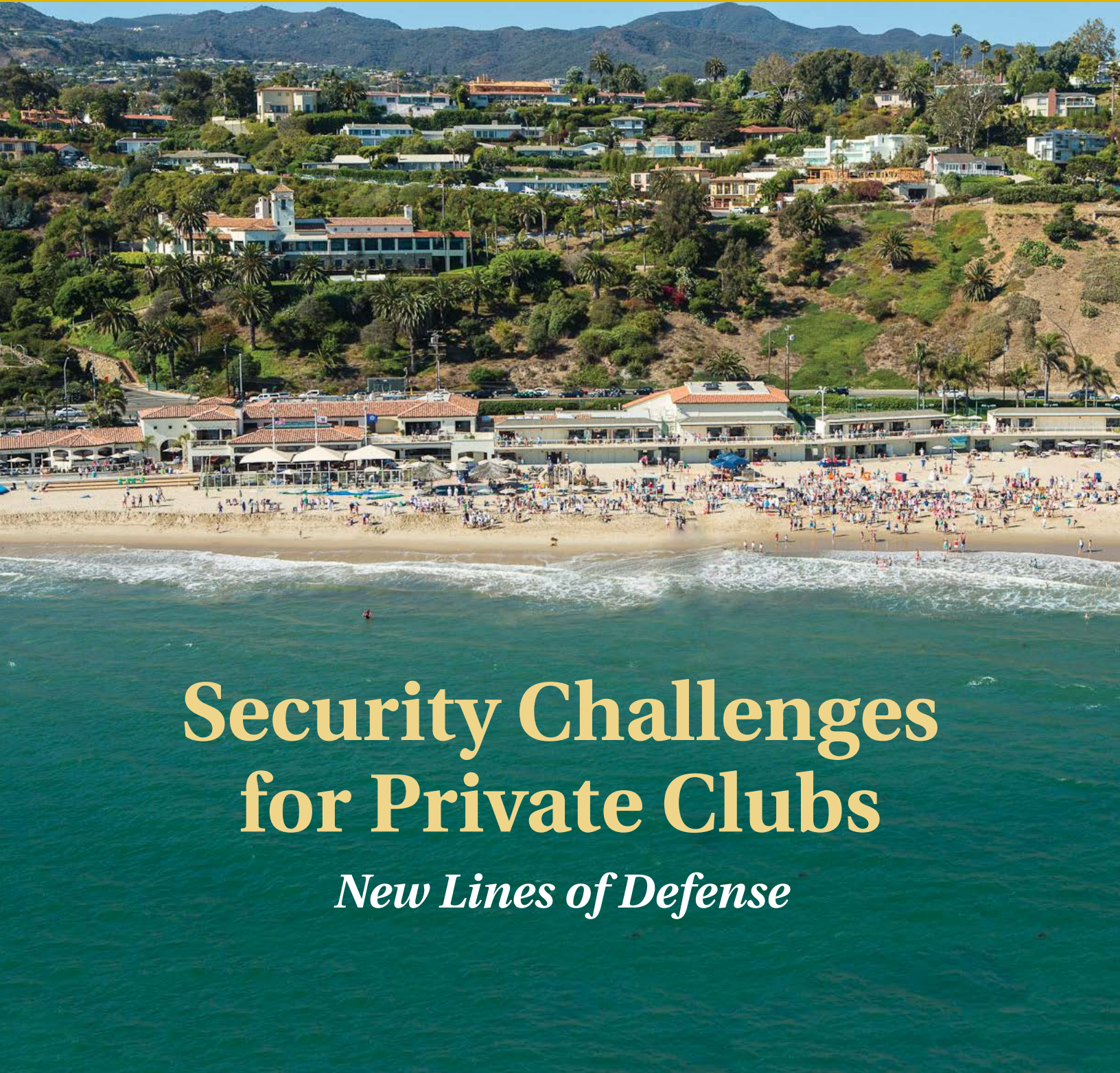


NATIONAL CLUB ASSOCIATION ♦ McMAHON GROUP

# CLUB TRENDS

STRATEGIES FOR SUCCESSFUL CLUBS



## Security Challenges for Private Clubs

*New Lines of Defense*



# Table of Contents

CLUB TRENDS | Summer 2017 | Volume 4, Issue 3

[mcmahongroup.com](http://mcmahongroup.com) | [nationalclub.org](http://nationalclub.org)

## FEATURES:



**Cyber and Physical Security Risks:**  
How to Protect Your Club and Its Data



**Taking the Pulse on Club Security:**  
Physical and Cyber Protection



**Cyber Security:** The Threat Rising



**Security and Safety:** A Club Manager's Guide



**Our Safe Haven:** The Growing Importance of Club Safety

## CASE STUDIES:

**Piece of Mind at Desert Highlands** .....16

**Canoe Brook Country Club:** Physical Security at the Club.....18

**Members Only! Case Studies on Security and Control:**  
**The Granite Club & Bel-Air Bay Club** ..... 20

Cover image: Bel-Air Bay Club

Copyright 2017, National Club Association and McMahon Group.  
All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise without prior written permission of the publisher.

