Community Expectations for Campus Computer and Network Security

Joe St Sauver, Ph.D.
joe@uoregon.edu or joe@internet2.edu
Internet2 Security Programs Manager

April 27th, 2010, 4:30-5:30PM, Salon A
Internet2 Member Meeting, Arlington VA

http://www.uoregon.edu/~joe/community-expectations/

Disclaimer: The opinions expressed are those of the author and do not necessarily represent the opinion of any other party.

The Original Campus Expectations Task Force

- The original charge for the Campus Expectations Task Force (CETF), circa 2005, was described by Bill Decker, head of the Task Force in a talk he did for the Fall 2005 Internet2 Member Meeting, see www.internet2.edu/presentations/fall05/20050920-cetf-decker.ppt

  Articulate a current set of expectations for what it means to be an Internet2 member campus.
  - *Consider focusing on what the campus infrastructure needs to be 2-5 years out in order to support advanced applications.*
  - *Areas considered should include campus network configurations, campus directory implementations, privilege management, data storage, image transfer/management, computation,* ***security,*** *campus bandwidth management, collaboration environments, and others.* [JES-emphasis added]
  - *Consider the responsibilities that come with supporting sponsored participants and SEGPs.*
  - *A series of case studies that illustrate the best practices of campuses in resolving these issues will also be created.*
  - *Seek input from a broad range of constituency groups, including but not limited to CIOs, application developers, GigaPoP operators, network engineers, support staff, faculty, researchers and other users.*

Expectations Function #1: Minimum Standards

- It was clear by 2005 that it made little sense to have a high speed nationwide backbone (such as Internet2), if existing campus or regional networks were slow and congested, or if key servers and researchers were only connected via 10Mbps chokepoint links.
- Put another way, if you made the effort to connect to an advanced national R&E network, other sites might reasonably expect that your network had more than just "vanilla IPv4" capabilities, perhaps including the ability to support advanced network protocols such as:

  -- IPv6,
  -- IP multicast, and
  -- jumbo frames (e.g., 9K MTUs)

Expectations Function #2: Keeping Us All Stretching Just A Bit

- The CETF process was also envisioned as serving an important "forward looking" role, going beyond just saying "where should we be now?" to laying out "where should we be two to five years from now?"
- In the simplest of terms, if campuses had 100Mbps backbones in 2005, we needed to be actively working to get upgraded to gig backbones, while planning for 10 gig backbones (and maybe even doing basic research needed to make 100 gig backbones a reality when they're needed)
- The general expectation was/is that we should be "challenging" ourselves at least just a little; Internet2 shouldn't be just about living comfortably at a currently adequate but not exceptional level.

Note: Not All Expectations Were Purely Technical

- While some expectations were technical, others were not.
- One might also expect organizational commitment to advanced networking, including support from institutional executive management, appropriate institutional financial commitments, commitment of personnel and facilities, etc.
- Metaphorically, if you were going to be part of the "club," you were expected to actively participate, making a reasonable effort to "stay up with the pack" and to contribute to advancing the good of the order.
- Explicit articulation of community expectations has the potential to serve an important normative function, allowing people to identify areas where success has already been attained locally, and areas where more effort is still required.

Expectations Also Served to Reassure

- For instance, note the explicit reference to supporting SEGPs and sponsored participants in the original charge.
- At the time that charge was prepared, there were worries that when Internet2 allowed connection of state K12 networks (as SEGPs), or smaller institutions with less of an instituional emphasis on advanced networking (as sponsored participants), that that step might result in the creation of substantial new operational burdens, burdens which might be born by the community as a whole rather than by the sponsored or sponsoring site.
- Of course, in retrospect, we know that anticipated deluge of potential problems didn't occur, but at the time, some were worried and wanted reassurances.

Expectations Also Were Meant to Educate, And To Be Demonstrably/Provably Attainable

- In particular, the case studies mentioned in the charge were meant to illustrate how members of the community were actually meeting the community's articulated expectations, thereby showing peer institutions at least one proven path that presumably could also be replicated by others.

