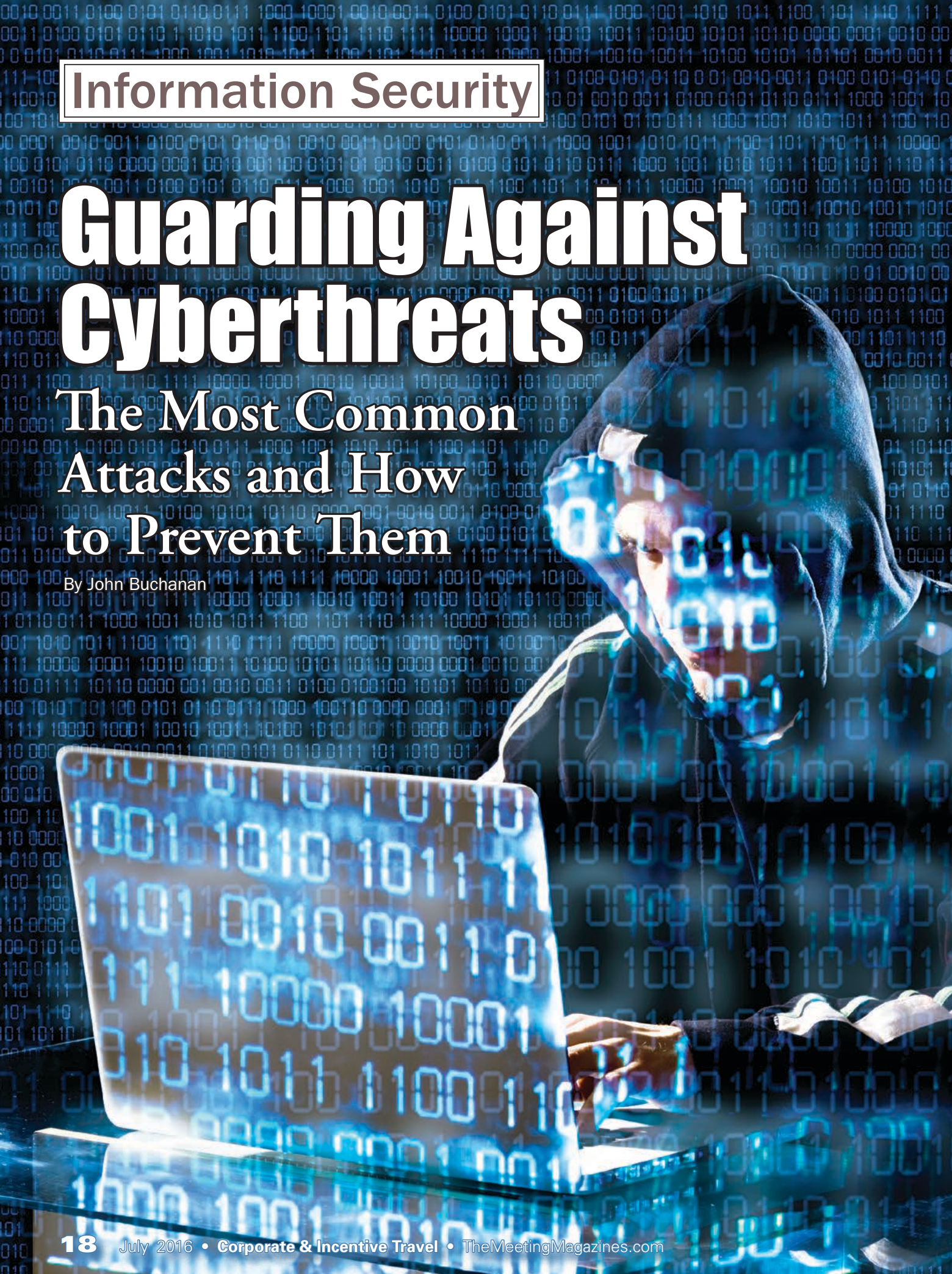
Information Security

Guarding Against Cyberthreats

The Most Common Attacks and How to Prevent Them

By John Buchanan



For any meeting planner or attendee who watches the evening news or reads a major newspaper, it's well known that cybersecurity breaches have become a regular occurrence, often carrying with them severe consequences. So it's surprising, experts say, that planners and attendees do not fully comprehend the unique vulnerabilities they face at an offsite event.

