
Newsletter of the InfraGard Vermont Members Alliance, Inc.

Next Meeting 02/26/2010

Our next chapter meeting will be on Friday, February 26, from 1:30 – 4:15 PM, the place and directions will be announced shortly. See www.vtinfagard.org for details. This is an open meeting for anyone interested and guests are most welcome. The speakers will be Frank Thornton of Blackthorn Information Systems and George Bakos of Northrop Grumman. The topics will be *Wireless (in)Security* and *Advanced Persistent Threats*, respectively. For those who cannot attend, we will try for a follow-up report and post copies of any handouts.

There will also be an election following this meeting for IVMA members to vote for the three open positions on the Executive Committee. The terms of Rich Parker, Mike Stridsberg and Frank Platt expired in 2009. We will call for nominations shortly. And in accordance with our bylaws, we are planning that all IVMA members can participate in the vote, whether or not they are able attend the meeting.

New Membership Cards

Tom Leene still has many new membership cards to replace the old ones that expired three months ago. Those still without their new cards please see Tom at the February 26 meeting. Otherwise, please contact Tom and arrange to pick up yours or ask that he mail it to you. His address and phone are on our Web site. And please be sure we have your correct address, email, phone, etc.

What Do You Want from InfraGard?

What are your thoughts on how we can better inform ourselves and our constituents, businesses, and the public? How can we make more people aware of potential trouble and how to avoid it? How can we get more people to report unusual events so that law enforcement can better protect us? How can we better access and utilize the restricted security information available to InfraGard member to avoid trouble? What do you want our chapter to do to meet the needs and wants of the Vermont community?

Coming soon from national are some new initiatives, re-focusing of some old ones, and others dropped. Some of these can be useful in Vermont, while others are beyond our scope and capabilities. However, before we consider any new programs, we want comments from both members and non-members.

What programs do you want to see? How can we reach out to communities, business and industry, professional groups, and academia and others involved in security? How can we establish and maintain good relations with each of these groups. What do you want from this newsletter? We are only volunteers and short-handed at that, but we can still provide some valuable services.

Between now and the February meeting, we hope to visit many state and federal officials to ask how we can better assist them, provide valuable input and share information with them in confidence, and how we can augment their own outreach objectives. As we meet with these people, what do you think we can and should do to coordinate effectively with state and federal agencies?

Expert Intuition

Often times, people with a lot of experience can look at a situation and come up with an analysis totally unsupported by the known facts at hand so far. When there are not enough dots to connect into anything valid, bring in experts and ask for their intuition. This may appear illogical, when actually there is probably a subtle logic based on what they have seen elsewhere. Ask them what facts are missing and which dots may be irrelevant, misleading, or just plain wrong. Ask for their theories and then test whether they are plausible.

Expert Intuition is not quite that easy, but let's consider an example of an event that doesn't quite seem to make sense.

Suppose that the Christmas Day bombing mission in fact turned out exactly as planned. What if they (al-Qaeda?) did not plan to bring down Flight 253 – in fact they didn't seem to plan much at all for this attack. Instead, this was to be just a jab to cause a big stir and observe our responses. Why think this? Well, consider first that al-Qaeda is very experienced with the explosive used. They know how it is difficult to detonate it. And they must know that a syringe would only create a pop and a fire, which is all that happened. Consider also that to down a passenger jet descending to land, a very large bomb would be needed and this placed very strategically within the aircraft. Otherwise, you could blow a hole in the fuselage and cause a lot of panic, but the plane could still land safely. The bomber probably didn't know any of this and probably expected martyrdom. But then he didn't seem to make any of the final personal preparations that martyrs usually make before their mission. It looks brief instructions and cash for airfare were all the training he received – probably from someone he didn't even know by name. Nor would he have known the identities anyone else involved in the plot, so interrogating the bomber would yield little. This doesn't make much sense, agreed, so what might they hope to gain?

Had the plane crashed, American support would have coalesced immediately behind the President as it did on 9/11 and security would be strengthened without delay or argument. So let's assume that the attacker did not intend a plane crash to happen. Instead, this was just a jab to test our response. If so, what were their goals? To create fear, panic and dissention: Accomplished. To re-incense world opinion that Americans are thugs and bullies by firing up the "kill-em-all" and enhanced-interrogation advocates: Somewhat successful. To have us fixate on airport security, whereas al-Qaeda may be planning other disaster vectors: Accomplished. To test our defenses and response strategies: Accomplished with the help of the press; our system failed. To test how the new Administration would react and whether business and the public would support them: Accomplished, but also a win for the Administration.

