JERICHO FORUM
OPEN MEETING, SEATTLE, WA, USA
September 21-22, 2006

hosted by
The Boeing Company
at the Museum of Flight & Marriott Sea-Tac, Seattle

Meeting Report

The Jericho Forum thanks the Boeing Company for hosting this meeting, at the Museum of Flight and then at the Marriott SeaTac Airport.

Lead Contacts

Ian Dobson - Director, Jericho Forum (from The Open Group)
Chris Parnell - Business Manager, Jericho Forum (from The Open Group)

Steve Whitlock - Chief Security Architect, Boeing (our host for this meeting)
Ben Norton - Director of Computing Security Infrastructure, Boeing (hosting this meeting)

Speakers:
Steve Whitlock, Boeing
Chandler Howell, Motorola
Carl Bunje, Boeing
Conrad Kimball, Boeing
Jeremy Hilton, Cardiff University

Thursday Meeting

Setting the Scene for the Meeting

Ian Dobson (Director, Jericho Forum) gave a short introduction to the hosts, logistics, agenda, and delegate-pack, for this 2-day meeting. He explained the objectives were for attendees to take away good understandings on the security issues the Jericho Forum is addressing - to the point where they will want to become involved, and for the Jericho Forum to benefit from attendees feedback. The first day of the meeting was intended as workshop-style sessions challenging views on effective security for clients, networks, and applications/servers. The 2nd day aimed to invite evaluation of the Jericho Forum's "principles for good security" (Commandments), its Position Papers, migration challenges as the effects of de-perimeterization arise, and views on how security will evolve in the next 1-3 years and beyond.

He emphasized that this is an informal meeting, where Chatham House rules apply (no-one will be attributed outside the meeting), so the Jericho Forum hoped that attendees would speak freely and thereby make this meeting a genuine 2-way exchange that benefits all participants. All the slides presented in this meeting would be freely available from the Jericho Forum's Web page - www.jerichoforum.org, and a summary report from the meeting would follow. He closed with a slide which offered a brief visit to the terms Jericho and de-perimeterization.

Our De-perimeterized Environment - Responding to the Challenges

Steve Whitlock (Boeing) gave an introductory slide presentation on the Jericho Forum. It came together during 2003 when a group of 4 like-minded CISOs decided the time was right to raise awareness of their requirements for security solutions which provide effective security in their evolving business environments. These environments were different, and were all changing rapidly, but were all characterized by their firewalls being increasingly eroded. Other CISOs joined this groundswell of realization, and came together in January 2004 to form a customer-led group called the Jericho Forum, under the infrastructure of The Open Group. These Jericho Forum members shared the same view, that the traditional approach to security - maintaining a network perimeter defended by firewall - was crumbling, with "holes" allowing e-mail, Web, VoIP, encrypted traffic (SSL/TLS, SMTP/TLS, VPN) through, and was being largely ignored by wireless/mobile devices. They wanted security solutions which provide cost-effective security for their increasingly leaky perimeters. More - they needed cost-effective business solutions that would enable them to deploy globally distributed IT systems networked over the Internet - from any device, anywhere, anytime, on any network.

The answer was clearly not to be found in hardening the perimeter. In their first year, they focused on articulating the requirements they needed as customers, so they excluded influences from vendors with bags full of traditional-style security solutions. The outcome was the Jericho Forum's Vision white paper, published in Feb 2005, which included a range of business scenarios exemplifying the requirements for security solutions that would be effective in a de-perimeterized environment. This was quickly followed by the first Annual Conference in April 2005, where members broadcast the Jericho Forum's vision:

- To enable business confidence for collaboration and commerce beyond the constraint of the corporate, government, academic & home office perimeter, through
    - Cross-organizational security processes and services
    - Products that conform to Open security standards
    - Assurance processes that when used in one organization can be trusted by others

and mission:

- To act as a catalyst to accelerate the achievement of the 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

In early 2005, having completed its initial Vision paper, the Jericho Forum opened its doors to vendor members. The Forum has moved on to publish a series of "principles" (called Commandments) that give guidance on evaluating whether a security solution meets requirements for secure operation in a de-perimeterized environment. It is also developing Position Papers which address key challenges for providing security in de-perimeterized environments. To date 5 position papers have been published and a further 7 are under development. All completed Jericho Forum publications are freely available from the Jericho Forum's Web site - www.jerichoforum.org

Good progress has been made, but big challenges remain, not only to continue to get the Jericho Forum messages and approach out, but to push these messages and requirements into the vendor community where development of products which provide effective security in de-perimeterized environments must come from. The customer members (and vendor members who also consume security solutions) have huge budgets for buying and deploying these solutions. The Jericho Forum welcomes more members - from customer and vendor sides - to increase the momentum for development and delivery of the security solutions we all need in the next 1 month to 5 years.

