



# Deedoc Consulting

“What will your company do about protecting against future attacks?”

Lesley Lumbu  
Vice-President of Marketing Operations  
Deedoc Consulting & Deedoc Managed  
Security Services (DMSS)

## IT Auditing Knows No Geographical Boundaries

As information technology is increasing in importance, coverage and in reliability, many businesses are now implementing IT processes, procedures, or policies in managing their technology. Whether you are a small business using Windows-based servers, or a medium-size company setting up an internal network with Cisco routers or a large corporation setting up VPN or SSH connections between different buildings or branches, there is still an immense need to manage them securely.

The importance of having proper procedures and policies that highlight managing each component of the daily tasks, as related to your IT assets, and also the protection of such assets is the most important component of your business

information technology strategy. In order to measure such policies, companies need to constantly audit themselves, and periodically have a third-party auditing firm perform evaluations on policies, procedures as a means of enhancing business functions. The importance of auditing, especially IT auditing, is crucial in preventing public humiliation, loss of client data, theft of artificial property and in some cases lack of due care in the court of law. Regardless of industry, information has become a value-added asset used for competitive advantage, thus a source of revenue. In hindsight, information equals value, which equals revenue. Losing such information will lead to loss of corporate value, loss of money, and revenue. For example, the recent

hack on Sony's PlayStation Network (PSN) in April of 2011 in which close to 100 million user accounts were compromised that lead Sony to shutdown the service in America and Europe devalued the company in terms of public relation. This could



**PLAYSTATION®Network**  
PLAYSTATION®Network

have been prevented, or at least better mitigated if processes had been in place to reduce the risk. Not so much as in prevention but more in regards to how Playstation dealt with the problem.

The combination of these two events led to Sony's largest hack since its inception. During the first week of the April Sony hack, which exposed approximately 100 million account information, a class action lawsuit was filed against Sony for failure to "encrypt data and establish adequate firewalls to handle a server intrusion contingency", failure to "provide prompt and adequate warnings

of security breaches", and delay in "bringing the PSN service back online."<sup>1</sup> Sony was also accused of violating the Payment Card Industry (PCI) security standard that prohibits companies from storing cardholder data. Sony as of their recent release cannot show evidence that credit card information were exposed to the hackers, but did not rule it out. Of the four accusations Sony is facing, three could have been prevented with proper vulnerability assessment and proper audit been performed. A specific security audit should have been performed to reduce the risk of what occurred from April 17 to 19 to test firewall rules, procedures on incidence response, and compliance to the full



PCI security standard. Sony even admitted to the fact that they failed to follow the PCI DSS. In the audit procedures published by the PCI Security Standards Council, PCI DSS requirement 3.1 states

<sup>1</sup> <http://www.informationweek.com/news/security/attacks/229402362>

“Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.”<sup>2</sup> Just by not conforming to this one requirement, Sony put 100 million customers at risk of identity theft, monetary theft, and has downgraded its reputation. It is clear that Sony failed to conduct and/or solicit an external audit on its compliance to data protection and its security infrastructure.

From America to Europe to Africa, there are preventable breaches in security that leads to loss of money. Even a bank in the Democratic Republic of the Congo faces hacking from external sources. The Central Bank of Congo was hacked in late 2010 by an unknown attacker that took down its accounting and financial system (Navision), its market trade system managed by Acumen, Microsoft Outlook, and other critical applications. The breach had occurred by the start of the business day when IT

---

<sup>2</sup> Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures Version 2.0 (pg. 28)

specialists, upon turning on their workstations, were greeted by a screen filled with insulting remarks directed at certain executives of the Central Bank of Congo. While the IT security staff attempted to discover the origin of the attack, the staff noticed that there was the destruction/deletion of files, folders, databases, servers and back-up servers. At the end of the investigation the culprit was never found, and a lot of corporate and transactional data were destroyed

with no back-up data available to restore. The company would have to restore data and information



manually, which will take time, cost money, and lose reputation in the public eye. The Central Bank of Congo would nearly have to spend between \$10 to \$25 million to reestablish and strengthen its infrastructure.<sup>3</sup> As in Sony’s case, the Central Bank

---

<sup>3</sup> “Hold up a la Banque Centrale du Congo” <<http://afrique.kongotimes.info/mobile/economie->

of Congo failed to have proper security standards, policies, controlled backup solutions, was delayed in its incidence response, and failed to have the necessary firewalls and intrusion detection/prevention systems and configurations that could have prevented the breach regardless of its source. In order to identify these failures ahead of times and before an actual security breach, an IT security audit would have been a primary source of evaluation that shows due diligence and accountability. If the Central Bank of Congo were to be sued, it would face similar accusations and fate as Sony, due to its lack of due diligence.

Regardless of company size, internet presence, geographical location, and industry, the chances of being hacked are normalized at best. Sony is a large international conglomerate with at least 100 million customers on the PSN network, while the Central Bank of Congo is a national bank in a country with a lower customer reach in the global market. Both organizations were hit with hacking attacks that struck a financial blow,

litigations, and extensive time of recovery. It begs to question, does your company fall in the same category as either Sony or the Central Bank of Congo? As a customer of similar companies, is your personally-identifiable data easily exposed to a determined hacker? Are you safe from identity theft? Does your company have proper and necessary security in place, which is compliant with industry standards? There are many questions you may ask yourself, but there is one that is proactive: “What will your company do about protecting against future attacks?” There are multiple answers for the last question, but the infrastructure of a business is determined by its governance, so I would say auditing would be a great start.

---

[technologie/economie-congolaise/hold-up-a-la-banque-centrale-du-congo.html](http://technologie/economie-congolaise/hold-up-a-la-banque-centrale-du-congo.html)>