

# Understanding the Risks: Can you Ever be Secure?

Brian O'Higgins  
CTO, Third Brigade

Toronto, Feb 21, 2008

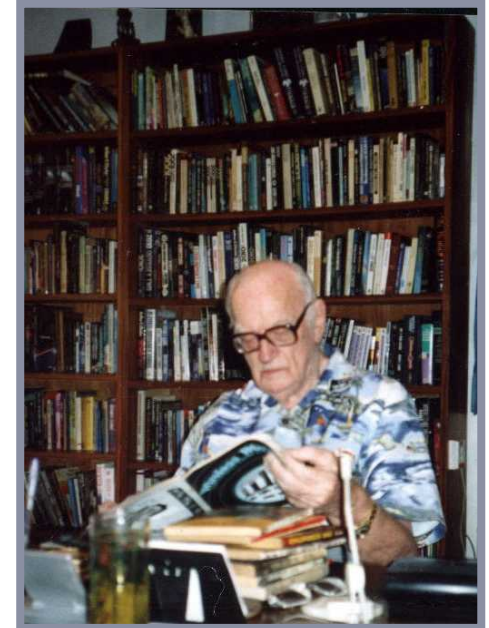


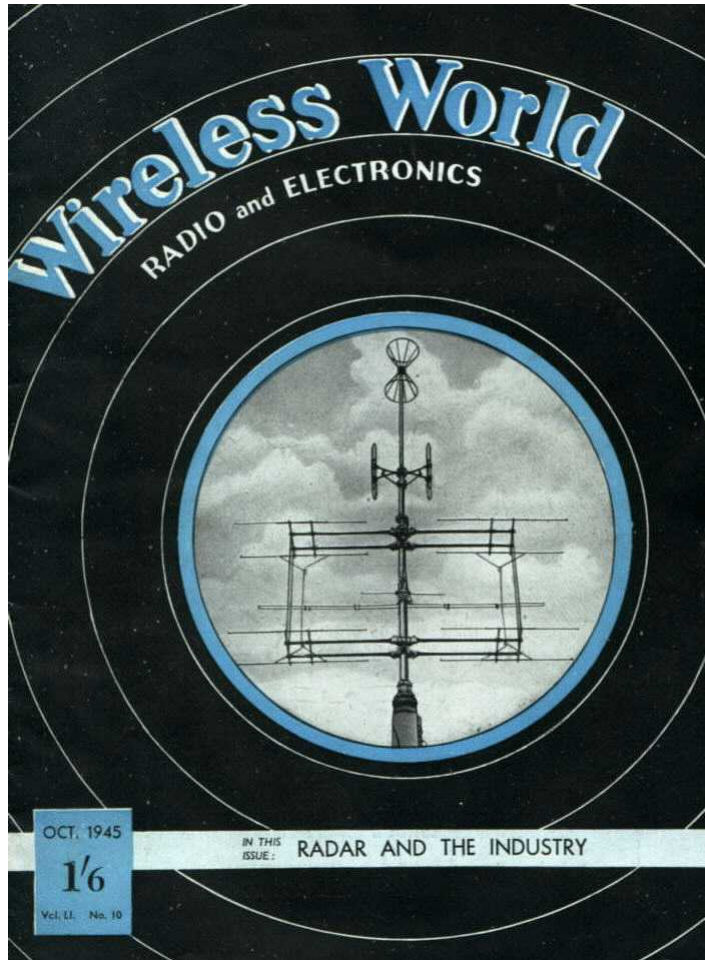
“Any sufficiently advanced technology is indistinguishable from magic”.

Arthur C. Clarke

"Profiles of The Future", 1961

(Clarke's third law)





## EXTRA-TERRESTRIAL RELAYS

### Can Rocket Stations Give World-wide Radio Coverage?

By ARTHUR C. CLARKE

ALTHOUGH it is possible, by a suitable choice of frequencies and routes, to provide telephony circuits between any two points or regions of the earth for a large part of the time, long-distance communication is greatly hampered by the peculiarities of the ionosphere, and there are even occasions when it may be impossible. A true broadcast service, giving constant field strength at all times over the whole globe would be invaluable, not to say indispensable, in a world society.

