



Protect Attendees And Your Organization From Identity Thieves And Corporate Spies

By Mickey Murphy

Information security. Identity theft. Black hat hackers. This all sounds like three-alarm lingo from some old DC comic book: “Immediately sign over all of your wealth, or I will hack you and steal your identity!” What do these oblique, non-intuitive terms mean? Here is how Wikipedia defines them: Information security — “Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or

destruction.” Identity theft — Fraud that involves someone pretending to be someone else in order to steal money or get other benefits.” Black hat hackers (also known as crackers) — “Hackers who specialize in unauthorized penetration” of computer systems, as opposed to white hat hackers who test computer systems for companies to determine their penetrability.

However we characterize them, information security, identity theft and so on represent major challenges today.

A prime example of consumer vulnerability came last year when federal

auth
oritie
s
indict
ed
three
men
on
char
ges



“The meeting attendee turns on his laptop, sees this free network and connects to it. He thinks everything is OK. It is not. ...the attendee is now plugged into the rogue network...”

**Mike Foster, IT Security Specialist
The Foster Institute, Dallas, TX**

of hacking into computer systems at numerous Dave & Buster’s restaurants and stealing credit card information. The federal government accused the men of stealing “Track 2” magnetic stripe data — which includes account numbers, expiration data and security codes — from customers’ credit cards, and then selling this information to others who used it to make fraudulent purchases.

And as this article was being written, an e-mail message showed up on this writer’s computer stating that I had purchased something over the Internet for \$423.98. I had not. A subsequent check indicated that the message was fraudulent, and that the senders were “phishing.” This is a fraudulent attempt to acquire sensitive personal information by masquerading as a trusted entity via an electronic communication.

Big Problem For The Meetings Industry

Yes, information security and identity theft are serious problems that in an information age everyone must confront. In this dangerous environment, meeting attendees and meeting planners are particularly attractive high-profile targets to identity thieves and corporate spies.

Denver-based identity theft expert and professional speaker John Sileo explained why: “Meeting planners are like symphony conductors. They are incredibly busy. They tend to be overworked. Everything culminates for them in a one-day or multiple-day event, where they are in charge of many important activities at a high level. The byproduct? They are distracted, overstimulated and rushed. These are the states of mind that identity thieves and corporate spies love to exploit. When you combine this situation with travel, where identity theft is common, you have a cocktail for real trouble.

“Also, the attendees themselves are sitting ducks because they are traveling and are focused very narrowly on what they are doing at the meeting or event,” Sileo said. “When people get focused on something, they tend not to notice the other little things around them. This opens people up to risks like identity theft or intellectual property theft. Put a thief in the middle of this volatile situation, and it becomes very easy for that

“If your registration company is PCI-compliant, this means they have taken the most stringent measures to protect data.”

Corbin Ball, CSP, CMP, Meetings Technology Speaker and Consultant, Bellingham, WA



person to steal information. This could be personal information

that leads to identity theft: credit card numbers, Social Security numbers, addresses and other private data. Or it can result in intellectual property theft: a company’s financial data, new product information or even the recipe for the prized secret sauce.”

The author of *Stolen Lives: Identity Theft Prevention Made Simple* (Da Vinci Publications, 2005) Sileo knows whereof he speaks. He is a two-time victim of identity theft. Years ago, a criminal was able to steal Sileo’s Social Security number and other important personal data. Among other things, she used this personal information to buy a \$260,000 home in Sileo’s name and against his credit. Also, Sileo’s former business partner used similar information to steal from his and Sileo’s clients. As a result, Sileo’s computer sales company, a family firm for more than four decades, went out of business. Sileo successfully defended himself in court against criminal fraud charges. The partner confessed to identity theft, and later served jail time for his fraudulent activities.

Noted information security expert Eugene Spafford, a professor and executive director of the Center for Educational Research in Information Assurance and Security (CERIAS) at Purdue University in Lafayette, IN, agreed that meeting planners and their groups can be easily victimized by identity and intellectual property theft. “The average meeting planner has so many things to think about that information security often is not high on his or her list,” Spafford said. “As busy professionals, many planners handle such a wide variety of meetings that they don’t understand some of them will be potentially high-value targets.”

