Hal Berghel

PCI INSECURITY AND LIFE IN A SHADOW ECONOMY

IT Compliance Imperitives

There are a few key IT compliance imperatives that affect everyone in gaming: SOX, MICS and PCI/DSS are certainly at the top of the list. And within them all is a mission-critical security component. In this column, I'll focus on some of the high-level threats that impact PCI security because our casual analysis of media coverage suggests that the threat vector not only remains with us, but may be growing by leaps and bounds despite PCI security.

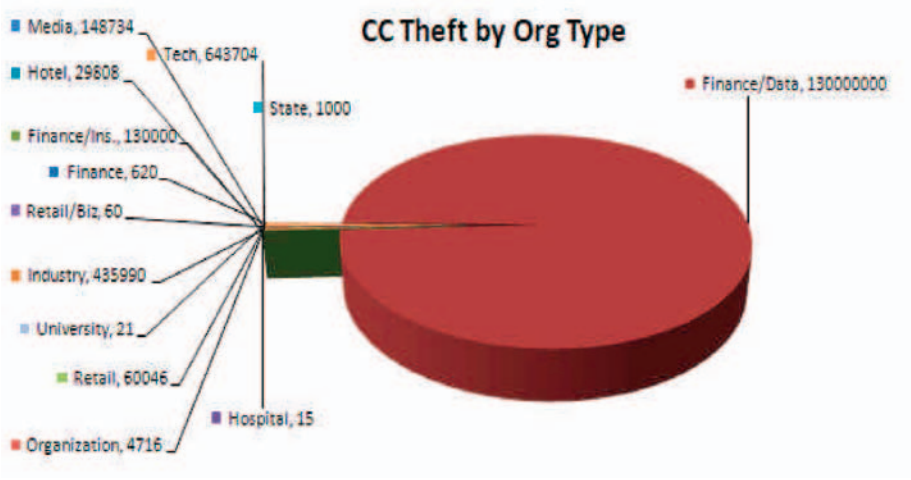

Figure 1: Breakout of Credit and Debit Card Theft by Industry Source. Source: www.itffroc.org. (Artwork by Colin Izumo)

The Payment Card Industry Data Security Standard is a relatively new program in digital security. The first version, PCI DSS 1.0 was released by the Payment Card Industry Security Standards Council (https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml) only as far back as September 5, 2006! (The latest release, version 1.2, was announced October 1, 2008.) In the world of digital security, this is a newbie.

The motivation was "to minimize the "merchant-based vulnerabilities [that] may appear almost anywhere in the card-processing ecosystem, including point-of-sale devices; personal computers or servers; wireless hotspots or Web shopping applications; in paper-based storage systems; and unsecured transmission of cardholder data to service providers. Vulnerabilities may even extend to systems operated by service providers and acquirers, which are the financial institutions that initiate and maintain the relationships with merchants that accept payment. (Source: PCI SSC "Quick Guide" - https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf). And toward that end, it has been very effective. However, as we shall soon see, PCI DSS only deals with the most visible aspect of credit and debit card vulnerability. It doesn't have much effect when upstream data stores in financial institutions leak like a sieve.

Let me illustrate with a few examples. Our Identity Theft and Financial Fraud Research and Operations Center (itffroc.org) routinely collects media reports of credit/debit card compromises. During 2009, we posted reports and news links that covered 300,000,000 compromised credit/debit cards. In just one exploit in August, 2009, 130,000,000 credit cards were stolen! The breakout of the source of these compromises by industry appears in Figure 1.

Note the small percentage of compromises under the "retail/business", pure retail, and hotel categories. This strongly suggests that the PCI DSS is working - very well, in fact. However, it didn't prevent the larger risks to 300,000,000 card holders. The security chain is only as strong as its weakest link.

Another interesting data point is the breakout of the compromise of personal information by organization type (see Figure 2). Note in this case, that the financial and data processing industries aren't even the largest source of leakage. In fact, in 2009 the largest source was government - that's right, the beneficiaries of our tax dollars.

