, the HHS, and the media in certain situations. If more than 500 residents from a state or jurisdiction are affected, the covered entity must notify the prominent media in the state or jurisdiction. Covered entities have 60 days to notify the individuals and media, if required. The Secretary of

the HHS must be notified within 60 days for breaches greater than 500 records. Breaches less than 500 records can notify the Secretary on an annual basis. The Privacy Rule also provides specific guidelines on the method of disclosing the data breach to all parties.

Include the following when creating the CSIRP for HIPAA data.

- Determine the number, type, and location of PHI records managed by the organization, if any.
- Identify the person or group responsible for notifying the individuals, the media, and the Secretary. This could be more than one person or group in a large organization.
- Clearly document the time requirements for notifying the individuals, media, and the Secretary. HIPAA requires notification within 60 days for data breaches over 500 records.
- Create a draft or template of the communications.

2.2. Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, removed many barriers among banks, security companies, and insurance companies. The GLBA defines financial institutions as "companies that offer financial products or services to individuals, like loans, financial or investment advice, or insurance." Under the authority granted under the GLBA, the Federal Deposit Insurance Corporation (FDIC), a U.S. corporation that insures deposits against bank failure, created the "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice." The guide requires financial institutions to have an incident response plan to address incidents of unauthorized access to sensitive customer data. The CSIRP should begin with a risk assessment so that the financial institution can create the response based on the type of breach. To meet the GLBA requirements for an incident response, the CSIRP must contain procedures for:

- assessing the nature and scope of the situation,
- notifying the primary Federal regulator as soon as possible once the organization has determined there has been unauthorized access,

- notifying law enforcement immediately in the case of Federal criminal violations,
- taking the appropriate steps to contain and control the situation, and
- notifying customers when warranted.

When an institution determines there has been unauthorized access to sensitive customer data, the affected financial institution must determine the likelihood that customer information has or will be misused. If it is determined that misuse has occurred or is likely to occur, then the customer must be notified as soon as possible. The guide explains, "The contents of a breach notification should contain the following elements:

- a general description of the incident and the information that was the subject of unauthorized access;
- a telephone number for further information and assistance;
- a reminder "to remain vigilant" over the next 12 to 24 months;
- a recommendation that incidents of suspected identity theft be reported promptly, and;
- a general description of the steps taken by the financial institution to protect the information from further unauthorized access or use" (Johnson, n.d.)

The guide defines sensitive customer information as "customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account."

The timeframe for notifying affected parties is significantly shorter under the GLBA than allowed under HIPAA. The incident response plan should reflect the shorted timeframe.

Include the following when creating the CSIRP for financial data.

- Determine if the organization is a financial institution as defined by the GLBA.
- Determine the number, type, and location of any sensitive customer information managed by the organization.

Bryan Chou, bnchou@live.com

- Build a relationship with contacts at the primary financial regulator and law enforcement. The contact information should be included in the CSIRP.
- Identify the person or group responsible for notifying the individuals.
- Identify the person or group responsible for contacting the financial regulator and law enforcement.
- Create a draft or template of the communications.

2.3. FISMA

The Patriot Act of 2002 included the Federal Information Security Management Act (FISMA). Whereas HIPAA covered health care information and GLBA covered financial institutions, FISMA covers the federal government. "FISMA… explicitly emphasizes a risk-based policy for cost effective security" (NIST, 2016). The National Institute of Standards and Technology (NIST) is responsible for developing the security standards, guidelines, and processes for federal agencies to secure their systems. NIST created "Computer Security Incident Handling Guide" to provide guidance federal agencies and other organization on how to handle a security incident.

In the event of an incident, a federal agency must notify and consult with US-CERT regarding the information and information systems. The notification requirements of an incident by a federal agency are significantly more stringent under FISMA. Federal agencies must report any security incidents to the United States Computer Emergency Readiness Team (US-CERT) within one hour of identifying the security incident (US-CERT, 2016).

Security professionals working in a federal agency will need to make sure their incident response plan meets the requirements under FISMA. The "US-CERT Federal Incident Notification Guidelines" provides detailed steps for notification and assessment of a security incident. The CSIRP should include those steps and the information that must be included with the notification. With only one hour to notify, there will be little

time to research and determine the proper course of action in the middle of a security incident.