“Identity theft can mean millions of dollars of losses each year,” said Michael Johnson, CMP, a meeting planner at Vanguard Integrity Professionals Inc. Johnson’s Las Vegas-based firm provides security administration software for mainframe computers, as well as consulting services to help secure mainframes. The company also performs “ethical hacking,” that is, “penetration testing” of computer systems and networks.

“As meeting planners, we have a higher level of threat than the general public,” said Johnson. “We are at greater risk because we take a large group of people to a relatively insecure offsite location. If anybody wants to target a particular group of professionals, a meeting is the best place to do it.”

Online Registration: Where Information Security Starts

For identity thieves who can hack the system, online registration presents a golden opportunity to steal the attendees’ valuable personal information. Many times, this can include their credit card data. What is the best way to protect this critical portal? Planners can learn much from how Johnson handles things. As a meeting planner with 23 years experience who also, serendipitously, works for an information security firm, Johnson brings solid credentials to this exercise.



“If someone asks to connect to the their Facebook page...they may be contacting the attendee to go ‘phishing’ in order to access that person’s privileged data.”

Eugene Spafford, Professor and Executive Director CERIAS, Purdue University, West Lafayette, IN

“The online registration process is probably one of the most vulnerable components for attendees,” said Johnson. “Their personal information and credit card data are at risk as soon as they enter data into the Web site. That is where security must start. There are some great ways to protect things, but none of them is foolproof.”

HTTPS. Johnson’s first recommendation is to always use a secure online registration Web site. This is one with “https” in the Web address, instead of just “http.” The “s” stands for “Secure Sockets Layer,” an SSL connection that provides encryption (scrambling) of any data that transmits across that connection. “Without that protection, anyone can grab onto the data anywhere from point to point and look at it and read it in clear text,” said Johnson. “As meeting planners we need to provide a portal to attendees that offers secure data. A good Web designer will help planners build Web sites so they are secure and have SSL connections.”

Johnson warns planners against trying to handle the development of online registration themselves, as well as turning the job over to low-end software service providers who provide online registration packages that don’t really protect.

Meetings technology speaker and consultant Corbin Ball, CSP, CMP, MS, agreed with Johnson. “The main warning flags are homegrown registration sites that planners may try to set up on their own,” Ball said.

Sileo also feels that when it comes to data security, the do-it-yourself approach is not a good one. “The problem is that some planners take a little technical knowledge and think they can apply that to online

registration,” said Sileo. “But usually that is flawed thinking. It is like believing you are proficient enough to install a sophisticated alarm system in your home. Yes, some people can handle this job, but most cannot.

“When it comes to data security, the planner should invest in proportion to the value of the information,” said Sileo. “When setting up any computer network or online registration system, planners should hire a technician, a consultant or a firm that is expert at this type of work.”

What about a member of the IT department with no security training for this task? IT Security Specialist Michael Foster of The Foster Institute, Dallas, TX, advised against it. “You wouldn’t go to a dentist to get knee surgery,” said Foster. “Nor would you go to an orthopedic surgeon for a root canal. Companies think they save money by turning over IT security responsibilities to members of the IT department with no security training. But really, they are just setting themselves up for disaster down the road.”

So what is the best option for online registration? Johnson suggested that meeting planners deal with specialty firms such as Cvent or RegOnline. He claimed that they can expertly handle this type of professional work.

PCI. The term PCI refers to Payment Card Industry Data Security Standards. These are extensive industry guidelines and practices that the major credit card companies set up regarding the security of credit card information. Merchants and other users who deal with credit card data — including meeting planners and their groups with regard to online registration — must fully meet these security standards. “If your registration company is PCI-compliant, this means they have taken the most stringent measures to protect data,” said Ball.

Therefore, any online registration site that the planner sets up for his or her group should be PCI-compliant. If not, and if there is a breach of registration data, the consequences for the planner and his or her group could be severe.

Unfortunately, many meeting planners are not knowledgeable regarding PCI standards. Indeed, this is also true for many merchants for whom credit cards are their lifeblood.

