The Network Is Naked:

The security consultant's new clothes

Marcus J. Ranum

WARNING!
CONTAINS 30%
CYNICISM
BY VOLUME
ingest with a grain of salt

1

Factoids

- 80% of males believe they are in the top 80th (or higher) percentile of automobile driving skill
- Most managers that are afraid of connecting to the Internet are operating under the dubious assumption that they are not *already* connected

2

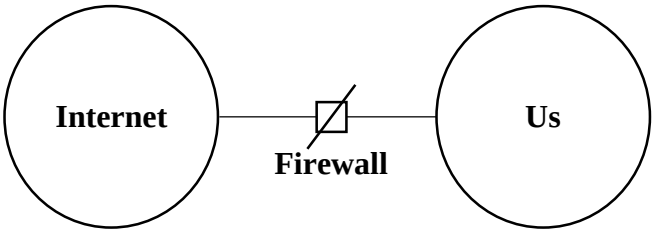
Lesson #1: Contents

- How to lie to the consultant
- How to lie to the press
- How to lie to management

3

Lying to the consultant

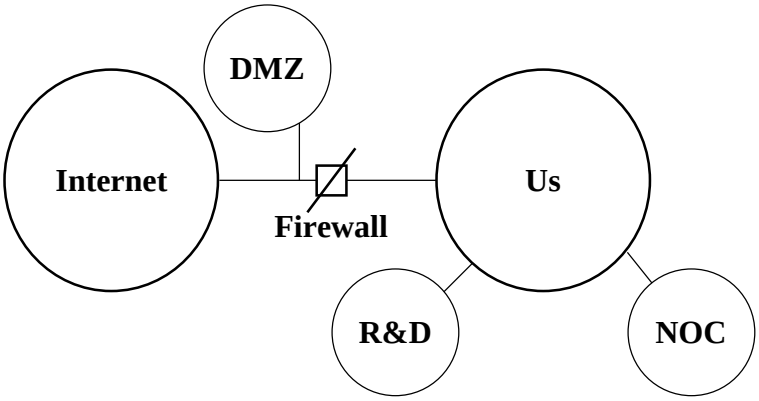
Kickoff Meeting: Network Map



4

Lying to the consultant

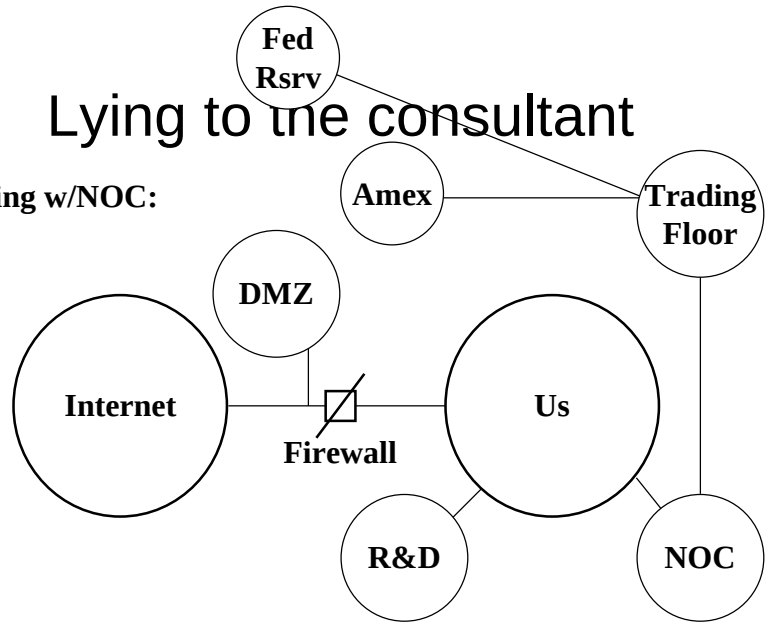
Second Meeting: Network Map With Detail



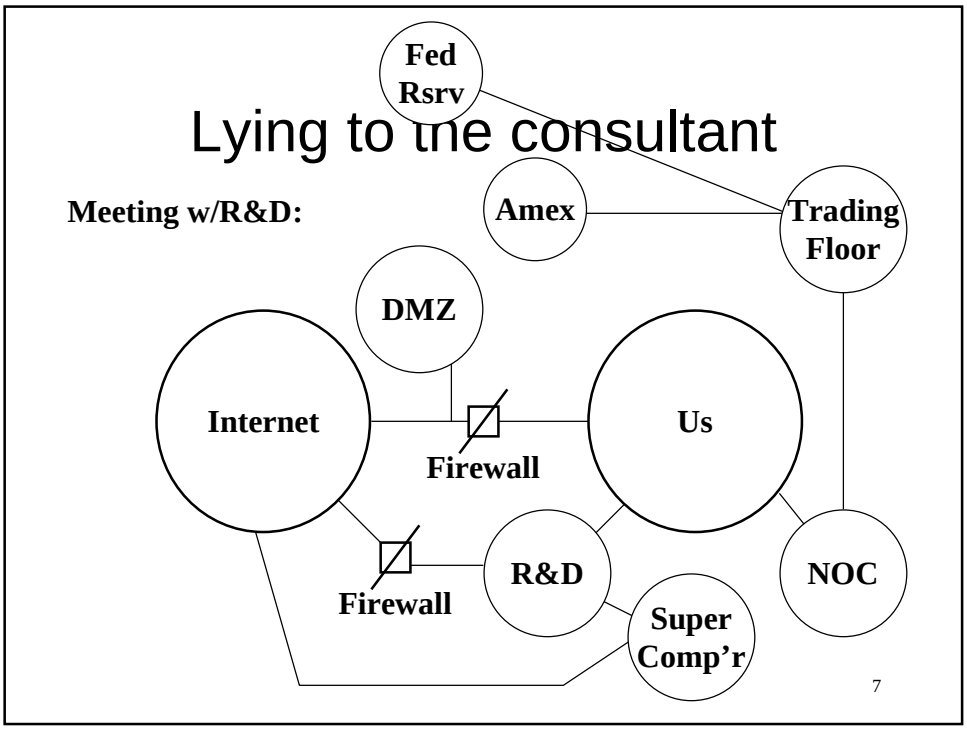
5

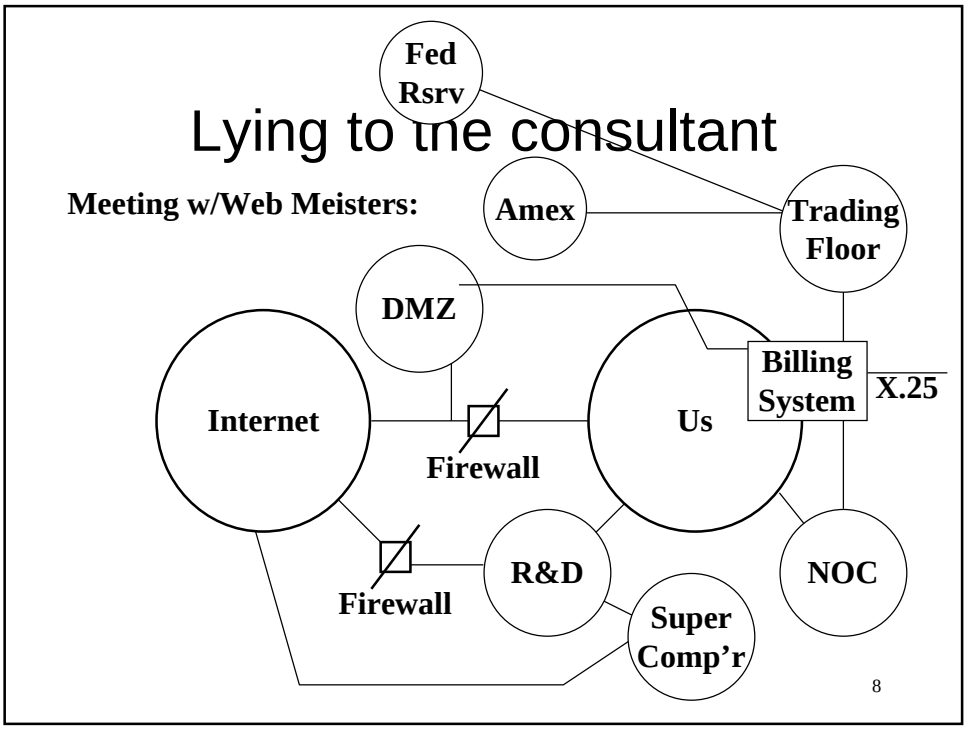
Lying to the consultant

Meeting w/NOC:



6



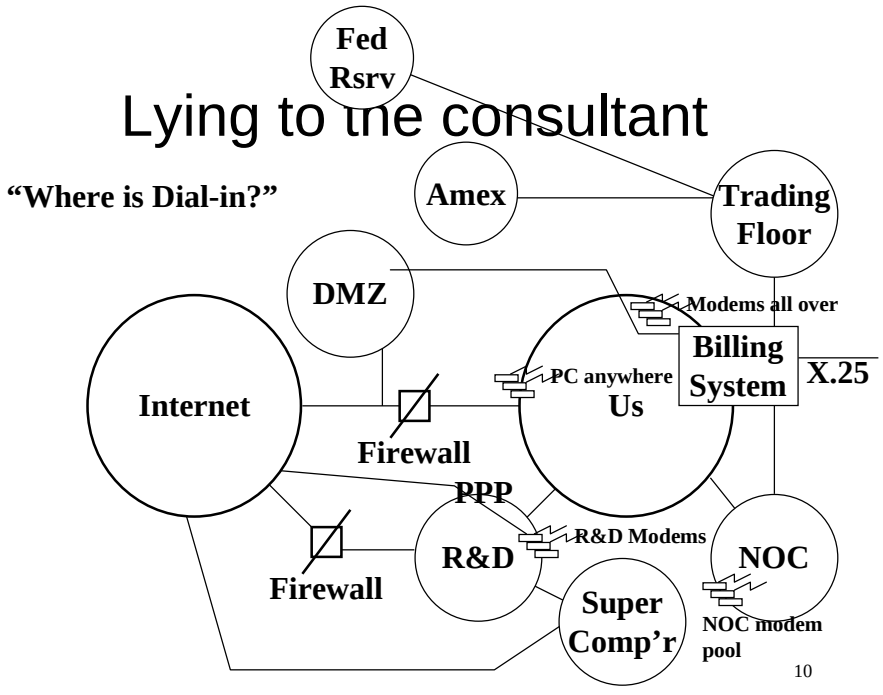


Lying to the consultant

- At this point you have an Excedrin #999 headache
- Being a glutton for punishment, you decide to make matters worse:

9

Lying to the consultant



10

Lying to the consultant

- The previous diagram was dramatically over simplified so it would all fit on one page

.... We didn't put on the links to customer support, and our business partners that we exchange Email with ... and then there are the remote offices...

11

Lying to the consultant

- Auditing a modern network is a completely hit-or-miss affair
- As networks grow larger the problem will grow worse: ***it is already unbearable!***
- Joking aside: they're not deliberately lying to the consultant
  - Nobody knows what's on their network

12

Lying to the press

- The press has a completely distorted view of reality
- Looking at the network through rose-colored glasses
  - When you call to interview someone about security *you always get routed to someone who cares about security*
  - Tell the press how bad it actually is and they think you're a nutcase (I am!)

13

Lying to the press

- Results of distorted view:
  - Security incidents are a *surprise*
  - Security incidents are *newsworthy*
- Scary examples cut in many different ways:
  - One reporter believes all of *redundancy.redundancy.gov* is behind a single firewall

14

Lying to the press

- Does anyone even know how many Internet connections *redundancy.redundancy.gov* has? Including *redundancy.redundancy.gov*?
- Will that reporter write a negative article about the firewall next time *redundancy.redundancy.gov* is broken into?