For information about purchasing copies of this report, please contact:

McMahon Group, Inc.  
670 Mason Ridge Center Drive, Suite 220  
St. Louis, MO 63141  
Phone: 314-744-5040 or 800-365-2498  
Fax: 314-744-5046  
Questions: [info@mcmahongroup.com](mailto:info@mcmahongroup.com)  
[mcmahongroup.com](http://mcmahongroup.com)

National Club Association  
1201 15th Street NW, Suite 450  
Washington, DC 20005  
Phone: 202-822-9822 or 800-625-6221  
Fax: 202-822-9808  
Questions: [info@nationalclub.org](mailto:info@nationalclub.org)  
[nationalclub.org](http://nationalclub.org)

## CLUB TRENDS TEAM:

### McMAHON GROUP

**William (Bill) McMahon, Sr., AIA, OAA**  
*Chairman*

**Frank J. Vain**  
*President*

**Bill McMahon, Jr.**  
*Consultant & Editor*

**Jim Fisher, PhD**  
*Data & Marketing Consultant*

**Richard Lareau, CCM, ECM**  
*Director of Dining Operations Enhancement*

**Jake Fisher**  
*Writer*

### NATIONAL CLUB ASSOCIATION

**Henry Wallmeyer**  
*President & CEO*

**Cindy Vizza**  
*Vice President, Communications*

**Phillip G. Mike**  
*Senior Communications Manager*

**Curtis Rogers**  
*Senior Marketing Manager*

**Bridget Gorman Wendling**  
*Writer*

### DESIGN & PRODUCTION

**Tim Smith**  
*Design and Production*

**Sharpdots**  
*Printing*

*Club Trends* is published quarterly by McMahon Group and the National Club Association. Periodical postage paid at Washington, DC, and additional mailing offices.

**POSTMASTER:** Send address changes to *Club Trends*, National Club Association, 1201 15th Street NW, Suite 450, Washington, DC 20005.

*Club Trends* is distributed to McMahon Group subscribers and NCA members. An annual subscription is \$650. NCA members receive two copies as a benefit of membership. Individual issues are available for \$195.

---

## Risky Business

**A**s club leaders set the agenda for the future health and vibrancy of their clubs, there is probably no area more important than the one summarized in this issue of *Club Trends*—safety and security.

The challenge is twofold. First, as the digital dimension of modern life continues to expand, the idea of security has an inescapable duality, playing out in both physical spaces as well as online, where we find the residue of our daily activities increasingly piling up as so many bits and bytes.

Unfortunately, the damages suffered on this “virtual” plane of existence are no less real or costly as those incurred in the so-called “real” world. Wealth, reputation, and now, even personal health and well-being are threatened on the cyber battlefield.

Second, some of our most cherished notions about safety and security are now subject to reappraisal if not exactly outright assault. What were once considered the safest of places—schools and places of worship, for example—are tightening up access and considering the prospect of active shooter drills. Will the oasis of club life be next?

Managers cannot bet their future nor the safety and security of their members and staff on wishful thinking. This issue provides the knowledge and resources to accelerate your plans, policies and procedures for professionalizing your approach to risk management.

A new, comprehensive survey of the macro-environment identifies both a wide range of threats to safety and security as well as the responses that represent the frontline of protection and containment of these threats.

This issue provides a look at what club managers and leaders are doing to manage risk. The Pulse Survey offers a quantitative snapshot, which is supplemented by an array of case studies and reports from the field.

Thought leaders and experts also weigh in by identifying important trends as well as practical management guidelines.

Clubs have always offered a protected haven for members to enjoy the good things of life—family, friends and leisure in a stimulating and gracious environment that is both safe and secure. Let’s work to keep it that way!

---



# Cyber and Physical Security Risks

## HOW TO PROTECT YOUR CLUB AND ITS DATA

By Phillip Mike

Cyber threats have increasingly become part of nationwide security discussions, impacting virtually all individuals and institutions from personal bank accounts, to big business to the federal government. Private clubs in particular are vulnerable to such attacks as they often house sensitive data regarding some of the most wealthy and prominent individuals in the world. Along with managing threats to their physical plants, clubs must be more prepared than ever to mitigate security risks. Here are some of the latest trends in cyber and physical security.

