

Traditional security architectures for office environments build a perimeter that defends all of the company to the best of its abilities. Yet the modern workplace has and will continue to have increasing outsourcing, mobility of users and shared resources across the perimeter. Often the perimeter heavy model interferes with the business goals. This talk focuses on one such less traditional approach that departs from risk management to create a more flexible solution and potentially inherent more secure solution for the more adventurous security architect.

About

Section 66

Swa Frantzen

Security Consultant
swa@section66.com

Handler at the
SANS Internet Storm Center
<http://isc.sans.org/>

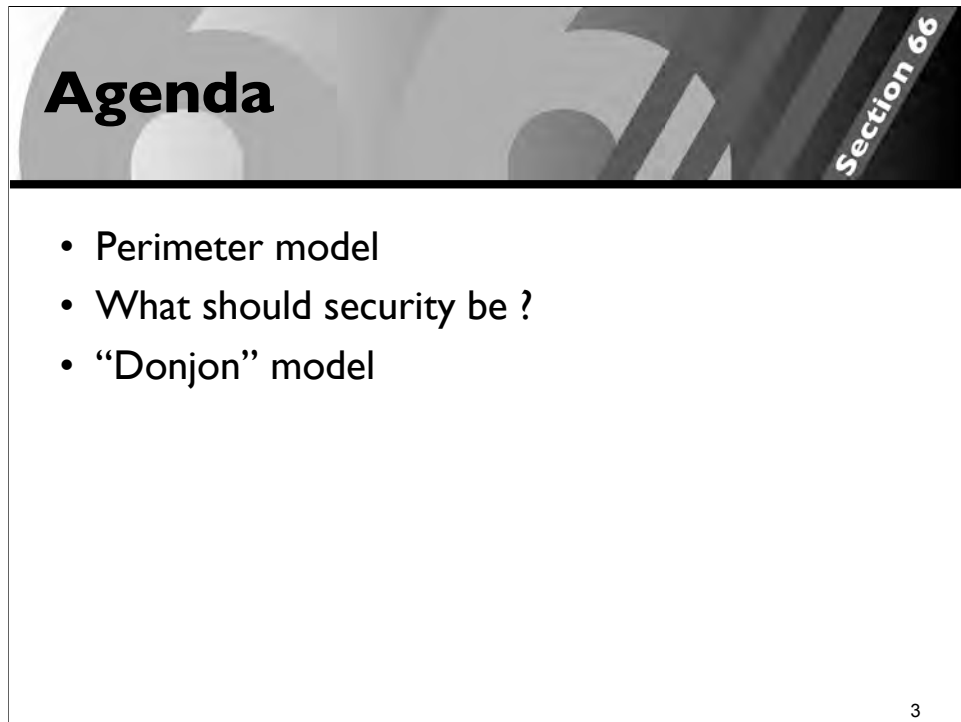
2

I'm an independent information security consultant during the day

After hours I am a handler at the Internet Storm Center.

I'll tell you today about security architecture. As such that is by definition less technical for most of you. I hope that if you don't do architecture yourself it is at least a pointer to how things could be in the future and where you could migrate to in a few years.

If you are a hardcore techie, use what I tell you as a way to try to understand what drives management in your company, because just as you feel they don't understand you, they feel the same. Teaching upper management technical skills is hard. So giving you some understanding is going to help to bridge the gap in the communication.



The slide features a decorative header with the word "Agenda" in a large, bold, black font. To the right of the header, the text "Section 66" is written vertically in a smaller font. Below the header, there is a list of three bullet points. The slide is numbered "3" in the bottom right corner.

Agenda

Section 66

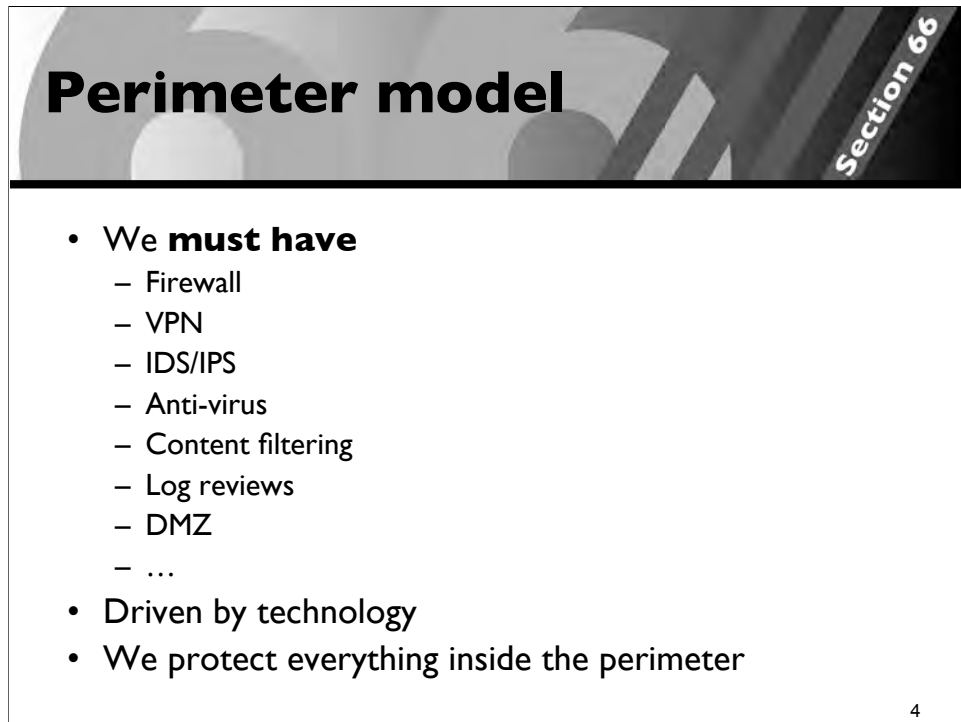
- Perimeter model
- What should security be ?
- “Donjon” model

3

First we talk about the perimeter heavy model we all use today.

Next we talk a little bit about what security could be today or tomorrow. The things in there are just not popular with most security professionals.

Finally we get to the reason of this talk and to provide a model that allows to combine what many in the information security field feel to be an oxymoron. It's rather early to switch to this model today but you can use elements from it today and prepare to migrate to it in the next year(s).



Perimeter model

Section 66

- **We must have**
 - Firewall
 - VPN
 - IDS/IPS
 - Anti-virus
 - Content filtering
 - Log reviews
 - DMZ
 - ...
- Driven by technology
- We protect everything inside the perimeter

4

Who uses perimeters in the physical world ?

- Military
- Prisons (kind of reversed, the bad guys need to stay inside)

What is a perimeter ?

- A line (or sphere in 3 dimensions) that you protect. You keep the good inside, the bad outside.
- Choosing it right is critical: drawing a line in the sand is what you do, but if you try it on a crowded beach it's going to get run over easily.

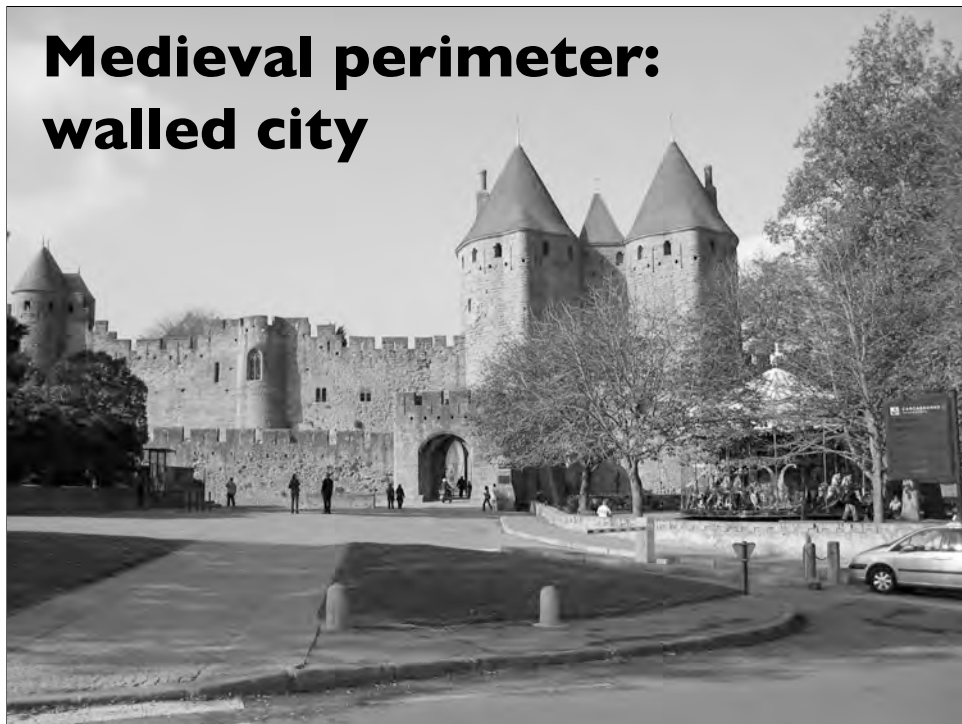
Perimeters work well if you can keep all the good inside and all the bad outside, yet it's not easy as we all know.

Today we are told we **MUST** have a load of things. Often this is done without giving a reason why you need it in your specific situation. It's a general rule that you need it and so you shall have it.

It's also driven by technology, Take the example of an IPS. A few years back there was no such thing, so nobody needed to have it. Come along the vendors adding capabilities to their IDS devices and we all **need** one more device.