- "Let me show you what we did. When you check out what we did, you'll see that it's worked well for us."

- Those are the sorts of things that were originally envisioned (or at least that's my recollecton)

The CETF Final Report Was Issued Spring 2006

- A final report from the CETF was produced in Spring 2006, and remains available online at http://www.internet2.edu/files/CETF-FinalReport.pdf

- A discussion of that final report is also available, see http://www.internet2.edu/presentations/spring06/200604225-cetf-decker.ppt

- Somewhere along the line, though, we all got a little distracted, and work on shared community expectations got postponed or deferred, even though the need for shared community expectations was ongoing.

Fast Forward Now to The Fall of 2009

- In the Fall of 2009, during discussions of the Internet2 Salsa Security Advisory group, the issue of community expectations came back up, with input from Salsa members including members of the Applications, Middleware and Services Advisory Council.

- Consistent with Tasks G ("Implement Security Best Pracatices") and J ("Cooperate on Security Challenges"), the Internet2 community has been working with Educause and the REN-ISAC in providing security information to our colleges and universities.

- But that information is just that: informative/descriptive, not normative/prescriptive.

"A Normative Campus Security Agenda"

- In May of 2008, for the Educause Security Professionals Meeting, I put together a presentation called, "A Normative Campus Security Agenda," see www.uoregon.edu/~joe/spc2008/security-professionals.pdf

- That list of normative activities included things such as:

  -- have antivirus
  -- respond to incidents
  -- have a campus AUP
  -- etc.

- But that was a LONG document, 103 slides, and frankly, probably just too dang long for folks to pay attentionoto.

How About A Much Shorter List: Just Ten Items

- Coming back from the Fall 2009 Internet2 Member Meeting in San Antonio, I snagged my colleague Dale Smith from the University of Oregon to help, and together we came up with a list of just ten items that one might take as a starting point for basic Internet2 community expectations relating to security.
- Before I show you what we came up with, **I'd like for each of you to take a minute and think about the ten items that YOU might suggest for such a list.**
- What *should* campuses be doing in terms of security (limit yourself to no more than ten items). Note that these items would need to pass suit-level scrutiny, as well as geek-level scrutiny, and they'd need to be things that people can actually do/live with...

Your List of Top Ten Security Expectations

1)

2)

3)

4)

5)

6)

7)

8)

9)

10)

The Ten Items That Dale and I Came Up With

- 1) Have a cyber security officer/group
  2) Have a cyber security plan/acceptable use policy
  3) Site license an antivirus software product
  4) Participate in the REN-ISAC
  5) Have an intrusion detection system (Snort, Bro, etc.)
  6) Be able to translate a reported IP address to a MAC address to a switch port to a machine/person (even if there are NAT related complications involved)
  7) Route traffic on campus, don't just switch
  8) Locally firewall important assets and provide encrypted VPN access
  9) Eliminate clear text passwords (telnet, ftp, pop, imap, unencrypted administrative web applications, etc.)
  10) Work on identity management/some sort of centralized authentication

1) Have A Cyber Security Officer/Group

- Someone needs to "own" cyber security at every site -- this might initially be a lone cyber security officer, but eventually this will probably be a cyber security team.
- The security group will typically:
  -- report to the CIO and/or institutional executive mgmt
  -- handle abuse complaints and work security incidents
  -- proactively identify and harden vulnerable systems by scanning the network for unpatched systems
  -- watch network traffic for signs of intrusions with network monitoring tools such as Snort or Bro
  -- operate firewalls, VPNS, central log repositories, and other network security infrastructure
  -- provide security policy leadership
  -- deliver security training, etc.

2) Have A Cyber Security Plan/AUP

- Most university cyber security programs will have a formal cyber security plan. While the exact content and format of those plans will vary from site to site, a typical plan might include:
  -- security roles and responsibilities
  -- security goals and objectives
  -- campus security resources and contact information
  -- information classification guidelines
  -- incident response plans
  -- a description of the school's security training program
  -- minimum standards for system and network hardening
  -- an acceptable use policy and a privacy policy
  -- information about information security governance and oversight
  -- etc.