### PHISHING

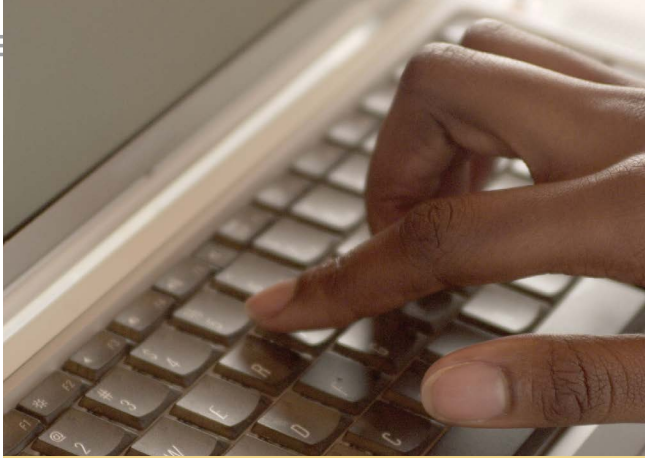
2016 saw the most phishing attacks in history, reports the Anti-Phishing Working Group (APWG). According to the APWG's new *Phishing Activity Trends Report*, the total number of phishing attacks in 2016 totaled 1,220,523—a 65 percent increase over 2015.

Phishing is a popular hacking method because “it primarily relies on fooling people,” said APWG Senior Research Fellow Greg Aaron. This makes it imperative for employers/employees to learn how to identify these threats before they harm their places of work. (See sidebar, “Glossary of Cyber Attacks, page 3.)

### RANSOMWARE

Ransomware attacks, in which hackers use malicious software to encrypt a user's data and then extort money to unencrypt it, increased 50 percent in 2016, according to a report from Verizon Communications Inc. and McAfee Inc. The average price to retrieve captured data was \$1,077, reports Symantec. This number represents a 266 percent increase over 2015. A recent IBM Security study discovered that 70 percent of businesses attacked by ransomware paid the ransom. Half of those paid more than \$40,000 to get their data back.





## Glossary of Cyber Attacks

Here is brief description of some of the most common cyber attacks.

**Malware:** Harmful software, including viruses and ransomware, that performs a variety of actions that can sabotage a system. They include taking over a machine, monitoring actions and sending confidential data from a computer to a hacker.

**Phishing:** A strategy used by hackers to trick users into clicking malicious software. The software can be disguised as legitimate emails, attachments or files sent to the user.

**SQL Injection Attack:** SQL or “sequel” (structured query language) is a programming language used to manage data stored in databases. An SQL injection attack targets these servers to force them to divulge information such as credit number numbers, usernames, passwords and other personal information.

**Cross-Site Scripting (XSS):** Similar to an SQL injection attack, malicious code is sent to a website, but instead of attacking the website, the software attacks users when they visit the targeted webpage.

**Denial of Service (DoS):** Overloading a website to prevent visitors, to crash it and prevent users from accessing it.









**Session Hijacking and Man-in-the-Middle Attacks:** This occurs when an attack hijacks the unique session information transmitted between a user and a web server in order to gain access to unauthorized data on the web server. The attacker can also use the data to pose as the user.

**Credential Reuse:** Users often reuse the same login information for multiple sites. Once attackers have a user's login credentials, they may attempt to, and successfully access other websites by using the person's login.

Source: Rapid7, a global technology security and IT consultant.

## WHAT YOU DON'T KNOW MIGHT HURT YOUR EMPLOYER

While clubs and other organizations might have systems in place to reduce the risk of cyber attacks, each employee's actions are critical to achieving a safe cyber environment. According to a recent Pew Research Center quiz that evaluated knowledge of cyber security among Americans, a majority of respondents answered fewer than half of the questions correctly. You can take the quiz at [pewinternet.org/quiz/cybersecurity-knowledge/](http://pewinternet.org/quiz/cybersecurity-knowledge/) to see if you can score better than these results:

-  **10%** could identify an example of a multi-factor authentication screen
  -  **13%** know the purpose a Virtual Private Network (VPN) serves
  -  **33%** could identify an encrypted URL
  -  **39%** knew “private browsing” mode does not prevent internet service providers from monitoring subscribers’ online activity
  -  **48%** could correctly define the term “ransomware”
- Organization “insiders” (i.e., employees) are the cause of 30 percent of cyber attacks, reports Haystack Technology, a leading security analytics platform provider.
-  **60%** of organizations believe privileged IT users/ admins pose the biggest cyber threat to the company
  -  **57%** believe it is contractors and consultants
  -  **51%** believe it is regular employees

## GENERATION GAP?

Generations view cyber security differently. A 2016 study by Forcepoint, a computer security software company, showed that nearly two-in-three millennials use their cell phones for both work and personal use. While 70 percent of this group says they understand and use strong passwords, 42 percent use the same password across multiple systems and apps.