“Too many merchants don’t know that they are contractually obligated to comply with PCI standards,” said hospitality industry attorney David T. Denney, principal, The Law Offices of David T. Denney, PC, in Dallas. “When you get a credit card machine, people don’t read those massive contracts. I don’t think people know to what they are obligating themselves. I would assume that meeting planners are much less familiar with credit card processing rules than a typical retail merchant.”

Liabilities. So what are the potential liabilities? “Credit card holder agreements contain damage provisions to which the credit card companies will hold those whose credit card data is breached,” said Denney. “These are contractual liabilities. If there is a breach of the planner’s data, the

“If there is a breach of the planner’s data, the credit card companies will schedule a full audit of his or her online/onsite registration system. This will cost the planner’s group in the neighborhood of \$10,000.”

**David T. Denney, Principal
The Law Offices of David T. Denney, PC, Dallas, TX**



credit card companies will schedule a full audit of his or her online/onsite registration system. This will cost the planner’s group in the neighborhood of \$10,000,” said Denney. “Plus, the planner’s group or company retains liability for any cardholder damages if there is any identity theft. The extent would be how many credit card numbers were stolen and how flagrant was the breach.

“Another hard cost of \$30 per card goes with reissuing credit cards to all the registering attendees who had any compromised data,” said Denney. “With all of this comes accountant and attorney fees, plus any fines and penalties that the credit card company charges.”

How likely is it that the planner’s group would become liable for all of these heavy expenses if there were some type of data breach and it was not PCI-compliant? “It is a contractual liability to the credit card issuer,” said Denney. “The credit card processing agreement gives the issuer the ability to take these actions and debit the bank account of the company, association or group that the planner represents. As for individual victims of identity theft, anyone can sue anybody for anything.”

Firewall hardware. OK, the meeting planner now has the attendee personal information data in the group’s computer system. And because the online registration site was built with security in mind, the data is secure. Now how does the planner keep it so? Johnson explains that a firewall is needed, which prevents unauthorized users from accessing the data in any way. And for ultimate security, this firewall should be hardware, not software, according to Johnson. He uses the PIX 515, made by Cisco Systems. “It looks like a square box with a lot of phone wires coming into it. A network specialist programs this appliance so that only the people you want to gain access to the data can do so,” said Johnson. “A firewall really is a doorway into your database. It is a combination. If you don’t have the combination, you cannot get in.”

Johnson takes his PIX 515 with him whenever he is onsite at a hotel or some other venue for a Vanguard meeting or event. The Cisco appliance acts as the interface between his laptop computer and the hotel’s cable

connection to the Internet. With this vital firewall in place, nothing can breach his laptop's security.

Of course, Johnson further controls access to his valuable computer data through password protection. No one without an authorized password can access it. "You create different levels of protection where password strength and integrity are vital," Johnson said. "Also, it is very important to change passwords every 30 days. This is vital to securing your data."

Another important point regarding data security: Foster recommends that planners invest in quality anti-virus software to protect their data networks, and to update this software on a regular basis.

"In addition to anti-virus, having current operating system and application security patches installed will help protect the computer system," Foster said. "Have a good backup of your system before applying the patches, and make sure the patches came from the original manufacturer and not a bogus source."

The Hard-Copy Hang-Up

Making hard copies of valuable attendee and other proprietary data is one area where many meeting planners routinely make a mistake regarding data security, according to Johnson. "Many meeting planners print out their data, which then goes into folders," said Johnson. "This can include attendee registration data and other valuable information. Planners then bring these folders with them to the conference or meeting. And because they are planners, everything is neatly labeled and organized. The problem is, if this information falls into the wrong hands, it can be just as dangerous as someone hacking into the planner's computer system.

"So, there are two sides to the security equation: the electronic data and the hard-copy data," Johnson said. "At Vanguard, we protect the hard copy data by using unique six-digit ID numbers for all attendee registration information. This unique identifier enables me to quickly find anyone in my database. But the only thing that prints out is the attendee's full name and the special ID code."