2.4. PCI

The Payment Card Industry (PCI) is an organization formed by American Express, Discover Financial Services, JCB International, MasterCard, and Visa. The PCI Council agreed to the Data Security Standards (DSS), which specifies the requirements for protecting cardholder data. All organizations involved in the processing of payment cards must meet PCI DSS requirements.

Requirement 12.10 states that an organization will "Implement an incident response plan. Be prepared to respond immediately to a system breach" (PCI Security Standards Council, 2016). The CSIRP must include communication and contact strategy including, at a minimum, notification of the payment brands. PCI DSS does not specify any additional parties that must be notified. However, other parties that should be notified include customers and third party vendors involved in the payment process. PCI DSS is not prescriptive when it comes to the method of communication of the timeline.

Companies that must follow PCI DSS should consider the following.

- Identify the cardholder data environment (CDE). The smaller the CDE, the less area to protect.
- Identify all the locations of any cardholder data.
- Document the contact information for all payment brands, card processors, and any third parties that process or store cardholder data.

2.5. State Privacy Laws

State governments have acted to protect their citizens by passing their own cybersecurity laws. Except for Alabama, New Mexico, and South Dakota, all the states and the District of Columbia has some kind of local data security or privacy law. Businesses that operate in multiple states must know the breach laws in place for each locality. In-house counsel will generally not have expertise in all the states. Local counsel, especially in the case of a breach, should be consulted to make sure that the local laws are followed.

Bryan Chou, bnchou@live.com

The CSIRP must consider the notification laws for each location in which it operates. The state laws will vary with respect to whom must comply with the law, what constitutes personal information, what constitutes a breach, and who must be notified. From a planning standpoint, the most arduous task is to collect the requirements for each state and keep up to date on any changes. Counsel should be consulted to ensure compliance with applicable laws.

The key items to consider for any organization that does business in the U.S. include:

- keeping a list of states and jurisdictions where the organization operates,
- working with counsel that has expertise on the local data protection and privacy laws, and
- documenting the notification laws and privacy laws for each applicable state in the CSIRP.

2.6. Privacy Shield

The European Union (EU) has very different approaches to privacy and data protection compared to the United States. The 1995 Data Protection Directive and the 2002 E-Privacy Directive cover data protection and privacy for the EU. The Data Protection Directive will be superseded by the General Data Protection Regulation starting May 25, 2018. In contrast, the privacy and data protection laws in the United States are based on industry segments and type of data. As discussed earlier, HIPAA covers medical information, GLBA covers financial institutions, and FISMA covers federal agencies. States have their own privacy and data protection laws. Furthermore, the approach to developing privacy differs greatly. In the U.S., "the starting point for any discussion of privacy rights…begins with the question of how it will affect business. The Europeans… began their rule-making discussion four years ago with an understanding that privacy is a human right." (Lazarus, 2015). The Data Protection Directive of 1995 allowed U.S. companies to collect data on European citizens if they met certain privacy standards. This voluntary program was known as Privacy Safe Harbor. In November 2015, Maximillian Schrems v Data Protection Commissioner invalidated Privacy Safe Harbor because the National Security Agency (NSA), an intellence organization in the

United States, was engaged in espionage. The Privacy Shield framework was developed by the U.S. Department of Congress and the European Commission to replace Privacy Safe Harbor. Privacy Shield created a way to meet EU data protection requirements when personal information of European citizens is transferred to the U.S. The new program has additional controls but still does not address the issue with NSA spying. For this reason, many companies have not rushed to join Privacy Shield (Wright, 2016).

Privacy Shield includes seven principles for protecting personal information: (1) notice, (2) choice, (3) accountability of onward transfer, (4) security, (5) data integrity and purpose limitation, (6) access, and (7) recourse, enforcement, and liability. These principles are designed to protect the personal data of EU citizens when the data is transferred to the U.S. Privacy Shield does not have any notification guidelines on who needs to be contacted and how quickly in the case of a data breach. Despite the absence of specific guidelines, the CSIRP still needs to include procedures for notifications in the case of a data breach.

