

Welcome

Welcome to Tim Cornish who is now a member of the Executive Committee, appointed to fill out Doug Oftedahl's unexpired term through 2010. We welcome Tim's experience and appreciate his willingness to serve. The committee is now back up to full strength.

Consider the CTF Challenge

The New York Metro chapter of IG offers to host a *Capture the Flag Challenge* with a few other IG chapters. This will be a very-big undertaking but also interesting and very valuable – if we can handle it. First, they'd like assurance of 50-100 participants. We will need a large venue, partners and assistance, and financial support. There are two weeks to consider our options and find interested partners. We will advise New York Metro whether we wish to apply following our next Executive Committee meeting on August 12th.

New York Metro's event was July 21st and 22nd at the offices of Cisco Systems in Manhattan. For information, visit the co-sponsors: The NYM Chapter at (www.nym-infragard.us) and White Wolf Security LLC (www.whitewolfsecurity.com). They challenge corporate teams and individual participants to come down and try out their pen testing and protection skills. Here are some details from the Web sites and information provided us directly:

Three rooms are set up. The Blue Cells are scored on their ability to keep systems up and available and their ability to respond correctly and promptly to inject requests. The Red Cells are scored on their ability to gain and maintain entry into the defenders' systems and for capturing flags such as entries in a database and cleartext passwords. The third room is for "Law Enforcement" and we believe they will try to protect everybody, monitor and seek to stop trouble from spreading. Competition can get fierce. And if some Blue Cells are representative of many organizations reported as still unprepared, they may not even realize their flags are gone until they see them waving elsewhere. This is indeed a challenge to management to demonstrate security preparedness, monitoring, early warning, response, recovery and, most important, damage control. Also important, of course, is not wasting money on too much or too little security.

NYM and White Wolf are offering to come to a few IG chapters, set up the equipment and systems, and coordinate the exercise. However, they need a suitable venue, Internet access, and free meals and lodging. If Vermont is selected, they will probably want to come here in May or June of 2010. Ideally, we should also host a dinner after the first day to present the risks and defenses to managers and officials responsible for good security. And we should issue an after-action report to the participants describing what was done and without naming names report what happened, where trouble occurred, and suggest mitigation measures to minimize future occurrences.

Our best venue is probably academic and students and staff from regional institutions are a good source of challengers. However, the likely dates look bad: exams, grading, and graduation. Another option is to invite a large systems house to co-host this (as it appears did Cisco Systems in NYC). They can then set up their wares and demonstrate how bulletproof their stuff actually is. There will be significant good publicity if their stuff performs well. And any who decline could be tarred with over hype. (Vermont already has a good candidate to co-host this, one already looking to boost their security bona fides. Or a major systems house might set up in a venue we can provide. Ideas!) Another possibility, is a public-private sector exercise in accordance with Homeland Security methodology, for which significant grant money might be available. Every state and local government is required to do such exercises and the private sector is urged to do so, if only to validate their security and avoid allegations of negligence. (I'm sure we can get FEMA on board and I can explain the HSEEP process, the benefits, and that it will probably be cost free).

It would be quite a coup, if IVMA can pull this off. And considerable value to participants to validate their proficiency. We'd like anyone's ideas and suggests as soon as possible. Again, our decision to apply deadline is August 12th.

Next General Meeting

It looks like a general meeting in late August is problematic at best. With vacations and schools starting, no one has had much time for a meeting. So now, we're looking at November when more can attend and we have more time to set this up and invite guests. The tentative focus is the affect on security and continuity-of-business of a pandemic or other health emergency (when perhaps 25% - 40% of the workforce may be unable or unwilling to work). If enough people can help set up this meeting and publicize it, perhaps we can have an all-day event: both a speaker and a panel discussion, provide exhibit space for vendors, and attract a large turnout. If anyone has suggestions or can help, contact Rich Parker or Gary Kessler directly.

We'll also need an exit strategy. The second wave of a pandemic often brings a crisis. If the swine flu should return to the U.S in October - December, public gatherings may be prohibited. The swine flu storm clouds are gathering now in other countries, so whether or not we can have a meeting, organizations may want to review their response and continuity-of-business plans.

Expanding the Executive Committee

Although the Executive Committee is now up to full strength in accordance with our bylaws, we really need to expand the committee. With a limit of five members, there is too much work for too few people, no backup, no bench for support, no opportunities to train new officers, and no opportunity to retain elder statesmen as directors. Per our bylaws, the Executive Committee appoints the officers who then serve at the committee's pleasure. The President, Vice President and Secretary should be committee members. The Treasurer need only be an IVMA member. The remaining one or two members are Members at Large. Our role as directors is to provide governance and oversight, but we also must provide management and often staff work as well. A cohort of five volunteers is simply not large enough to handle all these functions. Normally, a volunteer board is 15-25 people and often with a paid director or coordinator. For now, we suggest the Executive Committee increase to nine members.