Unsatisfactory though the telephony and telegraph position is, that of television is far worse, since ionospheric transmission cannot be employed at all. The service area of a television station, even on a very good site, is only about a hundred miles across. To cover a small country such as Great Britain would require a network of transmitters, connected by coaxial lines, waveguides or VHF relay links. A recent theoretical study<sup>1</sup> has shown that such a system would require repeaters at intervals of fifty miles or less. A system of this kind could provide television coverage, at a very considerable cost, over the whole of a small country. It would be out of the question to provide a large continent with such a service, and only the main centres of population could be included in the network.

The problem is equally serious when an attempt is made to link television services in different parts of the globe. A relay chain several thousand miles long would cost millions, and transoceanic services would still be impossible. Similar considerations apply to the provision of wide-band frequency modulation and other services, such as high-speed facsimile which are by their nature restricted to the ultra-high-frequencies.

Many may consider the solution proposed in this discussion too far-fetched to be taken very seriously. Such an attitude is unreasonable, as everything envisaged here is a

logical extension of developments in the last ten years—in particular the perfection of the long-range rocket of which V2 was the prototype. While this article was being written, it was announced that the Germans were considering a similar project, which they believed possible within fifty to a hundred years.

Before proceeding further, it is necessary to discuss briefly certain fundamental laws of rocket propulsion and "astronautics." A rocket which achieved a sufficiently great speed in flight outside the earth's atmosphere would never return. This "orbital" velocity is 8 km per sec. (5 miles per sec.), and a rocket which attained it would become an artificial satellite, circling the world for ever with no expenditure of power—a second moon, in fact.

the atmosphere and left to broadcast scientific information back to the earth. A little later, manned rockets will be able to make similar flights with sufficient excess power to break the orbit and return to earth.

There are an infinite number of possible stable orbits, circular and elliptical, in which a rocket would remain if the initial conditions were correct. The velocity of 8 km/sec. applies only to the closest possible orbit, one just outside the atmosphere, and the period of revolution would be about 90 minutes. As the radius of the orbit increases the velocity decreases, since gravity is diminishing and less centrifugal force is needed to balance it. Fig. 1 shows this graphically. The moon, of course, is a particular case and would lie on the curves of Fig. 1 if they were produced. The proposed German space-stations

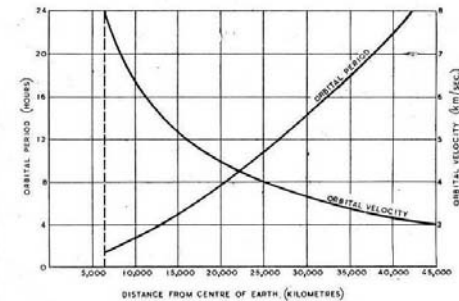


Fig. 1. Variation of orbital period and velocity with distance from the centre of the earth.

The German transatlantic rocket Aro would have reached more than half this velocity.

It will be possible in a few more years to build radio controlled rockets which can be steered into such orbits beyond the limits of

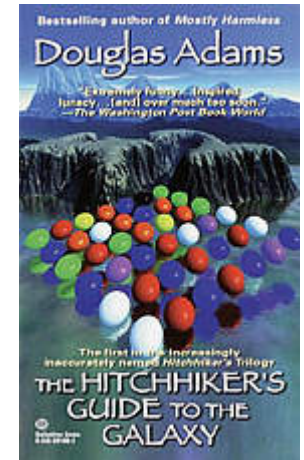
would have a period of about four and a half hours.

It will be observed that one orbit, with a radius of 42,000 km, has a period of exactly 24 hours. A body in such an orbit, if its plane coincided with that of the

# Building Secure Systems

“A common mistake that people make when trying to design something completely foolproof is to underestimate the ingenuity of complete fools.”

Douglas Adams, *Mostly Harmless*



# Planning for the Future

“Prediction is very difficult,  
especially about the future”

Neils Bohr



# Planning for the Unknown

“...because as we **know**, there are **known knowns**; there are things we **know** we **know**. We also **know** there are **known unknowns**; that is to say we **know** there are some things we do not **know**. But there are also **unknown unknowns** -- the ones we don't **know** we don't **know**.”