3. Collecting Evidence

Preservation of evidence is required if an organization plans to pursue prosecution after a security incident. The top priority during a security incident is to contain and remediate the situation. However, steps taken during and after the security event can preserve the evidence for prosecution. Electronic forensic data can be used for prosecution under certain circumstances. Forensic science is the application of identifying, collecting, examining, and analyzing data. One of the objectives of forensic science is to preserve the integrity of the data while maintaining a strict chain of custody. The use of forensic science will primarily occur after the security incident has been contained and remediated. Preparing and planning during the creation of the CSIRP will help preserve the evidence.

3.1. Prosecuting Cybercrime

If there is a possibility for prosecution after a security event, CSIRP should contain specific steps for preserving the integrity of the data and documenting the chain

of custody. Law enforcement should be contacted to improve the chances of prosecution. The "Computer Security Incident Handling Guide" states "one reason that many security-related incidents do not result in convictions is that some organizations do not properly contact law enforcement" (Cichonski, Millar, Grance, & Scarfone, 2012). Some organizations will collect their own evidence during the security incident, hand it over to law enforcement, and wait for prosecution. Even if the data's integrity is perfectly maintained, there is the question of the chain of custody. To make an analogy to the physical world: prosecuting a murder requires collecting evidence from the crime scene. The property owner could collect all the evidence and hand it over to the police. However, that would raise serious questions about the evidence that would make prosecution difficult. Similar rules apply to the digital realm. The Federal Rules of Evidence was codified in 1975 and provides rules on the admissibility of evidence. The authenticity of the evidence must be established for it to be admissible. Engaging law enforcement will help establish the chain of custody of the evidence and reduce the risk of inadmissibility of the evidence in court.

There are many law enforcement organizations that can assist with the investigation process such as the FBI, Secret Service, district attorney office, and local law enforcement. The organization should build relationships with the law enforcement organizations prior to an incident.

The CSIRP should consider the following to engage law enforcement:

- criteria to report an incident to law enforcement and which law enforcement agency,
- identify the individual responsible for making the final decision on whether or not to contact law enforcement,
- identify the primary point of contact for working with law enforcement which may or may not be the same as the decision maker,
- law enforcement contact information, and
- procedure for reporting the evidence, which will vary depending on the law enforcement agency.

3.2. Collecting Evidence

Electronic evidence collected for the purposes of prosecution must show the integrity of the data and the chain of custody. The NIST 800-86 publication, "Guide to Integrating Forensic Techniques into Incident Response," provides detailed information on establishing forensic capability. The document focuses on forensics on PCs, but the forensic techniques works for other types of systems such as servers, tablets, and smart phones.

Per the NIST 800-86 document, the basic phases of forensics are collection, examination, analysis, and reporting (Kent, Chevalier, Grance, & Dang, 2006). The integrity of the data and the chain of custody can be preserved by following the forensic process. The phases are each briefly described below:

- Collection – Data is identified, labeled, recorded, and collected.
- Examination – Forensic tools and techniques are used to identify and extract relevant information from the collected data.
- Analysis – Analyzing to the results of the examination to answer the questions that initiated the forensic examination.
- Reporting – The final report from the analysis of the data.

Chain of custody must begin in the collection phase. Keeping a log of everyone that had physical custody of the data, the actions performed, and the date and time is a necessity. Everything should be documented, such as, notes, pictures, and all actions taken. The data should also be stored in a secure location. There is some evidence, such as logs from the ISP that is best gathered by the law enforcement agency. Counsel should be consulted to determine when to go to law enforcement for evidence.

During the security incident, sometimes a decision will be made to continue monitoring the attacker rather than cut them off. The objective of this action is to collect additional information about the attacker. For example, the attacker can be redirected to a sandbox to limit the damage while monitoring the sandbox activity. This decision must be made carefully because if the organization knows a system has been compromised and lets the attack continue, the organization can be held liable if the attacker uses the

compromised system to attack someone else (Cichonski, Millar, Grance, & Scarfone, 2012).

To maintain the integrity of the data, examination should be performed on copies only. A write blocker prevents any changes to the original media when taking a copy for examination. A message hash should be taken of the original data using the write blocker to avoid changing any data. After making a copy, a message hash should be taken of the duplicate and compared to the original. Being able to verify and maintain the integrity of data is critical to using the evidence for prosecution.