3) Site License Antivirus Software

- Malware is an ongoing cyber security threat.
- Even though newly released malware is becoming increasingly adept at avoiding detection by signature-based antivirus products, anti-virus products do still detect (and block or remove) at least some malware. Thus, sites should site license an antivirus software product and insure users have current A/V definitions.
- Alternative antivirus products should be deployed on servers, for overlapping coverage and defense in depth.
- Additional malware management strategies should also be considered. For example, most malware continues to target Windows systems -- some sites may decide to standardize on alternative operating systems that have lower levels of malware in circulation (such as Macs).

4) Participate in the REN-ISAC

- The Research and Education Network Information Sharing and Analysis Center (REN-ISAC) is a private community of trusted members sharing sensitive information regarding cyber security threats, incidents, responses, and protection. Participation in the REN-ISAC provides timely warning about ongoing operational cyber issues, a channel for abuse reporting, professional security education and generally serves as higher education's security operations center (SOC).
- Membership is open to colleges and universities, teaching hospitals, research and education network providers, and government-funded research organizations.
- For more information about the REN-ISAC, see http://www.ren-isac.net/

5) Have An Intrusion Detection System

- Intrusion detection systems such as Snort or Bro passively monitor network traffic for indications that local systems have been compromised or are acting maliciously. By identifying malicious traffic early-on, security incidents may be able to be quickly identified and mitigated.

- Network traffic may be monitored at a site's border, or at alternative locations such as at subnet boundary).

6) Be Able to Map IP Addresses to Users

- Oddly enough, when some sites receive reports about unwanted traffic, they may find it difficult or impossible to map a given IP and timestamp to a responsible user.
- All sites should insure that they can map a reported IP address (with a trustworthy timestamp) to a MAC address. The MAC address should then be able to be mapped to a switch port, and the switch port to a machine or system (even if a NAT'ing firewall is involved).
- This process typically requires the network to retain firewall logs, logs of DHCP address assignments, copies of ARP table data for ethernet switches, records of switch port to wall plate wiring work, login/logout records for multiuser hosts, syslog data, etc. Automating the process of querying these records may save a lot of time.

7) Route Traffic On Campus, Don't Just Switch

- This is perhaps the most unusual recommendation of the ten: campuses should employ routers on their campus network, rather than just ethernet switches. (Note: when we refer to "routers" we mean actual Ciscos or Junipers, NOT little consumer grade "broadband routers" from Linksys, etc.)
- While routers are typically more expensive and more complex than ethernet switches, routers offer important security advantages, and should be part of your network architecture:
  -- routers limit the extent of each broadcast domain; limiting the broadcast domain can be helpful when it comes to things like limiting the impact of rogue DHCP servers
  -- routers make it easy to deploy BCP38 anti-spoofing filters, and filters for other sorts of unwanted network traffic
  -- routers can support redundancy via HSRP or the equivalent
  -- routers can export Netflow records, allowing you to get more insights into campus traffic patterns

8) Locally Firewall Important Assets; Provide Encrypted VPN Access

- Firewalls are often considered by many to be the foundation of a site's cyber security, even though firewalls can introduce many problems if incorrectly architected or configured.
- For example, perimeter firewalls may not be particularly effective if you have 20,000 or more users within your security perimeter. Sites should push distributed local firewalls closer to campus ERP systems or other high value assets to minimize the hosts within the trusted perimeter and to maximize the protection they deliver.
- Provide encrypted VPN access to those resources, thereby providing yet another measure of protection against unauthorized access and traffic sniffing.

