THE SILENT KILLER: HOW REGULATORY COMPLIANCE HAS WORSENED THE STATE OF INFORMATION SECURITY

INFORMATION IN THIS CHAPTER

- Regulatory Compliance Telemetry
- Transborder Data Flow Restrictions
- ISO Security Standards
- Health Insurance Portability and Accountability Act (HIPAA)
- Family Education Rights and Privacy Act (FERPA)
- Payment Card Industry Data Security Standard (PCI DSS)
- North America Electric Reliability Corporation: Critical Infrastructure Protection (NERC CIP)

Introduction

The cornerstone of information security is made up of three fundamental principals called the CIA Triad; confidentiality, integrity, and availability. Confidentiality is the prevention of disclosure of sensitive information to individuals not authorized to view the information. Integrity is the ability to guarantee that data have not been modified without the proper authorization. Availability is the ability to guarantee that one with the proper credentials has uninterrupted access to data. The similarities across all these core concepts revolve around data. More importantly, these have been around for well over 20 years. In the security community, these are security 101s at a very high level and a lot has changed in the last 20 years in terms of the threat landscape and the ability for someone to access data 24 hours
a day no matter what geography they are located in. Additionally, with almost everything being connected via the Internet, we have seen the development and enforcement of regulatory compliance in terms of security controls placed on organizations. Best practices, which we like to call best efforts or checkbox security, have and will continue to place organizations at risk in terms of being targets for cybercrime, insider threat, or corporate/industrial espionage to name a few. This is important as we go over the various types of regulatory compliance and best practices that our industry has developed and enforced. As we transition into the next generation Internet, which is highly collaborative and connected, it will affect the way in which we protect and control sensitive data.

Regulatory Compliance Telemetry

When someone mentions regulatory compliance, the first thing that comes to mind is the Payment Card Industry Data Security Standard (PCI DSS). Unfortunately, we never hear the stories of how the great PCI DSS was effective in stopping sensitive information from going into the wrong hands. What we do hear are the shortcomings of corporations that have been hacked and have lost thousands of client records that have passed a PCI audit. Does this mean that PCI DSS is ineffective? No, it is important to note that a PCI audit is a point in time marker on having all the proper security controls in place, but unfortunately the threat landscape is dynamic and constantly changing at such a rapid rate that although all the proper controls are in place, the bad guys will always find a way in. It is important to realize that almost every country has its own set of regulatory compliance. The top industry verticals that typically have to adhere to compliance standard are governments, financial institutions, defense industrial base, health care, retail, electric and utilities, and education. If you search hard enough, you will find some form of compliance or standards around information technology. Before we cover regulatory compliance, let us discuss transborder data flow restrictions.

Transborder Data Flow Restrictions

Transborder data flow is typically a term used when talking about the transmission of data outside a country’s border. This is common in a lot of countries and will continue to mature as many companies are continuing and will continue to expand
their business presence globally. One could imagine that when the European Union (EU) was being formed the participating countries would have to share data some of which is sensitive for government and business purposes. The EU has implemented Directive 95/46/EC to insure the protection of data that need to be transferred electronically out of country borders.

This specific directive addresses eight core principals that are enforceable to any of the countries that have to transmit data.

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant, and not excessive
4. Accurate
5. Kept no longer than necessary
6. Processed in accordance with the data subject’s rights
7. Secure
8. Transferred only to countries with adequate protection

The directive lays out a very concise and enforceable framework for information sharing. However, in the event that one is in violation of the directive, they can receive fines and even prosecution. Just recently, the Ministry of Justice in the United Kingdom was reported by SCMagazine on the validity of Directive 95/46/EC. This is a great point since the Directive was implemented in 1998 and according to the Lord McNally “We want to gather evidence and views on whether the current data protection laws are working in light of social and technological changes since the mid-1990s.” This brings up a great point and as technologies change, so must the policies that govern the protection of data. However, it is important to note that transborder data flow restrictions govern the handling of data period. This goes beyond specific industry vertical regulatory compliance like PCI DSS. As Lord McNally pointed out, Web 2.0 has brought in a new era of information sharing and collaboration with the introduction of social networking and the proliferation of Web-based email. These technologies have continued and will continue to challenge the countries that have to enforce Directive 95/46/EC. The eight core principals in Directive 95/46/EC are straightforward and easy to comprehend. However, number 8 that deals with “Transferred to countries with adequate protections” is one that is going to be challenging to enforce with the emergence of Web 2.0. We have been approached