Millennials are also vulnerable due to their use of public Wi-Fi networks. Ten percent use public Wi-Fi to access work systems and accounts, 23 percent download content to their work devices from public networks and 10 percent do not change their online habits when using a private versus public wireless networks. Perhaps most alarming, 54 percent of millennials said they would rather boost their internet speed than improve their personal online security. Just 33 percent of millennials have secure passwords compared to 53 percent of baby boomers.

When it comes to cyber security knowledge, younger generations tend to know more than older groups, however, it

varies depending on the subject, reports a Pew Research Center quiz. While respondents ages 18 to 29 correctly answered questions regarding private browsing and GPS tracking—at more than 23 percentage points higher than respondents 65 and older—the younger generation was worse at identifying a phishing attack by two percentage points.

Overall, those ages 18 to 29 answered six of 13 questions correctly while those 65 and older answered five correctly.

## CYBER INSURANCE

According to a 2016 survey by the Risk Management Society, a nonprofit made up of risk management professionals, 80 percent of responding organizations had purchased stand-alone cyber insurance. The number grew 29 percent from the previous year.

The respondents' biggest areas of concerns were reputational harm (82%), business interruption and expenses from a network outage (76%), costs related to notification (76%), cyber extortion (63%) and trade secret and IP theft (42%).

Eighty-one percent of surveyed organizations said they have a cyber attack response plan in place and 85 percent of that group said their legal department was involved in that plan.

## What Hospitality Employers Should Do Now

Employers in the hospitality industry should consider the following steps to reduce their cyber threat risk:

- **Adopt appropriate policies** to prevent data breaches, and take special care to protect devices with access to point-of-sale information.
- Be aware that drafting policies is effective only if **employees are adequately trained** to follow those policies.
- **Never assume** that employees already know or follow data security best practices.
- If you have a high employee turnover, **consider conducting frequent trainings** to ensure that recent hires are aware of applicable security policies.
- In addition to taking steps to prevent security breaches, **develop a security breach rapid response plan and team** that includes a procedure for alerting impacted customers, employees and financial institutions.

Source: Epstein Becker & Green Law Blog





## PHYSICAL SECURITY

Clubs and other segments of the hospitality industry, and schools now have more tools to maintain safety on their campuses.

### *Beacon Technology*

Innovations like beacon technology can communicate with users' devices to send important information. Beacon technology can tell users, such as school children, where buildings and classrooms are by using a multi-level mapping system. It can also identify who is on the campus and where they are located. Combining these features, users can be told where to go in case of an emergency.

### *Biometric Technology*

Spanning the areas of both physical and cyber security, biometric technology's presence is growing. A survey by Market Wired forecasts that the global biometric technologies market will reach \$41.5 billion by 2020 from a total of \$14.9 billion in 2015.

On platforms like mobile payment and online banking, biometrics can be utilized via smartphone to read a user's fingerprints. The same type of verification is now being applied to point of sales machines as well. MasterCard has gone as far as to develop a concept called "selfie pay," which allows users to verify their identity through a picture of themselves.

## THE PHYSICAL PLANT

Securing the physical plant takes comprehensive planning. It involves having a disaster planning team, sufficient staff training, emergency contacts, a site map, routine inspections, IT preparation and equipment to ensure the facility can operate while in an emergency.

Vital equipment during a disaster or emergency include:

*Generators/Surge protectors/Battery backups:* These can keep a club powered during an emergency or crisis.

*Server protection:* These store and share vital information for your club's needs and should be kept running and out of harm's way during an emergency.

*Data Backup Systems:* These systems protect a club's critical information.

*Key communications systems:* A reliable internet connection, two-way radios and other phone systems can facilitate vital communications during a club's most vulnerable moments.

## RELIANCE ON TECHNOLOGY

As clubs and other businesses increase their reliance on user-friendly and easy access technology, it is becoming more important to protect organizational data and those it serves from cyber criminals. The expansion of technology has provided numerous benefits to the private club industry; however, these advancements also pose serious threats to clubs' reputations, services and members. By implementing up-to-date cyber security measures and monitoring the latest threats and best practices, clubs can reduce the threat of a cyber attack and mitigate any damages from a data breach. ♦

---

## Top 10 Threats to Club Security

- 1 Potential threats go unrecognized and unmitigated.
- 2 Security gaps go unidentified and unmitigated.
- 3 Attacker perspective not applied.
- 4 Lack of imagination in considering the range of a possible threat.
- 5 Lack of a holistic risk management plan.
- 6 Lack of an incident response plan.
- 7 Lack of a proper command and control mechanism.
- 8 Lack of local medical, fire and police integration to security plans.
- 9 Member safety undermined by a 'convenience over security' approach.
- 10 Over reliance on technical security countermeasures.

