Management — An Achilles Heel of Information Assurance Security: A Case Study of Verizon’s Data Breach Reports

Pedro A. Diaz-Gomez¹, Alfonso Valencia Rodriguez², and Luis E. Gomez H.²
¹Computing & Technology Department, Cameron University, Lawton, OK, USA
²Ingenieria de Sistemas, Universidad Piloto de Colombia, Bogota, Colombia

Abstract—As society becomes increasingly interconnected electronically and new avenues for getting data and information become available, the assurance and security of data and information in businesses are more critical, not only as a legal requirement or business compliance, but also as a responsibility to customers and as a first step in pursuing business continuity. Attacks on data and information are a continual threat, but it has been shown that basic countermeasures can detect some of those at early stages of penetration or misuse. This paper focuses on managerial principles that help organizations prevent security breaches on data and information, and it presents a systemic view of Information Security Management.

Keywords: Data breach, information assurance, information security, security management.

1. Introduction

Every year, security institutions like Verizon and FBI report data breaches, and security recommendations in order to prevent and/or mitigate information assurance/security incidents [1], [2], [3], [14], [15], [16], [17]. The goal of this paper is to highlight those recommendations that are simple to implement and could have the potential to address many data breaches (See Section 3). At the same time, the basic recommendations proposed in this paper could be seen as steps in the ladder of quality improvement suggested by managerial principles. The information assurance/security management system of planning, doing, evaluating and updating as a continuous process must be present [5], [18].

The basic controls that appear in this article do not pretend to minimize the security problem organizations face nowadays. Attackers of computer resources are developing new techniques that allow sophisticated penetrations and anti-forensics [16], [17]. In response, security policies, procedures, standards and computer and network countermeasures have been proposed; however, a fault in management has allowed computer penetrations to permeate organizations without notice for hours, days, months and even years [15], [16], [17].

The order of this paper is as follows: Section 1.1 summarizes the Payment Card Industry Security Standards (PCI), Section 2 presents the Verizon Security Standards (PCI), Section 2 relates to the analysis of the statistics presented, Section 4 describes the information assurance/security management system, Section 5 proposes security architecture in a systemic way, Section 6 proposes basic controls, and Section 7 presents conclusions.

1.1 The PCI Security Standards

PCI security standards are private and mandatory for institutions and their partners that offer electronic card payment. Not being compliant overcome monetary sanctions or revocation of service and loss of prestige [13].

PCI security standards are general and simple, which does not mean easy to implement and/or maintain. Ultimately one of the most important PCI mandates is to maintain a policy that addresses information security for all personnel. Security policy is the road map of data and information assurance/security, and all personnel must be committed to it (see Section 4). A security policy for an organization belonging to the pay card industry must begin by including the PCI security standards, which could be summarized as physical security, backups and encryption of data, security mechanisms like firewalls and antiviruses, tracking and monitoring, the develop and maintenance of secure systems and applications, and the regularly testing of them. PCI is proposing a proactive approach through security testing of computer systems, applications, networks and security mechanisms that can anticipate the discovery of vulnerabilities and weaknesses that could be re-mediated depending on the risk and benefit/cost of countermeasures.

2. Statistics Verizon

This paper has focused its analysis in the reports provided by Verizon because those reports reflect forensic investigations of security data breaches. It is not an easy task to find consistent data about violations of information security [6], or statistics presented in a consistent way as Verizon does.

As the Verizon Team points out, their study is focused on real data breaches, not network activity, attack signatures, vulnerabilities, or public disclosures. It needs to be emphasized that the economic sectors presented in Verizon’s reports are those in which Verizon has done investigations, and those are probably not a statistical sample carefully selected to make inferences that could be applied to other organizations. However, communities can learn from such experiences, or, unfortunately the bad experience of others.
Verizon’s statistics are presented in this paper following the Five W’s: what, who, where, when, and why, + one H how.

2.1 What Organizations & # of Records

Table 1, that represents the percentage of breaches by sector analyzed by Verizon from 2004 to 2010, shows a steady rate around the 30th percentile for the financial sector and an increase in breaches for retail and hospitality in the 2008 - 2010 period. However, it seems this is not the result of an increase in the number of breaches to targeted organizations, but most likely of opportunistic attacks, as shown in Table 2, left half. Targeted organizations are those the attacker first chose and then attacked. Opportunistic organizations are those in which the attacker first finds or knows a weakness or vulnerability and thereafter decides to attack, exploiting the vulnerability [14], [17].

