Cybersecurity Roundtable

March 19, 2009 ● City Club ● Washington DC

Participants in the Roundtable discussed the following topics.

Trusted Internet Connection (TIC)

The group agreed that the concept of TIC is good, but it has not been properly managed. OMB guidance was not specific enough, telling agencies to do it quickly with no additional funding. There was a lack of clarity and no real alignment of the policy with a realistic implementation plan.

The group agreed that TIC is a significant architectural issue. That being said, members said that rather than it being an individual agency architecture issue, TIC should be implemented as part of a "bigger picture", focusing on what governmentwide architecture for TIC should look like with a clearly defined end-state.

Issues with TIC implementation focused on:

- Timeframes for implementation are a lot more than originally estimated; that GSA and the Networx carriers are not offering services quickly enough; thus it's hard to meet schedules and deadlines. One member said "GSA provides the lowest common denominator on TIC through Networx."

- There has been an underestimation of the difficulty of the task itself; and rogue connections exist in both DOD and civilian agencies.

- Initial TIC standards were not clearly defined by OMB in 2007; and some implementation contracts were issued based on those unclear standards. That has caused uneven protection and missed deadlines.

The group agreed "that while the train has left the station" on TIC, in the future TIC like solutions (e.g. upcoming governmentwide Cybersecurity plans) need to be managed closely at both the technology and policy levels. In fact policy should not be issued before technology solutions are thought out and tested (if possible).

Federal Desktop Core Configuration (FDCC)

Like TIC, the group agreed that FDCC is much more complicated to implement than people think. "You don't find out until you try to implement it," said one member. "The ideas were birthed in a vacuum," said another. Also, as in TIC the FDCC mandate was issued before the solution was there and pilots demonstrated in one agency that if all the settings are used, then all the functions don't function.

Once again, the group said the problem is "aligning policy with practicality and aligning practicality with a real plan." If you have to do it in a specified timeframe, have a solution that works – and is tested.

The groups also felt that both TIC and FDCC were hatched from the perspective of compliance rather than a risk-based approach to requirements. The evidence is how they measure success with a yes/no answer on how you comply with FDCC. There is no risk-based view; the group felt that in the issue of risk mitigation versus compliance, compliance is winning out and it should be the other way around.

Thus the consensus was we really need to handle FDCC on a case by case basis, agency by agency. It's not feasible to have a one size fits all because many agencies have heterogeneous environments and

older equipment; and infrastructure won't fit in as defined in a standard. (Should that hold true for cybersecurity as well?)

Also, there was discussion that perhaps some of the procurement rules could be used to manage security configurations. If we have heterogeneous environments, there must be a way to define minimum baseline standards; then use the procurement regulations to enforce standard configurations as we move forward and modernize.

The question of different product versions also was discussed as to "what does that mean for support from vendors?" asked one member. "With different versions brings in different vulnerabilities." That needs to be worked out.

The DISA Equivalent in Civilian Agencies, Purchasing, Sharing Information

The group also discussed whether civilian agencies should have a DISA equivalent because they generally don't have engineering expertise in-house.

This civilian "DISA" would be a group that would coordinate all of these cyber initiatives. If this is not feasible (and it probably isn't), then start off with each agency having a "DISA like entity" in- house and then over time you can consolidate across agencies and move to a more centralized way to manage cybersecurity.

And by having a "DISA" for the dot gov agencies, this would lead to more collaboration and coordination for Information Security.

Another member said we need to stop developing "silos of excellence"; and that agencies should be able to buy networks and services from a central source using SLAs to manage operations. Once again the question arose of different versions of solutions from different vendors; and what does that mean for support from vendors, because with different versions you bring in more vulnerability.

The group also discussed certification issues that stymie nimbleness and make it hard to get the latest solutions. Once again, it is difficult to achieve a balance between risk mitigation and compliance strategies.

There was a discussion of the FPCC – Federal Platform Core Configuration -- and governmentwide architecture. This is being discussed by a CIO Council subcommittee, along with whether we should include common language in contracts and how to keep a pulse on the vendor supply chain.

Members discussed inventory and asset management policy asking the question "do you know what you have?" and "how well are we managing IDs and threat analysis?"

The thought was that the CIO Council subcommittee could be a clearinghouse, not telling people what to do, but to telling them "who is doing what", placing coordination among those who are working the "pieces" (DHS, US CERT etc) as a top priority.

Another key point discussed was "how do we take information we have, declassify it and push it out to others in the dot gov space?" How do we cross pollinate and get information from the private sector so we get better view of this world? Some don't want to give out the information, but if everyone knows everything, then everybody benefits.

Information Sharing could be increased through the use of Social Networking sites. Right now many are frustrated because of lack of access. (Something the Obama Administration is tackling in its Transparency and Open Government efforts plan due May 21)

The group also discussed budgets and the desire to buy COTS products for basic infrastructure services including security so that the focus is on real needs. One member said "We aren't going to succeed unless agencies can buy services like the Navy can buy from DISA. If I have to spend 80% of my budget on security, then I can't buy the applications I need to do my job."

Balance between Protecting the Perimeter versus Protecting Data

The group discussed that fact that the President's comprehensive cybersecurity program tends to be aimed at the perimeter and blocking bad bits coming into the country.

Rather than focus the majority of resources on that, there needs to be a balance between protecting the perimeter and protecting data at rest and in motion.