Discussion raised awareness that to many security practitioners it is a Risk Management challenge, where the business's managers must balance the risks against the threats, and it is the security practitioner's role to understand and explain these to their business managers so they make informed decisions.

One questioner asked what would be the best outcome for host Boeing from this meeting. Steve answered awareness of the challenges and how to go about addressing them. Boeing does business in many countries worldwide with thousands of suppliers and customers, and they depend on reliable and secure IT transactions for their business to be successful, so they support the Jericho Forum including it's outreach events such as this one. They look forward to attendees feedback, particularly in the challenge workshop sessions.

Client Machines

Chandler Howell (Motorola) led this workshop session. In his slide presentation he posed the following questions and invited discussion on them:

- What is a client?
- Requirements - what do we need to do?
- Capabilities - what can we do?
- Gaps - what can't we do (yet)?
- Progress - what are we doing about it all?

He explained that Motorola is now into working using untrusted networks - 30% of its workforce is mobile. What is a client - it is every device you can possibly think of that can connect to an IT network. The key requirement for all these devices is to keep them up-to-date with patches - patch management was absolutely essential to maintain the security of these devices. A questioner asked why should the user have to worry about security - surely it should simply be there anyway? Chandler answered that this is about trade-offs you willing to make - the cost of managing effective configuration of devices and mitigation measures you are willing to bear, against the risk of a security breach. A comment on this was that business is often willing to accept risk. Another was that good practice could be to configure for several scenarios then allow exceptions based on informed risk.

Chandler continued that another good practice is to allow users to have rights sufficient to do their expected tasks and no more - the impact of unwise actions on other users is often not taken into consideration; business policy should address this explicitly and ensure that policy is enforced. Remember too that when the "client" is not just another machine, it is the human user together with the device, and it is not easy to model this combination. In this context, we need batter practice for risk transfer, and recognition of ownership of and accountability for risk. Another comment was that there is a significant disconnect between what people are prepared to put up with as opposed to what they're willing to do using their IT system client devices.

Ultimately, Chandler noted that the goal is to have mechanisms in place that will minimize information loss in the event of a security breach - as well as to maintain continuity of service to legitimate clients. In the end this can be translated to a goal where consideration of the security of the client device should be irrelevant, because the key asset is the information content of the data. We should focus on this key asset and secure it

Network controls

Carl Bunje (Boeing) led this workshop session, which he described in his slide presentation as a discussion on the approach and implications on networks controls for a de-perimeterized enterprise. He emphasized we have to accept responsibility for our business IT activities and should expect to have the tools that enable us to exercise that responsibility. Key to being able to do this effectively is understanding our control environment, and especially our network environment. He listed key architectural principles and desired characteristics for secure operations (least privilege, defense in depth, plus personal responsibility for correct behavior). He then presented a generally accepted layered access control model which identified the path from an accessing device, through an external network, then through the business's perimeter & DMZ to their internal network, then to the target host, then the application, then perhaps through an encryption or DRM layer, to the data. He reviewed this model in the context of 3 scenarios:

- the traditional perimeter with a trusted internal environment and a policy enforcement point (PEP) at the perimeter
- a reduced perimeter, where the concept of the trusted environment is enforced through one PEP enforcing access control at the "soft" perimeter, another internally for internal user devices, and a 3rd controlling access to internal applications
- no perimeter, where the external network is part of the internal business domain, leaving 2 PEPs - one for user devices and the other for access to applications.

and then invited feedback on his view of this problem space:

- are there other relevant scenarios that will illuminate the issues?
- what characteristics to these PEPs need to have?
- what would be the impact of shifting or removing any of these layers of control?
- what does an architectural model of the "no perimeter" scenario look like?
- what constrains deploying the "no perimeter" scenario in you business environment?