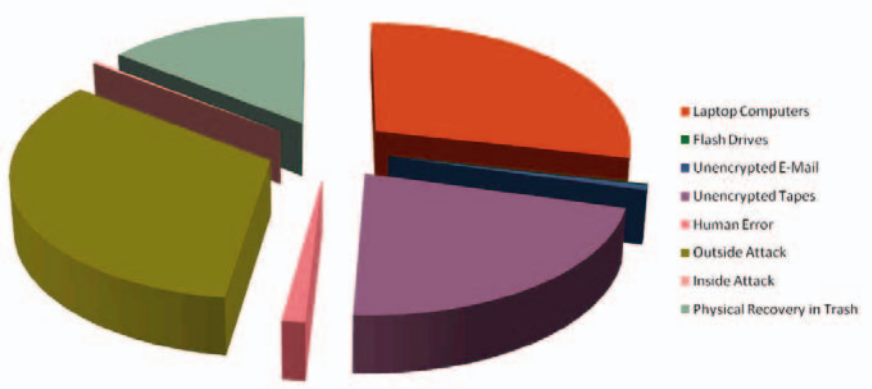

Figure 2: Breakout of Personal Information Leaks by Type of Organization. Source: www.itffroc.org. (Artwork by Colin Izumo)

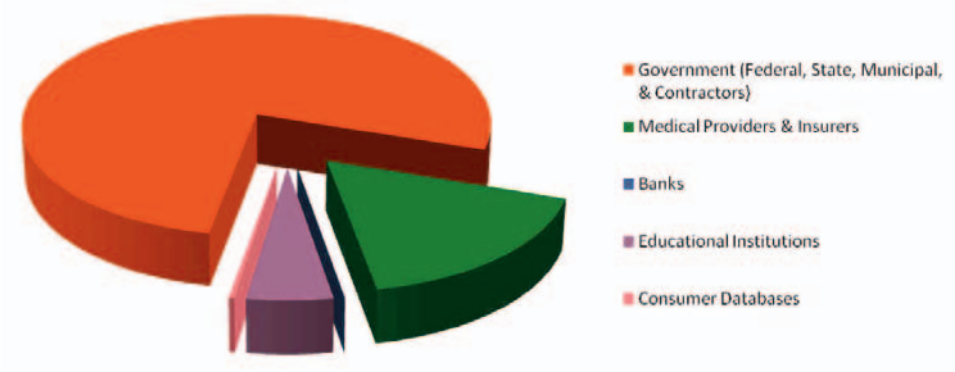

Figure 3: Breakout of Risk by Technology or Human Error. Source: www.itffroc.org. (Artwork by Colin Izumo)

	Monetary transactions	Non-monetary transactions
Illegal activities In the shadow economy	• trade in stolen goods • drug mfgr and dealing • money laundering • prostitution • gambling • smuggling • counterfeiting • credit/debit card fraud • identity theft • hacking • industrial espionage • tax evasion	• barter economy • smuggling • theft • software piracy • media piracy
Legal or quasi-legal activities In the shadow economy	• "check cashing" culture • wages from unreported work	• trade of services • do-it-yourself work

Table 1: "Not everything is Illegal in Shadow Economies." Adapted from Schneider and Enste, "Shadow Economies: Size, Causes and Consequences", Journal of Economic Literature, March, 2000.

Figure 3 compares by source of exposure. We observe here that computer notebooks, unencrypted tertiary storage, external attacks (e.g., hacking) and good old-fashioned dumpster diving lead the pack.

Life in the Shadow Economy

The infamous Nigerian 419 Scam taught the IT community a lot about the shadow economy. This scam dates back to the 1980's. It's a variation on the 15th century "Spanish prisoner's dilemma," whereby the dupe is lured into investing front money for a share of a much larger sum that will accrue once the prisoner is released. (If you're interested in more information, see my column in the winter, 2008 issue of G&L.) The variation derives its name from the section of the Nigerian penal code that deals with such fraud.