VPNs For Proprietary Data

While at a meeting or event, planners often need to access important proprietary data that is stored on the company's servers back at headquarters. How can they do so without worrying about being hacked? The answer is VPN, which stands for "virtual private network." This is a computer network in which some of the links between the nodes are carried by open connections or "virtual circuits" in some larger networks such as the Internet. The VPN uses cryptographic tunneling protocols to provide the intended security and confidentiality.

"Most meeting planners set up their virtual offices at hotels, but need to access the data back at the office," said Johnson. "The way this works is simple. Let's say I am organizing a meeting in New York City. I buy a random connection from my hotel there. I then need to build a 'tunnel' to Vanguard's servers in Las Vegas. This is the VPN. The PIX 515 acts as

the firewall to the hotel's computer hook-up. Nothing unauthorized will get by it."

Laptop Lapses And Wireless Network Scams

While the meeting planner must always be vigilant to guard against data breaches and related information security problems, attendees themselves must also be careful at meetings and events. They must assume responsibility for their own data security.

"A lot of this actually falls to the individual attendees. They must be on their guard even if they are at a resort location or a business meeting where they know all their colleagues," said Spafford. "So explicitly warning the attendees about possible data security problems is a good thing. Warn them before they attend the meeting, then during the event as well.

"Laptop security is a big problem at meetings," Spafford continued. "I have been at meetings of only 25 people, with some vigilant staff person in the meeting room at all times, and laptops still have disappeared. It is a good idea for attendees to invest in laptop locking cables. If they leave laptops in their hotel rooms, they can lock them to furniture. Of course, they can also put them in a hotel safe.

"If the meeting planner sets up a special network for attendees during the meeting, it is important to announce this in advance, and to include information about it in the handout materials," Spafford said. "Let attendees know there is an official network, and how to connect to it. Make this through passwords. This prevents anyone in the lobby or parking lot from easily connecting to the network. Warn attendees not to connect to other available networks. Doing so can mean trouble," Spafford said.

Foster added, "The meeting attendee may be staying at the same Hilton hotel as Joe the cyber-criminal. Joe sets up his own wireless network, which he calls 'Hilton Free Access.' The meeting attendee turns on his laptop, sees this free network and connects to it. He thinks everything is OK. It is not. Because the attendee is now plugged into the rogue network, Joe the cyber-criminal can potentially monitor his or her communications and infect the computer with spy ware to learn all sorts of personal data, including credit card numbers and so on."

Credit Monitoring

Foster recommends that meeting planners and attendees, indeed, everyone, should invest in credit monitoring. This is the best way to nip credit card fraud in the bud. "Credit card monitoring will often let you know if some unauthorized person is using your identity to open accounts," Foster said. "You must pay a small service fee, but it is tiny compared to the protection you get."

Foster also advises planners never to put attendees' names and addresses online in a list format. "This is a huge no-no unless you get permission from the attendees first," Foster said. "Some attendees may be concerned that burglars can use this information when the individual is away from his or her home to attend the meeting or event."

Social Networking

In recent years, social Web sites such as Facebook, Twitter, Flixter, LinkedIn and MySpace have become highly popular with Internet users. Do these social Web sites pose any special security problems for meeting attendees and planners? Spafford believes that they do.

“In these online environments, as well as at meetings, there is a natural human feeling that when you are within a special community, something of which you are a member, you can be more trustful,” said Spafford. “If you are out on the street and some random stranger comes up and starts to speak to you, the natural tendency is to be suspicious. But if someone at a meeting who is wearing a name tag comes up and starts speaking to you, your reaction will be very different.

“It is the same thing online,” said Spafford. “If someone sends the attendee an e-mail and asks that person to connect to their Facebook page, the attendee might be more likely to do so, especially if the name looks familiar, or if he or she know details about that individual. Of course, people online can use any name they want. They may be contacting the attendee to go ‘phishing’ in order to access that unsuspecting person’s privileged data.”

Share Best Practices

Spafford said that, when it comes to meeting attendees vis-à-vis data security, forewarned is forearmed. “Meeting planners should make an extra effort to let attendees know that they have developed a safe meeting environment for these individuals,” Spafford said. “Planners should also inform attendees about best practices regarding data security. This is a good way to reduce risk.”