The other example is that if any of the typical big 5 auditors come in and check the financial results they will instruct us to review logs. Reviewing logs is like seeking a needle in a haystack. Computers are good at it if you can define exactly what needles you look for. Unfortunately they don't tell you what needles to look for ...

Key thing to remember is that you protect all inside with the same measures. Measures that cost work and other resources.



Let's take a step back and look at what physical equivalent we (re-)build in the electronic world.

A medieval city as Carcassonne (France) got preserved pretty well and illustrates a perimeter very well.

Notice the modern perimeter around the old one, it's defenses are much more flimsy, yet they work very well to make you pay for using the parking lot.

This shows one of the two gates into the city. The gates themselves are relatively small (no big truck would fit through it).



Carcassonne, France

- 2 layers of walls
- Towers offering active defenses

Notice the modern gate as well.



Carcassonne, France

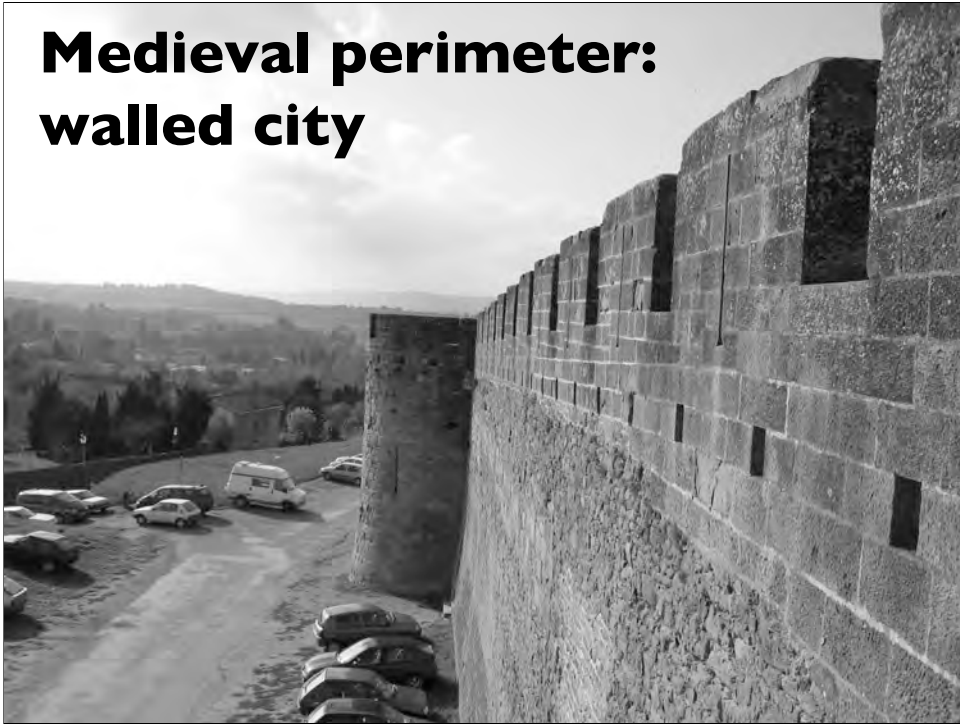
In between the two layers of the walls.

Notice the difference in level of the floor inside the walls and on the outside. The outer wall cannot be pushed over as it's supported by solid mass on the back side.

Also (not show here) the openings for the gates in both walls do not line up.

Once you are here and not a guard, you have certified your bad intend.

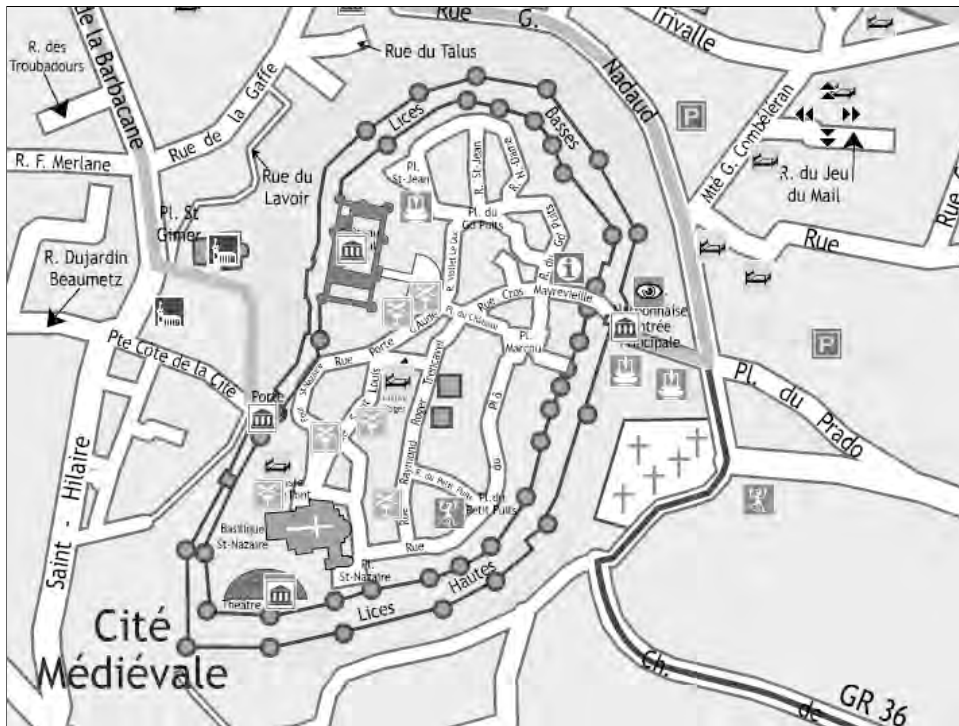
Medieval perimeter: walled city



Carcassonne, France

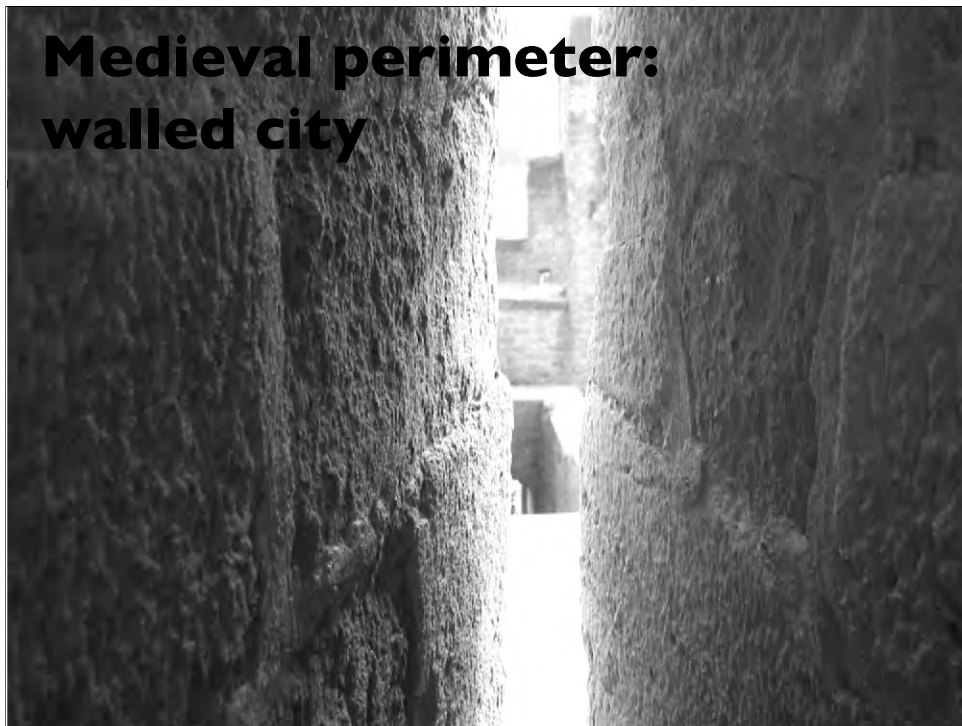
- High ground, overlooking the surroundings

This gives the defenders ample warning of the approach and intent of the opposing armed forces.



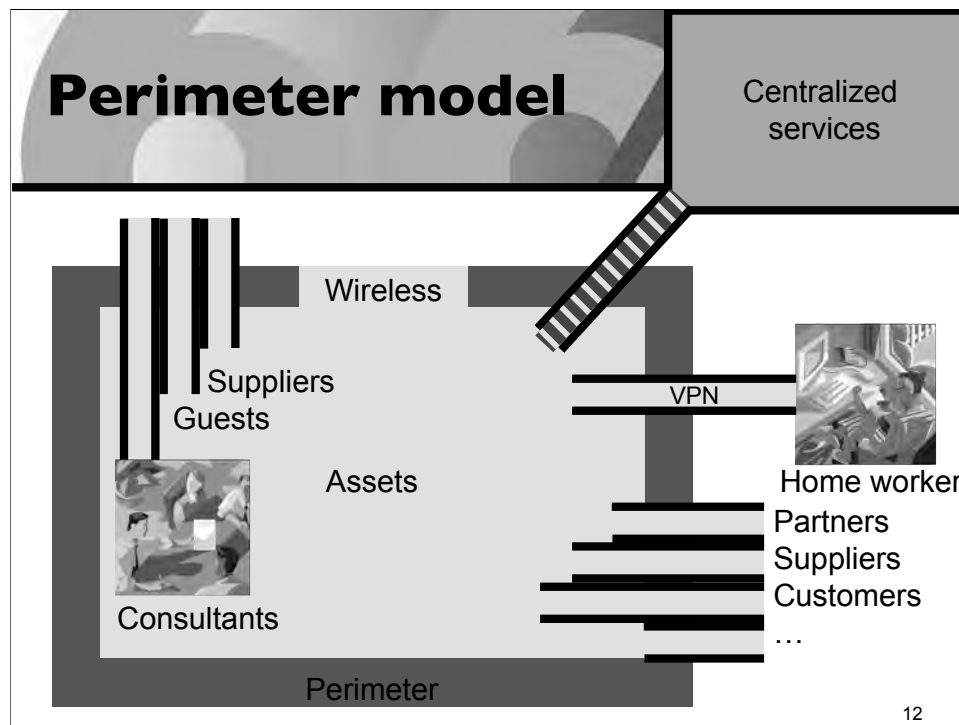
Part of a map borrowed from the tourist office of Carcassonne clearly showing the dual outer walls forming the formidable perimeter. It also shows the 2 gates through the walls.