What we learned from this scam is (1) that email users are a lot more gullible that one would expect, and (2) that the scammers had to have some stroke with local authorities because the source of the scam email was not that difficult to determine. Although we didn't recognize it as such, the 419 scam was really the IT professional's introduction to the inner sanctum of the shadow economy.

Table 1 provides an overview of the shadow economy landscape. This classification scheme, due to Schneider and Enste, categorizes legal and illegal activities in the shadow economy with whether they involved money. We note that the credit/debit card fraud that we discussed above falls into the illegal/monetary category.

The question naturally arises: "Just how large are these shadow economies?" Fortunately, Schneider and Enste provide information on this as well (Table 2). We note that the source of the 419 scam, Nigeria, also leads the world in terms of percentage of GDP that's shadowed. We also observe that countries that are frequently mentioned as major players in international money laundering and narcotrafficking are also high on the list.

Conclusion

The PCI DSS represents an important advance in protecting individuals from identity theft and digital fraud. The supporting evidence is overwhelming that the PCI DSS is an effective deterrent to digital fraud and identity theft within its domain. And yet, as our data shows, individuals continue to be exceedingly vulnerable to credit/debit card fraud - well after the implementation of the PCI DSS. What does this tell us?

When we looked to the sources of these vulnerabilities we found that they were outside the domain of PCI DSS. In effect, we fixed the leak in the nozzle only to find out that the hose had ruptured. But why is this surprising. The answer is that the PCI DSS focused primarily on the transaction/merchant end of the financial data recording and reporting industry. This is where an understanding of the broader shadow economy comes in. Note that the illegal/monetary quadrant of the shadow economy is technology and source neutral. That is, with a little imagination we should have been able to foresee that the entire financial data chain was equally vulnerable, and that if we plugged leaks at one end, leaks were likely to appear at the other.

It has been claimed that when John Dillinger was asked why he robbed banks he replied "because that's where the money is." The reverse analogy with regard to PCI DSS is that the reason that the transaction and merchant are no longer appealing targets is that's where the vulnerabilities aren't. The soft underbelly of the payment card industry is no longer at that end - it's the digital crypts and ossuaries that retain credit/debit card data which are much higher up in the financial food chain. Think of this as the equivalent of reversing the direction of flow in the Chicago River: it doesn't get rid of the sewage, it just sends the sewage down to Springfield for others to deal with. In order to be maximally effective, PCI DSS really should have been built into a larger security protocol - maybe as a piece of SOX or GLB. The failure lies in PCI DSS requirement 7: "Restrict access to cardholder data by business need-to-know." More specifically, the problem lies at the intersection between the IT enterprise data stores and the PCI-regulated sides of the house. From what I can tell, the largest leaks come from unregulated stores. The great challenge for the next decade will be to lock down access to cardholder data in online data stores.

In any event, the lesson learned is that effective security has to be understood in the broader context that goes beyond the immediate and parochial.

Country	%GDP	Country	%GDP
Nigeria,Egypt	70%	Tunisia,Morocco	40%
Mexico,Panama	50%	Chile,Venezuela,Brazil	30%
Thailand	70%	Philippines,Malaysia	45%
Hong Kong,Singapore	15%	Hungary,Bulg,Poland	25%
Romania,Czech	12%	Georgia,Ukraine, Azerbaijan	35%
Russia,Balkins	25%	Greece,Italy,Spain,Portugal	25%
Scandanavia,France, Holland,Germany, England	20%	US, Japan, Australia, Switzerland	10%

Table 2: "Countries with the Largest Shadow Economies" adapted from Schneider and Enste, ibid.

Hal Berghel is Associate Dean of the Howard R. Hughes College of Engineering at UNLV and Director of the new UNLV School of Informatics. He is also Director of the Identity Theft and Financial Fraud Research and Operations Center. His consultancy, Berghel.Net, provides security and management services to government and industry.

It has been claimed that when John Dillinger was asked why he robbed banks he replied "because that's where the money is." The reverse analogy with regard to PCI DSS is that the reason that the transaction and merchant are no longer appealing targets is that's where the vulnerabilities aren't.