4. Attorney-Client Privilege

Litigation following a data breach has been increasing. Gibson Dunn partner Alexander Southwell stated, "Often very quickly following an incident or breach there is litigation which brings substantial expense and potential for exposure" (Preserving Privilege Before and After a Cybersecurity Incident (Part One of Two), 2015). Attorney-client privilege can be used to protect the legal analysis before and after a cybersecurity breach. Attorney-client privilege is a "client's right privilege to refuse to disclose and to prevent any other person from disclosing confidential communications between the client and the attorney" (Garner, 2014). The judicial system established privilege to allow free and open communication between attorney and client without fear of ramifications. In order to establish attorney-client privilege, the organization must separate regular operational tasks and legal analysis. If the work is performed under the direction of an attorney, it is called work product privilege and may be protected by attorney-client privilege. Most tasks performed by IT and the CSIRT are considered normal operational tasks and would not be privileged.

The Target data breach provided precedence for privilege for cybersecurity activities. On October 23, 2015, a Minnesota district court found that some documents created in the post-breach investigation were protected by attorney-client privilege and work product privilege. The Target case "is one of the first cases we are seeing in the data breach context where the privilege issue has been tested," said Michelle A. Kisloff, a partner at Hogan Lovells (Target Privilege Decision Delivers Guidance for Post-Data

Breach Internal Investigations, 2015). After the data breach, Target launched two investigations using the Verizon Business Network Services. One investigation was non-privileged and performed on behalf of the card brands. The other investigation was privileged and launched to educate the Target lawyers so they could provide legal advice in anticipation of litigation.

4.1. Planning for Privilege

Planning must be performed prior to the incident to establish privilege. Counsel must be involved in the planning of the CSIRP. Counsel cannot only be invited to the team and attend meetings. To establish privilege, the counsel must be intimately involved in the entire process. Counsel should be guiding and directing the actions of the team. The technical team cannot run the investigation under the direction of management and copy counsel on the final report. Superficial involvement is not sufficient to maintain privilege. Some IT operational activities cannot be separated. However, specific activities that need to fall under privilege should be established under the guidance of counsel. Counsel can be involved to ensure that security controls meet regulatory requirements and that the company has reasonable security measures in place. The CSIRT should consult and work closely with counsel to prepare for privilege in the case of a data breach.

Jeff Kosseff, assistant professor of cybersecurity law at the United States Naval Academy, provided these tips for maintaining privilege:

- Engage cybersecurity resources through external counsel.
- Contracts should be between counsel and the cybersecurity resource.
- Contract should state that the work is being performed to get legal advice. If services are procured after an incident, the contract should state the work is in anticipation of litigation.
- Counsel should be the point of contact, not IT or the CIO.
- Counsel should be included in every email or communication that involves the company and the cybersecurity consultant.

- Emails and communication should have "Attorney-Client Privilege/Confidential" at the top of every page. Other deliverables should have "Attorney Work Product" at the top of every page. Do not overuse this designation or the case of privilege will weaken.
- Counsel should direct the work of the cybersecurity consultant.
- Be careful about sharing data with third parties especially vendors that may be the root cause of the data breach.
- Limit access of the information to those that really need to know.
- Educate all employees on privilege.

4.2. After an Incident

Preserving privilege is a major concern when evaluating risks of post- breach litigation. Counsel should be engaged immediately in the case of a security incident. It is much easier to go from privileged to non-privileged than vice versa. The planning phase is critical to make sure privilege is preserved. One of the first steps in the CSIRP should be to contact counsel. This will give counsel the opportunity to direct actions and provide legal counsel.

Communication protocols following a breach should be established. Right after a breach, members of the CSIRT are prone to speculate on the cause and impact of the breach. The most damaging communications usually come from this period because of incomplete information. Communication should lean toward more phone calls and face-to-face meetings and less emails and written communications. Written communication and emails can be turned over during the discovery process. Since there is no documented record of phone calls or face to face meetings, they cannot be turned over during discovery.

5. Conclusion

The primary objective of a CSIRP is to identify, contain, and remediate a security incident. The job of the security professional is to secure information and ensure business continuity. When a security incident occurs, the CSIRT is focused on getting

the business back to normal operations. However, there may be legal ramifications from the security incident. Proper planning is needed to adequately address the legal issues.

