Steps to protect an organisation against an internal data leak

SOURCE: http://www.cyanre.co.za/downloads/avoid-internal-data-leaks.pdf
Cyanre, The Computer Forensic Lab | 20 April, 2016

- **Do not keep client data unnecessarily.** Manage your risk, by outsourcing the data hosting or leaving it on the client's system and arrange access by your lawyers to the client's network. You could make use of our sister company, LexTrado's **Virtual Data Rooms (VDR), Data Vault, E-discovery - or Digital Case Management platforms** to host client data in a highly secure environment. Outsource the risk and the responsibility.
- **Classify and segregate data**. Intellectual property, critical or confidential data must be kept separate from other information. If information is not classified by the user, it will end up being intermingled and access control cannot be instituted. If the data is classified and segregated, the access can be controlled and monitored. This information can also be blocked from being e-mailed. A consideration is also to use Cyanre's "Chinese Rooms ", where sensitive information is kept offsite, in a protected and encrypted environment.
- **Incident Response and Forensic Readiness Audits and Retainers This** must be put in place to ensure that when a breach occurs an organisation will be able to investigate the incident and determine who was responsible. This is coupled with the fact that an organisation must have a pre-approved IR plan in place**.** An organisation must evaluate and appoint service providers in this field prior to an incident, since this is not the type of appointment, which should be done in a crisis. Cyanre has one of the largest Digital Forensic teams in South Africa to assist you along with our Incident Response team who can assist your security team during any incident.

- **Encryption of data and communication**. All sensitive data and communication should be encrypted. In any business where employees are moving around with laptops or memory sticks it must be encrypted in the event that it is stolen, lost or forgotten in a cab, bus or restaurant.
- **Device control**, allows an organisation to flag classified information when it is copied to a external device and can also restrict employees to only use authorised encrypted external devices which can only be read by a company computer. If information is copied to these devices no other computer can read it.
- **Understand your network**, where is data kept? Where are backups stored? Who has access to the data? In many instances management does not know exactly how the IT department is managing a firm's data, e-mail or backup. You might receive an instruction from a client to destroy or delete their data, but unbeknown to you it might be in Mimecast, SharePoint or in a backup. You must also know who has the passwords or access to these storage facilities. It might be that your HR manager, IT administrator or IT technician have the password and can without your knowledge logon to your mail archiving system and read all your e-mails.
- **Exit Policy,** any person who leaves an organisation computer must be copied, preferably a forensic copy which also contains everything that was deleted and the copy kept for future reference. In many instances it only becomes know what a person did or planned to do a few months after leaving an organisation. If his laptop was given to him as a parting gift you will never know what they carried out the front door on the laptop.
- **Supplier management.** If suppliers need to work on your network, supply them with a company laptop, which is given to them every time they arrive on your premise this allows you to control what programs they have on it.
- A single **dedicated and trusted IT technician** must be the only authorised person to work on executive member's computers.
- **Monitoring of the network**. You might think that the IT department is doing their job and that you have a firewall but in very few cases are alerts from the firewall actually monitored and in fewer instances are the logs reviewed. Have a chat to Cyanre's Incident Response team to assist with this.
- **Access control.** All employees, including administrators must have their own logon credentials so that you can determine exactly who did what on the network.