And given the constantly rising level of the threat, the experts say, they become more aware and better prepared.

"What we've seen in the last few years," says Alan Brill, the Secaucus, New Jersey-based senior managing director at global security firm Kroll, "is that hacking of personal and financial information has gone from being shocking and unusual to the point where even a hack that gets the information of hundreds of thousands of people (is almost) not even newsworthy simply because it is so common now. Today, hacking is just a fact of life."

Beyond that, Brill says, "The risks involved in meetings and conventions — and traveling in general — have actually grown at a faster rate than any other sector."

> ***"The risks involved in meetings and conventions — and traveling in general — have actually grown at a faster rate than any other sector."***
>
> **Alan Brill,** Senior Managing Director
> Kroll, Secaucus, NJ

Wi-Fi Networks

At the center of the issue for meeting planners and hosts is the simple fact that hotel Wi-Fi networks are infamously vulnerable. "If you're logging into a hotel's Wi-Fi network, that really opens you up for something to happen," says Vivian Marinelli, senior director of crisis management services at consulting and research firm FEI Behavioral Health in Milwaukee, Wisconsin.

Her expert advice: Never use a hotel's free Wi-Fi network for a meeting or event. "Most people believe it is secure," she says. "And it is not."

The irony, of course, is that free Wi-Fi has been among the most in-demand amenities requested by budget-conscious meeting planners ever since the recession of 2008–09. And today, free Wi-Fi is increasingly available — and risky.

Hotel Information Systems

Last year, security firm Cylance discovered and exposed the serious vulnerability in some models of the commonly used ANTLabs InnGate Internet router found in hotels around the world. In some cases, Cylance found that the router was integrated with the hotel's property management system (PMS), meaning a hacker could strike gold with all data in the hotel's information system, including credit card numbers and the property's door-locking system.

ANTLabs released a security patch soon after Cylance released its report.

But, says Cylance's Irvine, California-based security researcher Brian Wallace, "We did not receive a copy of the patch from ANTLabs to verify that it's actually valid."

Of course, such a revelation raises an obvious question: Why can hotels not eradicate the risks of hacking? And the answer is disappointing, if not surprising. "In general," Marinelli says, "the hackers are always going to be smarter."

Brill is even more direct. "The honest answer to why the hotel chains cannot eliminate the risk is that the problem is not one that can be solved," he says. "The bad guys are just too good at what they do. And they always find a way to stay ahead of the technologies that hotels and other venues like convention centers are using. That's why an understanding of the level of risk and doing your

Physical Security

Although cybersecurity gets almost all of the media attention these days, physical security — and the efforts required to ensure it in meetings and events — remains an important issue.

"Because of the terrorist threat around the world now, the climate has changed when it comes to physical security," says Dean Mazzoli, director of complex security at Walt Disney World Swan & Dolphin Resort in Orlando. "So the big issue now, when it comes to working with meeting clients, is intelligence and communication. And that intelligence can be corporate intelligence or from law enforcement agencies."

The key for planners, Mazzoli says, is to be more aware of and more attuned to the nature of the event and what could potentially happen. "And a lot of times, that is just not what meeting planners are thinking about," Mazzoli says. "They're thinking about their event. They're not always thinking about what their event could bring with it."

Fortunately, he says, he has seen a shift over the last year or so where planners are starting to pay more attention to physical security. "But part of that is also because we, at the property level, are doing a better job at reaching out to our clients to discuss these issues."

The most basic exercise or best practice is to make sure a security plan, including an evacuation plan, is in place — and in writing. And the larger the company, the greater the awareness of the issue should be and the more comprehensive the security planning.

The most obvious rule, Mazzoli says, is to anticipate anything that could possibly happen — such as, for example, action by a disgruntled former employee or an organization that opposes something the company is doing or stands for — and be prepared for any eventuality based on such analysis.

"And that plan, which should be in writing and reviewed with the hotel's security department, should be as detailed as possible in terms of what the risks are for the meeting and what is being done to mitigate those risks," Mazzoli says. And every security plan also should include evacuation protocols for a natural disaster, such as a hurricane, flood or tornado.