Questions included what is the Network Applications Consortium's position on these issues - the Jericho Forum should take them up with the NAC. Also, where should we

position authentication protection to manage identities - at the end points or around the resource? This presentation brings out that we don't have good models for what we want to implement. When you think about where to put the PEPs you need to understand where you end points really are in your business model so you can create safe perimeterized enclaves. We need to understand the risks of allowing external access - it depends a lot on context. No-one accepts any more that we can ever have a trusted internal network. How should we evaluate trust in other business's networks? - federation seems the only solution in town right now.

When setting up PEPs on resources, we have to enable access controls for different levels of confidentiality and this requires classification schemes. It is likely that for PEPs to operate effectively that will have to co-operate, and in this respect a top-down hierarchical control system is unlikely to work well.

Regarding compliance with policy, there have to be penalties for non-compliance. This implies need to involve legally binding terms and conditions. Standard contracts for this would be a valuable resource for businesses. Carl noted that Boeing establishes business trust relationships for authenticating users through the Aerospace industry's Certipath Bridge, who have now cross-certified with the US Federal Bridge. The ever-present requirement in authentication mechanisms remains - that changes/leavers (de-provisioning) need to be kept up-to-date as well as starters (provisioning), and enforcement of this is again a business policy issue that needs to be assigned to responsible individuals with appropriate penalties for non-compliance.

Application/server

Conrad Kimball (Boeing) led this session, posing the question "If the perimeter disappears, how do I still accomplish computer security?" In his slides he presented thoughts on structuring and answering the issues that need to be addressed, and offered a reference model that clarified the landscape for where control points can be established and what the implications on inserting them at selected points might be. He began with a summary of Boeing's core business requirements are when exposing a computing system to external users, what this means in IT system infrastructure terms, what has to be achieved to provide the required protection (but not how it is achieved - that is up to each business. There no single "right" way, so it will perhaps be helpful to build a catalog of mitigation techniques, identifying which protection categories each addresses, characteristics of each as a technique (e.g. described in a design pattern), and strengths & weaknesses of each, thus providing an openly available resource including best practice guidance.

Conrad continued by presenting the same layered reference model as Carl used, and reviewed the potential points where access controls could be placed around computer hosts and data repositories, and the implications in each case.

Discussion in this session noted that encrypted data ensures secure transmission but subverts intrusion detection that is based on plain text recognition. It is useful to remember the distinction between jail-like enclaves (can't get out) versus fortress-like enclaves (can't get in). On a direct de-perimeterized question, where do you map the controls in the perimeterized version of the reference model presented here? - the answer was if they don't fit in the perimeter zone then find somewhere else or conclude they are not needed.

It was noted that the holy grail of DRM is that data protects itself, irrespective of which host or application it is created with or read by. Also, we should focus on that 15% or so of "crown jewels" data that we really do need to protect from a business perspective; lower-level controls are probably sufficient for the other 85% of less valuable less confidential data. Also, if the data protects itself then the repository is not a big issue provided it is reliable (and not dogged by DNS problems). Additionally, can we use the concept of privileged data, where depending on your access rights you may be restricted to seeing only part of a document? - it was noted that this approach has been patented in the USA - the technique using encrypted sub-parts of a document plus XML metadata pulling the whole document together. A comment on this was that if this is a business process patent then it is not enforceable in European law.

While the reference model presented here helps clarity of thought and discussion, it does imply a straight in-out path from the perimeter client to the data, whereas in practice this path is usually more complex - can we adapt the diagram to show this complexity? Conrad immediately presented an additional slide where he has considered this, with resulting agreement that it was hard to follow so for this session we will stick to the simpler single system version. There was general agreement that Boeing's reference model diagram here helps establish a common basis for ensuring we evaluate security mechanisms with a clear understanding of the layer we are addressing; however, in any given instantiation, not all these levels need to exist.

Data/Information Security

Jeremy Hilton (Cardiff University) gave a short presentation on the problem as described by the Jericho Forum - to be addressed in a positioning paper members are currently developing - that access to data should be controlled by security attributes within the body of the data itself (Jericho Forum principle/commandment #9), and that current access control models do not scale in a de-perimeterized environment. Jeremy's slides summarized the proposed solution/response, then the background arguments/rationale involved, and described the challenges to the industry as requiring a consistent:

- policy definition language
- information classification scheme
- access control infrastructure

to facilitate sharing. The proposal includes what in effect is an interpretation of the DRM approach to fine-grained access control (mentioned in the previous Application/server discussion), based on open standards.

