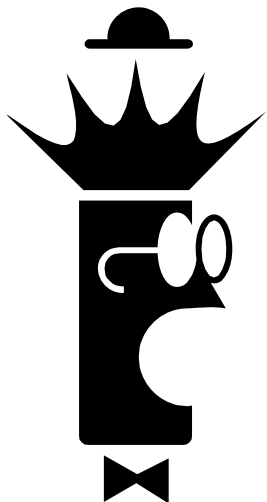


## Security as a Core Business Strategy

People and Process... what makes technical solutions sound

- You have invested in the best physical and system security
- Your patch management and virus signatures are updated daily
- You conduct regular network vulnerability scans
- Your team passed the third party audit with flying colors
- You sleep well .....





You suddenly have one burning question -  
**HOW DID THEY GET IN ?**

The simple answer -  
**They asked for the keys...**



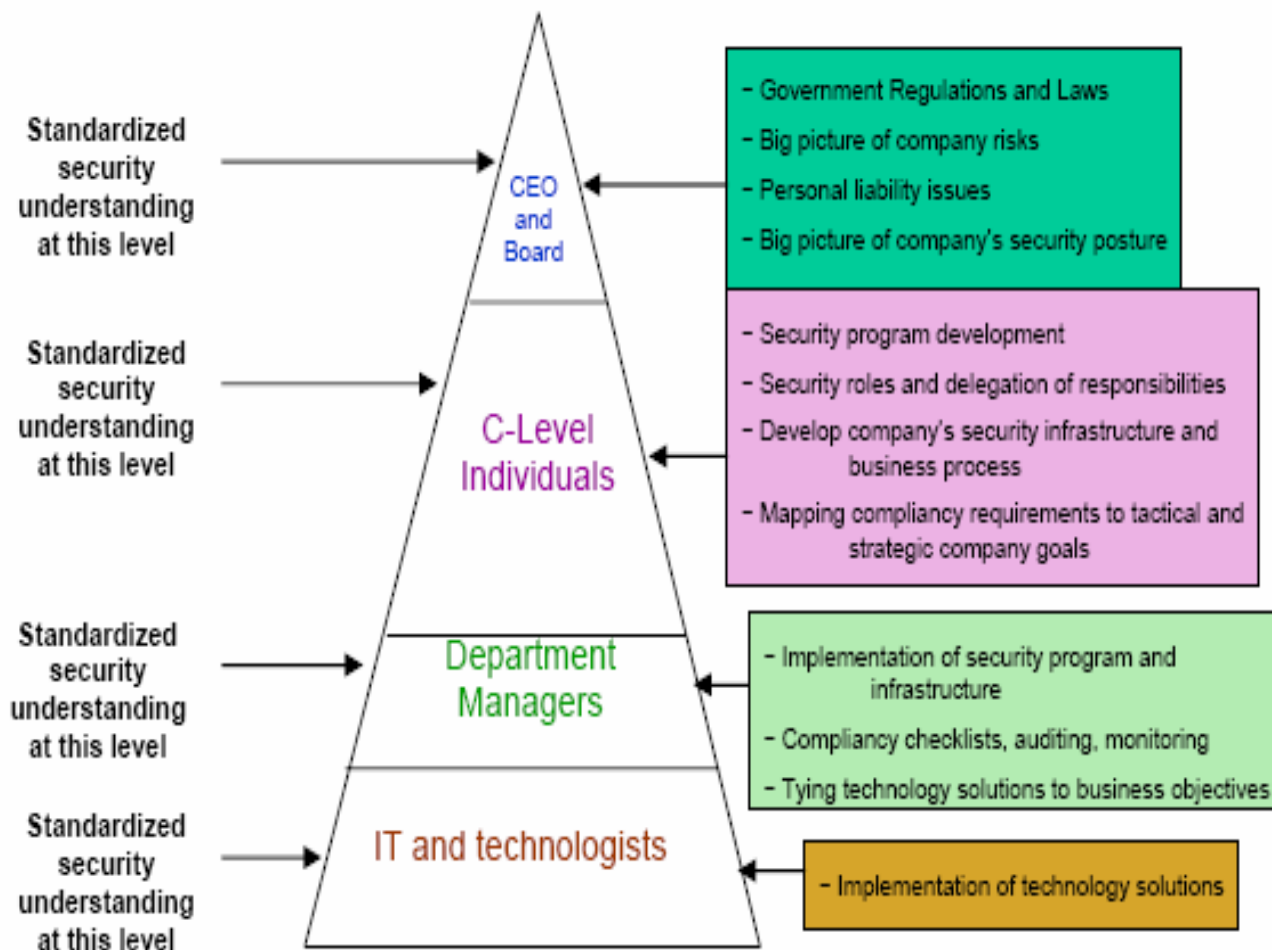
*"You can spend a fortune purchasing technology and services...  
and your network infrastructure could still remain vulnerable to  
old-fashioned manipulation"*

Kevin Mitnick

### The majority of security breaches are accomplished by social engineering and/or exploiting process gaps

- **Social Engineering:**
  - Techniques that rely on weaknesses in wetware rather than software - the aim is to trick people into revealing information that compromises a target system's security.
- **Common attack methods:**
  - Telephone - classic scams include phoning someone who has the required information and posing as a field service tech or a fellow employee with an urgent access problem
  - Dumpster diving – exploiting a gap in process such as the requirement to shred sensitive information
  - On-Line – Phishing attacks have outnumbered e-mails infected with viruses and Trojan horse programs for the first time, according to security experts. (Source: *cnet news 1/30/07*)
  - Password protocol – repeated use of simple passwords on numerous accounts. Many times these are utilized on casual interactions (discount clubs, newsletter, etc) which make capturing them an easier task.
  - Persuasion – impersonation, ingratiation, conformity, diffusion of responsibility, empathy and friendliness

## A culture of security begins at the top and permeates the organization



### Action Items

- **Develop a baseline for mitigating and evaluating risks**
- **Create and maintain an incident response team**
- **Classify threats and the related business risks**
- **Develop incident handling procedures**
- **Improve controls training and procedures following any incident**
- **Audit vulnerability management for compliance**
- **Determine acceptable risk to balance business impediments**
- **Create and regularly review practices and procedures**
- **Communicate expectations and the risk of non-compliance**
- **Train your people like your business depended on it**

### A few takeaways

- Like a good technical security solution, well designed processes and procedures should have several layers of defense.
- Empower your people to say “no”. It creates an atmosphere of accountability and dilutes fear of retaliation.
- Ensure that security does not become a roadblock. A cultural attitude of “efficiency and security is just doing the job right” is the outcome of a consistent management message and well designed processes.
- Think of security as an arms race. You are never really out of danger and the race has no finish line.
- Treat your password like your toothbrush – change it often and do not share it with anyone.
- Security is like a thumbscrew... if you do not hear an occasional scream, it probably is not tight enough.