SP
Securing the Payment Card Industry

Secure Payments Magazine, Q1, 2009

ROGUE WAVE

by Chris Mark *CPISM/A, CISSP, CIPP*

Recent data compromises have continued to illustrate the challenges of securing data in an increasingly hostile environment. Companies are faced with securing and protecting their valuable information from a growing number of increasingly sophisticated and organized groups determined to steal valuable data. Historically, the response to data compromises has been to pass and enforce increasingly strict standards, regulations, and laws detailing the specific steps companies must take to protect data and the required disclosure should data be compromised. Those companies that are the unfortunate victims of data thieves are criticized and vilified for 'losing data.' In spite of the efforts being focused upon compliance with the various laws and standards, data compromises continue their steep upward trend seemingly unabated. Programs such as the Payment Card Industry Data Security Standard (PCI DSS) and the state breach notification laws are often touted as the panacea of data protection. The various standards and laws are valuable tools but, like any tool, they provide limited value and must be employed in a broader strategy of risk management to adequately protect data. Without a comprehensive strategy to identify risk and employ the required controls to counter such risks, companies will continue to experience breaches of sensitive data.

DOCTRINE, TACTICS, AND STRATEGY

Doctrine is defined by Webster's dictionary as "a principle, or position, or the body of principles in a branch of knowledge or system of belief." [1] As stated in Anker's article Doctrine for Asymmetric Warfare, "Doctrine should succinctly express the collective wisdom about how US Armed forces conduct military operations." [2] In 1923, historian J.F.C. Fuller wrote that "...the central idea of an army is known as its doctrine, which to be sound must be principles of war..." [3] Doctrine explains how we expect to operate and act based upon past experiences and with the anticipation of what lies ahead. As stated in Anker's article, doctrine, "Provides a link between research, theory, history, experimentation and practice; Encapsulates a body of knowledge and experience so it can be applied; Provides common understanding and a common language, which allows us to articulate clearly and succinctly what (forces) should accomplish." [4] In a very real sense, organizational policies reflect the organizational doctrines to which the organization should adhere.

TACTICS

Tactics, in the military sense, refers to how units are employed during combat. In a business sense, tactics can be defined similarly as "how resources are employed in support of a defined strategic objective." Ignoring for a moment the term "strategy," tactics are the short term decisions and deployment of resources to accomplish a specific objective. Consider for a moment that the objective is to protect a website from network layer attacks originating from the Internet. A tactic that could be employed is to install and configure a network layer firewall in front of the webserver. Another tactic that could be employed would be to ensure that the webserver was hardened appropriately and all necessary patches were installed. As stated in Ancker's article, tactics consist of three interrelated aspects: 1) "..the creative and flexible array of means to accomplish assigned missions"; 2) "decision making under conditions of uncertainty when faced with an intelligence enemy"; 3) "understanding the human dimension - the effects of combat on soldiers." [5] While #3 is specific to the military aspect, #1 and #2 are clearly applicable to business and information security.

STRATEGY

While used with great frequency in business and in the military, the concept of strategy is often discussed, yet difficult to define. Depending upon the context, strategy can be defined somewhat differently. In a 1996 Harvard Business Review article, Michael Porter argues that strategy is "about being different" and adds, "it means deliberately choosing a different set of activities to deliver a unique mix of value." [6] In Top Management Strategy, [7] the term strategy is defined as "the framework which guides those choices that determine the nature and direction of an organization." The military genius Carl Von Clausewitz defines strategy as "the practical adaptation of the means placed at a general's disposal to the attainment of the object in view."[8] Evaluating each of the provided definitions in the context of the Payment Card Industry leads one to the conclusion that, while PCI DSS may be a doctrine to be accounted for within strategy, it is not, in itself a successful strategy for data protection.

PCI DSS AS DOCTRINE

Using the definitions provided in this article, standards such as the PCI DSS can be more accurately categorized as 'doctrines' to guide deployment as opposed to comprehensive data protection strategies. While the PCI DSS is a valuable tool and has certainly raised the overall security of the Payment Card Industry to levels previously unseen, the value of the standard, or any standard, is limited. The belief that adhering to a checklist of controls prescribed 'by the book' is a dangerous strategy that has caused more than one company to be surprised by an adversary who has read the same book and acted in a manner to counter the controls prescribed in the doctrine. Compliance with the PCI DSS, or any standard for that matter, does not constitute an effective strategy for adequately securing data or managing risk. Rather it constitutes a process of blindly following doctrine which is often mistakenly thought of, and promoted, as strategy. As stated by Anker:

"To the degree that doctrine becomes overly prescriptive, it becomes irrelevant. Worse, it instills a penchant for proceeding by the book whether warranted by the circumstances or not." He additionally states: "Those who expect doctrine and tactics, techniques, and procedures, to provide solutions and checklists

Copyright 2009 by The Society of Payment Security Professionals

for action are soon disabused of that notion during actual operations."