Every organization must follow a maze of laws and regulations. Federal and state laws and agencies have issued regulations. Industry groups have added even more regulations. All the laws and regulations should be researched and understood during the planning phase of the CSIRP. If prosecution is desired, then chain of custody and data integrity must be maintained. Law enforcement should be engaged to increase the chances of successful prosecution. To protect data gathered during the security incident, attorney-client privilege should be invoked.

Most importantly, throughout the planning and during the security incident, counsel should be consulted to ensure that all legal ramifications are considered and understood.

6. References

Chowdhry, A. (2016, Jan. 28). *Congress needs to catch up on cybersecurity issues*. Retrieved from The Business of Federal Technology: https://fcw.com/articles/2016/01/28/johnson-cyber-hsgac.aspx

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide*. National Institute of Standards and Technology.

Garner, B. A. (2014). *Black's Law Dictionary* (10th ed.).

Greenberg, P. (2016, Jan. 4). *Security Breach Notification Laws*. Retrieved from National Conference of State Legislatures: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Jarrett, H. M., Bailie, M. W., Hagen, E., & Judish, N. (2009). *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. Department of Justice, Computer Crime and Intellectual Property Section. Office of Legal Education.

Johnson, D. (n.d.). *Data Security & Customer Notification Requirements for Banks*. Retrieved from American Bankers Association: http://www.aba.com/tools/function/technology/pages/datasecuritynotification.aspx

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response*. National Institute of Standards and Technology.

Kosseff, J. (2016). Preserving the Privilege During Breach Response. *RSA Conference 2016*. San Francisco.

Kral, P. (2011, Dec. 5). *The Incident Handler's Handbook*. Retrieved from SANS Reading Room: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

Bryan Chou, bnchou@live.com

Lazarus, D. (2015, Dec. 22). *Europe and U.S. have different approaches to protecting privacy of personal data*. Retrieved from Los Angeles Times: http://www.latimes.com/business/la-fi-lazarus-20151222-column.html

NIST. (2016, Aug. 25). *Detailed Overview*. Retrieved from National Instititue of Standards and Technology: http://csrc.nist.gov/groups/SMA/fisma/overview.html

Office for Civil Rights. (n.d.). *Breach Notification Rule*. Retrieved from United States Department of Health and Human Services: https://www.hhs.gov/hipaa/for-professionals/breach-notification/

PCI Security Standards Council. (2016). *Requirements and Security Assessment Procedures*. Payment Card Industry.

Ponemon Institute. (2016). *2016 Cost of a Data Breach Study: Global Analysis*.

Preserving Privilege Before and After a Cybersecurity Incident (Part One of Two). (2015, June 17). Retrieved from The Cybersecurity Law Report: http://www.cslawreport.com/article/48

Santarcangelo, M. (2016, Dec. 6). *Why security leaders need to embrace the concept of reasonable security now*. Retrieved from CSO: http://www.csoonline.com/article/3147628/leadership-management/why-security-leaders-need-to-embrace-the-concept-of-reasonable-security-now.html

Sotto, L. J. (2015, May 20). *The Challenge of Coordinating the Legal and Security Teams in the Current Cyber Landscape (Part One of Two)* . Retrieved from The Cybersecurity Law Report: http://www.cslawreport.com/article/49

Target Privilege Decision Delivers Guidance for Post-Data Breach Internal Investigations. (2015, Nov. 11). Retrieved from The Cybersecurity Law Report: http://www.cslawreport.com/article/121

United States Department of Health and Human Services. (2003). *Summary of the HIPAA Privacy Rule*. Office for Civil Rights.

US-CERT. (2016). *US-CERT Federal Incident Notification Guidelines*. Retrieved from US-CERT: https://www.us-cert.gov/incident-notification-guidelines

Wright, B. (2016, Oct. 24). Turmoil in European Data Privacy Law. *STI Professional Lecture Series*.

Bryan Chou, bnchou@live.com

Last Updated: November 30th, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Essentials Australia 2021	**Melbourne, AU**	**Feb 15, 2021 - Feb 20, 2021**	**Live Event**
SANS OnDemand	**OnlineUS**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**