regarding many what-if scenarios by certain industry verticals that have to comply with Directive 95/46/EC. The typical what-if scenario usually deals with the use of Web mail when the internal corporate email server is unavailable and their employee has time constraint on getting an email out. Instead of waiting for the corporate email sever to come online, the employee decides to use his or her personal Web-based email account. Depending on the type of information being sent, the employee might have breached several internal data security policies, but more importantly, if he or she is using Gmail, that email might be sitting on a server in California. Although the employee had good intentions, in terms of Directive 95/46/EC, he or she might have violated the directive placing not only oneself but also the corporation one is working for in a compromising position. Now, there are technologies that can reduce this risk on the market, which we will discuss at the end of the book; however, this what-if scenario has been reported to us so many times that it is likely that this does happen and with the emergence of Web 2.0 it is only going to become much more of a greater issue to defend. As we mentioned, many countries have their own transborder data flow restriction and procedure to handle that flow into other countries. The United States Department of Commerce has developed what is called the “Safe Harbor Framework,” which has been acknowledged by the EU’s Directive 95/46/EC in order to share information outside the EU to the United States. The Safe Harbor Framework is different from that of Directive 95/46/EC because it is self-regulated by the businesses that want to certify themselves in order to be within compliance of the Directive 95/46/EC.

The following are the seven core elements of the Safe Harbor Framework:

“NOTICE: An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party(1).

CHOICE: An organization must offer individuals the opportunity to choose (opt out) whether their personal information
is (a) to be disclosed to a third party(1) or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

For sensitive information (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt-in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive.

ONWARD TRANSFER: To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.

SECURITY: Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

DATA INTEGRITY: Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data are reliable for their intended use, accurate, complete, and current.
ACCESS: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual’s privacy in the case in question, or where the rights of persons other than the individual would be violated.

ENFORCEMENT: Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by noncompliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual’s complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow-up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.”

The Safe Harbor framework addresses what is deemed adequate by the EU directive in order to transmit data across borders. By following various security best practices set forth in ISO/IEC 21007:2005, CobIT, and ITIL, a corporation can self certify that they are in compliance with the EU directive. However, attaining these best practices is costly and does not always equate to a risk-free environment but is a great step in the right direction.

ISO Security Standards

The ISO standards are very clear on a lot of topics they cover in terms of policy, common security risk, protection of critical information, and many more to name a few. What they are not clear in articulating is the controls used to mitigate common infrastructure threats. The predecessor of ISO 21007, ISO 17799

http://www.export.gov/safeharbor/eu/eg_main_018475.asp
discusses the need to protect against malicious code and the need to apply the appropriate controls necessary for protection. Looking through the lens of checking the box, one could conclude that anti-virus is all that's needed in terms of checking the box. This is not to say that the ISO standards are wrong; they pulled together an incredible framework, have to remain vendor agnostic, and have to convey a technical polythetic approach in their recommendations for security controls. The interruption of the ISO standards rests on the security team in terms of the solutions they prescribe that will allow a corporation to be in compliance with the ISO security standards. As a security expert and having worked for technology companies that make security products, I have learned that all security products are not created equally. The security gaps that many products introduce and broad claims for coverage range from general to in-depth. That is why most security frameworks will cover many controls that provide reasonable protection. In closing, transborder data flow restrictions are not commonly discussed among the security industry as PCI DSS, HIPAA, and other regulatory compliance, but as businesses continue to expand their footprints into other geographies, transborder data flow restrictions will be another layer of defense that will either compliment or complicate your current IT security deployments.

**Health Insurance Portability and Accountability Act (HIPAA)**

Depending on what industry you are covering, you are likely to find a set of regulatory compliance that govern the protection of sensitive data. The health care industry has the HIPAA. This governs the protection of IT systems that contain protected health-care information (PHI). There is a vast amount of controls that deal with authentication, access, encryption, and transmission of PHI to name a few. There have been only a handful of cases prosecuted under HIPAA that it leads to speculation that either the controls are implemented well or violations are not being reported. The most noted HIPAA violation dealt with employees trying to access former President Bill Clinton's medical records at Columbia Presbyterian Medical Center. They were able to trace that 17 individuals tried to access his records and all of them were suspended.

The penalties for violating HIPAA can range from 100 to 250,000 USD in fines and up to ten years in prison. The HIPAA security guidelines are crisp and concise as they cover physical
and logical security. However, just like the ISO standards, they suggest the appropriate controls; HIPAA states the following: “implementation of reasonable and appropriate security measures also supports compliance with the privacy standards, just as the lack of adequate security can increase the risk of violation of the privacy standards.” This is pretty straightforward and left to a lot of interpretation. Reasonable and appropriate security measures are in the hands of those who interpret the HIPAA guidelines. The bottom line really comes down to the cost of security, as some solutions are economically cheaper than others. One might conclude that open source security is reasonable and appropriate. It is not that uncommon to see open source security being used in the health care vertical; we have come across many organizations that have augmented their vendor security solutions with open source security as a secondary line of intelligence and defense, and to be clear, we have never seen organizations totally relying on open source security as their primary compensating control.