See <http://www.carcassonne.org/> for the full version.



Carcassonne, France

- Overlooking one of the gates you can actually see outside to shoot arrows at the intruding forces should they get through the outer doors.



We start off by gathering our assets, and protect them by our perimeter.

Next we discover we have home workers that are essentially good guys (i.e. assets) but that they are outside the perimeter. Of course there is a solution to this common problem; A VPN is called to the rescue.

But there are more of those outsiders that need some access to our assets on the inside so we create more holes to let them in, even if we have little to no control over what they do.

All inside isn't under control either. We have consultants that need a way to get back to their assets inside their perimeter while stationed with us. Similarly suppliers deliver us with equipment that will call home and report problems before we know about it. It's cool to receive a hard disk to repair our storage array before we reported the problem to the supplier, but that array might hold stuff that vendor has no business with just as well. Also we all know the guests we end up with in a meeting room that need to check their email, show us a demo on the Internet or the like.

Wireless networks are a special breed on their own. The physical limit of communication is a factor of BOTH sides, so we cannot control how far it works. Equally annoying is trying to protect it with broken encryption, hard to maintain authentication and the like.

Add centralized services:

- Push email from your service provider to your phone, blackberry, ... requires the service provider to have access to your mailbox. So they basically get the spare key and will safeguard it for you.
- .mac users make backup of their machines and store basically everything at Apple
- Gmail users store their email at Google
- Google desktop users allow indexing at Google form stuff on their machine
- ...

Your laptops also don't stay inside the perimeter, they are used in hotels, at conferences, in airports, on the beach over a hotspot, at home on a broadband connection, ... so we need to protect them equally well.

Outsourcing

- The business might need to outsource to get a economically viable model, yet it's a security nightmare to integrate it.

Mobility

- Who's the first to walk into your office demanding to connect the newest wireless "toy" ?

Basically instead of the fortified city we end up with the picture above. Swiss Cheese.

The bottom line is that we are afraid

Wireless & 'backdoors'

WiMAX, WiFi, GPRS, Bluetooth, modems, ...

3rd parties

Outsourcing

Contractors

Laptops

People taking data home on a laptop

Malware


Guests

...

Issues with the perimeter model

Section 66

- Maintaining the perimeter is hard
- We tend to forget important aspects
 - Data, Availability, Internal threats
- Things that threaten the perimeter model get a 'NJET' from security
 - Frustrated security staff & frustrated management
- No match with other management systems such as quality (ISO 9001), environment (ISO 14000) etc.
- Little to no buy-in from management



15

Maintaining the security perimeter is hard in a real business

- Lots of effort;
- Lots to loose if we loose the perimeter;
- Lots of fire-fighting to regain the perimeter with constant battering of requests to open up to some business need.

Data is to be protected, but we tend to focus on infrastructure. And tend to forget about all other means that data can leak.

Availability is an integral part of security, yet even in our inside jokes we forget it.

Insider threats are very risky to our data as they are inside the perimeter to start with.

Is your boss convinced you need security ?

Is you're the owner of the company interested in our technology, or is he interested in making a profit with a certain level of acceptable risk ?

Security staff often is much more worried about image and low level assets than the rest of the business, including marketing and upper management.

Security people are stuck with a model that often tends to conflict with the business needs, leading to frustration on both sides.

We do the same effort for all assets we have. And if we differentiate we generally add costs and effort, hardly ever do we decrease the effort spent.

Information Security needs to be managed, yet quality, environment, IT service delivery and lots more need the same kind of management and the same people across the organization need to be involved.

e.g.:

- Discarding laptops

- Aspects involved:

- Quality (if this brand is bad, we need feedback to purchase to try to do something about it)

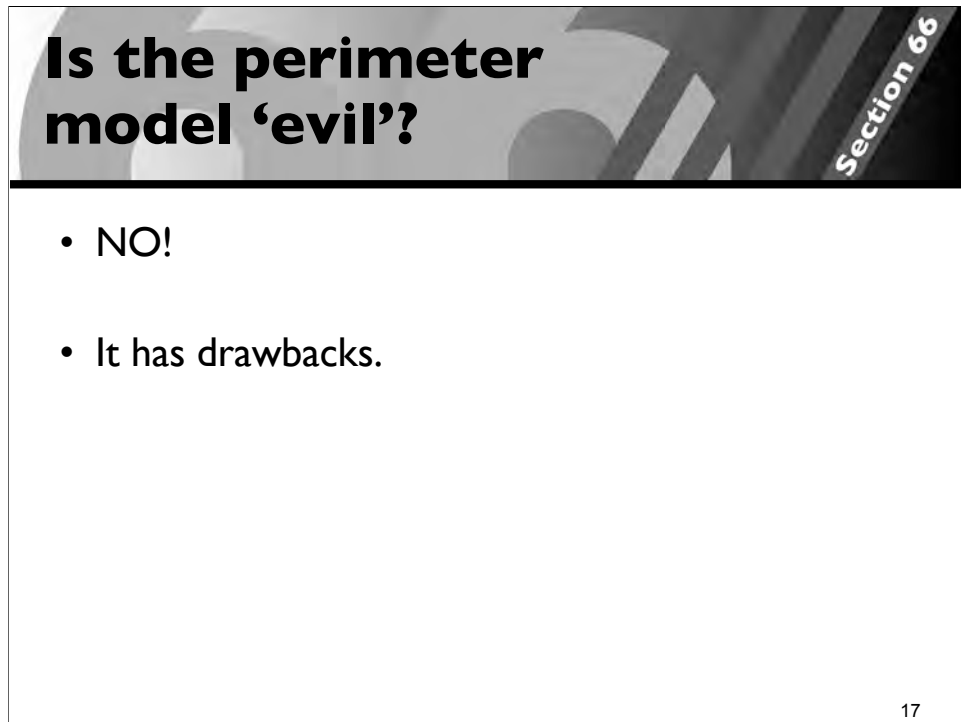
- Environment (contains stuff that should not be trashed)

- Security (hard disks etc can still contain data)

- ...

--> one low paid guy, at least half a dozen complex policies ?

- If the organization cannot create a one page instruction, something will go wrong.



Is the perimeter model 'evil'?

Section 66

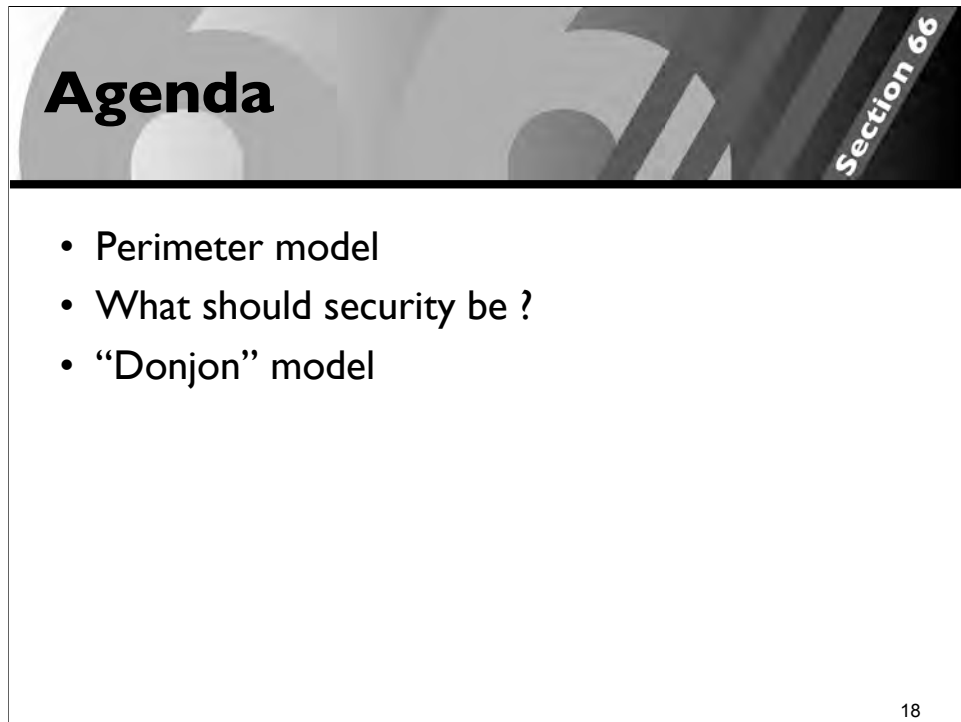
- NO!
- It has drawbacks.

17

While it has drawbacks, this is the model most of us use today. Our vendors cater for this model. Our auditors force us into this (unless you convince them).