What then are the lessons learned? The need for far more dots and better, faster analysis and information sharing. Continue to re-think all possible disaster scenarios: transportation, facilities, events, sites and icons. Use expert intuition to look over the horizon and around corners and then test theories that don't seem to fit the obvious facts. Increase defenses, surveillance, patrols and inspections and, especially, set metrics for preparedness, and remain vigilant for lax security. In other words, don't prepare for history to repeat or rest comfortably that we will thwart the next airplane suicide bomber.

Analysis by the 9/11 Commission reported failure of imagination. It looks like we are still unimaginative eight years later. Whether you call it expert intuition, wisdom or imagination, it is cheap and can be effective. So let's cut the rhetoric and do this before real trouble comes.

Still More Attacks and Scams

These notices are adapted from recent DHS Web pages:

1) America is Still Unprepared -- Computer Security Institute's annual security survey released on 12/01 noted big jumps in incidents of financial fraud, malware infection, denials of service, password sniffing, and Web site defacement. The survey also showed dips in wireless exploits and IM abuse. While the average loss due to security incident declined slightly last year to \$234,000 per incident, financial frauds cost enterprises \$450,000 on average. Interesting too is that 25% of responders stated that the majority of their financial losses were due to non-malicious actions by insiders. For more information, visit <http://www.gocsi.com/>.

In a related article released on 11/24 in "Government Security", "the FBI considers the cyber threat against our nations to be one of the greatest concerns of the 21st century. It goes on to say that spies, adversaries and criminal groups are becoming increasingly sophisticated and dangerous, many with a physical and technical presence inside our country, the government and the private sector. So far, jihadists have not learned too many harmful intrusion techniques and are paying others to spy and attack for them. However, "should terrorists obtain such capabilities, they will be matched with destructive and deadly intent." Source: http://www.govinfosecurity.com/articles.php?art_id=1962. This is based on a GAO report not available on the GAO or FBI Web sites. However, there are many GAO reports on cyber security cited on Google, and they all say that America is unprepared.

2) Banking commissioner warns of credit card scams -- The Department of Banking has recently received several complaints from people who received phone calls claiming to be from their credit card company and requesting that they provide their credit card number. Take note that this is something a financial institution would never do. In one case the caller claimed to be from Bank of America and said they wanted to verify certain activity on the debit card. The caller said they needed the credit card number in order to pull up the account. In another case the caller identified himself as being with Visa Services and stated that he wanted to lower the interest rate to 6 percent. When the consumer stated that they did not have a Visa card, the caller asked if they had a Mastercard and requested the credit card number. In both cases, the recipient refused to give their credit card information. "We want to remind Connecticut consumers to NEVER give out your credit card number or personal bank information to an anonymous caller," advised the Banking Commissioner. "If you are asked to do so it is likely a scam, even if they identify themselves as your bank or financial institution. The only time it is safe is if you initiate the call. The best thing to do in this case is hang up and call your institution directly, using the number provided on your card." Source: <http://www.acorn-online.com/joomla15/thewestonforum/news-local/43891-banking-commissioner-warns-of-credit-card-scams.html>

3) TSA to conduct full review after leak of sensitive information -- TSA officials say that a "full review" is underway to determine how a 2008 copy of its standard operating procedures for all airport security checkpoints was released in its entirety on the Internet. The document was "improperly redacted," according to TSA officials, meaning that with a few keystrokes what was once secret spilled out into the public domain. The document itself details screening procedures at metal detectors, explosive residue testers, and other elements of airport security. It outlines procedures for escorting certain travelers around security checkpoints, including air marshals, diplomats, and CIA officers. An annex to the document gives several examples of official credentials for agencies including the CIA, Congress, and federal air marshals and notes on determining their authenticity. Another redacted section of the document reveals that travelers are selected for screening if their passports are issued by any one of 12 specific countries. The TSA document, dated June 30, 2008, is stamped "Sensitive Security Information," a description of sensitive but not classified information. To redact the TSA document for public release, officials apparently used a computer program to blacken particularly sensitive parts of the handbook, including which types of travelers are exempt from various kinds of random and required screening, the

procedure for CIA officers escorting foreign dignitaries and others through checkpoints, the minimum gauge of wire used to calibrate X-ray machines, and the types of chemicals used for cleaning explosive residue scanners. The document was then published online as a PDF, a common file format used widely by the government. To redact it, officials obscured text using a program which successfully obscures the text as viewed on a computer monitor. But the information was not deleted. Highlighting the text of the PDF page and then using the copy and paste functions on a computer easily revealed the hidden information. Source: <http://www.usnews.com/articles/news/2009/12/07/tsa-to-conduct-full-review-after-leak-of-sensitive-information.html>

