Cyber Security and Finance

Sir Paul Judge

Nairobi

13th September 2012

Why do people rob banks?

Because that is where the money is.

(Attributed to “Slick” Willie Sutton)

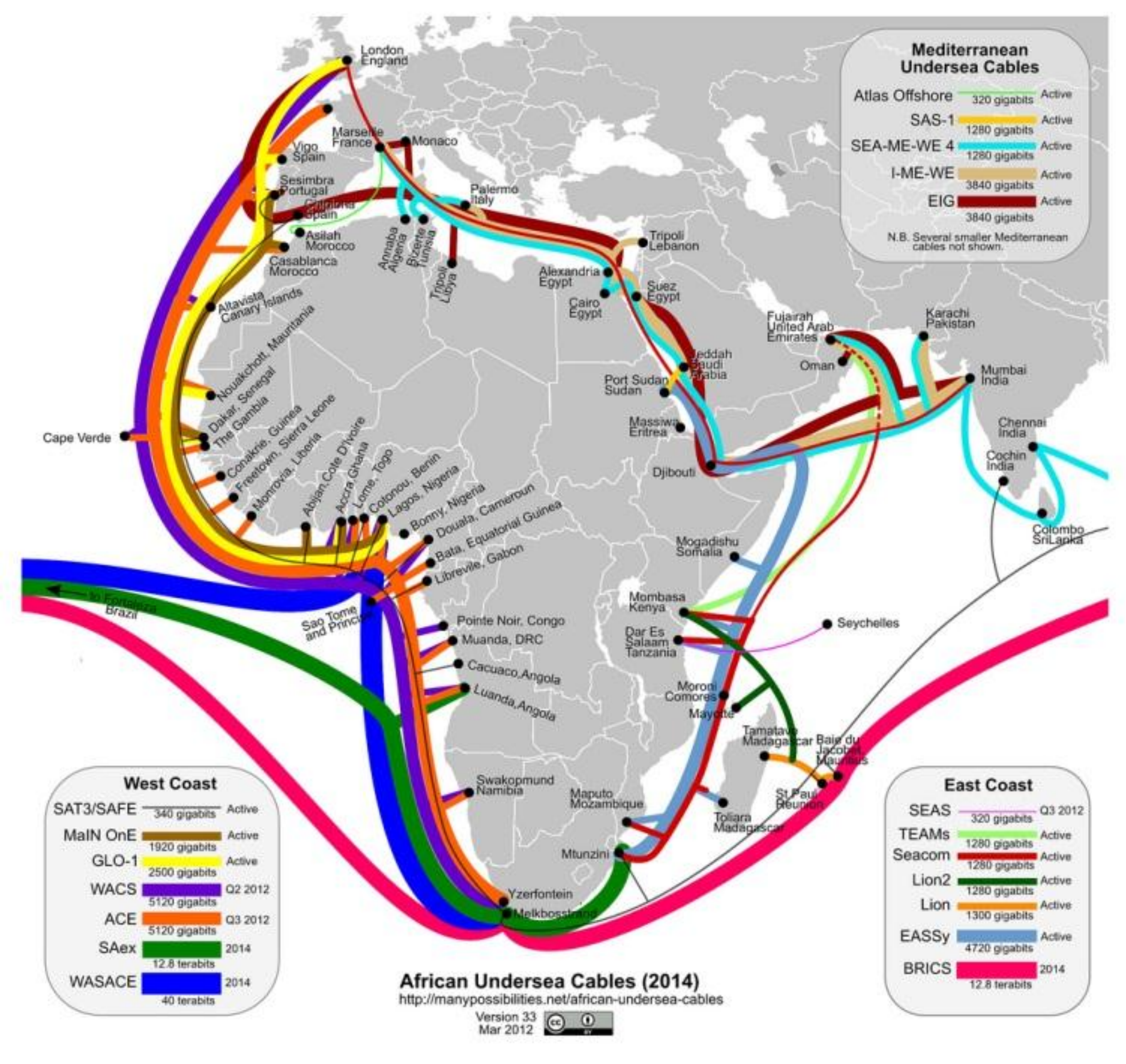
Willie Sutton

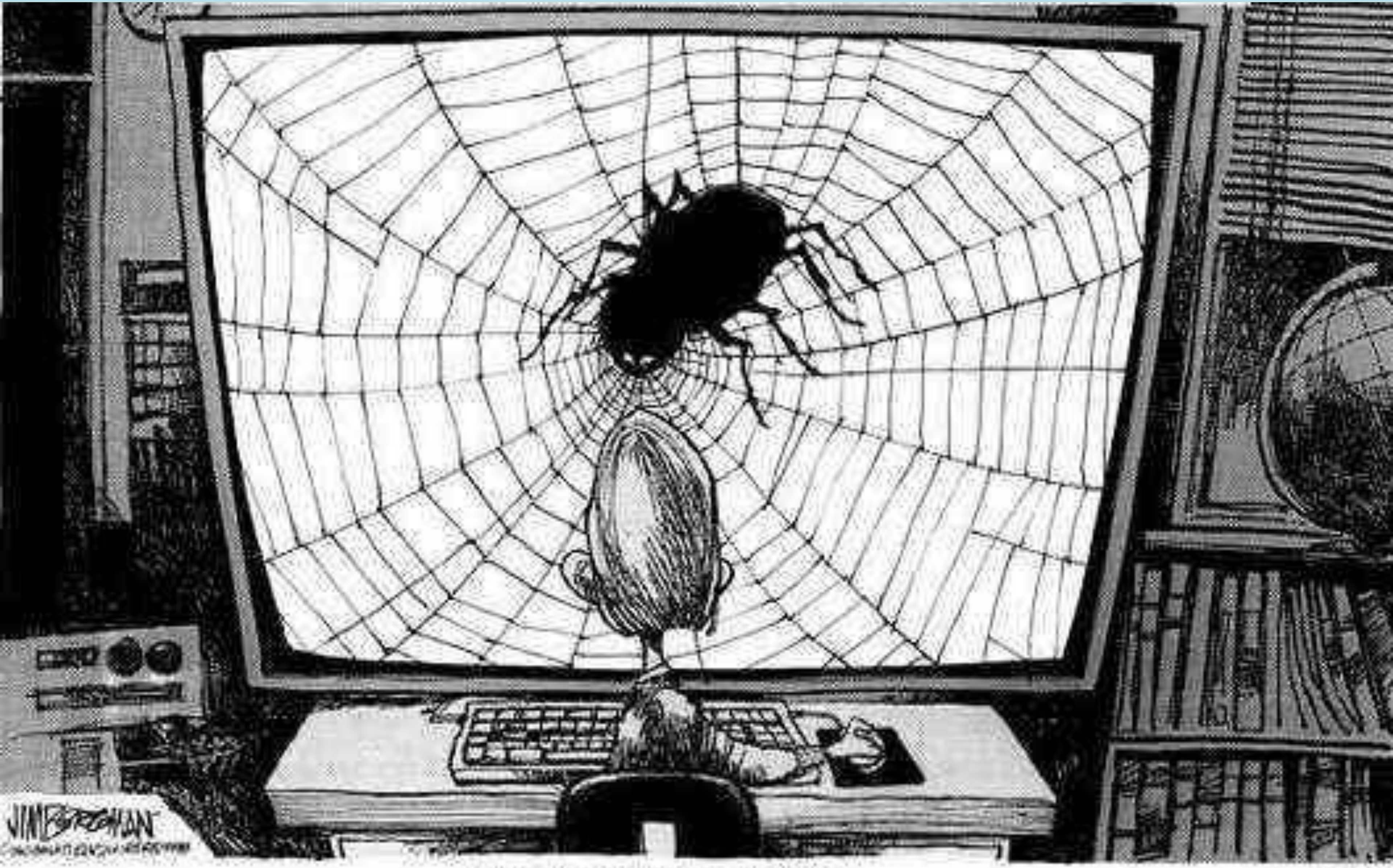
- Forty-year criminal career
- Accomplished bank robber
- Usually carried a pistol or a Thompson submachine gun
- Robbed about 100 banks from the late 1920s to his final arrest in 1952

Moore’s Law

The newest calculator:
16 bit, with hi-tech monitor,
including mouse ...
It is not worth it - in 18
months it will cost you half as much
STEIN