Donald Rumsfeld (a man “in the know”)



# Evolution of the Attacks

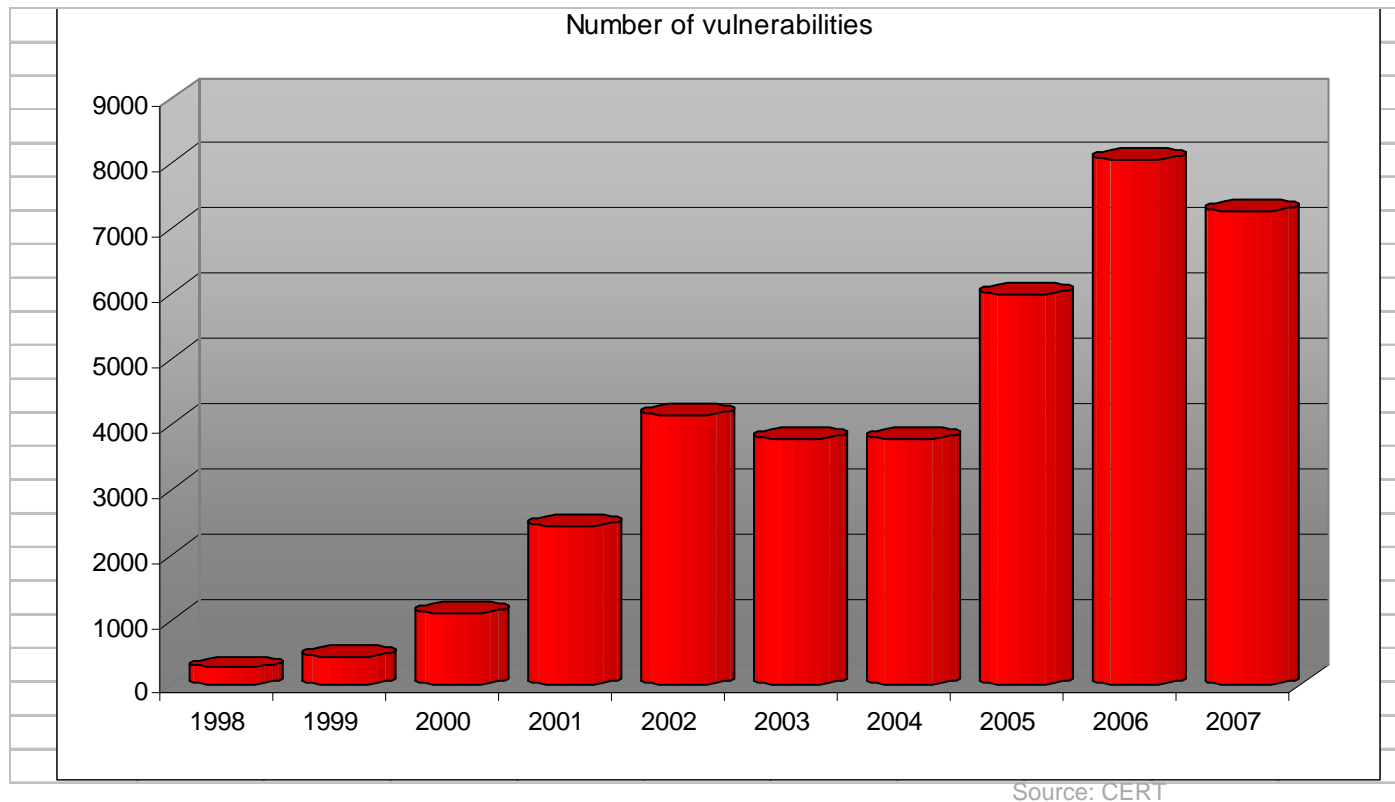
- Investment in network controls stops simple mass attacks
- Attacks now 'move up the stack', attack applications and users
- Targeted attacks work, and are often unreported. Growing faster than mass attacks. Economic damage increases. (TJX)
- Gartner says the cost of a sensitive data breach will increase 20%/yr through 2009.



?

# The threat landscape

- Number of vulnerabilities is increasing\*



\* Notwithstanding the 2007 number drop, the % of criticals increased dramatically

# Just last week...

## What a Week!

Vulnerabilities on the most critical list this week: 1 Microsoft, 2 Apple, 1 Novell, 1 Symantec, and 2 Adobe and 1 ClamAV. Add 9 more "high" criticality vulnerabilities and 3 of moderate criticality and you have the most challenging security week in many months.