15

Lying to the press

- The guy who has gaping security holes never gets interviewed
- The guy who gets interviewed is probably in the minority that cares about security and is actually doing something about it
- The rest of the organization is continuing blithely along

16

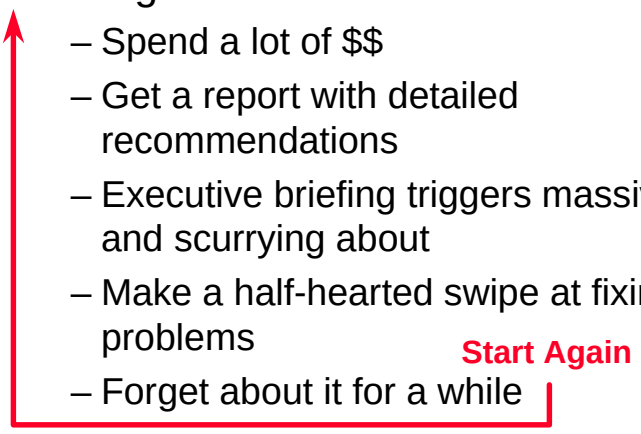
Lying to management

- Factoid: Management lies to itself too

17

Lying to management

- Bring a consultant/auditor in:
  - Spend a lot of $$
  - Get a report with detailed recommendations
  - Executive briefing triggers massive firedrill and scurrying about
  - Make a half-hearted swipe at fixing a few problems
  - Forget about it for a while



18

Lying to management

- What happens?
  - Recommendations imply change
  - People resist change
- Standard responses to security recommendations:
  - "That's OK for now."
  - "We know about that one but we don't have time or money to fix it right now."

19

Lying to management

- All-time favorite scenario:
  - "We can't fix that right now, the product is in beta test already"

  .... months later:
  - "Well, we haven't seen a problem with it yet and it's worked fine for the last few months and we don't have time to fix it anyhow..."
- Do problems only get fixed as a direct result of humiliation or financial loss?

20

Lying to management

- Often heard comment during presentation of audit report:
  - "You know, the *last* audit we had done, they said that too..."

21

Lying to management

- Security policies are really just something to get around
  - Or ignore completely
- Even Orange Book is just something to get around
  - Push towards open source intelligence is a clever way of getting around all the hurdles of handling classified material

22

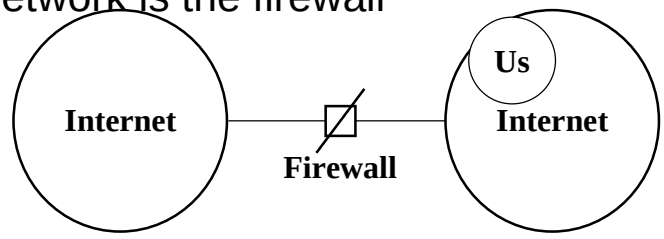
A thought

- Ranum's theorem:
  - If it can't run Netscape, in 2 years nobody will be using it

23

So where does that leave us?

- Usually the only secure system on the network is the firewall



24

So where does that leave us?

- If your management is putting you through hell about Internet connectivity and you see the symptoms of these other problems then Internet connectivity will not make the situation any worse
  - But try convincing them of that!
  - Closely held illusion that “we already have great network security”

25

To maintain security

- Network change control:
  - Can it work?
  - Audit and control all connection/disconnection, every modem, every firewall, every new network link
  - Does not scale

26

To maintain security

- Intrusion detection:
  - Does it help?
  - Detect successful attacks on network through abuse inference
  - Tells you “OK, you’re in trouble now”
  - Reactive not active

27

To maintain security

- Audit trails
  - Nice to have
  - Nobody looks at them until it’s too late

28

To maintain security

- Automated scanning for weaknesses
  - Tools like SATAN, Pingware, ISS, Icepick, COPS and Tripwire for host systems
  - Can be effective in detecting and correcting weaknesses
  - *Requires* top-level authority to *actually fix* weaknesses when found!
  - Can only find weaknesses that are already known

29

Conclusions

- Pull out all the stops
  - If you need secured systems you need to audit, implement change control, perform active probing and intrusion detection
- Do it
  - Cut across red tape and just *fix* it
  - Politics can no longer be an excuse
  - “We can’t change it” is for losers

30

Conclusions

- Alternative:
  - Lie to management
  - Lie to press
  - Lie to yourself

31