Many use variations on the perimeter heavy model adding:

- Defense in depth: it is adding more layers (building thicker perimeters).
- Compartments: The titanic was built with compartments. They obviously failed to work as intended in that case. But the principle is sound and still used today in shipping.



Agenda

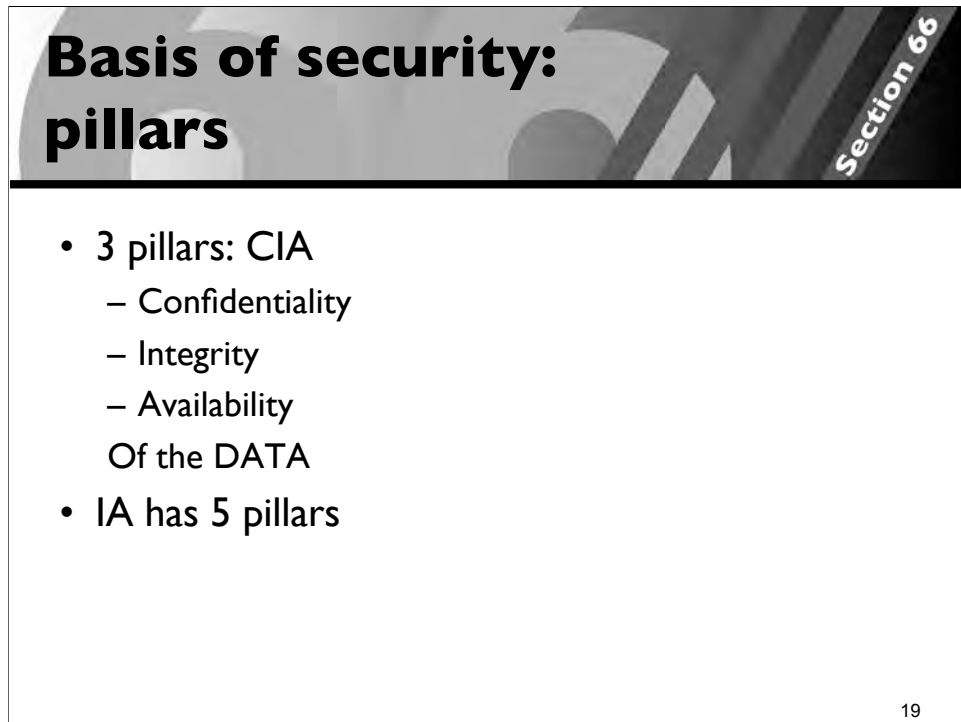
- Perimeter model
- What should security be ?
- “Donjon” model

Section 66

18

What should security be ?

This section contains a description of a few of the things that we could be doing today. While many of us know we could/should be doing it, for some reason many of us aren't really.



**Basis of security:
pillars**

Section 66

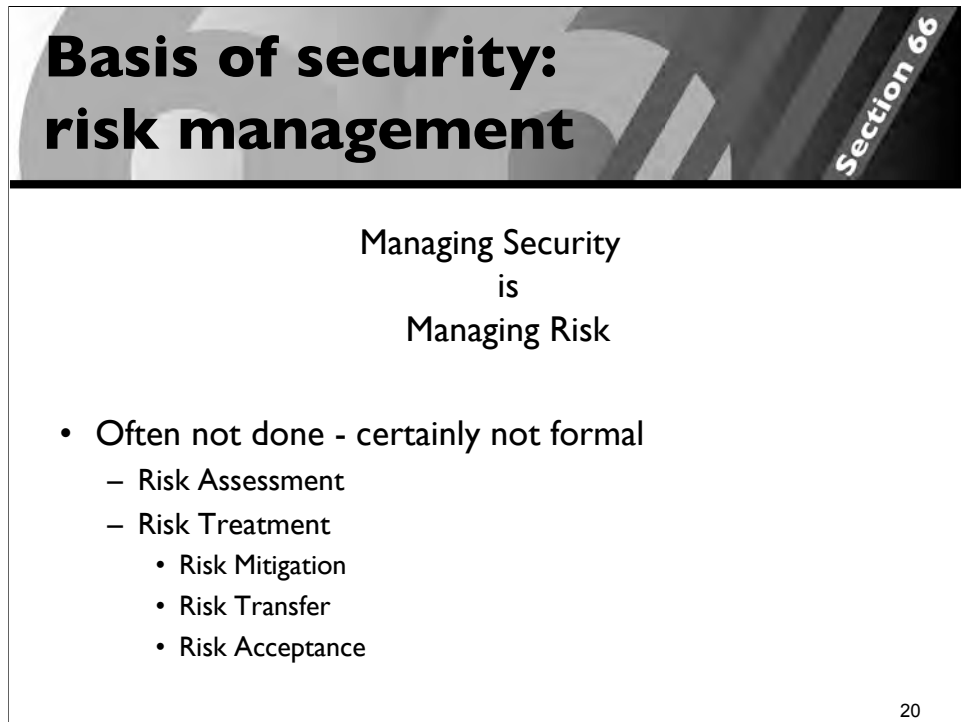
- 3 pillars: CIA
 - Confidentiality
 - Integrity
 - Availability
- IA has 5 pillars

19

Information Assurance (IA):

Non repudiation and authentication are emphasized, in the CIA model they are included in the rest.

The important part is that availability is in here, so we cannot forget it anymore and the solutions that ignore it are automatically invalidated.



**Basis of security:
risk management**

Section 66

Managing Security
is
Managing Risk

- Often not done - certainly not formal
 - Risk Assessment
 - Risk Treatment
 - Risk Mitigation
 - Risk Transfer
 - Risk Acceptance

20

Managing risk to CIA

Risk to each of them individually.

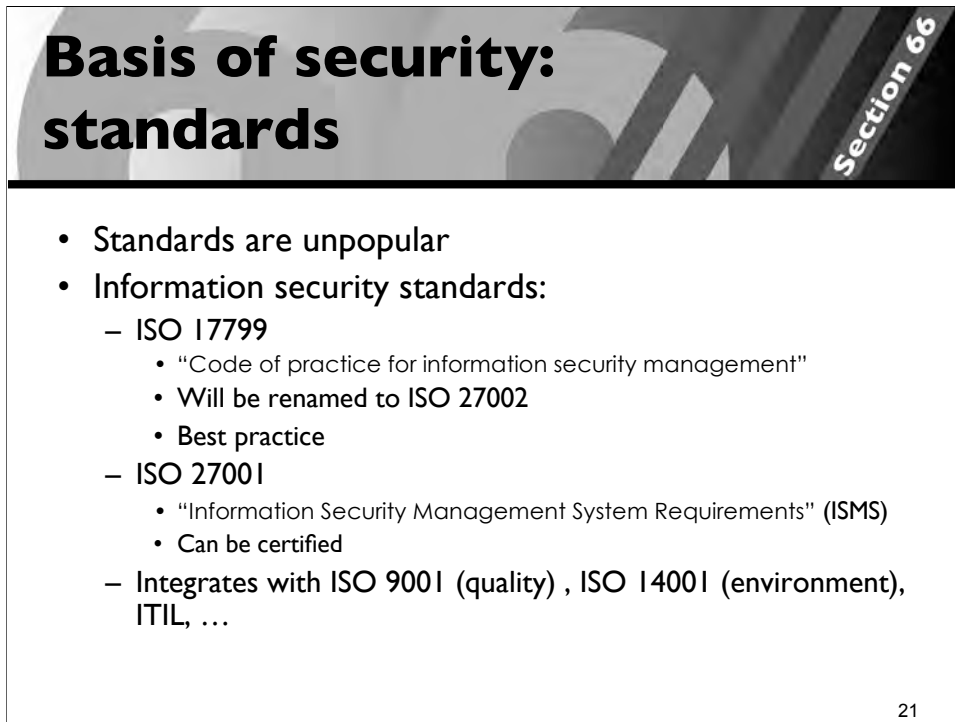
Risk assessment is mathematics: Risk = sum (impact x chance), but at the end of the day we calculate with guesses to end up with an educated guess.

Dealing with risk is something we do daily, we take risks from the moment we wake till we go to sleep (and even then).

Yet, even despite our familiarity with risk, it is still very deceptive to us.

Example of aircraft vs. car: we are more scared of planes, yet we know they are statistically safer than cars.

Example of earthquakes in e.g. California. From a distance, we tend to see it as a high risk, yet with the regulations out there and the low chance of a specific place being hit by a “big one” the risk all in all is low.



Basis of security: standards

- Standards are unpopular
- Information security standards:
 - ISO 17799
 - “Code of practice for information security management”
 - Will be renamed to ISO 27002
 - Best practice
 - ISO 27001
 - “Information Security Management System Requirements” (ISMS)
 - Can be certified
 - Integrates with ISO 9001 (quality) , ISO 14001 (environment), ITIL, ...

21

Security standards are not popular for some reason. Yet they are there and could be used if we wanted to.

Part of the unpopularity might be that you can create a situation where the certification differs from the real situation (paper only exercise) . The other part might be that the certification is seen as a hassle. But you do not need to certify to get most of the benefits.