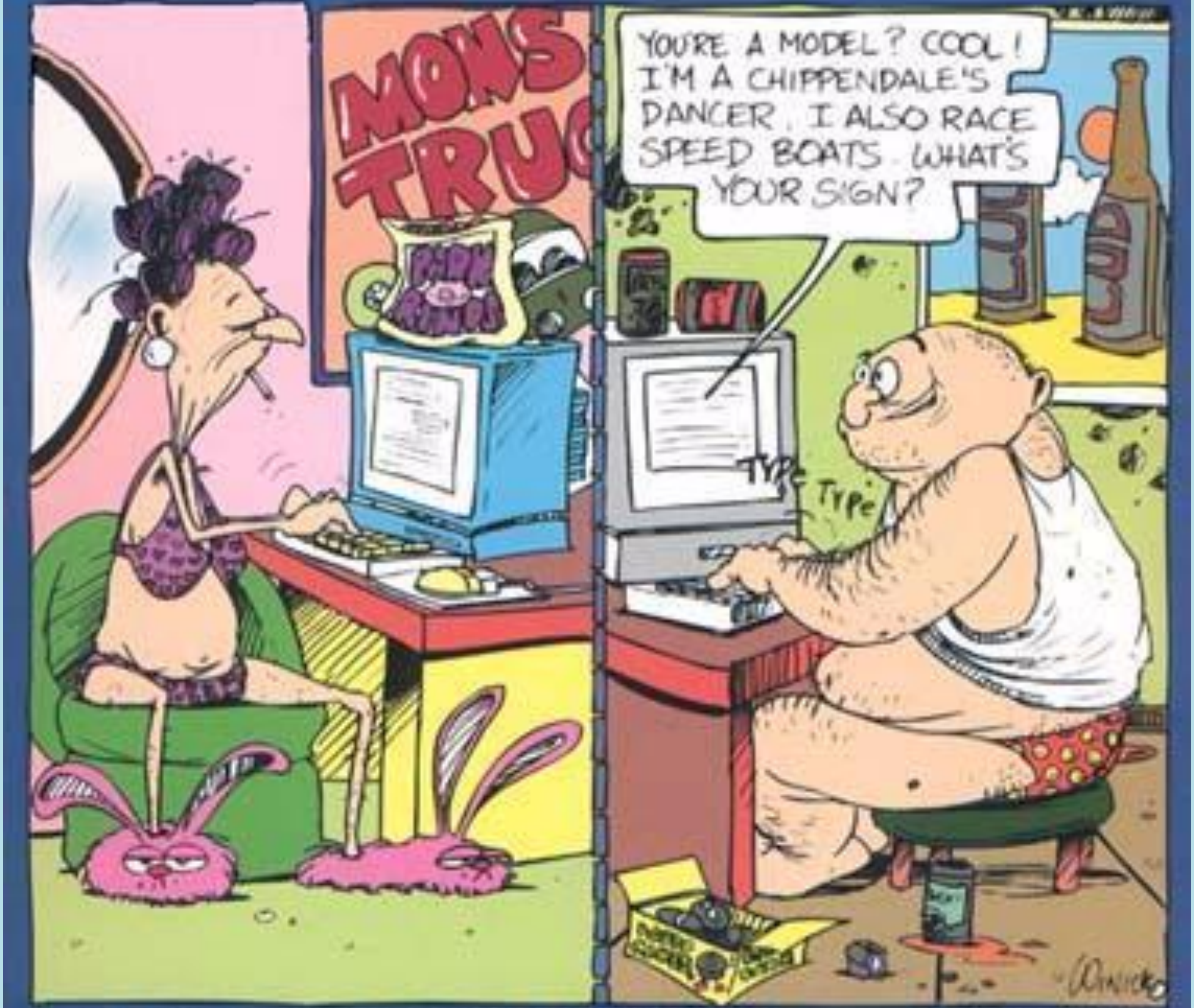
Coastal Cables





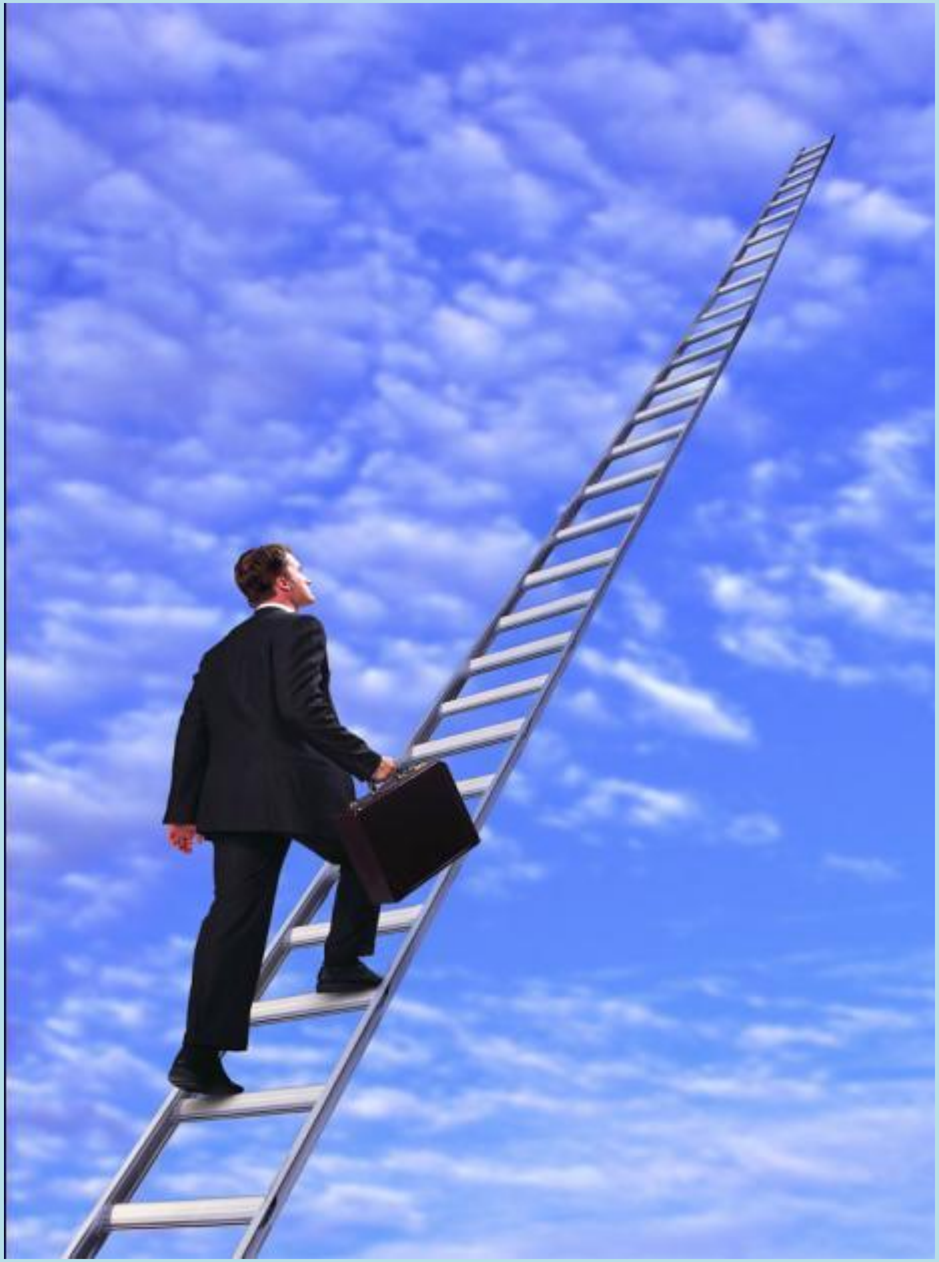
World Wide Web

FPG


YOU'RE A MODEL? COOL! I'M A CHIPPENDALE'S DANCER. I ALSO RACE SPEED BOATS. WHAT'S YOUR SIGN?
MONS
TRUC
TYPE
TYPE

HONESTY ON THE INTERNET

Despite, or because of, the fast changing world – Opportunities abound…



But

It only takes one person or incident to damage a company's reputation

21 June 2012

Mail Online

NatWest finally fix computer glitch that left customers unable to use accounts... but backlog could last for days

