
Newsletter of the InfraGard Vermont Members Alliance, Inc.

Welcome

Welcome to Mike Stridsberg who is now our Treasurer. He remains an Executive Committee member where he has served since 2007. Mike brings us banking experience as the IS Program Manager with the New England Federal Credit Union in Williston. We appreciate his willingness to take on this new role. Thanks also to Richard Moss who served us for the past two years.

General Meeting will be November 18th

Our next general meeting that will be on Wednesday, November 18th at 1:30 PM at BlueCross/BlueShield of Vermont headquarters near Montpelier. The topic will be pandemic and continuity-of-operations planning, preparedness, compliance, and risk management. We hope to provide a lot of timely and valuable information, and many handouts with sample plans, procedures, and instructions.

It is possible that the H1N1 flu will be upon us by November and that public meetings banned and non-essential travel discouraged. Therefore, we're building an exit strategy in case the meeting must be cancelled. We will try to send out information and handouts well in advance, so anyone unable to attend is well informed. (A Webinar or a conference call are as yet too expensive.) One thing sure is that infrastructure threats and cyber attacks will continue and probably escalate should a flu pandemic occur.

The continuity aspect of a health emergency is still generally under planned, even by critical groups that must remain fully functional at all times. Many anticipate their key people will telecommute, but have not considered that Internet access and telephones may be unreliable or that strong security and positive authentication will be needed. Many organizations simply plan to fall back on alternate facilities that may themselves be unreachable or inoperable. We hope to address these issues during the meeting and by handouts sent beforehand.

We're still looking for some good speakers and volunteers to invite many others to attend. More details later. Meanwhile, mark your calendars and come if you can.

Capture the Flag Exercise – Not for Now, But Maybe Later

Despite efforts to solicit a venue, co-sponsors, suggestions and volunteers, we came up far short of what it would take for Vermont to pull this off. A large obstacle is the likely timeframe of May/June of next year when colleges are engrossed in final exams and commencement. Accordingly, we advised the New York Metro alliance that IVMA is unable to apply.

Nonetheless, a CTF can be a valuable exercise in Vermont to show we can protect our information systems in real time and against real, experienced, and dedicated attackers. Prestige, hype and claims of protection are one thing, but actual performance is where the rubber hits the road and reality emerges. Therefore, we hope to do something like this in the future, on a smaller scale, one day only, with setup in the morning, afternoon testing, and finally a meeting to report and discuss that actually happened. We hope to get a security vendor to demonstrate their wares for all to see whether penetration is possible. We are not out to endorse or embarrass anybody, but only to validate their claims.

Ideas are still welcome, as well as venues and vendors we can approach and when best to do this.

Expanding the Executive Committee

We will start in September via the members-only mailing list to discuss and seek approval to expand the Executive Committee to nine persons from the current five. Any member may comment. If it appears we have a strong consensus, we will then invite nominations and ask candidates to introduce themselves briefly. The final step will be voting. We will post a ballot to first approve expanding the Executive Committee and then to choose four new members. Our bylaws prohibit e-voting and require voting in person at a general or an annual meeting, which is simply not practical if we are to get anything accomplished. Therefore, we will ask members to print out the ballot, fill it in, and then send it

by First Class Mail to Tom Leene, our FBI Coordinator. This way all members can participate and vote, even those unable attend meetings.

Sharing Security Information

This is an actual bulletin recently issued by a Vermont financial institution, slightly edited: Security researchers have been issuing warnings over the past month about a blend of new and old fraud techniques dubbed "Man-in-the-phone" attacks, which are designed to steal a customer's identification information. In a typical attack, the fraudster calls a customer and impersonates a company representative, asking the mark if, for example, he just purchased a wide-screen TV in California. The victim of course says "No Way," whereupon the fraudster asks him to wait on hold while he connects them to the Fraud Department. He then dials the real department on a second line, goes to mute, conferences the two lines, and listens in hoping to gain identity or access information. This attack is particularly effective at large call centers, where customers are routinely asked for identification as part of the greeting (i.e. "Thank you for calling Big Bank or Big Credit Card, may I have your account number please?") but our own staff should be mindful when taking calls, particularly if there is confusion as to who called who.

Visit http://voices.washingtonpost.com/securityfix/2009/07/high_crimes_using_low-tech_att.html for more information.

This is yet another social engineering variant. The person who shared this with us mentioned that many institutions are quickly updating their procedures to freeze an account immediately while discussing it with the customer. Many utilize caller ID, which will show something amiss. Note that the source was not a trade association but the *Washington Post* that few of us read. The key to its success is in stealing the information and immediately bleeding the account. This fraud is not perfect, yet it is working. While the call-in number can be traced back to the scammer, this may be of little value if the call came from a large switchboard or a hotel with 2-line room phones or from overseas.