In the ensuing discussion, fair use of published information was recognized as a separate issue - through copyright, licensing, or derivative re-use/re-processing. Scalability to handle high volumes of data is an essential feature, and the profile for the data protection scheme must allow for ease of assigning classifications. Again, the classification scheme must facilitate assignment of different protection levels. Transferring responsibility and liability for classification of their data to the creator/owner of the data has been a goal for a long time - it puts control back to where is really should belong. The data classification scheme should have an associated enforcement mechanism to ensure it is appropriately applied.

Responding to the question "is protection of sensitive data a de-perimeterization issue?, the Jericho Forum's answer was yes, because we take protection down to the data level.

Friday Meeting

After a further short introduction, and recap on the meeting sessions on Thursday for attendees who did not attend the Thursday meeting, Ian Dobson set the agenda rolling for the Friday meeting.

Keynote

Ben Norton (Director of Computing Security Infrastructure, Boeing) said he has been with Boeing nearly 30 years, for the first 13 years as a programmer/analyst, and for the past 12 years managing security, not in the sense of defining policy but rather building the technological controls that implement the policy. Boeing's culture is a "can do" approach. So for example, when management wanted single sign-on for all Boeing employees on all UNIX systems, and after 2 years he reported back that it can't be done, his management put together another team to do it (- they came to the same conclusion). He recalled his first involvement in Boeing's first presence on the Web - all went well until a plane crashed and the news bulletins mention the Boeing Web site, in no time at all the site was swamped with access calls and it fell over. This was a significant learning point, that you have to be careful about using the Internet, so Boeing built perimeters which were deliberately over-engineered with a focus on protection rather than ease of assess to authorized users. But traffic grew, and volumes of data grew, giving them another new challenge. Then VPNs offered a tractable solution - strong authentication, encrypted data, secure clients. As Boeing has grown its business, VPNs increasingly provide the common way to connect outsiders to Boeing's host computing systems, with filters and other techniques adding the increasing protection as new security requirements evolved.

Boeing recognizes that de-perimeterization has been happening for years now. But awareness needs to be translated into concrete steps to meet real business problems. Their business needs for their IT systems remains that they have to be rock-solid yet enable efficient business flow. They cannot demand that all clients are perfectly configured and with up-to-date patches. Their highest priority is to protect the factory production process, so the challenge was to plan then organize the IT systems in those areas into carefully partitioned highly protected enclaves. But we all live in the same pool - requiring similar secure and reliable IT systems - so they set up access zones with different security requirement levels suited to their sensitivity. Having set this up this for existing production and development business requirements, the latest being the 787, demand then arose from the new 747-8 teams to have their own enclaves. Clearly there are major cost savings to be achieved if they can use the existing infrastructure yet still keep pace with evolving security requirements. In creating more protection, it is vital to also keep in mind the "exploding shield" lesson - that whenever you evaluate a protection mechanism, be sure to check that if the protection fails it will not cause greater problems than if it was not there in the first place.

Looking at the situation now, Ben felt that the Jericho Forum has done a good job in bringing the security challenges and issues to the fore. Now, it needs to demonstrate it is not just a place for talking about the problems, but a real force for enabling delivery of concrete solutions. It has to press for delivery of the solutions it demands, and take leadership in sharing best practices, all this contributing to solving real business problems - improving security, reducing costs, improving reliability.

The Commandments

Jeremy Hilton (Cardiff University) presented a slide set covering the Jericho Forum "principles" - or commandments. The current set comprises 11 commandments, referred to as JFC#1 through JFC#11. These may increase or decrease (through merging 2 or more) as experience and evolution in understanding of the underlying principles evolves. The commandments aim to capture in a set of high-level statements a set of criteria by which information security requirements and solutions can be evaluated as responding to the challenges posed by de-perimeterized environments. It is important to appreciate that these commandments are not a set of principles for information security in all environments, but solely to distinguish what is different and necessary security for de-perimeterized environments.

Comments as each commandment was presented were:

JFC#1: suggest commute "must" to "may be an opportunity to" - de-perimeterization involves some degree of fragmentation, so you need to match the control involved to the value of the asset at risk.

JFC#2: "simple" in what way? - this needs clarifying.