- Bank apologises for meltdown after resolving the 'initial problem'
- Problems are expected to continue into NEXT WEEK as they deal with payment delays
- Branches will open on Sunday to help in emergencies
- Customers STILL reporting that salaries are not being paid in and payments are not being made
- Up to 12 MILLION customers are being affected by the problem
- Customers of Royal Bank of Scotland and Ulster Bank also affected
- Problem reportedly arose after staff tried to update software

Cyber Security West Africa

- E-Crime consultant Albert Antwi-Bosiako says it is important that cybercrimes are not allowed to disrupt development
- He says the phenomenon is seriously harming the economies of West African states
- *“There are merchants in Europe, retailers online and e-commerce platforms that are not accepting credit card payments from Ghana and Nigeria.”*
- *“Retailers will change their policies only when they see improvements from West Africa.”*
- *“People here tend to act only when problems have occurred.”*

BNAC Report - Examples

Examples we highlighted included:

- A multimillion-dollar infrastructure enterprise was unable to conduct business for more than 36 hours after a concerted, very sophisticated denial of service attack.
- Dozens of western corporations have seen vital business data lost or stolen because of inadequate controls and neglect of security in outsourcing contracts to India, China, and the Philippines.
- Several banks had to pay millions of dollars in restoration fees and penalties because poor initial authentication protocols left their customers open to phishing attacks.

False Requests

- Scam emails saying that someone’s relative has died
- There is a lot of money which can be shared with the lucky message recipient.
- The fact that these emails have persisted for years shows that they do find people who send their bank details and subsequently lose significant cash

Responsibility From The Top

- In evaluating risks, boards need to know what is being done to prevent data compromises
- It is accepted that boards must ensure that their chief financial officer has managed their funds appropriately
- Similarly they must be convinced that the CIO has taken all reasonable steps to safeguard the company's digital resources
- This must include business partners, suppliers and customers

Standard Bank Data Centre

- Only purpose-built tier-4 data centre in the southern hemisphere
- Cost of $200 million excluding the computer equipment
- 65,000 sq m site consisting of two adjacent properties
- Allows for up to eight data-centre modules of 1,500 sq m each
- Self sufficient in power and water

- The technology is only part of the problem.
- There are people outside who operate the machines
- As Isaac Newton said 300 years ago, “I can measure the motion of heavenly bodies but I cannot measure human folly”.

"Excuse me, could you see if this virus ruins your computer, too?"

- All organisations say that their employees are their greatest asset.
- However training is often not provided to help employees understand their computers.

"Look what I found on the web! Waste-the-whole-morning.com!"

- In many organisations there are no real policies about how the computers should be used and what is acceptable and what is frowned upon

"Sure, you can fire me, but I'll just hack into the HR computer and hire myself again. That's how I got this job to begin with."

- Even without a concerted attack there will always be problems of data reliability.
- People may just make genuine mistakes
- Employees may change records for personal reasons.

"Billy! You're all grown up! Gosh, our customer data must be terribly out of date."

- Information is still not given the real value which it should have.
- This is only realised when the data is lost.
- Companies who lose information are normally too embarrassed to make this public.

Use Of Official Hackers

- Director of Abraaj Capital, the largest emerging markets private equity company.
- Computer systems had been given a clean security bill of health by one of the Big Four auditing firms.
- As part of its risk evaluation activities we invited a company based in the US to see if it could hack into our systems.
- The company provides this service for free as it is confident of success and can then charge for consultancy to put things right.
- It hacked right in within an hour, including into the CEO’s own PC and turned on camera
- You can imagine how effective that was when the hacking firm made their presentation.
- Every company should undertake a similar exercise.

Key Requirements

- Establish a comprehensive information security policy
- Hold a company-wide security audit to expose vulnerabilities
- Underpin a robust security culture with frequent and rigorous testing
- Keeping abreast of changes in security technology and best practices

Complacency

Picasso

"Success is dangerous - One begins to copy oneself.

It is more dangerous than to copy others

IT LEADS TO STERILITY!"

AFP

- Cyber security is a core business issue
- CEOs and governments must move it to the top of their agendas