Note how many of these vulnerabilities are NOT patched by Microsoft's automatic updaters. Too many companies are not updating applications other than Windows products. That's more than dangerous.

Alan

\*\*\*\*\*

@RISK: The Consensus Security Vulnerability Alert

Feb 14, 2008

Vol. 7. Week 7

\*\*\*\*\*

# Application Software = Current Achilles Heel

**“75% of attacks now take place at the  
application layer”** *Gartner, 2006*

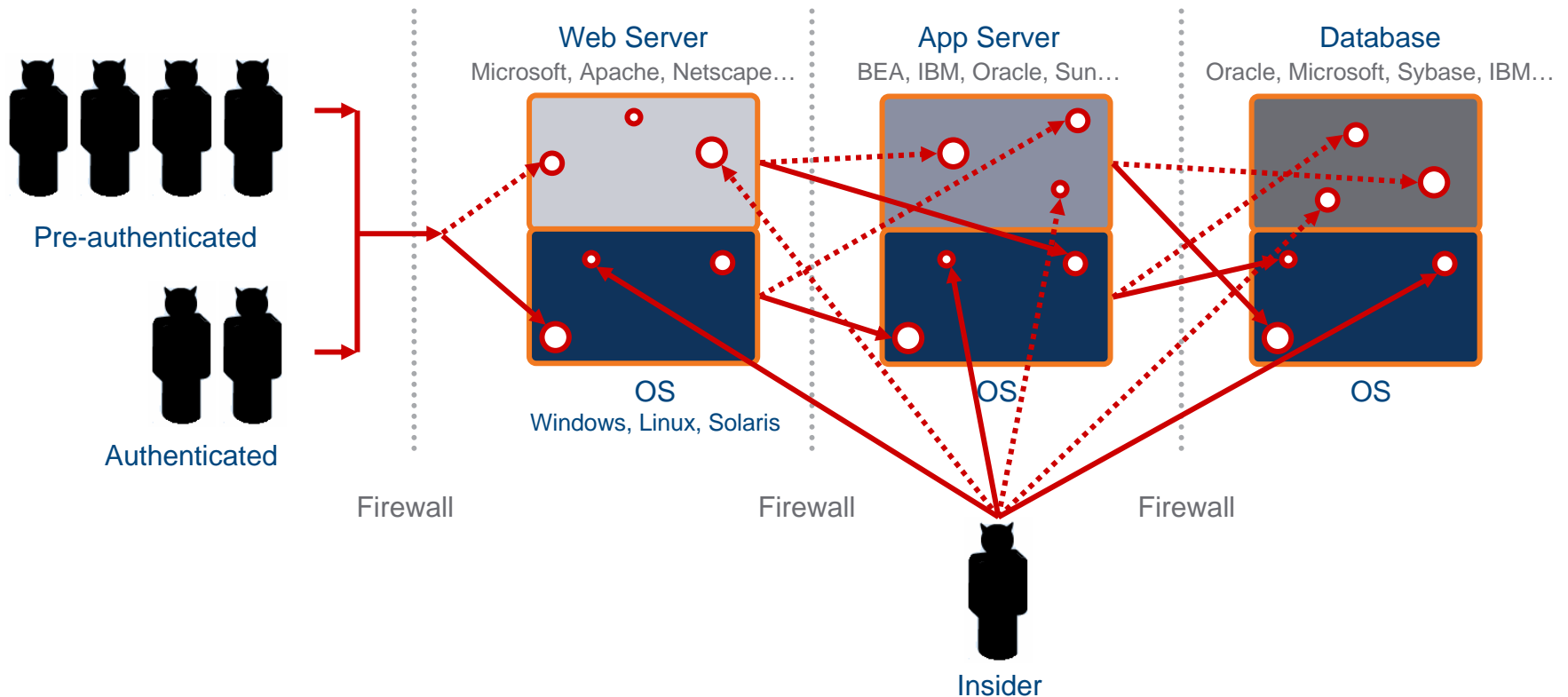


**“4,375 vulnerabilities in the first 9 months  
of 2006. Web flaws are the 3 most common.”**  
*Mitre Corp, 09/2006*

**“Customization of off-the-shelf software is  
the weakest link in application security”.**  
*Gartner, 09/2005*

**“By 2009, 80% of enterprises will fall victim to an  
application attack”.**  
*Gartner, 2007*

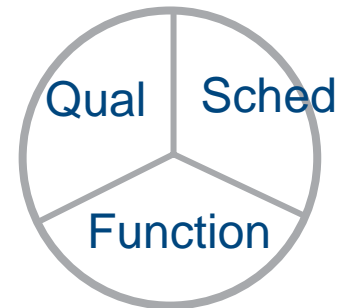
## Many ways to exploit a vulnerability with targeted attacks