The PCI DSS is a standard that is owned by the PCI SSC. The PCI SCC promotes the believe that the PCI DSS represents the "best" method of protecting cardholder data. As stated in the PCI SSC Statement on Malware:

"The PCI SSC believes that the best way to protect cardholder data that is stored, transmitted, and processed is by implementing the PCI DSS and remaining in full compliance." [9]

It is interesting that there is no mention of risk analysis or a comprehensive risk mitigation strategy only a focus upon compliance with the standard. The guidance provided by the PCI SSC is simply to implement controls according to "the book." The challenge with this thinking is that the tactics employed by criminals to access and steal data are dynamic while the PCI DSS is relatively static. Both of these points are supported by the PCI SSC. In a document title Ten Common Myths of PCI DSS, published on the PCI SSC website, Myth #4 states:

"PCI WILL MAKE US SECURE"

Successful completion of a system scan or assessment for PCI is but a snapshot in time. Security Exploits are non-stop and get stronger every day, which is why PCI compliance efforts must be a continuous process of assessment and remediation to ensure safety of cardholder data." [10]

In spite of the fact that it is recognized that the security landscape is ever changing, the PCI SSC has opted for a 24 month life cycle on the standard. As stated in the PCI SSC's "Lifecycle Statement":

"...PCI security standards balances the need to evolve to face the challenges of a rapidly changing landscape with the need for constancy. With that in mind, the Council is implementing a 24 month life-cycle review and change process."[11]

In recognition of a landscape that is "ever changing" it is difficult to envision how complying with a prescriptive, static standard that may be outdated by 24 months represents the "...best way to protect cardholder data that is stored, transmitted, and processed..."

The PCI Security Standards' statement on Malware, for example, released on April 29th, 2008 states that:

"Adhering to the Standard provides protection against hackers installing malware such as a 'sniffer' in order to capture and access data without being detected."

In the subsequent sentence it states that the "..best way to protect cardholder data.." is through the implementation of the standard. It is unfortunate that many companies that read these statements may have been led to believe that compliance alone would have protected them from the malicious software attacks that have been the cause of several of the largest compromises in history. In fact, a major card brand appears to support implementing controls that go beyond those stated in the PCI DSS. The Visa Data Security Alert dated October 6, 2008 states:

"Although key loggers can be difficult to detect, the following best practices should be utilized..." Six suggestions are provided including the implementation of heuristic technology: "...(if) available on an organization's anti-virus product, enable it to detect unknown malware."

This is an interesting statement. The card brand concedes that there is malware that is not currently known or even identifiable except through heuristic technologies. In fact, Visa provides a list of MD5 signatures for previously unknown malicious software for organizations to use in their detection efforts. As the only card brand that has taken the step to truly offer guidance to protect data, this is laudable. It could be argued however, that this position contradicts the stated positions of the PCI SSC. For companies that were adhering to the strict controls outlined in the PCI DSS, they could certainly be considered compliant with the standard and but not be adequately protected.

In yet another Visa Data Security Alert dated June 19, 2008 there is another recommendation provided that is not required by the PCI DSS. Under recommended mitigation strategies for Packet Sniffing it states:

"While not required by the PCI DSS, consider encrypting transmission of sensitive data to protect and render 'sniffed' data unreadable."

Finally, in another alert related to malicious software there are recommendations to implement both a network based Intrusion Detection System (NIDS) as well as a Host Based Intrusion Detection System (HIDS). The PCI DSS only requires the implementation of either a network based intrusion detection system, or a host based intrusion detection system but not both. This recommendation goes beyond that which is required by the PCI DSS.

SUMMARY

In summary, while standards such as the PCI DSS are good tools that can be employed to raise the overall security of an industry, they do not represent comprehensive methods of risk management or data security. It is important to understand the limitations of such standards, as well as their uses. Understanding the limitations of these standards provides a better perspective for creating a comprehensive information security strategy that will address both compliance and real data protection.

CHRIS MARK *is a CPISM/A Trainer and co-founder of the* SPSP.

Copyright 2009 by The Society of Payment Security Professionals

REFERENCES

[1] http://www.merriam-webster.com/dictionary/doctrine

[2] Ancker, C.J. Doctrine for Asymmetric Warfare; Military Review; July-August 2003

[3] J.F.C. Fuller, The Foundations of the Science of War(Fort Leavenworth, KS: U.S. Army Command and General Staff College Press, 1993), 254, Reprinted from the original 1926 edition

[4] Ancker

[5] Ancker

[6] Competitive Strategy (1986). Michael Porter. Harvard Business School Press.

[7] Top Management Strategy (1980). Benjamin Tregoe and John Zimmerman. Simon and Schuster.

[8] Carl Von Clausewitz, On War, Book Two, On The Nature of War, chap.6

[9] https://www.pcisecuritystandards.org/pdfs/04-28-08_malware_statement.pdf

[10] https://www.pcisecuritystandards.org/pdfs/pciscc_ten_common_myths.pdf

[11] https://www.pcisecuritystandards.org/pdfs/pci_security_standards_council_statement_on_Lifecycle_Statement.pdf

All materials contained on this site are protected by United States copyright law and may not be reproduced, distributed, transmitted, displayed, published or broadcasted without the prior written consent of the Society of Payment Security Professionals, Aegenis Publishing, or in the case of third party materials, the owner of that content. You may not alter or remove any trademark, copyright or other notice from copies of the content.

The material may be downloaded from the Secure Payments Archive Page (one machine readable copy and one print copy per page) for your personal, noncommercial use only provided that you (a) keep intact all copyright and other proprietary notices, (b) make no modifications to the Content, and (c) do not use the Content in a manner that suggests an association with any of our products, services or brands.

Without limiting the generality of the foregoing, you may not distribute any part of this Service over any network, including a local area network, nor sell or offer it for sale. In addition, these files may not be used to construct any kind of database.

All trademarks, service marks, trade names, and trade dress are proprietary to us and/or our licensors or licensees. We may change the Society of Payment Security Professional Sites or delete Content or features at any time, in any way, for any or no reason.

Copyright 2009 by The Society of Payment Security Professionals