Family Education Rights and Privacy Act (FERPA)

FERPA covers the handling of student personal identifiable information (PII). This information can range from student transcripts, SSN, contact information, and grades that are disclosed to the institution that is governed by FERPA. The Family Policy Compliance Office has the right to audit any school that has to comply with FERPA and if it is not in compliance, it can face the termination of receiving federal money. In terms of security controls, the FERPA act is fairly high level in pointing out what types of sensitive data need to be protected. It does not go into the details of the technologies needed to comply with the act. Although FERPA is enabled to protect student information and confidentiality, it can be overruled by the U.S. Attorney General under the Patriot Act in the event that a foreign student is suspected or engaged in terrorist activities. There are many cases involved where hackers have penetrated universities and have stolen student SSN along with other data that would fall under the PII blanket. This has led to some universities changing their system from tracking their students by SSN to another numbering scheme. This is not a trivial task for most educational institutions but aids in one last place for someone to harness your identity.

4 www.hipaasolutions.org/documents/HIPAAEnforcementUp-Date-2008.pdf
Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard is by far the most popular regulatory compliance discussed among security professionals. Additionally, it is one that we often read about in the Wall Street Journal and other magazines when a retail company’s security has been breached. The main objective behind PCI DSS is the safeguarding of credit card transactions and information. What separates PCI DSS from HIPAA and FERPA is that the regulatory requirements regarding the security controls are spelled out.

The following is an outline of the 12 requirements of PCI DSS:

**Build and Maintain a Secure Network**

**Requirement 1.** Install and maintain a firewall configuration to protect cardholder data

**Requirement 2.** Do not use vendor-supplied defaults for system passwords and other security parameters

**Protect Cardholder Data**

**Requirement 3.** Protect stored cardholder data

**Requirement 4.** Encrypt transmission of cardholder data across open, public networks

**Maintain a Vulnerability Management Program**

**Requirement 5.** Use and regularly update anti-virus software

**Requirement 6.** Develop and maintain secure systems and applications

**Implement Strong Access Control Measures**

**Requirement 7.** Restrict access to cardholder data by business need-to-know

**Requirement 8.** Assign a unique ID to each person with computer access

**Requirement 9.** Restrict physical access to cardholder data

**Regularly Monitor and Test Networks**

**Requirement 10.** Track and monitor all access to network resources and cardholder data

**Requirement 11.** Regularly test security systems and processes

**Maintain an Information Security Policy**

**Requirement 12.** Maintain a policy that addresses information security”

These requirements are very specific in what they are trying to address, and to a high level, they are just as clear as other

---

5https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
regulatory compliance for other industry verticals. The difference with PCI DSS is that they not only point out high-level Requirements, but are also very clear on the compensating controls that are necessary in protecting cardholder data. For example, Requirement 11.4 clearly states the need for either an intrusion detection system or an intrusion prevention system and Requirement 6.6 clearly states the need for a Web-application firewall. In outlining the specific technologies that are needed as compensating controls, it is a much different approach than we see with FERPA, HIPAA, and other security frameworks that we mentioned earlier in the chapter. This is not to say that those regulatory compliance and security frameworks are inefficient. In terms of PCI DSS, one might think that it is too specific in certain areas of the 12 requirements necessary for protecting cardholder data. There could be a lot of controversy spun up around Requirement 11.4 as it refers to the use of either an intrusion detection system or an intrusion prevention system. Although the specific technology serves the same purpose, the way in which they are implemented can have a dramatic effect in the level of security efficacy as one is detecting and alerting whereas the other is preventing and alerting. In terms of time to protection in eradicating data loss, it might not be such a bad idea to place this specific technology in prevention mode. In terms of being PCI compliant in using an intrusion detection system as noted in Requirement 11.4, you have definitely provided the capability to be notified in the event that a vulnerability or exploit has been triggered, but by the time you take any corrective measure against the attacker the damage has already been done. The authors also realize that some organizations might not be comfortable with in-line technologies such as intrusion prevention systems; however, the rate at which information can be lifted from your network is too high not to leverage prevention capabilities in any of the technologies related to PCI DSS. This really leads to the question of why we hear about so many examples of organizations that are PCI compliant but get breached. It is important to understand that regular audits occur for organizations that have to be compliant with PCI. These audits are really a point-in-time check of the implementation of all 12 requirements. A lot can happen between audits in terms of shifts in the attack landscape, introduction of new technologies, and upgrades to the IT infrastructure. Playing armchair quarterback without having all the proper information at your disposal, it is very easy to get caught up in the failures of PCI DSS. Additionally, the cost of doing
security is not cheap, which could lead to decisions based on economics, and what is deemed reasonable from a security perspective is a risk that some security professionals are willing to take.