Finally

Yes, finally, some glimmer of hope for better security. Since 9/11, we have had enough rhetoric, far too many acronyms to understand, enough money poured into countless new and immature procedures, and far too much irrational optimism. "The system worked," "Heck-uv-a-job, Brownie," "Mission Accomplished." Still not so just yet, but through no lack of many good people trying. Finally, from a guy with enough explosive in his crotch to maybe blow an airplane out of the air, we have an Administration demanding we all do better and right now. A major disaster may have been averted on Christmas Day, partially due to quick-thinking passengers with the guts to rush in while many others fled in panic. Big trouble was averted due to the bomber's ineptitude, even though this was the same explosive the Shoe Bomber tried eight years ago. Or maybe no big trouble was intended (See above). In any case, there may well be glimmers of hope for better security preparedness.

Looks like the government will start doing its job, listen to the experts, and abandon the rhetoric and the foolish optimism. Looks like they will try to fix the systems, and establish stronger and better computing, fully share information and be able to issue warnings before trouble hits. While this is an almost-insurmountable challenge, at least they now appear to be trying and not just talking.

But now, it's also time for the public to get realistic and get involved, to help protect themselves, and to stop demanding that someone else protect us. It is time we realize that no effective security is possible without the public's full support and participation. It is time to end the criticism and carping (that are often devoid of facts) and pull together on all sides of the public-private divide. And in this light, there are many ways that InfraGard can do much more, assist and add considerable value. We are vetted subject-matter experts, we know local conditions and can work effectively with local organizations, and can observe unusual situations and report them to the FBI and encourage others to do so too.

The first problem is that few organizations understand the risks that may occur, nor do they fully appreciate how costly such risks can be if not prevented or at least mitigated. As independent subject matter experts, we can advise, assist and facilitate to:

- Review and participate in risk and vulnerability assessments to help organizations better understand the risks they may face and how seemingly unrelated events can seriously impact them
 - Help review and test continuity and response plans and help prepare after-action reports and improvement plans and explain these to management
 - Provide security awareness training for users and stakeholders and provide executive briefings so that management has a better understanding of the risks they face and how best to avoid and mitigate them
-

Now let's think about how the government can better connect the dots to stop trouble before it happens. Here is where the President admitted the system failed. Despite many red flags the Undiebomber was permitted to board Flight 253 with concealed explosives and a detonator. Here, the dots didn't connect in time to prevent trouble. However, the dots are the fundamental element of good security: many tidbits of information from diverse sources that are very difficult to decipher. So let's expand everyone's efforts to give the government more information and then more ways to analyze it. Here is a role the InfraGard can effectively play.

- Report unusual events to the FBI and encourage all our constituents to report either to us or to the FBI
- We can perhaps offer expert intuition based on diverse knowledge and local conditions

There is a difference between unusual events and suspicious ones. The latter is profiling and this does not work. You are simply reporting your own prejudices, and the last thing a troublemaker wants is to appear suspicious. Our reports of unusual events and our urging others to report unusual events can be of enormous benefit to the government. This is spontaneous insight to augment the fruits of often long and costly surveillance. Our input is also timely in that it reports local conditions that can portend trouble brewing that the government may yet know nothing about.

Security is always flying blind. At least we can help the government understand local conditions and where trouble may be possible. We can also help local organizations understand the many new and serious risks that may affect them and how better to detect, protect and prevent costly trouble. If the public and private sectors can collaborate effectively with InfraGard as a catalyst, many possible disasters will be avoided.

We as IVMA are in a unique position to help and work with both the private and public sectors for more efficient, effective security, better response and continuity when it's needed, and to add value to systems that are otherwise costly and inefficient. Let's think about what we as IVMA can do to help.

As always, comments, suggestions and contributions are welcome.

Frank Platt, IVMA VP and Editor

[This space is available for members to list their products or services, post links to interesting sites, or contribute material of public interest. Submissions may be edited for brevity and to reduce commercial content.]

Franklin N. Platt
Office Planning Services

55 Paris Road
Stark, NH 03582

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

Profit from Good SecuritySM

Security Preparedness & Compliance since 1967

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