9) Eliminate Clear Text Network Traffic

- Clear text network traffic, including clear text passwords and clear text personally identifiable information (PII) continue to be a problem at some sites, although many have replaced telnet with ssh, ftp with sftp or scp, etc.
- Authorized network security staff or network engineers should periodically sniff network traffic (just as an attacker might). Can you see plain text passwords for POP3 or IMAP logins perhaps? Unencrypted traffic from campus administrative systems carrying PII? How about NFS traffic, or CIFS traffic, or network backup traffic?
- Some notes: (i) just because you have a switched network, you're not immune to sniffing attacks (see http://monkey.org/~dugsong/dsniff/); (ii) some sites are particularly concerned about wireless traffic being sniffed, but ALL sorts of network links need encryption.

10) Identity Management/Centralized Auth

- Federated authentication systems such as Shibboleth (http://shibboleth.internet2.edu/) and Incommon (http://www.incommonfederation.org/), become more valueable as more sites participate in those activities, whether as end user sites, or resources which accept those technologies for authentication and access control.
- Surprisingly, while 160 higher education participants (including the University of Oregon!) plus 60 other participants are part of Incommon, representing over four million users, there are still many other sites that have not yet modernized their identity management and authentication systems.
- Another authentication related item that might be worth tracking is replacing plain text passwords with something that offers strong security, such as hardware crypto fobs

Is That All That's *Really* Needed?

- Are the ten items that we came up with the ONLY ten security things that pretty much everyone should really be working on? No, clearly not.
- But remember, part of our goal today is to come up with a workable list of no more than ten security expectations that the whole community can agree to live with.
- It is easy to list lots of things that DIDN'T make the list, including things like:
  -- anti-spam and anti-phishing
  -- DNS security and wide area routing security
  -- security of IPv6
  -- managing distributed denial of service attacks
  -- mobile device and cloud computing security
  -- disaster recovery and business continuity
  -- privacy, etc.

Ten Items Goes Pretty Fast

- By the time you reach the tenth item, if you're like me, you probably found yourself thinking, "Boy, ten items sure goes pretty fast! I could probably easily do twenty if I had the chance…"

- Eventually, we might get to a second set of ten, but for now, I think it is going to be really important to keep the size of the list constrained to a doable (and not overwhelming!) list of items.

Items Should Be Important and Doable (But Not Universally Already Done)