BS 7799 started in 1994,

ISO 17799: (formerly BS 7799: part 1, last reviewed in 2005)

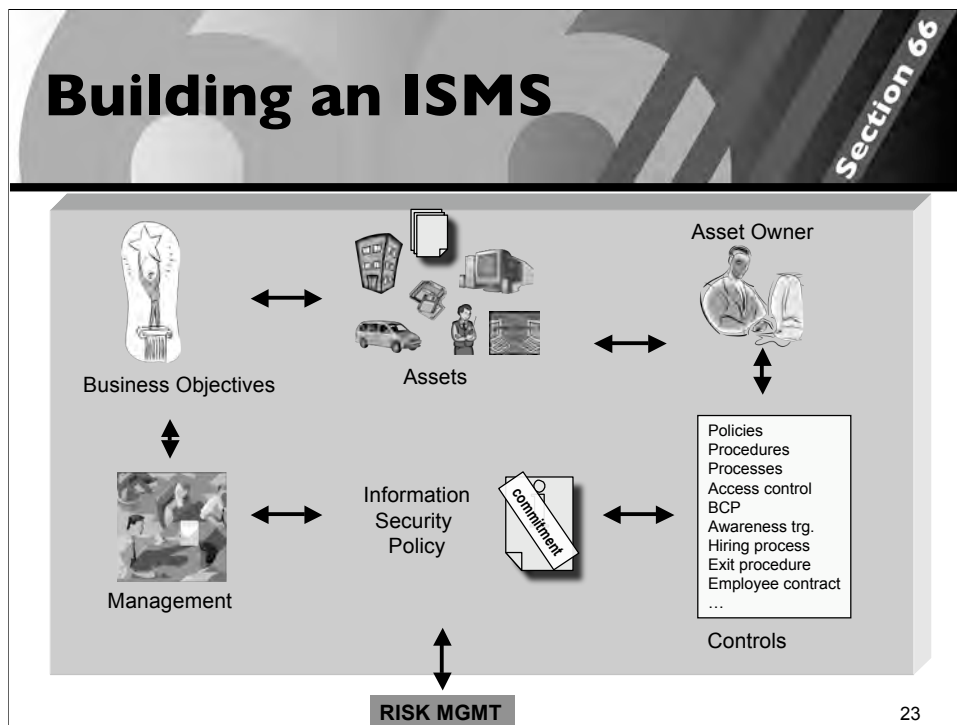
- The best practice that addresses itself to management.
- NOT technical
- Tells you what a business could consider to do and why it should be done.

ISO 27001: (formerly BS 7799 part 2, last reviewed in 2005)

- The part that tells you to do risk management
- Build a Information Security Management System (ISMS)
- And at the end you need to clarify which controls you added to ISO17799 (and also which you felt you did not need)

BS 7799 part 3 is still in the works. (Will be about risk assessment)

Integration of all management systems for all aspects into one management system is known as building an Integrated Management System (IMS).



It all starts (or stops) with Management.

The have Business Objectives. Business objectives are clear, and by definition important.

In order to achieve the objectives assets are needed.

Now take the assets, the objectives and their relative importance an do a high level risk assessment (just a few pages, noting elaborate needed).

From that result you know what is important to management and you can clarify why it is important.

A high level security policy tells why things are important, what we want to work on and is short.

That high level security policy has to empower the rest of the organization to do what needs to be done.

Management commitment to the high level policy is also the only commitment you'll need.

With the guidance given by the high level security policy, take the risk assessment to a detailed level with the asset owners. And get the components they need in the different controls (policies, procedures, processes) such as the Business Continuity Plan (BCP), awareness training, ... can be determined.

Now take a step back and integrate the components of the controls into the controls that are empowered by the high level security policy.

Once these are completed, you have an ISMS, 'all' you need to do is to implement a process of continuous improvement.

Having a (certified) ISMS is popular in the UK, and in Japan.

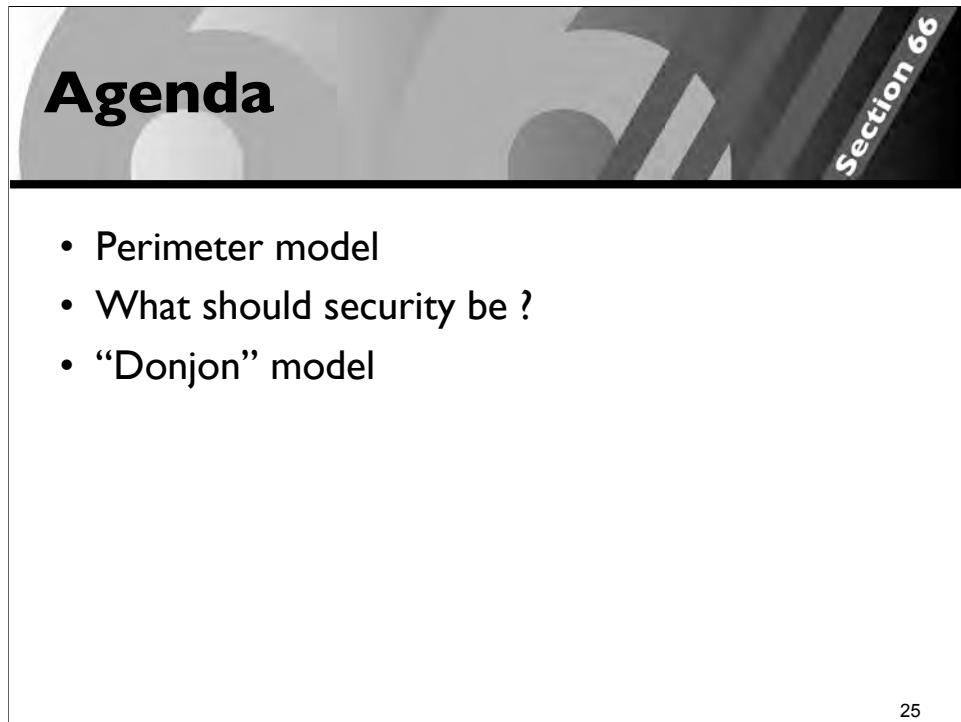
Suppose we have a formal ISMS

- Security becomes less of a technical problem
- The technical problems become implementation details
- At the core it is a management problem
- The goal is managing risk (not always reducing!)
- Management support is "automatic"

Take care: an ISMS can easily lead a life of it's own. The ISMS should not be the goal. Getting the security in the business under control should be the goal. Know why you do what you do.

Certify or not ?

In my experience, building an ISMS in order to get a certification is dangerous to end up with a paper only exercise. The alternative is to go slow and start small, grow into it. Use the continuous improvement cycle a few years. Once you have that, certification should be easy and gives an external confirmation you are doing the right thing.



Agenda

- Perimeter model
- What should security be ?
- “Donjon” model

25

Over the years I've been dealing with security I got shocked on a day a realized I was slowly migrating to a model that did not use the typical perimeter as we all know it. So be ready to get shocked. I'm handing this model to you as a piece of a puzzle that might fit in your puzzle. I'm not saying it fits today.

Actually I'm confident it will be a model that you can use in the future. Just remember that the world might not be ready for it yet.



Let's start with some more inspiration beyond the perimeter model from the medieval times.

This picture is taken in the town I was born in: Tongeren, Belgium

I'm not sure from exactly to which period this defensive work dates (Tongeren was built by the Romans), but notice the slope on the outside and the straight wall on the inside. It's noting compared to Carcassonne, but it would stop you in your tracks if you tried to get across in a coat of arms.

BTW: Tongeren also has walls, and in multiple layers, but that's another story.



Another moat that protected part of a village. The water level was intentionally lowered to reduce risk to modern usage of the area. It's standing water, which can be seen from the huge amounts of algae in it.

Donjon



A “Donjon” is actually a word with a French origin. It got used originally for free standing fortified towers like this one. Later it got used for the tower that was the strongest fortified place inside a castle. Now if you have a castle and few threats, you would not want to live your days in a tower without windows. So the tower got used for other things, such as keeping prisoners. From there the name turned into dungeon. And even when the function eventually migrated into the basement the name followed.

This particular Donjon is actually inside the moat in the previous slide. It’s located in a village (the center of the village is actually behind the donjon) The village is called Brustem and is located in Belgium as well.



Closer up views of the donjon. I'm standing in the moat while talking these pictures and the scaffold has been there for years. Many decades ago half of the tower collapsed when people tried to modify the function on the donjon. Originally it had 5 floors, each with different functions.

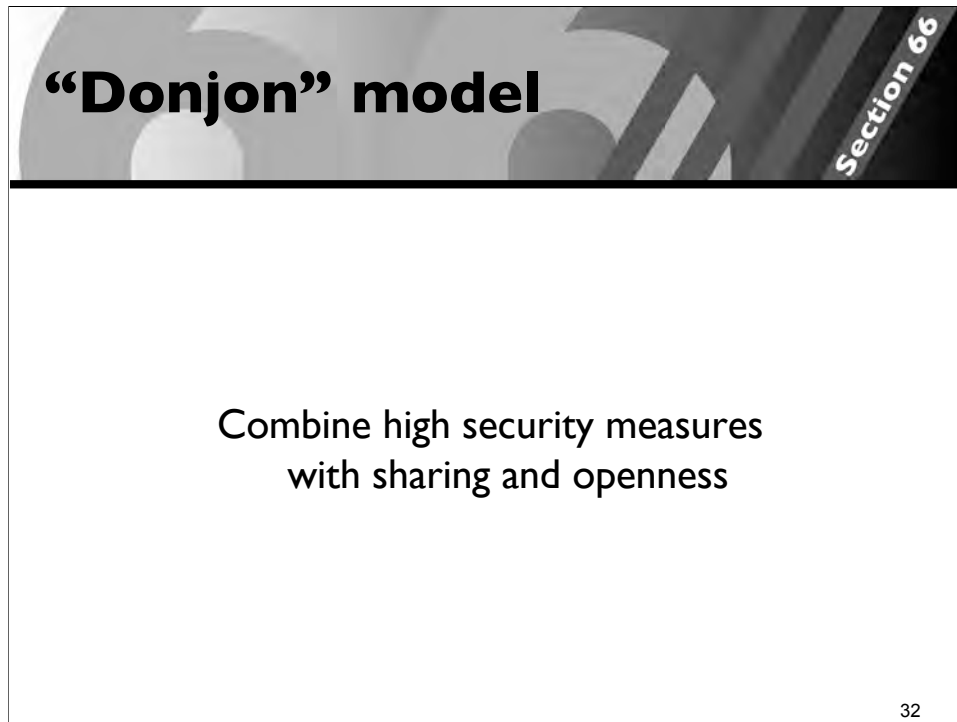


Aside from donjons, and moats some cities kept one of their most precious assets in a tower of another kind. The belfry generally kept the papers that gave the city the right to be a city (to be free). They kept it in this tower that served other purposes such as being able to see the surroundings and it was also used as a bell tower as well.