Member Information

Every IG member should be receiving emails from national. The latest is the *Chairman's Corner* newsletter dated 12 August 2009. There is a lot of useful information here explaining InfraGard and its many programs and benefits. On the other hand, the *IVMA News* covers items primarily of interest to Vermont. If any member has not received the national newsletter, please let us know.

The 2009 National Congress is scheduled for October 14th via a teleconference, which we very much hope our delegates can attend at the Burlington FBI office (and not have to travel to Albany, NY as last year). There will be new programs announced and updates on our current ones. You'll hear these via the national newsletters and then we'll try to tell you what's appropriate to Vermont.

Sectors

Many individual alliances have formed sectors and found these very effective in serving more members and reaching out to businesses and the public. For us, a sector is simply a subsidiary group of IVMA members, under our corporate umbrella, and headed by a Sector Chief who works closely with the Executive Committee. Effective sectors have been formed within colleges, large businesses, and professional groups.

The advantage is that sectors can meet readily at a nearby facility, hold closed meetings or invite anyone interested, arrange presentations and hold discussions, invite other IG members as speakers, and generally share information and advice – usually on a monthly basis. This is especially useful to those who cannot always attend our regular meetings. There is no formal process to forming an IVMA sector and no limit how many. Let us know who is interested and we work with you to make it happen. First, there must be IG members involved and then we ask you adhere to the same policies and procedures that we as an IG alliance must follow.

Sectors can be very valuable to the individual groups and to all of us in IVMA. Let's hear some ideas on institutions and organizations that might be interested and who to contact: the colleges and universities, big businesses, trade groups and associations, industry groups, perhaps even state government. Why not approach communications carriers, utilities, business groups (such as Rotary) and suggest how this can benefit them. This

can be particularly useful for people far removed from Burlington. Basically, our operating region is east of New York, north of Boston, and west of Portland.

Finally

We as IG members are neglecting our mission. We are still not sharing much information and not reaching out to the private sector that is still mostly still unprepared and non-compliant with the many laws, regulations, and best practices necessary to protect people and property properly. We should also be reaching out to government, as many agencies are similarly unprepared. American is risking big trouble and potentially big costs due to inefficient and ineffective disaster response. Katrina was deemed to be a man-made disaster triggered by a hurricane that was predicted in ample time for an effective response. We know how to prepare and how to comply. So why don't we just do it to protect ourselves and our property, infrastructure, information systems and data!

There are still many negatives as contributing factors: Denial, apathy, defeatism, ignorance. Many still believe that security is a waste of time and money because what will happen, will happen. Many say they are too busy, can't afford it, or simply don't understand. And almost everyone is comfortable that someone else will protect them. Legislating security has never worked well, because too many reject government intervention. However, what every manager should consider is their duty to protect, which is established law and enforceable, can be very costly and difficult to defend, and often results in large fines and compensatory damages. So why not just do it right and probably save a lot of money in the bargain!

First, however, is the recognition that sharing information is a fundamental component of good security and this is where our mission lags. Those with a need to know must know what's happening; how might penetrations occur; how to defend, monitor and quickly detect trouble; and how to respond and recover? We need all of these answers transparently and honestly. We can share this information generically so no one is defamed, libeled, or embarrassed and no how-to instructions are revealed. InfraGard is in a particularly strong position to share security information effectively and to work with the public, private organizations and all government agencies as well. Much talk nationally but still little action, so let's just do this now for ourselves.

All members can report suspicious activity to our FBI Coordinator (whose name, address and contacts are always on our Web site, www.vtinfragard.org), share security information on our members-only mailing list (Vtigsecure@clearbearing.net), or send it in confidence to any Executive Committee member who will sanitize and redact any personally identifiable or company-specific information and then get it out appropriately.

The next thing we need share are the private security bulletins issued by most businesses and industry groups. Now, this information is mostly squirreled away and often forgotten or ignored. But together, all of these bulletins and alerts and reports can add up to useful intelligence. They can also indicate where law enforcement should be looking for trouble. IVMA needs agreements with many individuals and groups to share in confidence to protect their sensitive information.

Lastly, when a breach does occur, don't just hush up everything. Let us all know, even if you must do so anonymously (as mentioned in the July *IVMA News*).

It's time that every member pitched in and helped. This is our mission and we need to do it. Security is everybody's responsibility; we cannot afford to leave it to others.

As always, comments, suggestions and contributions are welcome.

Frank Platt, IVMA VP and Editor

Franklin N. Platt
Office Planning Services

55 Paris Road
Stark, NH 03582

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

Profit from Good Security

Security Preparedness & Compliance since 1967

• Risk Management • Analytics • Due Diligence • Second Opinion • Validation • Training