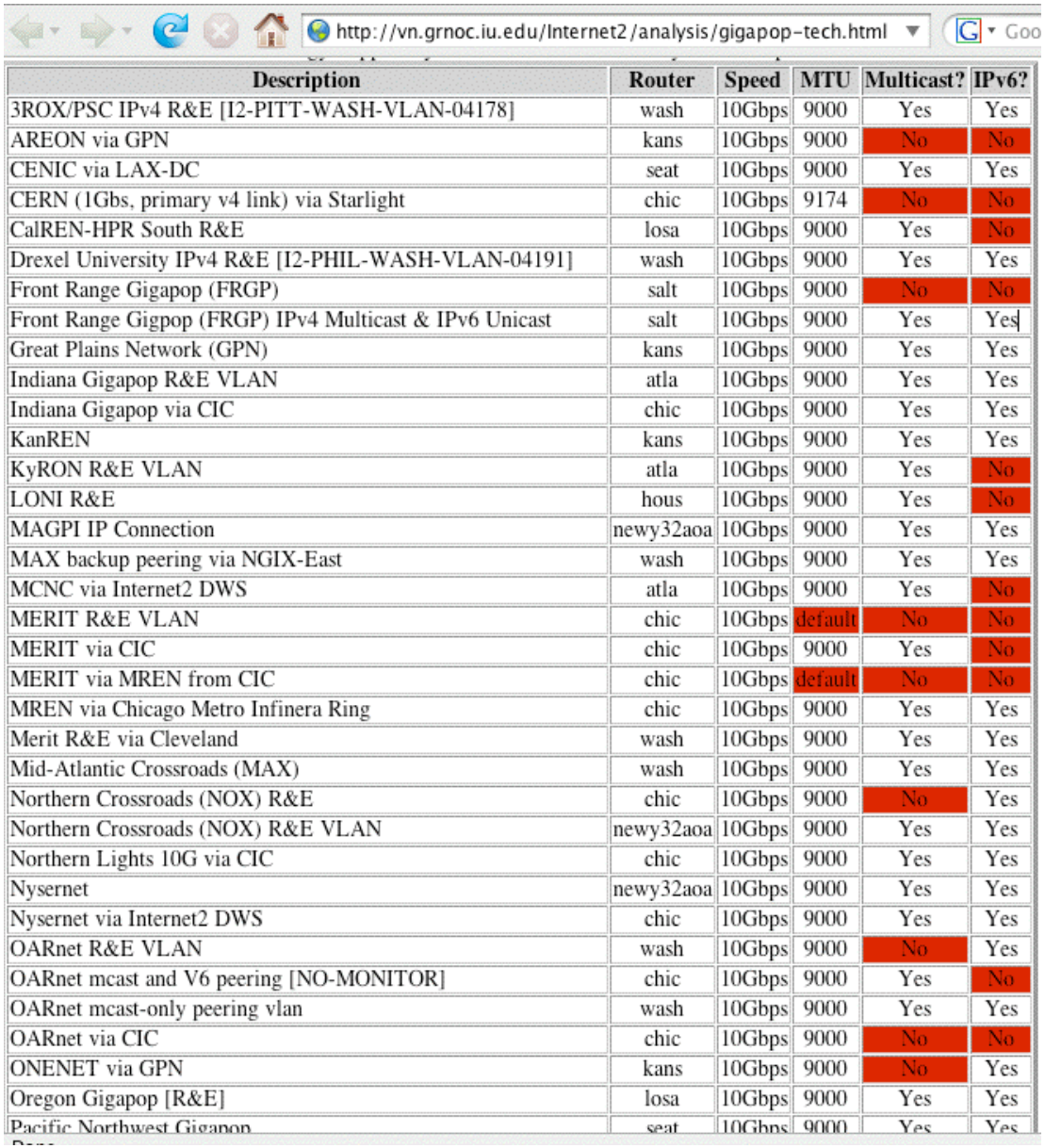
- To see what's meant by this, consider a non-security example: although it is important that everyone pass IPv4 unicast traffic, everyone's already doing that. Articulating an expectation that everyone "should" do that would be redundant/pointless, since **everyone** is ALREADY doing so.
- On the other side of the coin, again using a non-security example, there may not be any point to proposing that everyone do IPv6 multicast -- there's currently hardly any interest in that area, and it's hard to make a compelling case that people should take the time and effort to do so -- there need to be at least **some** people who are ALREADY doing a recommended technology for it to be worth putting on the list.

Do We Need A Public Scorecard?

- Unless we take the time to keep track, the Internet2 community will never know if their fellow campuses are making progress toward the security expectations that may get advanced. If our security expectations are important, we need to measure participation and institutional success.

- At many campuses, CIOs (or other members of the campus executive leadership team) may also appreciate having a clear picture of where their school is at, what they're already doing, and what they're not yet doing. CIOs should be able to see at a glance what is and isn't happening, and we should be able to clearly describe the implications of not doing any selected activity.