This particular example is from Herentals in Belgium. It's been rebuilt over the years and currently houses a.o. the tourist office.



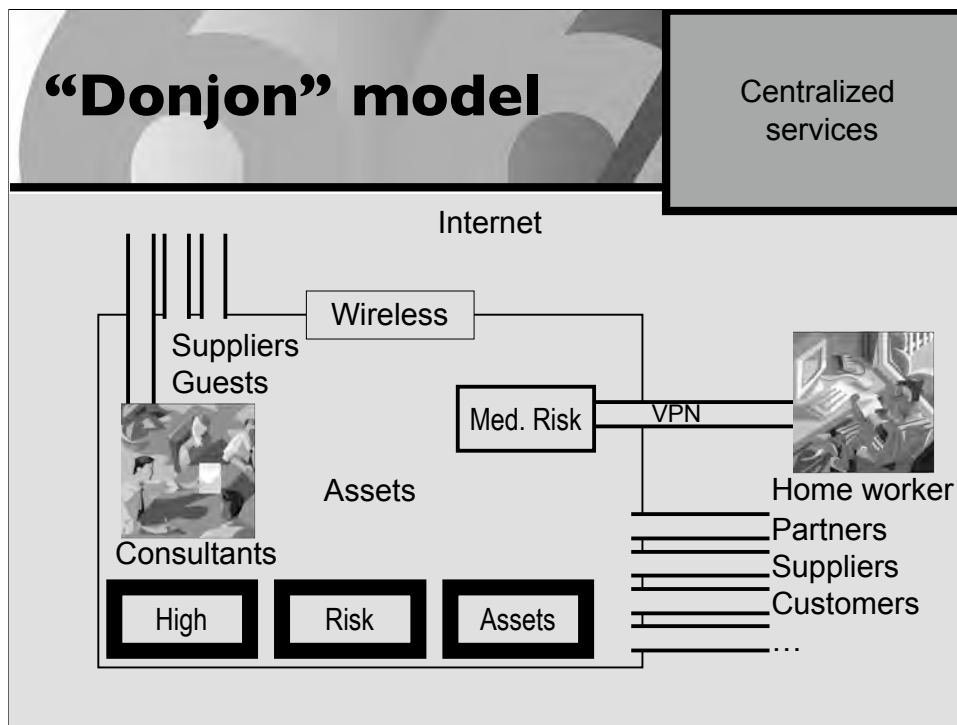
Castles or fortresses were other options. This particular Fortress was actually in Carcassonne in France inside those thick walls. It also had its own moat and drawbridge, but both of those are gone.



The slide features a dark header with the text "Donjon" model in white. A diagonal label "Section 66" is visible in the top right corner of the header. The main body of the slide is white and contains the text "Combine high security measures with sharing and openness" centered. The number "32" is located in the bottom right corner of the slide.

There you go, the mission of the model.

It does appear to be almost a contradiction, yet it could solve a lot of the problems we face with our current setups in the future.



Let's start with our assets, but instead of building out of habit a heavy perimeter around it, let's be open.

Still we need some protection, so let's start to classify our assets.

Risk assessment

- low
- medium
- high

We invest heavily in very tight protection of the high risk assets.

The medium risks assets might get a bit of protection,

We do the absolute minimum for the low risk assets. Basically we could try to get to a point where we do nothing that an average home user would not do.

It's important to try to minimize the high risk assets. You should have few. Part of the final kick I needed to get to this model was the realization I could not find any critical asset on one of the shareholders/managers of the company I was working for. I couldn't believe it myself. Amazing to me was the realization that he did not consider his business plans as "secret". He said that if his competitors did not know his business plans long ago they would be dumb.

Put most protection effort in high risk assets.

Embrace openness, wireless, gadgets, home workers, the use of all sorts of services in the low risk arenas.

If one of your home workers needs access to a medium risk asset, a VPN might be a good solution. But still you worry little about it. The things you focus most of your attention on are the high risk assets.

All the connections through the "perimeter" that contain our low risk assets don't worry us anymore all that much.

The thing we do worry about greatly are the high risk assets. And we'll go through extremes to protect them.

The starting point

Section 66

- High level risk assessment
- Management support
- Split assets
 - High risk: Donjons, strict rules, extreme protection
 - Each family gets their own Donjon
 - Low risk: openness, freedom, minimal protection.
 - A moat or palisade will do.
 - Trick to combine both.

35

Let's think back to the creation of an ISMS, we take the part of building the high level security policy in order to establish the importance of what we do, get a clear definition of the extreme measures we can take on the high risk assets and the acceptance of the risk on the low risk level assets.

You cannot do this without management support. Especially not since you deviate from the usual solution.

We need to create that link between what's important for the company and what we're doing.


Basically, to draw back on the medieval analogy, we divide the people inside our village into nobles (few) and the footmen (the rest). We protect the nobles, if we can we might do something to keep the rest happy at best, but we like them to be expendable and cost-effective.

The difference might be that we offer the nobles little to no comfort, but also little to no freedom. While we offer the other all the freedom we can.


80-20 rule ?

Section 66

	Low Risk	High risk
Assets	80%	20%
Effort	20%	80%



LOW RISK



HIGH RISK

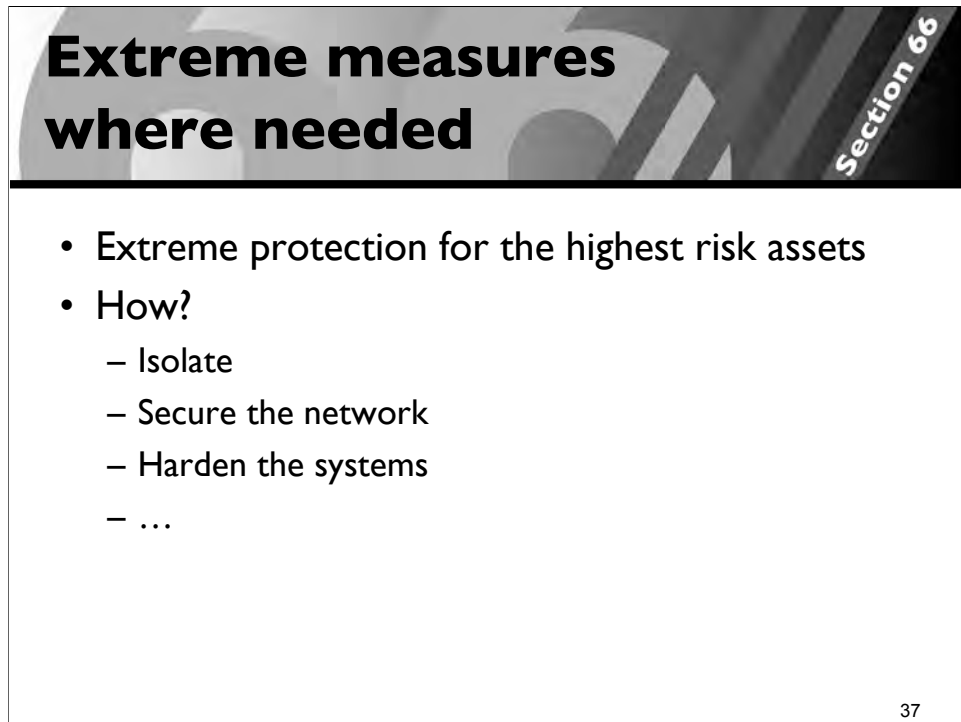
36

Managers love 80-20 rules.

Instead of spending 100% of the budget on protecting all the assets equally (which in a managers mindset will tell him only 20% of the money is actually spend on where it hurts), Telling them you are spending 80% of the budget on those 20% of the assets they identified as critical is a winner.

If you do this with a budget of 100\$ to spend on 100 assets in a flat perimeter heavy model, each asset would get 1\$. If you follow the above, you end up with the critical assets getting each 4\$. There is today no other way to increase you resources to protect critical assets by such a factor. It works here because we make sure the spending stays with the critical assets and does not get diluted by all other assets the organization has.

Of course you need to match it with measures to make sure those 20% of the assets are the critical ones and that the other 80% of the assets don't get infused with critical assets over time. But the potential savings on your security spending will allow for some inconveniences.