# Getting Harder to Defend

- Skills gap – attackers vs. internal
- Web 2.0 and futures
  - Non-programmers programming in scripting languages
  - Applications now cross firewall boundaries

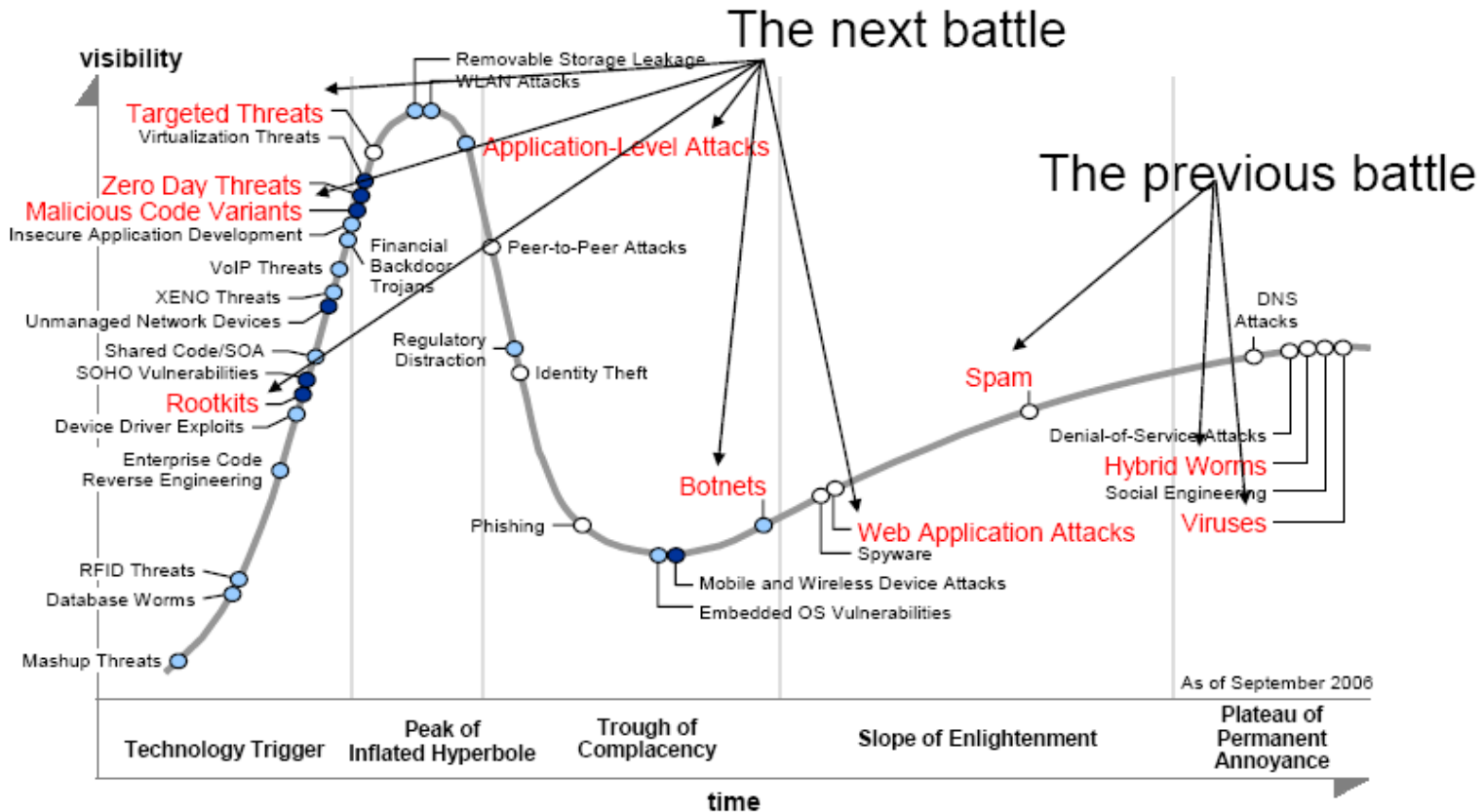
Choose 2:



## The Good News:

You don't have to be perfect to be secure...  
just stay ahead of the crowd

# Gartner Hype Cycle for Cyberthreats, 2006



Years to mainstream adoption:

○ less than 2 years

● 2 to 5 years

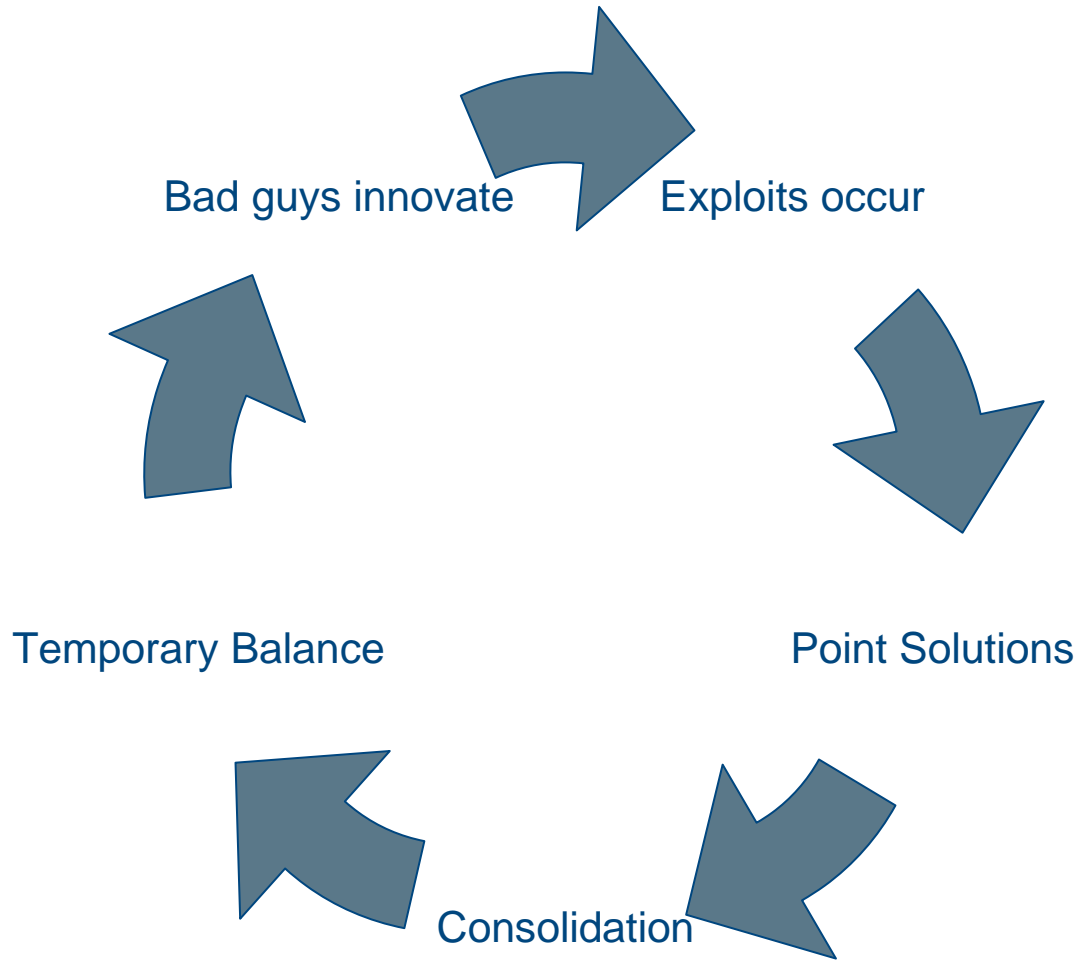
● 5 to 10 years

▲ more than 10 years

⊗ obsolete before plateau

**Gartner**

# Security Market Hamster Wheel



# Defining Risk

Risk = more things can happen than will happen

Risk = probability of occurrence X consequence

# Minimizing Risk

$$\text{Risk} = \left( \frac{\text{Threat} * \text{Vulnerability}}{\text{Countermeasures}} \right) * \text{Value}$$