JFC#5: "devices" is too limiting - should be something like assets aggregation, asset being autonomous

JFC#6: trust is moving towards peer-to-peer. We don't have a good definition here for what "trust" is. Each participant has to be capable and willing to provide information so that trust level can be evaluated. Not all devices have the ability to declare or negotiate trust. This has tight connection with "assume context at your peril".

JFC#8: in 1st bullet, suggest "rights of users" rather than "permissions of resources"

JFC#9: Security attributes of data was explored in great depth in the Thursday workshop sessions.

Jeremy asked if anyone saw any gaps or overlaps/duplication in the coverage of these commandments. One suggestion was that the bullet point rationale items for JFC#9-11 (Access to Data) can benefit from being expanded to include the discussion points arising from the Thursday workshop discussion. Also availability is not well addressed. In general the principles set out principles for good security hygiene – they could be extended to do this more comprehensively.

Position Papers

Steve Whitlock (Boeing) presented a set of slides explaining the objectives of the position papers the Jericho Forum is producing:

- they are used by members as collateral when talking with vendors, to show the consensus of Jericho Forum members on key problem areas and the kinds of solutions that our members want to buy
- they provide a valuable part of our shop window, publicizing the Jericho Forum message, particularly in raising awareness on issues and requirements - by explaining what is different about effective security solutions in de-perimeterized environments

- members use them as a basis for RFIs
- CISOs who embrace the Jericho Forum's approach use them to align their business solutions with the wisdom and experience of fellow members
- they provide a sanity check that our requirements and approach to possible solutions are coherent, with no significant gaps.

These papers are short (target is 2-3 sides) and to the point, and follow a very clear structure which explains the problem, why you should care, recommended solution/response, background argument and rationale for the proposed solution/response, the challenge this represents to industry, and the proposed way forward. Steve listed the set of papers published to date and those in preparation. He went into selected papers to illustrate how they achieve the intended purpose, highlighting features in the Papers on Wireless, Voice over IP, Internet Filtering and Reporting, Digital Rights Management, End Point Security, and Architecture for De-perimeterization.

Discussion on these papers agreed that the Jericho Forum as the right approach in asking the right questions and inviting answers rather than pushing any particular solutions. It was noted that the position papers don not explicitly include sections addressing priorities or dependencies – should they? Interest was expressed from several attendees on contributing to development of some papers currently in preparation. A specific interest was put forward on the Audit & Management paper, where Ian will follow up with the Institute of Internal Auditors and also on the Sidona Conference (legal, WG1).

Another interest was on the subject of Data Authenticity & Provenance, the proponent considering this to be one of the biggest overlooked issues. We should care about this because of the problem of the trusted insider - who could change data; how do trusted insiders prove they did not exceed their authority? We need a mechanism to achieve this. Ian Dobson will take this up with the proposer.

A further interest arose on the subject of Web Services and Perimeters. One attendee offered to take a lead on writing a "problem statement" and "why care" description for this proposal. Again, Ian Dobson will take this up with the proposer.

Further comments arose that Privacy is not covered in these position papers. Steve explained that we do have a very good draft paper on Privacy, but it was not clear how privacy is different in de-perimeterized environments compared to perimeterized ones, so it has not been published. Feedback from the audience was that they would welcome having this paper so this request will be taken back to the Jericho Forum members. In a similar way, they would welcome seeing a general position paper on the fundamentals of Trust, which Ian Dobson also mentioned as a planned background paper.

A general request from the attendees was that these papers, and the commandments paper, should be made available for review via our WIKI.

Questions

Q: Is the Jericho Forum the only forum for de-perimeterization or are there others covering similar ground? How about X9?
A: To our knowledge, no other forum is focused on covering the de-perimeterized environment from the customer/consumer viewpoint. It was because on existing forum was addressing this problem that the founders decided to set up the Jericho Forum. I-4 has broader interest, as does ISSA, ISF, and W3C. IETF is focused on protocols. OASIS

on anything XML. Other groups are industry-specific. We will investigate the recommendation on X9.

Q: What is the Jericho Forum's model for making progress?
A: It is a membership organization because it needs to fund its infrastructure (safe anti-trust home, email & Web facilities, technology & vendor neutral, administration for membership, management, legal, financial, marketing, publications). It keeps its membership fees low and progress high by encouraging members to contribute development work and involving selected university academics as fee-waiver members in exchange for research contributions (so avoiding use of high-cost consultants), and by accepting member sponsorship for hosting meetings. It does use surplus membership funds to contract expert consultancy in appropriate situations.