**Extreme measures
where needed**

Section 66

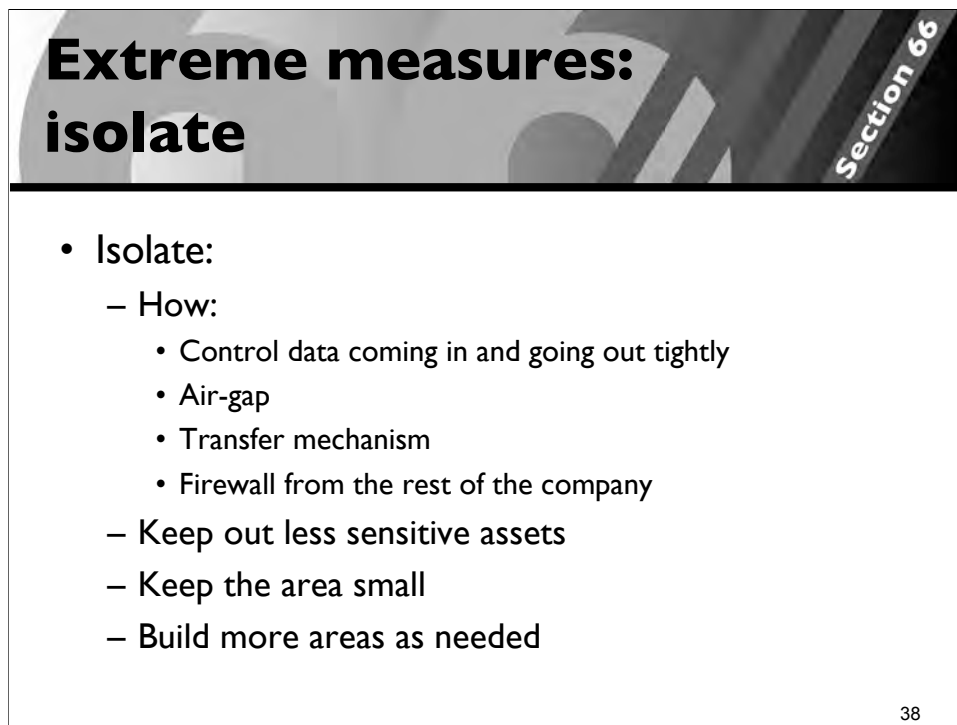
- Extreme protection for the highest risk assets
- How?
 - Isolate
 - Secure the network
 - Harden the systems
 - ...

37

We build a very high level of protection for the critical assets.

We make sure they are located in one place and take little care for usability and comfort of the users in there. We remind ourselves that availability is critical to maintain as well.

We build such an environment for each kind of critical data we have. Not one big one. Should anything go wrong with the protection at least we'll only have one of these donjons to deal with, the rest remains working as before.



**Extreme measures:
isolate**

Section 66

- Isolate:
 - How:
 - Control data coming in and going out tightly
 - Air-gap
 - Transfer mechanism
 - Firewall from the rest of the company
 - Keep out less sensitive assets
 - Keep the area small
 - Build more areas as needed

38

Transfer mechanisms are critical to get under control.

An air gap is a good idea but you'll soon discover there is genuine need to get data in and out in many cases. Controlling it right is the key to success.

Make sure you are guaranteed to know Who did transfer What, When and Why ? For added bonus know How and on who's Authority.

I've tried to build it with allowing CD-R's to be passed, but your audit trail is so weak that it's just not working. Similarly any solution using removable storage is weak. As it also allows data from the more critical network to leave the building all too easily.

From what I've built in the past, the easiest way to build this is to add a dual homed machine in between that is draconically configured.

E.g.:

- Machine logs every command given on the command line
- No graphical card in it,, no graphical libraries installed at all
- AV scanner on it
- Connect to both the more and the less critical networks.
- Fully configured firewall on it allowing only ssh connection to the less secure network and from the more critical network.
- Basically the transfer goes as follows: user logs in on the transfer machine from the more critical network; initiates an scp to copy from the less critical network e.g. an image for a router downloaded and tested in a test lab beforehand. Such test labs should not be critical assets. Next the user performs a procedure on it to verify the integrity of the file and to record the reason of the transfer. The users sets the file after verification in the transfer to the more critical side area and logs out. Next from the high risk side (s)he goes and fetches the file from the transfer machine.

Keeping the areas small and building more of them is a way to contain problems to a small subset of your assets. Divisions can be made on either the level of criticality and/or the set of people needing access to it. It's unlikely the accounting department needs access to the same critical assets as the engineering department.

Extreme measures: network

Section 66

- Network:
 - Prevent unauthorized machines
 - Prevent client-client communication

 - Disallow dangerous usage:
 - IM
 - Email
 - Surfing the web

40

An example of how to setup a network in extreme security mode is to make sure

- All ports of the switch are allowed to only learn maximum one MAC address (any unauthorized hub/switch will trigger a shutdown and incident response)
- All unused ports are shutdown
- All ports are documented what is supposed to be attached to it. A full inventory of the MAC addresses is available, any port learning a MAC address not authorized in the secure network will drop the machine in a separate VLAN blocking and logging all traffic and triggers an alert and incident response.

Sure this will generate some alerts and exercise in the first days, but people learn quickly that the critical network must not be messed with as it locks them out. I've found it works well in real life once people know they should not even think about it in that environment.

The other example of what you can do (especially if you have machines with “weak” default security) is to disallow client to client communication in the switches (higher end switches can do this, e.g. Cisco calls this private VLAN) Where you designate only certain ports that can talk to the others, the rest isn’t allowed to chat among themselves at all. While it might be unexpected for some users it teaches them quickly that they should not play on this network with e.g. peer-to-peer sharing of stuff (it simply looks like the machines are not connected)

If the highest threat comes from the Internet and the rest of the organization, keep the amount of interaction under control, just as you would do today, but you can disregard user objections and go much further in it.

More later on how to keep the users happy.

Extreme measures: harden systems

Section 66

- Harden systems
 - Build method: 100% reproducible
 - Turn off unneeded services
 - Keep data central and tightly controlled
- Monitor tightly
- KISS
- ...

42

Hardening systems goes beyond the scope of this talk, but you can go very far in it. Just make sure the machines are still capable of patching themselves, as you'll need that feature anyhow.

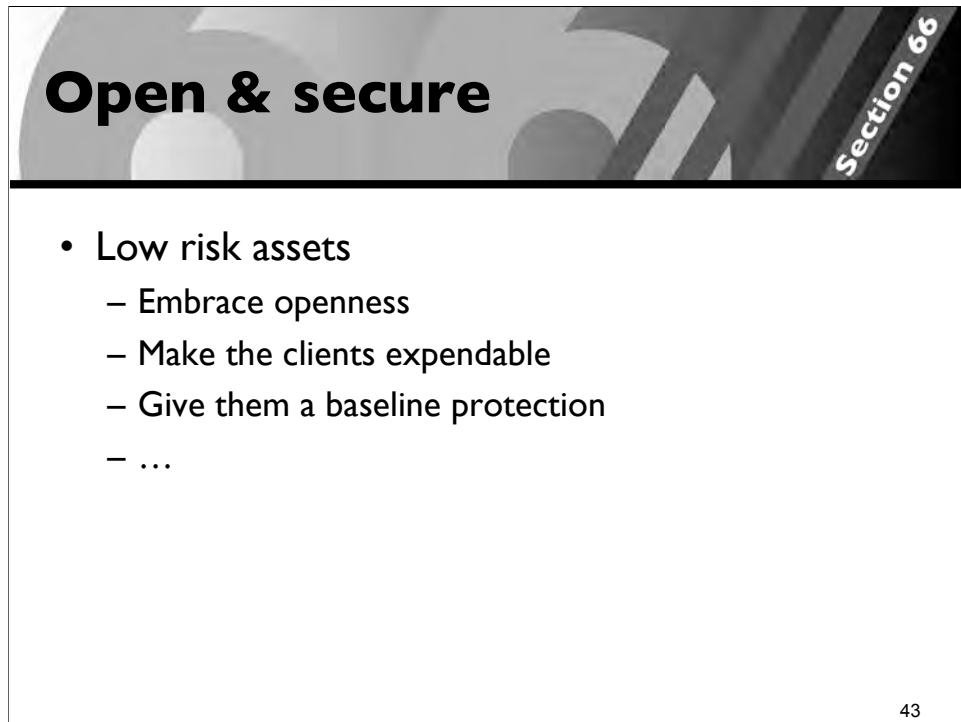
Make sure you can reproduce an identical machine quickly, this is not only good for the availability, but also to enable you to compare the running instance with a fresh copy and detect discrepancies. Either they can be justified through change management or either you have an incident to deal with.

Keeping data central and controlling it tightly with good audit trails helps a lot in case of incidents.

Monitoring tightly allows to detect problems early.

KISS: Keep it simple and Stupid

A general engineering principle, but use it, the simpler it is, the simpler it is to understand when it does not work as intended.



Open & secure

Section 66

- Low risk assets
 - Embrace openness
 - Make the clients expendable
 - Give them a baseline protection
 - ...

43

For all the non critical assets we step down on our security stance and just build the equivalent of a flimsy wooden palisade.

In here we allow freedom, keep usability very high on the agenda, we still make sure we are aware of any incident or deviation of the few policies we have left over.

Key to success: keep the critical and the less critical assets 100% separated.

Open & secure: embrace openness

Section 66

- Empower the users
- Mobility
 - Employees work from hotels, conferences, airports, home, ...
 - Wireless networks
 - “Get all the gadgets working”
- Guests: Internet access
 - GuestLAN

44

In my experience the first to show up with the expensive new gadget is nobody else then the big chief. Let them play with it, just keep them away with it from any critical asset. And if you've done the needed awareness they won't even ask for the critical assets unless you over-classified the data.