2.2 Who Made and Who Discovered

Table 3 shows the categories of penetrators: External which corresponds to hackers and malware; Internal, which corresponds to employees, independent contractors and interns with some privileges; Business Partners, which corresponds to third parties who share some kind of business relationship, like vendors, suppliers and customers; and Multiple Parties, which corresponds to multiple agents like employees in coalition with external parties. It is clear the External category is the one prevalent in all periods presented (See Table 3 for statistics with no intersections, and Table 4 with percentages that overlap, i.e., a data breach committed by more than one agent is counted in more than one category). Table 5 shows who discovered the data breaches. The Internal category which discovers fewer breaches, has two subcategories: active that includes countermeasures in place to detect intrusions, and passive that includes detections that occur as a matter of happenstance.

2.3 Where Data Breaches Occurred

Table 6 shows where data was compromised. Servers corresponds to data available in places like online databases, files or authentication/directory information on servers; User Devices include laptops and workstations; Off-line Data includes resources like backup tapes; People was included in the 2010 report because information can be stolen directly from people [16]; and Networks includes network devices like routers.

The category of servers has been the one that prevails in all the periods presented, but the category of user devices has increased from 7% in 2004 – 2007 period, to 56% in 2010.

2.4 How Data Breaches Occurred

Table 7 shows how data breaches are performed. Hacking corresponds to techniques that involve penetration of systems without authorized credentials; Malware is unauthorized code that is injected in computers in order to compromise or harm information assets; Privilege Misuse corresponds to authorized users who misuse their privileges; Physical relates to intrusions on physical facilities in order to steal computers or information assets; Social Tactics is the use of social engineering in order to commit a penetration; and Error is the category of human error or omission.

Human error was the highest category in the period from (2004 – 2008), followed by hacking, malware, privilege misuse, physical and social tactics with corresponding averages.
that suffered data breaches and are or are not PCI compliant. The year that shows the lowest compliant percentage with PCI is 2010, and at the same time, 2010 has one of the higher percentages of opportunistic organizations attacked. It can be inferred that the opportunity to commit a data breach (See Table 2, left part), as well as the ease of its commitment (See Table 8), can certainly be among the causes of data breaches.

3. Analysis

It is important to talk primarily about statistics as presented in percentages. The reader has to take into account that the percentages of one year or period give different numbers of cases [6]. For example, in 2009, there were 141 breaches, and in 2010 there were 761 breaches investigated [17]. If a statistic shows, say 10% in 2009, that would be 14.1, but in 2010, that would be 76.1. The other issue to take into account is that usually, as statistics are presented, percentages constitute more than 100% because of intersections. For example, Table 6 shows where data breaches occurred, but certainly a data breach could compromise more than one asset.

Retail and hospitality, as well as financial organizations, suffered a higher percentage of data breaches than other organizations (See Fig. 1 where 2008 shows the statistics from 2004 to 2007, and 2011 is the report of statistics corresponding to 2010 [14], [17]). Financial records with debit and credit card information have been appealing to attackers because of their easy conversion to money. However, the way the black market moves and/or later prosecutions that took place could make them look at other venues of data and information assets like authentication credentials (log-in and passwords), personal information (social security numbers, date of birth, name, address), and intellectual property [17].

Certainly there are specific targeted organizations, but the majority of attacks happen because attackers found or knew a weakness and/or a vulnerability (See Table 2, left part). The size of the organization is irrelevant as long as there is something to exploit. However, as table 11 shows, organizations of small and medium size (those from 11 to 10,000 employees) are the ones that have suffered higher percentages of data breaches.

Summing up column Simple & Cheap as in Table 9, and finding the average, gives 58.0% of simple and cheap countermeasures that could be applied for preventing data breaches. This result is conservative when compared with

<table>
<thead>
<tr>
<th>Year</th>
<th>Simple &amp; Cheap</th>
<th>Intermediate</th>
<th>Difficult &amp; Expensive</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>04 – 07</td>
<td>52%</td>
<td>28%</td>
<td>17%</td>
<td>3%</td>
</tr>
<tr>
<td>2008</td>
<td>53%</td>
<td>34%</td>
<td>10%</td>
<td>–</td>
</tr>
<tr>
<td>2009</td>
<td>64%</td>
<td>32%</td>
<td>4%</td>
<td>–</td>
</tr>
<tr>
<td>2010</td>
<td>63%</td>
<td>33%</td>
<td>4%</td>
<td>–</td>
</tr>
</tbody>
</table>

Table 7: How Data Breaches Occurred.