For Mazzoli, the key issue is awareness among the meeting planning team. "But there are just some who don't really think about security," he says. "And for them, it's our job to think about security. The most important thing, however, is for the planner to have a real partnership with the security department at your hotel. We're the experts and we want to make sure your event is safe and secure. And the only way we can do that is to communicate with you."

— JB

due diligence is more critical than ever for meeting planners and attendees."

Risks and Vulnerabilities

For meeting planners, there are three basic levels of risk involved in holding a meeting in a hotel. The first, oddly enough, is simply the fact that you are in a hotel.

"Hotel companies have been the subject of a huge number of data breaches in the recent past," Brill notes. "The series of incidents at companies like Wyndham or Hyatt or any of the other major brands are well known now. And hotel chains get hit because they are great targets; they tend to have so many customers and as a result, so much information available. And beyond that, there is also the perception that hotel customers, especially for meetings and events, are more affluent and therefore the information that can be stolen is more valuable."

The second risk category is the property Wi-Fi network. "It has become so easy to set up a phony Wi-Fi hot spot and make it look legitimate that it's almost expected at this point that if you use free Wi-Fi, you're going to get hit at some point," Brill says.

But instead of most people being aware of that reality, Brill says, their perception and attitude are the exact opposite. "So many people just say, 'Oh, I know all about those scams and the risks of Wi-Fi. I'm not going to fall victim to them because I'm either going to do my brows-

ing on my phone, or I'm going to use my personal phone as a hotspot and the only thing I'm going to allow myself to connect to is my own network.' The problem with that is that the bad guys have the same technology that the good guys do."

The best-practice solution Brill recommends to meeting planners is to use their own encryption for their events. Do not rely on the assumption that the encryption provided by your technology vendor is secure and safe, he stresses. "Unless you have your own encryption," he warns, "you are likely to get in trouble at some point."

Marinelli and Wallace wholeheartedly concur with that assessment.

Virtual Private Networks

The good news is that a readily available, easy to use and inexpensive solution is available — a virtual private network (VPN) that is set up and managed only for your event and your people.

However, Brill adds, it's important to not only arrange for a VPN, but it's also vital to instruct attendees before the meeting on its availability and how to use it.

"When the meeting planner sends out information about the meeting — about the hotel or the agenda or things to do in the destination — he or she should also inform attendees that there is a risk and tell them that as soon as they connect to the internet onsite, they must immediately initiate their VPN. And (the planner) should also inform attendees of how to do that and who the company's vendor is for the event." Brill adds that planners also can easily provide a link to an article that tells attendees how to set up their VPN and use it properly.

Given the ever-increasing cybersecurity threats at meetings, Brill says he is surprised that so few meeting planners set up a VPN and clearly instruct attendees what it is and how to use it. That is one area of planner due diligence that must be dramatically improved, he says.

Wallace goes even further and says that if highly sensitive information is being presented and reviewed at the meeting, a planner should skip wireless technology altogether and use an old-fashioned, hard-wired system for internet access. That is much more secure, he points out. "Essentially a hard-wired, dedicated internet connection decreases the attack surface to the maximum extent possible," he says. "It's a physical connection. And that is a lot harder to compromise."

"If you are traveling to certain parts of the world, such as Asia, there is now a suggestion that you take temporary devices issued to you just for that trip."

Vivian Marinelli, Senior Director, Crisis Management Services
FEI Behavioral Health, Milwaukee, WI

For her part, Marinelli stresses the issue of geography. "If you are traveling to certain parts of the world, such as Asia, there is now a suggestion that you take temporary devices issued to you just for that trip and not the devices you use every day," she says. "And that recommendation is made because the risk of malware and other cybersecurity threats is even worse in some parts of the world than it is in the U.S."

Her other caution is to attendees at meetings anywhere, including the U.S. "Be careful of what you do online," she says. "For example, never do your online banking while you're sitting in your hotel room, even in the U.S. If you do that, you are definitely opening yourself up to serious vulnerability."

Temporary Credit Card Numbers

The third and final level of specific risks that Brill invokes is credit cards — and especially those being used for a meeting or event. Their unique vulnerability should be universally comprehended by now, he says. But again, he says, the solution is simple.

"Some credit card vendors allow you to generate a one-time card number," Brill says. "So, you can have a card you only use when you're traveling to pay for your hotel. And now several banks, including Bank of America, offer that kind of more secure credit card technology. But unfortunately, most people have never heard of it, even though the technology has been around for years. But that kind of solution is something that more meeting planners and the companies they work for should become familiar with."