Sample Existing "Scorecard" for Some Items



Description	Router	Speed	MTU	Multicast?	IPv6?
3ROX/PSC IPv4 R&E [I2-PITT-WASH-VLAN-04178]	wash	10Gbps	9000	Yes	Yes
AREON via GPN	kans	10Gbps	9000	No	No
CENIC via LAX-DC	seat	10Gbps	9000	Yes	Yes
CERN (1Gbs, primary v4 link) via Starlight	chic	10Gbps	9174	No	No
CalREN-HPR South R&E	losa	10Gbps	9000	Yes	No
Drexel University IPv4 R&E [I2-PHIL-WASH-VLAN-04191]	wash	10Gbps	9000	Yes	Yes
Front Range Gigapop (FRGP)	salt	10Gbps	9000	No	No
Front Range Gigpop (FRGP) IPv4 Multicast & IPv6 Unicast	salt	10Gbps	9000	Yes	Yes
Great Plains Network (GPN)	kans	10Gbps	9000	Yes	Yes
Indiana Gigapop R&E VLAN	atla	10Gbps	9000	Yes	Yes
Indiana Gigapop via CIC	chic	10Gbps	9000	Yes	Yes
KanREN	kans	10Gbps	9000	Yes	Yes
KyRON R&E VLAN	atla	10Gbps	9000	Yes	No
LONI R&E	hous	10Gbps	9000	Yes	No
MAGPI IP Connection	newy32aoa	10Gbps	9000	Yes	Yes
MAX backup peering via NGIX-East	wash	10Gbps	9000	Yes	Yes
MCNC via Internet2 DWS	atla	10Gbps	9000	Yes	No
MERIT R&E VLAN	chic	10Gbps	default	No	No
MERIT via CIC	chic	10Gbps	9000	Yes	No
MERIT via MREN from CIC	chic	10Gbps	default	No	No
MREN via Chicago Metro Infinera Ring	chic	10Gbps	9000	Yes	Yes
Merit R&E via Cleveland	wash	10Gbps	9000	Yes	Yes
Mid-Atlantic Crossroads (MAX)	wash	10Gbps	9000	Yes	Yes
Northern Crossroads (NOX) R&E	chic	10Gbps	9000	No	Yes
Northern Crossroads (NOX) R&E VLAN	newy32aoa	10Gbps	9000	Yes	Yes
Northern Lights 10G via CIC	chic	10Gbps	9000	Yes	Yes
Nysernet	newy32aoa	10Gbps	9000	Yes	Yes
Nysernet via Internet2 DWS	chic	10Gbps	9000	Yes	Yes
OARnet R&E VLAN	wash	10Gbps	9000	No	Yes
OARnet mcast and V6 peering [NO-MONITOR]	chic	10Gbps	9000	Yes	No
OARnet mcast-only peering vlan	wash	10Gbps	9000	Yes	Yes
OARnet via CIC	chic	10Gbps	9000	No	No
ONENET via GPN	kans	10Gbps	9000	No	Yes
Oregon Gigapop [R&E]	losa	10Gbps	9000	Yes	Yes
Pacific Northwest Gigapop	seat	10Gbps	9000	Yes	Yes

What's A Good Format?

- The idea of having a readily comprehensible public score card ties nicely to the idea that we should consider describing our security expectations in a "what/why/how" format, a suggestion from Deke Kassabian of UPenn.

- Deke mentioned that he wanted to see:

  -- A succinct description of what's expected
  -- A briefly explaination of why that capability is important
  -- Information telling the reader how s/he can meet the expectation, e.g., pointers to documentation, software, or whatever

We Should Also Be Clear About Our Audience

- Remember that the original campus expectations task force charge was explicit in talking about Internet2's multiple audiences…
- There's sometimes a mis-perception that Internet2's only about large R&E universities, but Internet2 actually has many constituencies, including R&E universities, but ALSO:
  -- gigapops/regional optical networks
  -- statewide K12 networks (as SEGPs)
  -- smaller colleges/universities (as sponsored participants)
  -- international MOU partner networks
  -- federal agency mission network partners
  -- corporate members
  -- affiliate members
- Do we need separate sets of expecations for these diverse audiences>

With All That In Mind…

- Can we look at the top ten items that you all have come up with?

- It would be great if we could end up with a top ten security expectations consensus list from today's session…

The Group's Top Ten Security Expectations

1)

2)

3)

4)

5)

6)

7)

8)

9)

10)

Next Steps

- Unlike some security sessions, today's session wasn't meant to unveil a completed product, ready for broad adoption, it was just meant to introduce the topic and set the stage for ongoing community discussions, and to begin getting some input from you.

- We want and need to hear from you, Internet2's members, about what you think our community's collective security expectations should be -- after all, these are supposed to be COMMUNITY expectations, right? :-;

- If you're potentially interested in working on this topic, please send me an email at joe@internet2.edu or joe@uoregon.edu