



## Data Breaches – What is the County doing to Protect Data?

By Dr. Robert Pittman Jr.  
Chief Information Security Officer  
Office of the Chief Information Officer  
County of Los Angeles

Cyber-attacks have become increasingly sophisticated and persistent with an intent to compromise an organization's confidential and critical data based on hackers' motivation for financial, political, or other gains. During 2014, a series of mega security data breaches and cyber-attacks occurred starting with the Target breach and ending with Sony Pictures Entertainment. Attacks continued into 2015 with the recent massive Anthem Blue Cross data breach. Commercial, public and private organizations are reevaluating and strengthening their cyber defenses to fight cyber-crime, cyber-terrorism and, cyber-warfare.

The County's Information Security Program team is constantly seeking ways to mitigate risk and block malicious cyber activities that may compromise employee and constituent confidential data.

In 2004, when the Board of Supervisors' adopted the Security Program they directed the Office of the Chief Information Officer through the Chief Information Security Officer (CISO) to provide information security leadership and strategy. The CISO, with Departmental Information Security Officers' (DISO) developed a security program that focuses on people, process, and technology and now with Advanced Persistent Threats (APTs), disciplines such as Detect, Protect, and Respond must be deployed.

### ***Detect***

Employees' play a key role in mitigating threats and risks by detecting whether email is malicious or not. Legitimate looking emails may be phishing email seeking to obtain personal information or at times containing embedded cyber-attack code such as Ransomware that is designed to block access to your computer data until money is paid.

County security technologists are using various tools such as web application firewalls to detect suspicious and malicious behavior of a web application. Network monitoring systems are in place that can detect potential malicious activity such as a cyber-attack or malware software injections that are designed to damage or disable computer operations.

The CISO has developed a strong relationship with numerous agencies within the County and at the federal level whose goal are to maintain awareness of cyber-attacks and to protect data. For example, the District Attorney's Cyber Investigation Response Team, the Federal Bureau of Investigation, Department of Homeland Security, Multi-State Information Sharing Analysis Center, and the US Secret Service.

### ***Protect***

In 2007, a Security Program initiative required all laptops hard drives to have data encryption. In 2014, the Board adopted a motion from Supervisor Ridley-Thomas to expand the data encryption practice to include workstations containing confidential and or sensitive data. This action, when completed will protect critical data on 100,000 County computers.

Security Awareness is another key element of data protection. The Aberdeen Group states that security awareness training assists in changing employee online behavior and reduces the risk of a security breach by 45% to 70%. The County in partnership with Homeland Security has adopted the "**Stop | Think | Connect**" campaign, a national public awareness campaign aimed to empower citizens to be safer and more secure online by increasing the understanding of cyber threats.

Cyber awareness materials are available from DISO to increase departments' security awareness program. The CISO will soon be obtaining security awareness training content for all employees to view through the Department of Human Resources Learning Management System. Content includes basic security and privacy concepts along with more in-depth training content such as HIPAA (Health Insurance Portability and Accountability Act) security and privacy training content.

### ***Respond***

Reacting to a cyber-attack has to be quick, effective and efficient. These elements work best when there is a formal incident response (IR) processes. The County's Information Security Steering Committee has developed a formal IR process to assist the Countywide Computer Emergency Response Team (CCERT) when activated by the CISO. The DISOs lead and facilitate their respective Departmental Computer Emergency Response Team and reports back to the CISO of security-related incidents. Based on the incident severity the CISO may engage the District Attorney and federal cyber intelligence agencies.

### ***Security Program Theme for 2015 – "RICC"***

Sophisticated Advanced Persistent Threats are playing a significant role in the most recent security data breaches. To continue diligence to safeguard the County's employee and constituent data the CISO has prepared a pre-emptive Security Program strategy dealing with Risk, Intelligence, Communication, and Compliance that the County staff will focus on during 2015 and for the foreseeable future. "RICC" is defined as:

Risk a risk management approach that assesses impact to the County's business, financial, and services provided to employees and its citizens.

Intelligence gather, collate and aggregate cyber threat information from all local, state and federal cyber intelligence agencies.

Communications increase employee security awareness and encourages good cyber practices at work, home, and on mobile devices.

Compliance ensuring adoption by all employees of the Board adopted IT Security Policies.

The CISO and DISOs encourages employee involvement in RICC appreciates everyone's assistance. IT Security policies can be viewed at [www.mylacounty.gov](http://www.mylacounty.gov), or the Countywide Information Security intranet web site at <http://infosec.mylacounty.info>.