How it works: When it's time to check out of your hotel, you contact your bank

and have them generate a one-time credit card number specifically related to the payment of one transaction in a specific amount. "The card number is only usable for that one transaction," Brill says. "And that means that even if that card number is somehow stolen after that transaction, it's useless because the card number is no longer any good."

The Next Frontiers of Risk

As hackers get better at their work and identify more areas of onsite vulnerabilities at meetings, the risk level for planners and attendees will continue to rise, the experts say.

An emerging threat, as a result of their increasing use, is kiosks that assist with functions such as registration. They carry a high level of inherent risk, Wallace says. Like gas pumps, which are easily compromised with a small device, kiosks are uniquely vulnerable.

"They are computers that are essentially left out in the open," Wallace says. "So that means someone could just walk up with a USB stick that can insert code into the computer and get access to what's in the machine."

An issue Brill finds both interesting and concerning is the fact that technology providers now work more closely with hotels to provide solutions that enhance "the guest experience." At the same time, however, they are sometimes potentially putting guests more at risk.

One example: keyless entry via your smartphone. "That kind of new technology means that data security becomes even more important, because that data security issue now includes physical access to your hotel room," Brill says.

In effect, he says, such innovative technology represents a sort of Pandora's box that has not been opened yet. And the more common that technology becomes, the greater the risk.

"Essentially a hard-wired, dedicated internet connection decreases the attack surface to the maximum extent possible. It's a physical connection. And that is a lot harder to compromise."

Brian Wallace, Security Researcher
Cylance, Irvine, CA

The security-related technology that most interests Brill in that context is the use of biometrics, such as a fingerprint.

"What's interesting about that issue is that the challenge is not going to be technology," Brill says. "The challenge, or the problem, is going to be privacy. For example, those systems that use fingerprints convert your fingerprint to a digital signature. So the question then becomes what if someone steals your fingerprint? And that's an issue that no one can predict the outcome of yet."

Yet another area of unknown but potentially serious risk is the use of electronic, universal pass keys to hotel rooms by employees such as housekeepers. That technology represents yet another Pandora's box, because it's reasonable to assume that someday, hackers will gain access to all of the rooms on an entire floor — or floors — of a hotel. Few planners have likely ever pondered the possibility of attendees returning to their rooms at the end of the day to find them looted.

Such potential scenarios require ever more due diligence from planners, Brill says.

His advice: "Ask your hotel what their security protocols are when it comes to access to guest rooms and meeting rooms. But if they give you that too quickly and easily, that could be a bad sign, because it could mean they recently gave it to a bad guy who claimed he was interested in setting up a meeting in the hotel."