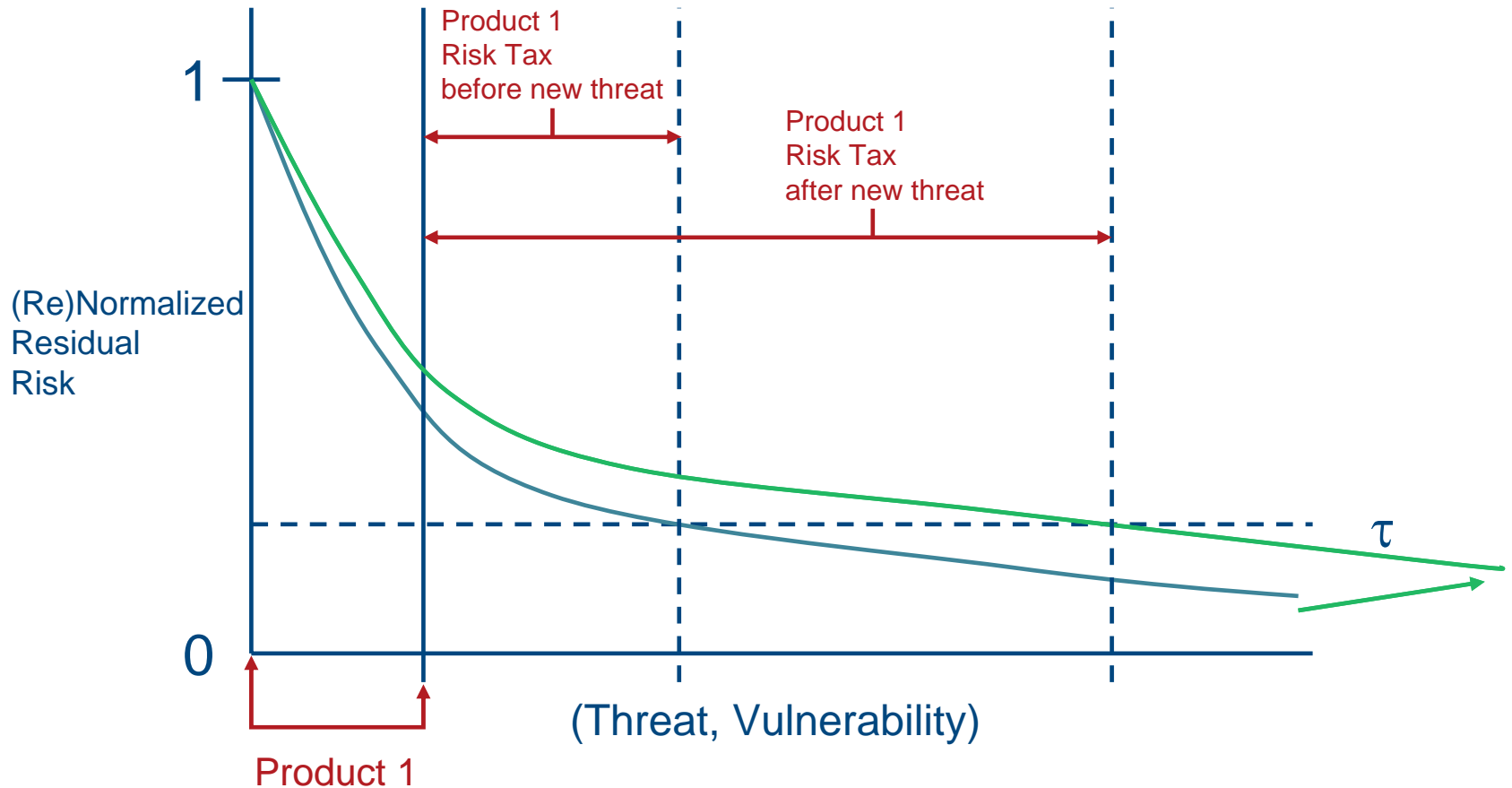
People or thing

Minimize this

Maximize this

Don't look at threat vs countermeasures.  
Consider vulnerability vs countermeasures.