Spafford indicates that staying secure often depends on simple common sense. “When attendees leave the hotel, they should remove their name tags,” Spafford said. “When you have a person wandering around some downtown street wearing a name tag from a conference, that basically is a sign that says, ‘MUG ME.’ In the final analysis, it still comes down to the attendees doing the right thing.”

Someone Else’s Problem?

Planners and attendees must face up to the fact the data theft is an increasingly common issue, and one that particularly affects those within the meetings industry. Even if the planner or attendee is careful, sooner or later that individual is liable to become the victim of identity theft or even open up his or her company to a corporate espionage attack. “Everybody thinks it can’t happen to me,” said Foster. “This is a fallacy. There is no discrimination when a data breach takes place. Everyone is vulnerable.”

Foster is right. Planners and attendees need to quickly take the necessary steps to protect themselves, and their valuable personal and professional data, when they are at meetings and events. There is far too much to lose if they don’t. **C&IT**

Securing Sensitive Data at Meetings and Events

Corporate & Incentive Travel interviewed identity theft expert, consultant and speaker John Sileo, president, The Sileo Group, Denver, CO, regarding the best ways to secure sensitive data at conferences, events and meetings.

C&IT: Identity thieves target meetings, events and conferences because of the sheer quantity and value of data circulating around these activities. What steps should planners take prior to the event to protect their data?

JS: Most important is to secure your online registration system. Invest in a system that delivers efficiency and security. It is your legal, financial and ethical responsibility to protect your attendees' personal data. Don't try to do it all yourself. Hire a reputable technology provider to ensure that all data is protected behind firewalls, encryption, passwords, updated operating systems, security software and so on.

C&IT: Any other suggestions?

JS: Minimize data collection. Collect only the data that you absolutely need and destroy it as soon as you are finished. Once you have processed credit cards, purge that information from your system. The quicker that you properly dispose of sensitive data, the lower will be your risk and liability.

C&IT: What about traveling to the event?

JS: Protect your laptop. Almost 50 percent of serious corporate data theft occurs because a laptop computer is stolen. In addition to the standard forms of protection — passwords, encryption, anti-virus, and so on — carry as little data on your laptop as possible. And never leave a laptop unattended unless it is locked in a hotel safe. Identity thieves target business travelers because they are generally rushed, distracted and carrying valuable data.

C&IT: Any tips on Internet hookups away from the office?

JS: Be careful of free Wi-Fi, which concerns communicating data wirelessly. It is very convenient — and very dangerous — to use a free wireless connection to the Internet that an airport, café or hotel provides. Unfortunately, it is nearly impossible to distinguish if you are on a safe network or one that allows thieves to pirate your information. Unless you are absolutely sure about the security in place, refrain from sending any sensitive material over a wireless connection that your IT department hasn't configured or approved.

C&IT: What should planners watch out for at the meeting venue?

JS: You must control digital access. Don't leave laptops or registration lists unattended, as they are goldmines of sensitive data. Deactivate your USB ports so that no one can easily copy the data onto a USB thumb drive when you aren't looking. One technique for doing this is offered at mydigitallife.info. Make sure that your contact at the hotel understands your security needs and concerns. This is part of the service they provide. Also, control physical access. Use a system of photo ID badges and room monitors to make sure that only

Use a system of photo ID badges and room monitors to make sure that only authorized attendees have access to highly sensitive areas. You don't want your biggest competitor to gain access to the meeting where you reveal next year's strategy. Another important thing is to shred unneeded documents. If you no longer need registration information on an attendee, shred it immediately. Every hotel or conference center should have shredders onsite that you can utilize. If they don't, ask yourself how well they are protecting your data.

C&IT: Any other thoughts?

JS: Above all, don't forget to educate your staff and attendees on the risks of data theft while attending a meeting, conference or event. Higher levels of awareness drastically reduce the incidents of attendee identity theft and corporate espionage. — **MM**



“It is your legal, financial and ethical responsibility to protect your attendees’ personal data.”

**John Sileo, President
The Sileo Group, Denver, CO**