Source: TorchStone

# Taking the Pulse on Club Security: Physical and Cyber Protection

By Bill McMahon, Jr.

More than 370 club executives responded to the latest Pulse Survey to learn about how clubs are handling their security in both the physical and cyber worlds. Here is a summary of the results:

## GENERAL SAFETY ISSUES

**Secure Environment:** Ninety-nine percent of respondents believe their club is a safe and secure environment for their members. Interestingly, only 49 percent stated they believe having a safe and secure environment is a main reason someone joins their club. Of the 51 percent who stated it is not a major reason, only 31 percent of this group thinks it should be.

**Security Budget:** The average budget for all security (physical and cyber) needs is approximately \$75,300 annually.

## PHYSICAL SECURITY ISSUES

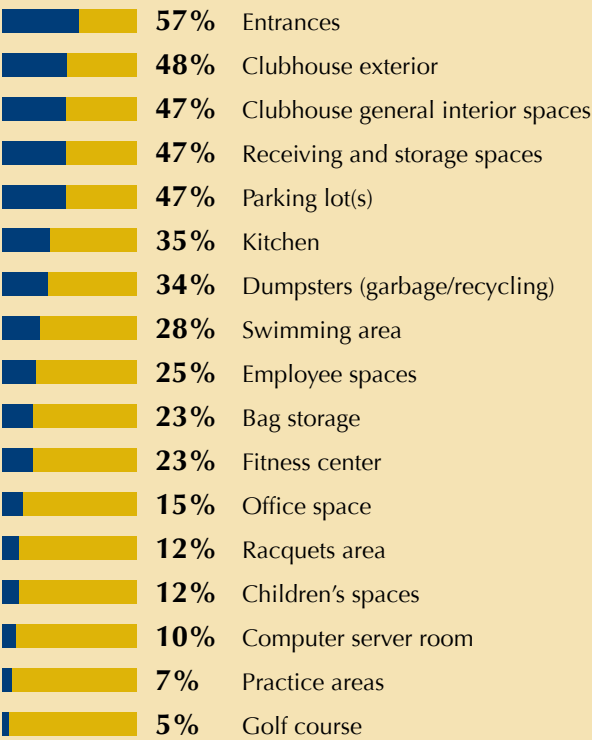
**Security Department:** Only 27 percent of respondents said they have a security department or staff at their club. Of this group, 62 percent said it was made up of club staff, 24 percent said it was an outside firm and the remaining 14 percent stated it was a combination of both.

**Security Incidents:** Sixty percent of the respondents stated that they had experienced a security incident at their club within the last five years. Below is a list of the top issues that occurred comparing the overall response to those clubs with more than 1,000 members, and to those clubs with an initiation fee over \$50,000:

Incident	Overall Response	Response from Clubs with More Than 1,000 Members	Response from Clubs with Initiation Fee Greater Than \$50,000
Trespassers	35%	58%	45%
Car break-ins	32%	42%	47%
Vandalism	26%	33%	25%
Theft in locker rooms	18%	40%	27%
Theft in clubhouse	15%	36%	12%
Intoxication/drug use	14%	36%	15%
Theft of maintenance equipment/supplies	10%	18%	8%

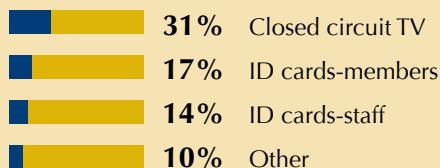
**Surveillance System:** Seventy percent stated they have a camera system monitoring their club grounds. Twenty percent of this group feels their system is ineffective. The average number of cameras being used at clubs is 23.

The areas being monitored the most are:

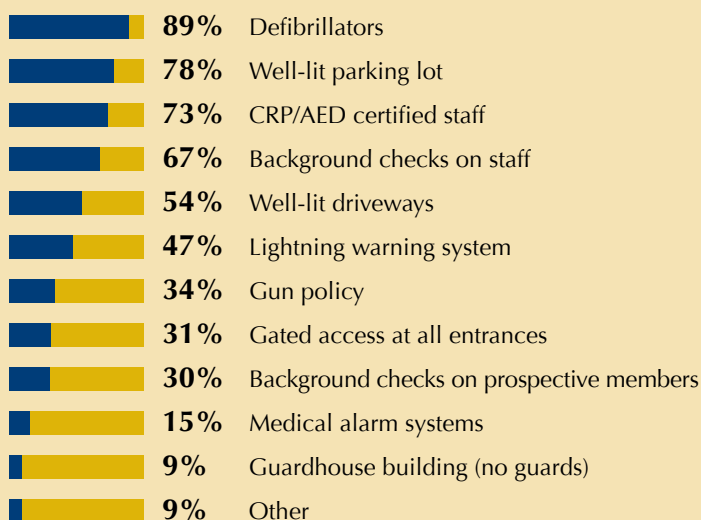




**Technology to Know Who is at the Club:** While only one respondent indicated that it uses biometric facial recognition technology, more clubs use beacon technology (4%) and RFID (7%) to track who is on club premises. However, the most popular ways clubs monitor staff and members on property are:



**Providing Safe Environment:** Here are the ways clubs are providing a safe environment for their members and staff:



**Security Policies & Plans:** Respondents were asked if they had a formal plan or policy for each and if they provide regular staff training or drills.