There are many cases that deal with the loss of cardholder data and the cost to the organization just in legal fees and fines can range in tens of millions of dollars. This does not include the brand damage associated with these highly publicized breaches. In some of these cases, the institution that was processing cardholder data just recently passed a PCI audit. Again, it is very important to realize that PCI DSS is a point-in-time audit and unfortunately with the sophistication of the cybercriminals to date, they will continue to find ways into your network. The most important key to take away regarding PCI DSS is that if you have the opportunity to place your technologies in prevention mode, you will significantly decrease the chances of your organization becoming a statistic. The following use case illustrates what can happen even though the organization has passed a PCI DSS audit. We have seen the impact.

**North America Electric Reliability Corporation: Critical Infrastructure Protection (NERC CIP)**

The North America Electric Reliability Corporation just recently started implementing the critical infrastructure protection guidelines. What PCI DSS is to the retail industry, NERC CIP is to the electric and utilities industry. These are a set of revelatory guidelines that address nine areas that are specific in terms of providing policy, education, auditing, reporting, and security compensating controls, to name a few. These guidelines are relatively new and are currently being enforced across all the electric utilities within the United States. The ability to gain control of an electric utility's infrastructure has been proven and reported on in the last decade. The stakes are much higher from a cyber security level due to the nature of a cyber attack on an electric utility. These specific outcomes are probably not the targets of your average cybercriminal but are certainly within reach of state and nonstate sponsored activity. Unlike PCI DSS, the security requirements in NERC CIP are at a very high level. An example is given below:

*CIP-005-2 R1 Electronic Security Perimeter—The Responsible Entity shall ensure that every Critical Cyber Asset resides*
within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).\(^6\)

The goal here is to provide access control and segmentation to a critical cyber asset (CCA). Again, like most of the best practices and regulatory compliance that we have mentioned in this chapter with the exception of PCI DSS, they fail to define an electronic security perimeter. This is important because this leads to a lot of different interpretations and types of technologies that could be considered in deploying an electronic security perimeter. In our research, we have found many third-party organizations that define the electronic security perimeter as deploying a firewall, UTM, and intrusion detection system. Although these are great compensating controls and best practices within any IT infrastructure, they lack the ability to prevent an attack. Protection of critical structures needs to go above and beyond adequate and reasonable security controls. The need for preventive and intelligent security solutions needs to be called out within the guidelines so that there is no ambiguity in terms of what needs to be deployed in protecting critical infrastructure. This is not to say that these specific guidelines are wrong or misguided. What they lack, in the authors’ opinion, is the level of detail in quantifying the electronic security perimeter. As we have mentioned throughout the entire book, advanced persistent threats, which we are calling out as subversive multivector threats, are real and extremely sophisticated and require preventative and intelligent solutions that minimize risk associated with these types of attack vectors that are common in this specific industry vertical.

**Summary**

In this chapter, we covered at a very high level, transborder dataflow restrictions, IT security best practice frameworks, and some of the well-known regulatory compliance. The security compensating controls that are mentioned throughout most of this chapter hinge on frameworks that are high-level, adequate, and reasonable for the purpose of protecting the access, authentication, and transmission of sensitive data. Adequate and reasonable security controls are left to the interpretation of those implementing the security. What is adequate and reasonable to a seasoned security professional is often much different for

\(^6\)www.nerc.com/files/CIP-005-2.pdf
someone who has less time in the security industry. This is not to say that someone with the appropriate certifications and less experience will recommend a far less superior solution. In terms of economics, having best-of-breed security is extremely costly and might limit one's ability to architect and deploy a solid security solution. In terms of security frameworks and regulatory compliance that are very specific on the type of technologies that an organization must deploy, the requirement may go above and beyond adequate and reasonable security. As we pointed out earlier with PCI DSS Requirement 11.4, the security team has a choice between deploying an intrusion detection system or intrusion prevention system. These technologies are very similar in terms of detecting well-known vulnerabilities and exploits. However, one provides a lot more protection in terms of preventing a system from being compromised. Cybercriminals are well aware of all the security frameworks, best practices, and regulatory compliance of the target organization they are trying to steal information from. The silent killer within all the regulatory compliance we discussed in this chapter is the interpretation of what is adequate and reasonable security by the individuals who are deploying the various solutions to be in compliance. Additionally, corporations that treat security as a checkbox and fail to go above and beyond will be drastically limited in their ability in providing reasonable safeguards to protect their critical assets. At the end of the book, we provide insight and technology recommendations that address the next generation security best practices.

**References**