# New threats increase risk

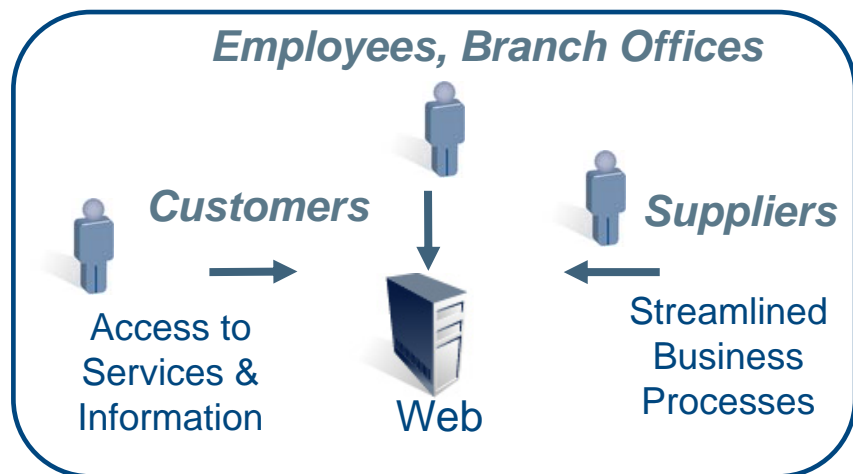


source: Bob Blakely, Burton Group

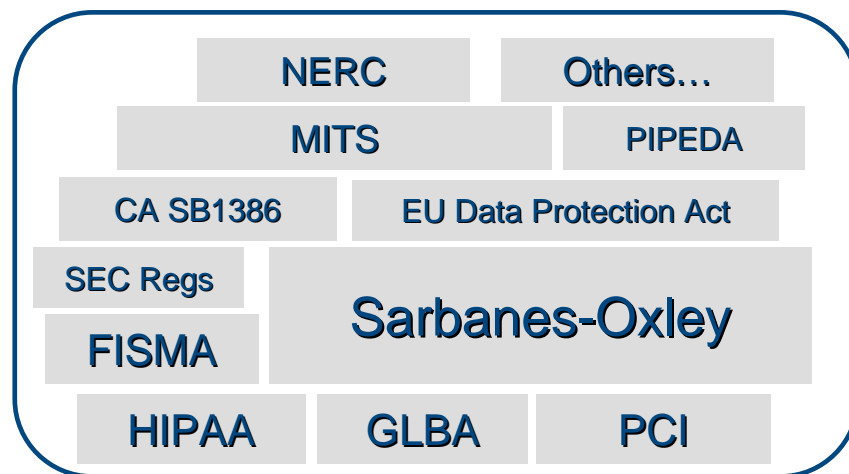
# Compliance Balancing Act is Hard

...and risk-based compliance is coming

## Extended Enterprise



## Governance & Regulation



**Policies, Procedures, Operations**

**Information  
Security Governance**

# Disappearing Perimeter

- Traditional IT security approach is to secure the network, however...
  - Technology shifts make the perimeter porous
  - An attack is an attack, internal or external
  - Protect IT assets from every threat, identified or potential
    - “it only takes one”: A single infected PC can take down an entire network

## Jericho Forum



<http://www.opengroup.org/jericho/>

- Promotes architectures and standards for the extended enterprise model, recognizing computing history as increasing connectivity over time
- Jericho Forum in a nutshell: “Your security perimeters are disappearing: what are you going to do about it?”



# Perimeter Security Controls now move to the Hosts

- Consider trying to spot the bad guy
  - In a crowded **football stadium**?
  - On the street in **front of your house**?
  - Trying to get **into a door or window** of your house?
- **Finer-grained filtering works.**
  - It is much easier to spot the bad stuff trying to enter the host. Knowing the application context helps a lot!

- Attacks keep increasing, and methods keep changing. Cybercrime is now a \$100B/yr industry
- Disconnect growing between danger levels and management estimations
- Application attacks recognized as a priority
  - Business critical traffic is main infection vector. Web and email cannot be blocked without shutting down the user
- Older network security controls not enough, host computers need to protect themselves
- Prioritize risks, work them in order