Addressing emerging Information Security risks in a changing work environment：The People Factor

Kwame Manu-Antwi
Head of IT, Unilever West Africa (Ghana & French West Africa)
Kwame Manu-Antwi

CEDEP (NGO)
(1999-2000)

Ghana Telecom
(2000-2002)

Unilever
(2002 – Present)
→ Ghana Plantations
→ Unilever Nigeria
→ Unilever Ghana
→ Unilever West Africa

Key Areas
• IT Management
• Project Management
• Information Security
• Database Management
(SQL, Informix)

My Profile in ‘word cloud’

www.wordle.net
Reality Check

**Poll 1**: I am aware of my company's social Media policy

**Poll 2**: In the last 1 year I have attended an information security awareness program (course, presentation or seminar)

**Poll 3**: I have signed a confidentiality clause in my company
Work

Key Business Considerations

Businesses locates factories, offices etc based on ... 

- Business Environment (tax, laws etc)
- Political Environment (stability, immigration etc)
- Route to market – distribution, roads etc
- Resource Availability
- Economy

Work is an activity and not a place/location
Work is Changing

- 57% Geographically dispersed workforce
- 60% Interpersonal coordination - more working with more than 10 people
- 50% More matrix organisation structure
- 50% High Volume of information – More time spent in finding and reviewing
- 67% More collaboration - more than 3 years ago
So are the ways of working

More agile structures are emerging with people working on the go over corporate VPNs and not necessarily from a physical office.

Virtual workplace - Working with more people you have not met is commonplace.

Sales are recorded electronically real time from field sales force.
New Tools, Terminologies and Systems

- BYOD
- Outsourcing
- Wearable technology
- 3D printing
- Cloud Computing
- Big Data
- Android
- Social Media
- Smart phones
- Tables
- Notebooks
Top IT Trends of 2013

Green IT (e.g. Energy Efficiency)
Offshoring
Internet of things
Social Media
Agile
Big Data
Cloud Computing
Information Security
Mobile Computing (e.g. integration of mobile devices into the business - BYOD)

Credit: British Computer Security

For more on future tech and trends go to www.fwthinking.com
Snapshot of risks in the new ways of working

**Information leakage**
Information sent out of the business through emails and storage.

**Device theft**
Mobile users are often vulnerable to theft and burglary.

**Loose talk**
People give out unauthorised information at social events.

**Social media lure**
Social media enticing people to share more information against good judgement.

**Unattended devices**
Field/travelling employees can leave screens unattended.
In 2013 people related breaches went down

.. But the cost increased

Staff-related breaches have dropped significantly compared to a year ago. However, staff still play a key role in security breaches.

58% of large organisations suffered staff-related security breaches (down from 73% a year ago)

22% of small businesses suffered staff-related security breaches (down from 41% a year ago)

31% of the worst security breaches in the year were caused by inadvertent human error (and a further 20% by deliberate misuse of systems by staff)

Credit: PwC 2013
Is security awareness and behavior matching the pace?
Structure of corporate information security programs
Some short comings

- Caveat Venditor
- Budget constraints
- Attitude – Journey and not destination
- Executive Example
The People Factor

Negative Behaviours
Left items in car parks, stadium etc

This includes packing by roadsides, drinking spots etc.

Advice
- Store notebooks, tablets in the boot of the car.
- For SUVs without non-transparent boot, it is not advised to store item in the car entirely.
Unattended machines – hotel lobbies, airports etc

- Always make sure that your screen is locked when stepping away at public spaces (Ctrl+Alt+Del)

- Device should be locked to an unmovable object when stepping away in public places
Be very circumspect about information released while talking on phone at public places (you may never know who is listening)
Social media discussions

Never share classified/unauthorised information on social media

-impending product releases, internal information
Whether your company provided home security or not, you are ultimately responsible for the safety of company information on your devices in your house.
Corporate Actions
Fixing The Issue
Key Areas of Focus

- Awareness is a journey and not a destination
  - Confidentiality Clauses

Tighter JML process

- Policy updates
  - Mobile Device Management

User responsibilities & Sanctions
Model for Driving Change

1. Tone at the top
   Strong executive leadership and take clear ownership

2. Power from the middle
   Fully engaged middle management taking the lead for specific change topics

3. Benefits for all
   Focus on changing and strengthening the routines in selected critical business situations in daily work.
Corporate Actions for Considerations

1. Sign off terms of equipment use for mobile devices
2. Investigate each loss of mobile device- apply sanctions for negligence
3. Employment/assignment of home security for employees carrying sensitive data on devices
4. Strong adoption of Mobile Data Management (MDM) tools
5. Annualised information security audits
6. ISO certification recommendation
7. Annual signoff of information security compliance policy/code
8. Dedicated corporate portal for ongoing education on information security. Keep this fresh
9. Reward good practice
10. Invest in tools to prevent data leakage/flight
11. Strengthen information classification practice in the business
12. All corporate data transferred over the internet should be encrypted
13. Strong handing over process based on legal framework for senior manager exiting the business
Poll Results
Thank You