Situation	Have a Formal Policy/Plan	Do Regular Training and Drills
Fire	81%	42%
Medical emergency situations	78%	51%
Active shooter	71%	35%
Natural disaster	69%	30%
Evacuation procedure	68%	34%
Missing child	60%	23%
Weather-related event	25%	11%
Hazardous materials	23%	12%

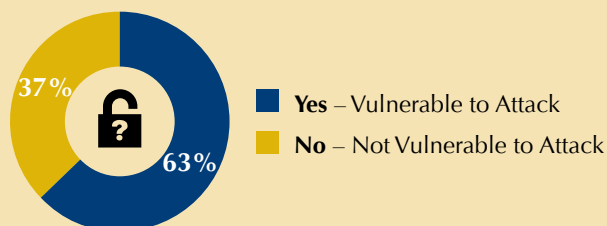
## CYBER SECURITY

**Cyber Security:** Overall, 78 percent of respondents feel they are informed or very informed about cyber security issues.

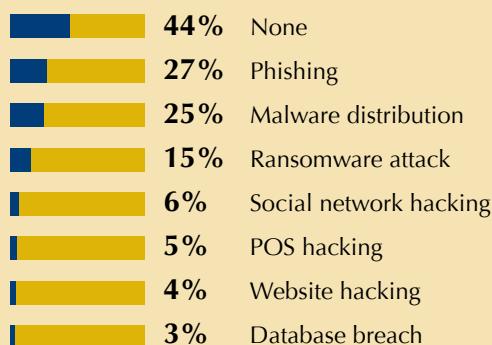
Only 41 percent of the respondents stated they have conducted a cyber security vulnerability assessment within the last year.

**Cyber Security Breach:** The chart below shows the concern over a possible breach. Among clubs with an initiation fee over \$50,000 the threat is even higher (72%).

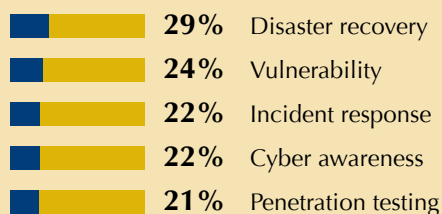
*Is Your Club Vulnerable to a Cyber Security Breach?*



**Cyber Security Breach:** Clubs were asked if they had any cyber security breaches within the last five years and the most common breaches identified by respondents were:



**Cyber Security Budgets:** In general, about a quarter of club respondents budget for cyber security measures, including:



**Cyber Security Awareness:** Less than half of respondents (49%) train staff on cyber security awareness. Only 53 percent of clubs brief their boards on cyber security, with 54 percent of those clubs briefing their boards once a year.



### GET THE REPORT

Pulse Survey Reports are complimentary to those who complete the survey. If you did not have a chance to complete this Pulse Survey, but still would like a copy of the report, please contact Bill McMahon Jr. at [wpmjr@mcmahongroup.com](mailto:wpmjr@mcmahongroup.com).



# Cyber Security: The Threat Rising

Bill McMahon, Jr.

***“In the very near future, cyber security exercises are going to be absolutely expected of all companies by regulators.”***

— Michael Vatis, partner in the New York office of Steptoe

We are living in a world today where it has become alarmingly simplistic for a cyber attack to wreak havoc on a government body, an organization or even an individual. A hacker's ability to hold an entity hostage or use human nature or ignorance to inadvertently harm the security of others or themselves is rapidly changing the world around us. Historically, the private club industry lags about five years behind the times in terms of technology and communications (think about how long it took for clubs to embrace websites, now apps). The industry is shortening that gap, but still needs to focus on protecting the information clubs are storing. One main issue with cyber security is that a club cannot just buy a device or software package to eliminate all cyber threats or entirely protect the club. It requires a thorough review of the network, allocation of

necessary resources and continuous monitoring as new forms of cybercrime emerge.

On page 6, the Pulse Survey on private club security issues reveals that an alarming 63 percent (many experts believe this is a low number) of responding club executives feel they are vulnerable to a cyber threat of some kind. No one can be 100 percent confident as human nature plays a large role in cybercrime; however, clubs need to emphasize improving how they protect their data, including personal information about their members.