Q: Are there instances of the Jericho Forum being able to demonstrate success – where a requirement or initiative has resulted in an effective response?
A: In influence and impact on what is being talked about - yes, but not in terms which can readily be measured, though we appreciate that being able to demonstrate a track record of success is important.

Migration to de-perimeterized environment

Steve Whitlock (Boeing) presented a set of slides titled “What Hath Vint Wrought”, in which he cited key features of the Internet that have necessitated businesses like Boeing to take significant actions to secure their IT operations in the de-perimeterized global environment where most of Boeing's IT transactions with their business partners occur over the Internet. His presentation title is a reference to Vint Cerf, who is generally recognized as the inventor of the Internet, and who never intended or designed it to be secure. This has not stopped business managers appreciating the low-cost high value of the Internet for global information transfers, and demanding their IT operations use it as a core part of their business. Of course, neither has it stopped business managers from extending their demands to requiring that their IT systems are made to use the Internet securely. So, now that business usage demands secure operations, we all have to respond to the unintended consequences of business adoption of the Internet as a globalized IT highway. Steve outlined Boeing’s plans for evolving their security strategy to achieve their business requirements here, which of course include legal & regulatory requirements.

Future Directions

Jeremy Hilton (Cardiff University) presented a set of slides introducing the final session of the meeting. He first looked at the requirements a de-perimeterized road warrior would need to be prepared to respond to. He went on to suggest how IT security is likely to evolve, in security technologies, in environment, identity, architectures, and data handling, and in human behavior. In listing the requirements areas, discussion included suggesting adding Audit Logs and Tracking, e-Wallet, and Instant Messaging as a bank. On Requirements for Laptop devices, it was recommended we change "Corporate applications" to "corporate resources". A comment on the Potential Roadmap for Technology was that this could provide a useful basis for evaluating return on investment in specific technology solutions.

Having suggested these extrapolations in the future, Jeremy invited "where next" feedback from the meeting attendees. One suggestion was that we should take care to avoid the buzz-word hot-topic diversions and focus on real business problems - e.g.

RBAC and Federated Identity are not specific business problems. Another was we seem to have found an effective mechanism for getting work done - papers, use-cases/scenarios, and liaisons with others to push for solutions. Perhaps we could develop the use-cases into producing use-cases for key vertical markets - legal, financial, and auditing are good ones to address - and then look for the common intersections. Jeremy noted we have a very interesting use-case presented by BP which we might build on here. A warning was that we do need to push our position paper requirements to the marketplace where solutions providers can't fail to see them and be challenged to respond; we should not expect them to come to the Jericho Forum. In this regard we should use best effort to get our message across - including on our Web site - and the most effective way to do this is through use-cases which bring out the risks/threats and ways to manage/mitigate these, including improvements to our Web site. A further suggestion was that a leading light in Sirius University - Gene Spafford (Spaff) - is involved in work which is very much related to the Jericho Forum's approach - can the Jericho Forum see itself in an "integrator" role here, to pull related contributory work and leading people together? Ian Dobson recalled we had hoped to make connection with Gene Spafford over 18 months ago (in a Jericho Forum meeting in Cincinnati) but Gene was unable to join us and this lead had not been followed up.

Discussion moved on to "what next" - what can attendees look forward to in order to continue their interest in the Jericho Forum's work. Becoming members is obvious but effective involvement is the key to getting best value, so what future meetings and other activities are planned. Arising from this came the suggestion for setting up regional groups. Two attendees expressed interest in taking a leading role to set one up in the Chicago area, and one in the tri-state area (New York, New York, New Jersey). Ian Dobson and Chris Parnell will follow up with the Jericho Forum on these offers.

Close

Ian Dobson expressed the Jericho Forum's thanks:

- to Boeing for their generous hosting of this meeting
- to the meeting presenters for their stimulating presentations and leadership of ensuing discussion throughout the meeting
- to the attendees for rising to the opportunity by engaging in lively discussion which has yielded valuable feedback to the Jericho Forum, and we hope equally valuable feedback to each attendee.

We will follow up to build on the outcomes from this excellent meeting.
