



Ministry of Telecommunications
and E-Commerce



ISACA - APRIL 2003

INFORMATION SECURITY: “COMING OF AGE”

Nigel Hickson
Department of E Commerce
Ministry of Tourism, Telecommunication & E-
Commerce
Government of Bermuda



AGENDA

- Why this talk?
- Objectives
- Bermuda: A bit of context
- We have come a long way
- Where we are now
- Where we should be
- How to get there – Role of Industry and government
- Conclusions



Why this talk

- A passion
- A belief
- An audience
- Time is right



Objectives

- To convince you it matters and we have a lot to do; pretty bad at present
- To tell you a bit about what is going on in Bermuda
- To give my view on a future global strategy



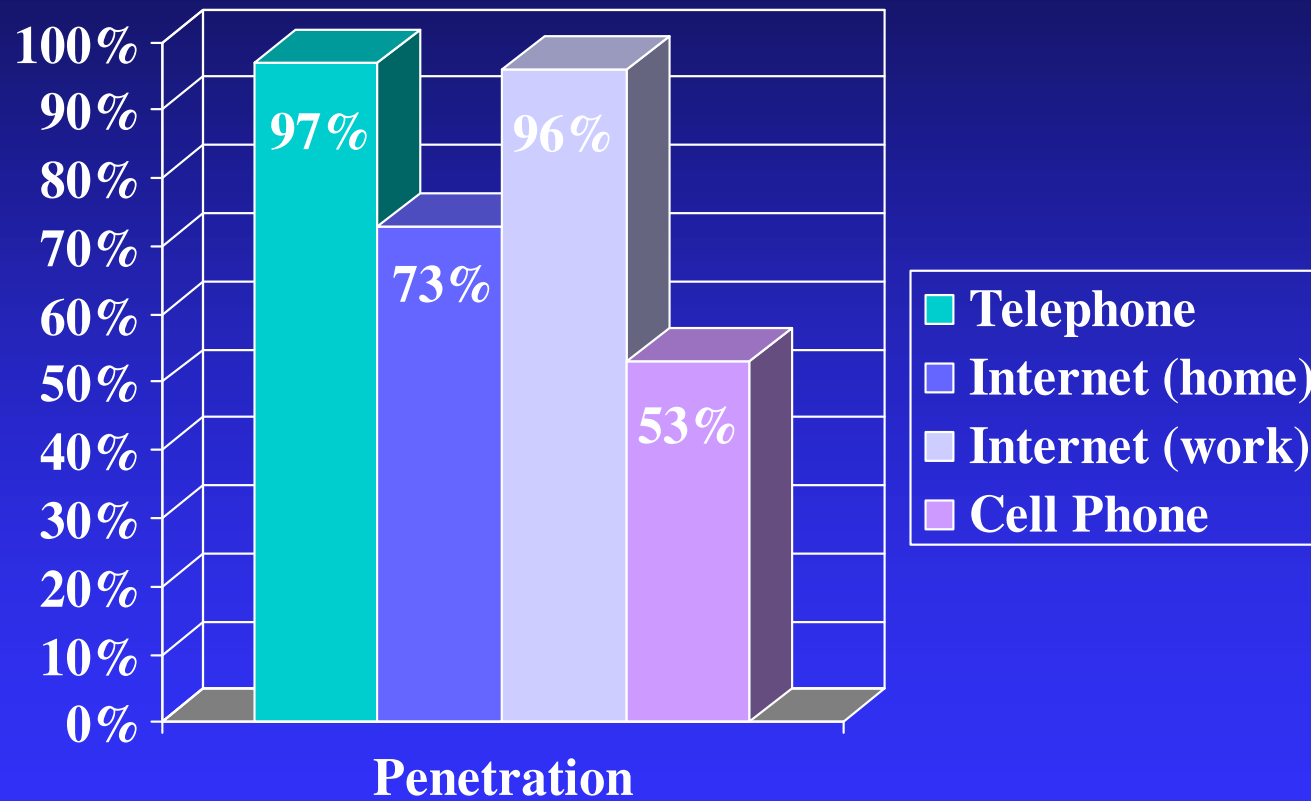
Bermuda – A bit of context

- 62 000 odd people
- 22 square miles
- 600 miles from North Carolina
- UK Overseas Territory
- 36 seat lower house
- Progressive Labour Party Government (2nd term)



A vision.....

“Bermuda, through its provision of e-business services and transactions, will become a leading jurisdiction for sophisticated and secure e-business. Bermuda will exploit this leadership at the forefront of the global digital economy to enhance the quality of life of all her people.”





e-government

IT &
e-business
policies



e-education

IT & Tele-
communications
Infrastructure

e-business
development
(local)



Why critical for us

- No point in having a “vision” if no IT
- “Availability” critical for E Government Portal
- Public and (importantly) civil service lose faith
- Personal Data at risk



Why critical for YOU

- Same reasons but different
- We rely on IT for everything we do
- So, increasingly, do our citizens
- Trust is and will be critical



Some facts and figures (1)

- 80% businesses think they have critical data
- 44% “malicious” breach
- 33% of these viruses
- 20% of these took a week to fix
- Altogether 70% were “outside”



Some facts and figures (2)

- Average cost of malicious incident \$50k
- Total cost (in UK alone) \$5bn approx.

- 27% had a security policy
- Only 15% knew ISO 17799

- Only 33% web-sites had intrusion detection software
- Only 60% of transactional sites had “authentication”

(www.secuirytsurvey.gov.uk)



Some facts and figures (3)

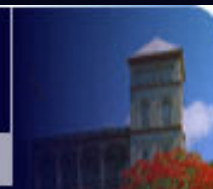
- Only 30% businesses had “business continuity” plans
- Only 8% bother to test plans
- One hour downtime for a bank: \$6.5m
- Airline bookings: \$90k per hour downtime
- Data centre: 10 days – bankruptcy

(www.ft.com/buscon2004)



A bit more context

- Not just a networking issue; as you can see
- The “mobile” generation expects!
- Reputation is everything
- Convincing citizens and consumers!
- Legal and financial implications



We have come a long way

- At least we talk about it
- The industry admits there are issues
- Gone is the “locked” door
- Governments realise “secrecy” not only concern
- Users care more
- Even some products are good



Some landmarks

- BS 7799 – now ISO 17799
- UNCITRAL Model laws
- OECD Cryptographic Guidelines
- Microsoft “Trustworthy Computer” Initiative



Where we are now

- Too complacent; look at those figures
- Too reliant on technologies
- Over sell viruses and hacking
- Lost our strategic thinking
- Not enough attention to “availability”
- Forget the essentials – the people



Where we should be

- Less waffle; more action
- More attention to risk and policy
- More on getting “basics” right
- Service Level Agreements with Consumers and citizens
- More “business” demand for solutions



How to get there

- A new partnership between business users, vendors and Government
- A new global initiative (United Nations?)



Bones of Global Initiative

- An agreed Information Management Standard
- A Risk Framework
- An agreed “kite mark” for technology
- Service Level Agreements:
 - Vendor / Business User
 - Business / Consumer
 - Government / Citizen



Conclusions

- We have come a long way but a lot further to go
- E Business “Revolution” depends on it
- There is a way forward!
- Lets make a start



Discussion / Questions

- Lets make it controversial

nhickson@gov.bm