To get better perspective on this issue, *Club Trends* reached out to information technology (IT) and industry specialists to help understand what they are seeing in this world. First, we talked with Noel Wixsom of Country Club Technology Partners (CC Tech). Wixsom said the biggest issue within private clubs is that there is a significant lack of education on this subject matter. He wants to see more education for managers who in turn can then properly educate their staff. However, there is no real set standard today for cyber security for any businesses. With the current

*Continued on page 10*



# Club Security

## Are Your Members Protected?

By Gary Raphael, TorchStone Global, LLC

Information security poses serious risks to club leaders, but it also provides an opportunity to protect your members and your club.

Private clubs are responsible for valuable data that malicious criminals want, including your members' personal contact and financial information. Attackers pursue this data because it can be sold or used to target your members. Losing personal member data can have a devastating effect upon the reputation and membership growth of a club, making it critical for clubs to secure their data. To do so, clubs should harden the measures used to protect their members' information. Many of those things are not technical, complex or expensive.



1. **The first step is becoming aware** (If you've read this far, you've probably already achieved this step).

2. **The next step is creating a proactive, positive security culture within the club.** This entails:

- Fostering staff information security awareness.
- Rewarding positive security behavior and institute accountability for poor security behavior.
- Understanding what information your club handles is truly sensitive.
- Protecting only what needs protection.
- Understanding your club's current security measures, determine if they are adequate and develop new measures if needed.

3. **Clubs should then eliminate their cyber gaps.** Common vulnerabilities include: Unnecessarily maintaining too much personal member data, providing member data access too broadly to staff, using short and simple passwords and single-factor authentication.

Information security is an evolving discipline, requiring constant monitoring of potential threats and implementing best practices to reduce the risk of an attack. While understanding cyber threats to your club are important, know your limitations—your time is best spent growing your club. A good information security partner allows you to do that, while protecting your members by:

- Providing a holistic assessment of your information security risk from the attacker's perspective and looking at all domains for technical, human and physical vulnerabilities.
- Reviewing or creating information security and hiring/firing policies and procedures to reduce your risk to intentional or unintentional insider actions leading to breaches.
- Providing a tailored set of recommended countermeasures for those vulnerabilities, leveraging current strengths and fitting within your financial limitations.
- Implementing the recommendations you accept.
- Ensuring that your club has a sustainable mechanism for protecting your club's lifeblood—the trust of your members.

For more information, visit [torchstoneglobal.com](http://torchstoneglobal.com).

environment in the cyber realm, Wixsom recommends two things you must have:

- **Cyber Insurance:** Your policy needs to cover you for any type of extortion, business interruption, data restoration and any credit monitoring. (See sidebar below for more information.)
- **Security Committee:** You may be thinking, “Not another committee.” You are in luck, this committee is really an internal one made up of the general manager, facilities manager, security director, controller, IT manager and IT vendor. This committee’s responsibility is to oversee the club’s security—both physical and cyber.

Detective Scott Slifer of the Lawrence, Kan., Police Department is an expert on the subject who deals with cybercrime cases in Kansas and across the country. He said the biggest threat today is ransomware (a software threat that blocks users from their information unless the user pays a ransom) and doesn’t see it going away any time soon. Slifer believes the path to a safe network revolves around an effective backup schedule, good firewall, and, most importantly, education of your staff so they can be better aware of issues. He also recommends clubs check with their IT provider to ensure they have cyber security certification.

From everyone we talk to about this very issue, they all are preaching the same thing—education. The more we understand about cybercrimes and how they affect us, the better we can be at preventing them or being able to function after an attack happens. We are never going to be able stop all attacks, but the goal should be that if one does break through you will have a plan in place to react accordingly. There are many quality vendors out there willing to help you with your cyber security needs from CC Tech to Cino Ltd. and TouchStone Global LLC, featured in this issue. Reach out to a professional to ensure your club is protected. ♦



## Keeping up to date

With the cyber world constantly evolving, be sure to continue to educate your staff and even members on cyber awareness. Here are how things are changing:

- **Data Protection:** It is critical to protect members’ personal data as well as all the club’s financial information. Programmers today are now building databases for clients using HIPAA (Health Insurance Portability and Accountability Act) standards to better protect the information being stored on networks and in the cloud. This is where data protection is going.
- **Passwords:** Educate staff on the importance of developing unique passwords and changing them often. Many companies are now even switching to two-step authentication requiring use of your mobile device.
- **Internet of Things:** More and more devices can connect to the internet these days from drones to printers to the thermostat. However, these devices often meet minimum security requirements allowing hackers the ability to easily access them to gain entry to your network.
- **Behavioral Technologies:** The use of biometrics and facial recognition will become more the norm in the future.