To change the Executive Committee we must first amend our bylaws. The procedure for this is also there. (See the bylaws on www.vtinfragard.org). Problem is that we are having enough trouble scheduling annual and general meetings. For now, special meetings for voting are just dreaming. Therefore, we plan to initiate discussion via the members-only mailing list. This reaches all our members, rather the few who can attend meetings. While electronic voting is prohibited, there is precedent for voting by First Class Mail. Via mailing list discussion, we can first agree on bylaw amendments, then call for nominations and let candidates introduce themselves, and then vote – all on one paper ballot. We can email every member a ballot and ask that they send it our FBI Coordinator for counting. This way, all members will know what is happening and can participate and vote. We hope that everyone will take the time to fill in the ballot and mail it in.

Sharing Security Information

A member recently sent me copies of an in-house security newsletter his organization publishes monthly and a security alert put out by his industry. The first is basically public information, but the second is restricted to members of the industry association. However, these issues and concerns are common to almost any organization and should not be stove piped. Worse yet, what is generally known is often nothing or incomplete or misinformation. InfraGard members have a legitimate need to know, we are vetted, and we can be trusted not to abuse disclosures.

Even though much of what I received is not sensitive, I've agreed not to disclose any identifiable information as to persons, organizations, places, or opinion as to where a scam or an attack may have originated. But none of this detracts from the value to other IG members who may know little about the currents threats or scams, attacks, or intrusions.

We'll start including abstracts in the next issue and may put out some of the more urgent threats on one of our mailing lists. Members are urged to contribute information and submit material in confidence. Many

industry groups send out security alerts. If we can all share sanitized and redacted versions of this material and in-house security newsletters, we can all benefit and better understand what is happening in security.

Membership Benefits

A member recently asked how he might be able to access his equipment in the event of an emergency when police or soldiers cordon off many areas. In particular, he wanted to know how to bring in fuel for his emergency generator. There are many horror stories of networks quitting during Hurricane Katrina, simply because administrators were denied physical access to their sites. The federal government regulates his particular industry and they are coming up with a procedure. But after months of jumping thru assorted hoops, there is still little progress. However, IG members have several options and anyone with a need might want to consider all of them.

IG is working out a process called *National InfraGard Credentialing* whereby a member receives a special ID to pass quickly through most security checkpoints during an emergency. Each person must have a valid reason for access; IG membership simply expedites things. For details, try the INMA Website and ask.

I also suggest contacting the Emergency Management Director for the jurisdictions where you might need access to equipment and infrastructure. Emergency Management will probably be glad to know who you are and how to reach you and they can probably provide whatever resources you may need during an emergency, such as an escort, transportation, a generator and fuel for it, food and water, fuel for your car, and lodging. Then, whether or not they can issue you a special ID, anyone at the scene can radio the Emergency Operations Center to verify that your name is on their list of critical resources.

Through IG, we also have ties to federal, state, and local law enforcement and homeland security agencies. They can probably suggest ways to facilitate your access when needed. You might also be asked to become a volunteer in some sort of an emergency management role where you will receive response training and be issued photo-ID that probably will get you to a sign-in sheet for admittance. You can also try putting your needs out on our mailing list (anonymously, if you prefer) and see who has comments and suggestions. It is senseless for systems to fail during an emergency simply because the administrators could not gain physical access to maintain them.

Finally

Again, we'd like your thoughts on utilizing our chapter as a social network? We already have the mailing lists for discussion, but we can also post Help Wanted and Help Available and other announcements of interest to you and your colleagues. This can lead to paid assignments for anyone who may want to freelance, moonlight, or even work anonymously though somebody else. There may also be future IG programs that can pay expenses and honoraria. Let me have your ideas. Again also, we offer an anonymous posting process for our mailing lists when for any of many valid reasons the writer wants to remain anonymous. (See the July news for details.)

Your comments and suggestions are welcome, as are announcements, items of general interest, and submissions. We all unpaid volunteers, but we can still collaborate to help and assist one another in many ways.

Best wishes,
Frank Platt, IVMA VP and Editor

Franklin N. Platt
55 Paris Road
Stark, NH 03582-6657

Profit from Good Security
Office Planning Services
Security Consultants, Risk Management, Analytics

Tel: (603) 449-2211
Email: Fnlatt@aol.com