<table>
<thead>
<tr>
<th>Year</th>
<th>Hacking</th>
<th>Malware</th>
<th>Privil. Misuse</th>
<th>Physical</th>
<th>Social Ins</th>
<th>Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>04 – 07</td>
<td>59%</td>
<td>31%</td>
<td>22%</td>
<td>15%</td>
<td>10%</td>
<td>62%</td>
</tr>
<tr>
<td>2008</td>
<td>64%</td>
<td>38%</td>
<td>22%</td>
<td>9%</td>
<td>2%</td>
<td>67%</td>
</tr>
<tr>
<td>2009</td>
<td>40%</td>
<td>38%</td>
<td>48%</td>
<td>15%</td>
<td>28%</td>
<td>–</td>
</tr>
<tr>
<td>2010</td>
<td>50%</td>
<td>49%</td>
<td>17%</td>
<td>29%</td>
<td>11%</td>
<td>–</td>
</tr>
<tr>
<td>Ave.</td>
<td>53.25%</td>
<td>39.0%</td>
<td>27.25%</td>
<td>17.0%</td>
<td>10.25%</td>
<td>–</td>
</tr>
</tbody>
</table>
the 85% of mitigation that can be addressed with the top four mitigation strategies proposed by the Australian Government Department of Defense [4] (see Section 6).

Tables 3 and 4 show the principal agents of data breaches. No expert view is needed in order to infer that the highest threat is external. Table 6 shows where data breaches occurred; usually, the two sides of the communication (servers and user devices) are the ones with higher percentage of data breaches. However, it is important to see a shift of data breaches occurring from Servers to User Devices.

Table 10 shows the time elapsed between point of entry and containment. The time from the point of entry to compromise is usually quick; the majority take place in less than a few days. The majority of discovery and containment take place during weeks and months, and a few during years (See Figure 2). A bit atypical was 2009 with one digit percentages in discovery and containment in minutes [14], [15], [16] (See Table 10).

The interested reader can look at Figure 2 [17], which shows the time slots for 2010, as in Table 10, and graphically describes the pattern stated previously. What one can infer is that there is not a straight relation when looking at columns.

For example, if one looks at columns minutes and hours, one can say that 47% of breaches took minutes and hours from point of entry to compromise, and of that 47%, fewer than 1% were discovered in minutes and 4% were discovered in hours. Of that 47%, fewer than 1% were contained in minutes and 11% were contained in hours. However, if just fewer than 5% were discovered in hours, how many fewer than 12% were contained in hours or less? In other words, if 4% was discovered in hours, how could it be that 11% is contained in hours? Certainly some discrepancies can be inferred, but one cannot miss the lesson taught in Figure 2: from the point of entry to compromise time is fast, but from compromise to discovery, as well as containment, could take weeks, months or years.

4. Information Assurance & Security Management System

Sections 2 and 3 reported a lack in management in preventing data breaches. Facts like the discovery of data breaches by third parties and, that the ones discovered by internals are mostly by chance; that the majority of data breaches discovered take months and that the majority of containment take weeks; and, that the application of the majority of countermeasures are simple and cheap are
spot lights that corroborate a lack in management in the information assurance process.

Assurance and security of information is an integral component of any business. It must be originated from the CEO and Executive Officers, and it must permeate the entire hierarchy of the organization [11], [18]. A commitment from shareholders guarantees resources to carry out the information assurance system; and well defined processes with responsibilities and accountability to stakeholders, guaranties its success.

Figure 3 suggests a quality improvement spiral of planning, doing, controlling and updating as a continuous system to help in addressing the lack of management as stated previously. The spiral can be seen along its concentric path or following the arrows [7]. For example, the Vision & Mission is framed in Law & regulation. Changes in one process could affect all other processes (see Section 5). Looking in the arrow direction, Strategic Planning is framed in the Vision & Mission. Likewise, Security Policies are framed in Strategic Planning. The spiral suggest a domino effect. Changes occurring in one process affect other processes.

The spiral shows an out-circular approach, where the big picture is in its center, and it spreads out detail processes. Processes permeate all along the spiral. However, at each out ladder, the process is refined or redefined based on the previous process and on the stage it is on. Each “ring” gives a specific level of abstraction.

Training & Education are part of the systematic process of information assurance and security. It is common to think that the use of security mechanisms is enough, but part of the system is the human factor [9], [19] (see Section 5).