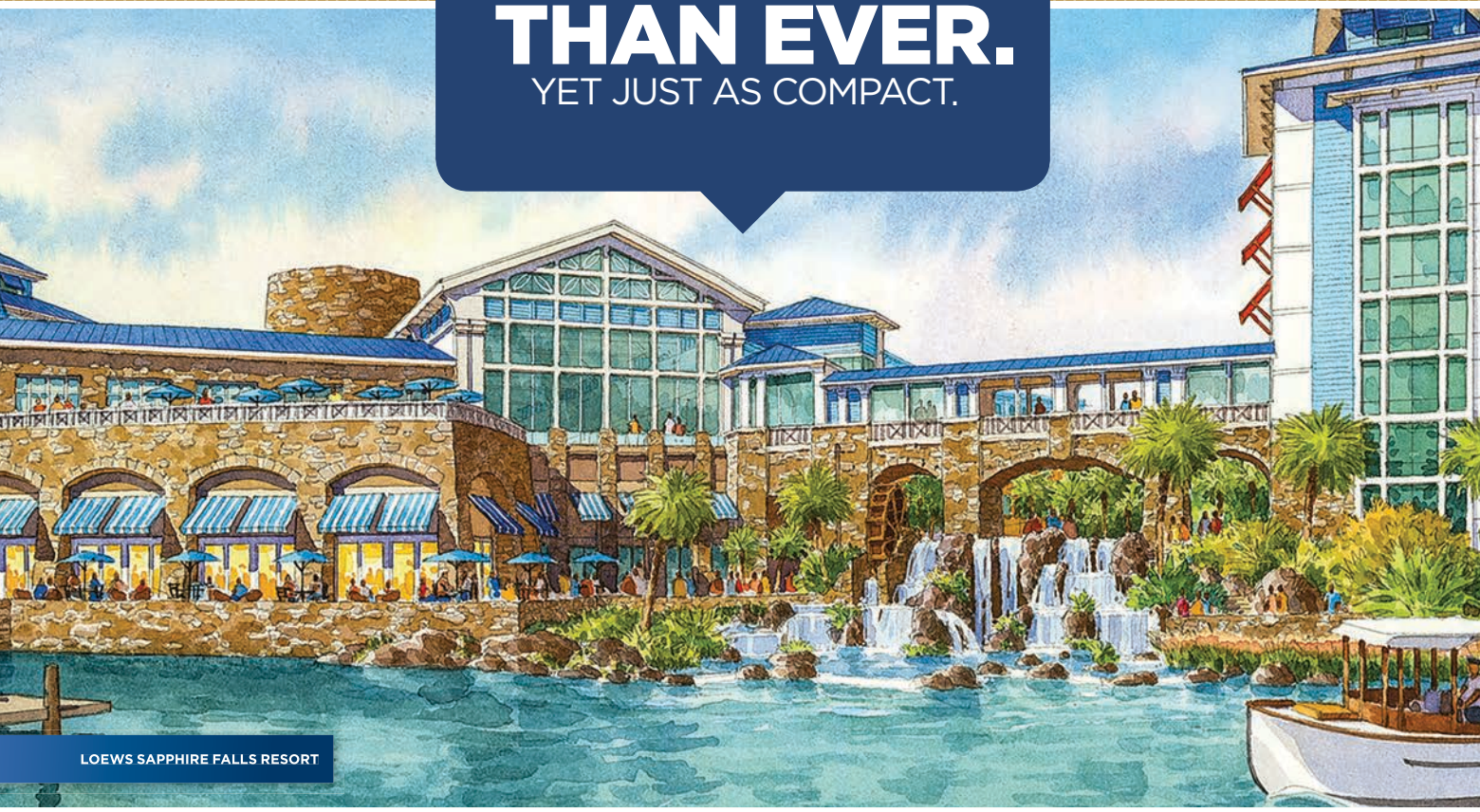
Planners Paying More Attention

The most fundamental challenge facing meeting planners, Marinelli says, is that solutions to security vulnerabilities are not available. "The problem," she says, "is that not enough people who go to meetings think about them often enough."

Put simply, she believes — and Brill agrees — that many meeting planners are unaware of the risks they face. "It doesn't surprise me though," Marinelli says. "The reason is that although there is more media coverage of cyberattacks, most people feel relatively safe. But the reason most people feel safe is just because they are not aware of how serious the risk of a breach actually is." ***C&IT***

BIGGER THAN EVER.

YET JUST AS COMPACT.



LOEWS SAPPHIRE FALLS RESORT

NOW GROUPS LARGE AND SMALL CAN CONNECT IN MORE WAYS THAN ONE.

Universal Orlando® Resort offers more hotels, more meeting space, and more exciting event options than ever before. With the 2016 opening of Loews Sapphire Falls Resort, you'll have your choice of five spectacular on-site hotels with 5,200 total guest rooms and a combined 295,000 square feet of meeting space. Plus, the new hotel connects with Loews Royal Pacific Resort to create The Loews Meeting Complex, complete with multiple ballrooms and a wealth of meeting and breakout rooms.

Best of all, each on-site hotel is within walking distance of the resort's theme parks and the Universal CityWalk® dining and entertainment complex. So, as a planner, you can host everything on your agenda in one convenient campus.

FOR MORE INFORMATION & TO SUBMIT YOUR RFP: WWW.UOMEETINGSANDEVENTS.COM/CIT • 888-322-5531

UNIVERSAL Orlando RESORT
MEETINGS & EVENTS

LOEWS HOTELS RESORTS

LOEWS SAPPHIRE FALLS RESORT | LOEWS ROYAL PACIFIC RESORT | LOEWS PORTOFINO BAY HOTEL
HARD ROCK HOTEL® | UNIVERSAL'S CABANA BAY BEACH RESORT