The group also agreed that most of the spending is going to protect the perimeter. One member said he is putting 85% of his resources on protecting the perimeter and there is a need to balance that out. Since we don't know all the access points to Internet, how can we protect what we don't know? Another member said rather than spend all money to protect egress points; we should focus on Tier 1, 2 and 3 ISPs and control them; that would be a better strategy.

In summary, all agreed we need a comprehensive plan that looks at the perimeter and the internal data that sits on that infrastructure. One member said "we need a new focus on protecting data; it's all about the data and all about access to the information."

Another member said "the perimeter is no longer identifiable especially with IPv6 coming." The question is: what is data? And how do we use the data?

He suggested "let's extend the tagging capability to beyond the content; tag data in terms of security level, privacy, authoritative duration and location; because two pieces of data today mean one thing, and tomorrow another comes in and then it means something else. Data changes and we need to look at it in that way; and then match up user access to the data.

Education Is Essential

Another offered that one strategy is "to focus on culture, capabilities and conduct and get the message out to peers." In other words Information Security is something that everyone must take a personal interest in. The message is "this is not all 'geek stuff' and you must defend core competencies" and "in the end it is a leadership issue and people must be held accountable."

The discussion also focused on the fact that people are not doing the basics, even the simplest things such as turn off their computer. This is not trivial at the user level. It is essential we lay out a clear picture as to what these threats are doing to them; one that gets leadership to understand. Doing this in each individual environment is the best way to make the business case. You have to visually show them the picture of what the threats are in their own environments. Then they "get it".

We need to decide how much risk to accept and then manage it with the reality that you can't secure everything all the time.

FISMA and the Network of the Future

The group expressed a variety of opinions on the effectiveness of FISMA. The consensus felt that FISMA keeps cybersecurity a priority and that is a good thing. However agencies should be judged on their performance against FISMA, not compliance with FISMA.

There was discussion that FISMA is certification along the system boundaries and we need to change the model so we would do it based on data and its sensitivity.

One member said "now we have data in the system, we secure the system and put in the authoritative privileges users should have. In the future we are looking at data in the cloud, platform as a service or SaaS. In the cloud we don't own the system anyway. We need to understand the data sensitivity level and who can access it. A different taxonomy is needed; is it database driven or tagging or something else?"

There was a suggestion that we look at future technologies; think about what the network of the future would look like and get input from private sector entities. We should start thinking about cybersecurity for that future network now, so that as we build future technologies and networks, we build cybersecurity in. Thus build future networks from the ground up. Start from the beginning because what we have now is a band-aid approach.

Also, on the network of the future, one member said new technology gives egress tagging and filtering capabilities as data traverses the networks. We can create an encryption point from who the user is from role-based access all the way to data center. Then we can encrypt that and protect traffic from attacks and further authenticate and validate as it goes across the networks. That is what we will be doing a few years from now, because there can be no weak links in the supply chain.

Cyber, Y2K and Risk

One member of the group talked about the relationship between what we did for Y2K and what we aren't doing for Cybersecurity. He talked about the fact that for many CIOs the focus on threat analysis leads to reactive security. Once again this is a band-aid approach that doesn't scale. You need to look at vulnerabilities and what are the exposure points and go after them.

It was brought up that for Y2K there was a process. There was a "unity of command" and "unity of effort". We should be doing the same for cybersecurity developing a long term strategy that uses some of the lessons of Y2K. Y2K had a centralized funding process and everyone agreed that it made a big difference. We need a governance model similar to what was done for Y2K.

There was then a discussion of leadership of this issue. We had it with Y2K. It was suggested that the President needs to make it clear to the world that cybersecurity issues are high priority.

And the President should inform agency heads of what needs to happen and hold them accountable. In this way we can evolve to a culture of security awareness and be more proactive on these issues. In other words we need to market our "national strategy for cybersecurity" like we did for Y2K.

That strategy is not being articulated to the rank and file. We need to reach the end user community even though things will take years to fix. We also need to share risks and how we deal with them with trusted partners.

Although we are improving cybersecurity, there are so many complicated issues that we are never going to be able to protect against everything. Thus we need to decide: what is an acceptable level of risk? If we can define and accept risk then we can define an acceptable level of protection against those risks.

One member spoke about how managing multiple policies is hard to deal with. "We can build TICs on different access points on the networks creating multiple TICs. We are going to zone area security and each zone must have one policy." Thus we need to start thinking about pushing controls on the network that are sophisticated and to manage multiple policies.

In summary he said it is way more complicated than protection at the edge and at desktop, there is middle part we need to deal with; and it has to do with performance, not compliance.

Final Points

Resources and budgets are huge issues with everything that is required. Look to the lessons of Y2K where there was a centralized emergency budget. Have a security innovation fund at every agency so IT is not always "begging for money".

Web 2.0 tools will put more strain on infrastructures. But we need to use these technologies to foster more collaboration, coordination and the sharing of information and lessons learned.

We must look at high level strategies and look at threats as a whole. Take a total approach with a total security architecture. This is not a geek issue, but a leadership issue. Having an information advantage is one of our key competencies and that must be protected. Thus, IT has to be seen as an essential business driver, not an overhead cost that is slashed whenever there is a budget crisis.

We need to take a long term view and make it clear to people why this is important. We need to declassify some of the data and show those in charge of budgets the realities of what is going on.

Finally, create and elevate a culture of security awareness, so that being protected is now part of everyone's daily job – and not a "why question" but a "how do we do it question".

It would be great if President Obama made this a priority for his Cabinet, measure their progress and hold them accountable; and then tell the world that we will use our power to go after enemies who are attacking us.