Quality Control is the checking process. Contingency & Recovery plans, and Security Mechanisms are tested, implemented and validated; based on the metrics defined, Operations take Assessment data that is used to produce Quality Improvement Reports. These reports are analyzed, looking at higher risks, so actions can be taken through Maintenance in order to minimize risks.

5. Security Architecture as Systemic Approach

Figure 4 proposed by Whitman [19] gives another view of Figure 3. The core is Data & Information, i.e., it is the asset to assure and secure. On the left part are People. On the right part is Technology; that includes media to access data and information like Systems, Networks, and the Internet, as well as assurance and security mechanisms like Access Controls, Encryption and Backups [19].

Figure 4 shows an interconnected net between processes and security mechanisms proposed by the authors. A systematic approach (see Section 4) is suggested: for example, Law & Regulation could affect security mechanisms like Monitoring (at different levels), and/or it could affect other processes like Security Policies.

Data and information are intangible assets [11], and technology has made them available in places that do not necessarily belong to the organization; so the idea to access data and information through networks and computer systems that belong only to an organization, does not always hold. Figure 4 (dash points) suggest some risks to data and information: People [9], [18], the interconnection to the Internet [12], and vulnerabilities in networks, systems and applications. However, Processes, and Security Mechanisms must be in place to help mitigate those risks.

5.1 Security Mechanisms

Security mechanisms are countermeasures that help to protect data and information. Figure 4 shows some examples which are mandatory for the Pay Card Industry like firewalls, encryption, backups and access controls.

Monitoring is a process quite related with quality control (see Section 4). Based on metrics previously defined, monitoring alerts deviation from “normality” and/or “misuse”. Processes like intrusion detection systems, revision of logs, auditing and certifications can be considered part of monitoring.

Firewalls are security mechanisms standard de facto that help to protect networks and systems monitoring internal and external traffic. Their importance is established by being gate keepers to access data and information that could implement secure protocols like IP Security (IPSec) [12]. Categories of firewalls range from packed filtering devices to application level firewalls like application servers. In the chain of security mechanisms, Patches & Upgrades, Encryption, Backups and Access Controls close the loop of protecting one of the most valuable assets in organizations: data and information.

6. Recommendations

Information assurance security is a systematic system that must focus on continual quality and improvement. Security
mechanisms like the ones proposed by PCI (interested readers can look at [10]) are one step on the ladder of this system (see Sections 4 and 5). Once security mechanisms have been implemented, maintenance and monitoring are a must. This step is probably an Achilles heel of information assurance security; a huge percentage of organizations are not compliant at the time of a breach (See table 2, right part), the opportunity of being attacked is on the rise (See Table 2, left part), and the discovery of data breaches is accomplished by third parties (See Table 5).

This paper accentuates that organizations with simple and cheap countermeasures, like the top four mitigation strategies found by the Australian Government of patching operating systems and applications, the assignment of least privilege, and the prevention of malware [4], plus monitoring of events logs, passwords, firewalls configurations, anti-viruses, physical and logical accesses, backups, and the encryption of sensitive data, could avoid or at least make data breaches more difficult (See Tables 8 and 9 concerning the difficulty of data breaches and countermeasures).

7. Conclusions

This paper summarizes data breaches investigated by Verizon from 2004 to 2010, following the guidelines of the Five W’s + one H, focusing on basic countermeasures that can be on place to mitigate them and proposing a systemic view of security management.

The PCI security standard is focused on the protection of card-holder data, which is the way information assurance/security should be addressed in the protection of the most valuable institutional assets: data and information [8]. However, data and information are intangible assets, and as such they are difficult to track and secure. The definition of who is the owner, who is the custodian, who is the user of data; as well as the data baselines and the countermeasures to protect them, are part of the management of information assurance/security. Data and information is stated here as the overall information resource of organizations: that includes users, employees, financial, technical and systems data, from general in scope to a specific record or a transaction view [11]. Once each baseline has been defined, the corresponding countermeasures to protect it must be defined and implemented. This paper has highlighted the fact that basic countermeasures certainly can mitigate data breaches. Organizations have to come back to the basics: a focus on where the data is, what networks, computer systems, applications and processes access it, how to protect it, and how to guarantee that information assurance/security is a continuous improvement system; this is a direct responsibility of information security managers.

8. Thanks

Thanks to Dr. Carolyn Lindsey Kinslow and Mr. Ellis Hooley for proofreading this paper. Thanks to the University of Oklahoma (Dr. Dean Hougen at the Computer Science Department), Norman, USA, for allowing us to use computer resources.

References