GuestLAN is basically the same technology as used in the extreme case: any unknown MAC address causes the port to be dropped in another VLAN. But this time the VLAN gives plain and simple Internet access. This is why they connected it in all likelihood. Be open ...

Open & secure: expendable clients

Section 66

- Laptops get stolen/lost/exploited/...
- Build clients with a easy to redo procedure
- Try to move data off of the clients
- Be strict to disallow all high risk information
 - It's to be only in the donjon

45

One way to get the low risk machines more expendable is

-To make sure there is an easy way to rebuild the functionality the user needs on another device.

-To make sure no data is stored on the machine (also removes a lot of trouble with backups).

-To disallow even consulting of high risk assets.

Open & secure: baseline protection

Section 66

- Anti-virus
- Patches
- Able to defend themselves
- Keep a (minimal) watch over their condition
 - Central reporting
- Diversity on a global scale

46

Anti-Virus.

•With the rapid pace of development it's still a question if the vendors will be able to keep up with the attackers. Considering the massive attacks are mostly over. And that the attackers now prefer more low profile attacks and highly targeted attacks. The question is much more if the anti-virus vendors will be able to help protect you at all as they might never get a sample for the thing the attacker made to hit *you* and designed to be there for years to come unnoticed.

•Anti-Virus measures are 100% sure also needed on non windows machines. No OS is not vulnerable to viruses, get the infrastructure to update signatures in place while you have the time.

Patches:

•Need them often, need them fast!

•Testing patches to make sure they do not interfere with critical assets: now much easier and much easier to take your time as those assets are in your Donjons that are not exposed. And the other assets will probably have to do with whatever the vendor did for testing.

•Most vendors still lack in admitting they messed up, in fast response, in not bundling with other features, in allowing individual things to be patched separately, in allowing you to do your own risk analysis of when to deploy, ...

Ability to defend themselves

- “personal firewall”, and anything else a typical home user would need. Is needed on your roaming clients.

Central reporting

- As you give more freedom, you need to replace it with monitoring so that e.g. you get reports of which roaming machines did not get the latest patch or did not get the latest signatures for their Anti-Virus.
- Make sure that you, as a shepherd, can go and find the lost sheep.

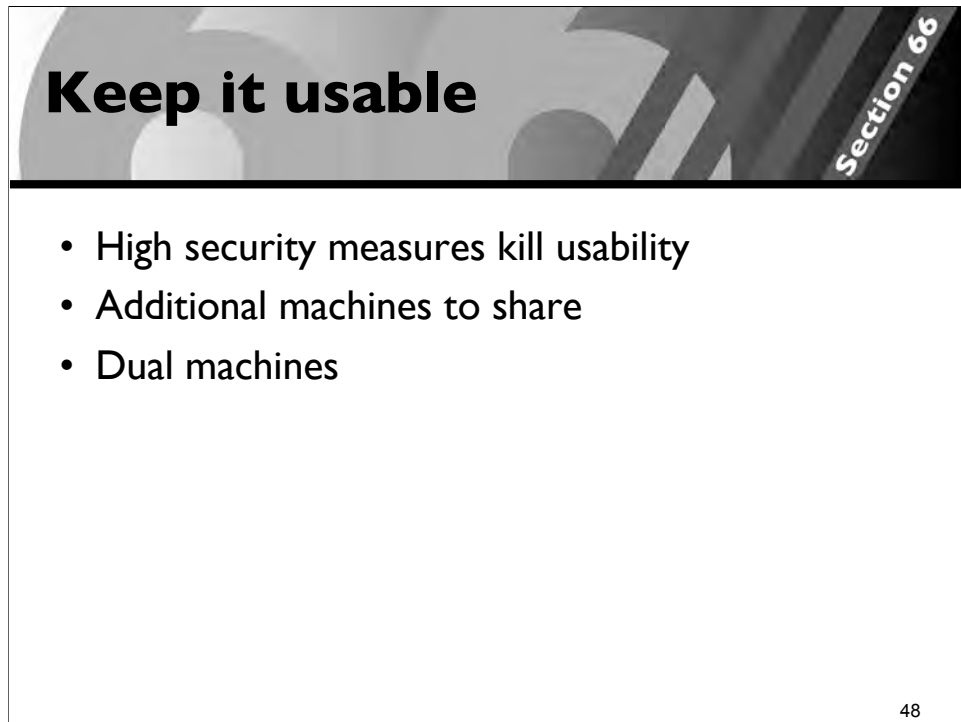
Diversity

To hackers it's interesting to create exploits and learn about flaws for a wide range of machines. It drives up the value of the exploit. Now if everybody uses the same, we all made ourselves more vulnerable as the bad guys need only to develop for one combination of application and platform.

- If 90% of people use a certain browser it's interesting to create exploits
- If 95% of machines use a certain strain of an OS ...

Do not make the bad guy's life easy.

A solution to allow simple applications to work for a wide range of platforms is to make sure their primary interface is purely web based, without any proprietary extension. Once you get there it becomes interesting to promote freedom in choices for the platforms in use.



Keep it usable

Section 66

- High security measures kill usability
- Additional machines to share
- Dual machines

48

The balancing act is easy to solve: sidestep it. You have just created two almost opposite solutions: the extremely secure one, but unfriendly to the users and the very friendly one that has all the gadgets. Now give those users that *need* access to the highly critical assets a second machine (via a Keyboard-Video-Mouse (KVM) switch if needed).

Or put up a few machines to share on the secure network.

It works great once you are used to it.



Example of a NOC using the dual machine setup. (NOC was in staging phase, no customer data on it at the time this picture was taken. Nor was it complete yet (no phones installed at this point)).

The screens on the right were the ones connected to the parent's internal network and could be used to surf the net, read company email etc.

The screen on the right was air gapped from the other and could only be used to manage systems and access customer network components under management by this managed network and security provider.

The difficult parts

Section 66

- Need to expose high risk assets ?
 - Front end copy
 - Match protection on other side
 - Set your standard
 - Match their standard
 - Audit
- Awareness of users
- Software vendors are most often not ready

50

The difficult parts can come back and haunt you, especially if you over-classify assets. If you build extreme measures to protect something it becomes much more harder to open them up to a 3rd party should you ever need to do that.

There are a few tricks you can use to overcome those limitations:

- Use of a front end copy and let them interact with that while you keep the master copy safe from them.
- Get matching protection on the other side (now this will be hard today, most 3rd parties will have a perimeter heavy model in place. But you can do things and one of these is a standalone PC to access your stuff that is air gapped from the rest of their network.
- Your user community is probably not aware of your architecture, so you need to make sure they understand it properly, even if they were used in their previous situation to a more flat model. Especially users inside one of your Donjon's need to be very security conscious.
- The traditional workstation software is not ready for this, but neither are the application ("just" connect it to the database) nor your internal developers. Most see security as an afterthought, or worse as a hurdle, rarely as an integral part of your solution.



Others

Section 66

- Jericho Forum:
 - “De-perimeterization”
 - Future
 - Standards

Jericho Forum 

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

51

Part of the solution for the problems might come from things the Jericho Forum is pushing.

While their goals are slightly different, they will push in a direction that enables you to solve the problems above as well.

► Vision Statement

To enable business confidence for collaboration and commerce beyond the constraint of the corporate, government, academic, and home office perimeter, principally through: ·

-Cross-organizational security processes and services ·

-Products that conform to open security standards and profiles (collections of logically related standards that make up a useful functional entity) ·

-Assurance processes that, when used in one organization, can be trusted by others

Note: The Jericho Forum is business-driven, but recognizes that the issues it aims to tackle affect all types of organization and individuals. Issues such as privacy and civil liberty can be just as important as the needs of the corporate.

► **Mission Statement**

Act as a catalyst to accelerate the achievement of the collective vision, by: ·

- Defining the problem space ·
- Communicating the collective vision ·
- Challenging constraints and creating an environment for innovation ·
- Demonstrating the market ·
- Influencing future products and standards

Note: The Jericho Forum will produce standards where there are gaps to fill, but primarily seeks to foster development of standards within complementary institutions; e.g., W3C, IETF, ISO.

Examples

- ISP-Telco
- MSSP division

53

A few examples where I used in the past elements from this already are:

I've worked for an ISP where the notion of the Internet being evil was not something that matched with the culture management had. They wanted openness and they were willing to take risks in order to have a mobile workplace.

MSSP (divisions): need extreme security measures to sell to very security conscious customers such as banks and manage their security and/or their networks. Yet such a division or a such a NOC needs to be part of the parent company, need to email and surf the web.

Drawbacks & Benefits

Section 66

Drawbacks	Benefits
<ul style="list-style-type: none">• Too soon:<ul style="list-style-type: none">– Common clients are not ready to stand the assault unaided• Problematic to communicate with the donjons.• ...	<ul style="list-style-type: none">• Rightsizing<ul style="list-style-type: none">– Match protection with risk– Extreme protection possible– Less wasted resources on protecting unimportant things• Embrace mobility and openness• ...

54

This space intentionally left blank

Conclusion

Section 66

- This “donjon” model must suit your environment
 - As shown by a risk assessment
- Other ways of thinking beyond the perimeter model are possible as well.
- Add it to your set of possible architecture solutions.

55

This space intentionally left blank



More information:

Slides

<http://www.section66.com/security/2006-sansatnight.pdf>

Section 66

<http://www.section66.com/>

E-mail

swa@section66.com

SANS Internet Storm Center

<http://isc.sans.org/>