## Cyber Insurance: How Is Your Coverage?

Cyber Liability insurance is readily available and most clubs have some type of policy (about two-thirds according to a recent Pulse Survey). Tom Walker, area executive vice president for RPS-Bollinger – Sports & Leisure outlined how cyber liability insurance protects businesses from:

- **Liability claims involving the unauthorized release of information** for which the club/business has a legal obligation to keep private or confidential.
- **Liability claims alleging invasion of privacy** and/or copyright/trademark violations in a digital, online or social media environment.
- **Liability claims alleging failures of computer security** that result in deletion/alteration of data, transmission of malicious code, denial of service, etc.

- **Defense costs in state or federal regulatory proceedings** that involve violations in privacy law.
- **The provision of expert resources and monetary reimbursement** to the insured party for the out-of-pocket (first party) expenses associated with the appropriate handling of the types of incidents listed above.

Walker adds that the limits of any policy will vary depending on the number of employees and the club’s gross revenues. The average premium for a \$1 million insurance policy in cyber liability is around \$3,000 (and can be higher for larger clubs). Now is a good time to review your cyber liability policy and make sure you are properly covered.





SECURITY AND SAFETY

# A Club Manager's Guide

By Jim Fisher, PhD

One of the principal attractions of club membership is that it offers protection and insulation from many of the common hazards that potentially threaten people in this uncertain and often troubled world.

Children, spouses and guests are all afforded a special measure of comfort, convenience and premium experience with an important, added aura of safety. They enjoy a level of security not ordinarily provided in the public space. This positive take on club life and its distinctive attractions also underlines the special responsibility of club leaders. They are the stewards and protectors of the club's hard-won reputation for safety and security.

## SO WHAT'S A MANAGER TO DO?

No organization is immune to threat. More than an annoyance or inconvenience, these risks are growing in frequency and intensity—a few may even rise to a level of organizational disruption and in rare cases, a threat to the club's viability.

Managers must counteract these threats through coherent and effective practices, including comprehensive appraisal and appropriate action that must be sustained over time.

This approach to security and safety falls under the category of risk management, which Peter Bernstein, author of *Against the Gods: The Remarkable Story of Risk*, defines as, “maximizing the areas where we have some control over the outcome while minimizing the areas where we have absolutely no control over the outcome and the linkage between effect and cause is hidden from us.”

At its most practical level, this means that keeping risk under control requires the focused attention of the manager.

## FINDING A BALANCED APPROACH: THE 4 Ps OF SECURITY

There are four risk management trends that club managers are following to control and contain threats to club security.

### Maximizing control

**1. Prevention** and education efforts to reduce security threats are broadening and will continue to gain momentum. Human factors continue to be the weakest link in our

chain of security. Clubs must plan and adhere to hiring procedures, background checks and workplace policies that both align and reinforce security aims. As staff awareness of safety challenges expand and as training in best practices deepens, the club's security system will also strengthen. The interview with Joseph Saracino (page 13), a security expert with experience in the club sector, reinforces the notion that breakdowns in security often trace to poor password habits, casual attitudes toward workplace security (including desktop access) and control protocols for club records and work product.

By the same token, club members are full partners in the challenge to bolster security. A similar awareness of the need for strengthening security is now taking place in the home and at work; therefore, members are increasingly ready to shoulder new responsibilities and to acquire a more focused sensibility that supports a safer club environment.

**2. Pervasiveness** regards the widespread adoption of controls and monitoring systems. The Pulse Survey finds that 70 percent of surveyed clubs use a camera system to monitor club areas. However, Saracino observes that the number, location and quality of camera equipment is subject to considerable variance. Confidence in substandard equipment is not warranted and, indeed, several Pulse Survey respondents report that club cameras on their grounds and facilities are scheduled for an upgrade—some to high-definition “prosecutable” cameras.

Best practices also include effective use of lighting, background checks of staff and the provision of first-aid support (e.g., training in CPR and equipment such as defibrillators). In general, it looks like club awareness and club policies are catching up with the perceived need. One large club has successfully installed a new card security system. Most of the 10,000-plus members have photo ID cards that are scanned on entry and can update the club member with individualized messages.

Beacon technology is also making inroads into clubs. This technology allows mobile applications running on smartphones to “listen” for beacon signals in the club to detect member presence, monitor movement and deliver

messages. Many members at the Union League of Philadelphia have a dedicated club app that uses this technology for a range of services including entry and identification, directions, valet parking and intra-club communications. The Granite Club in Toronto is using frictionless, biometric software to bolster its security, especially in restricted areas such as the childcare facilities. See the case study on page 20.

### Minimizing impact

**3. Persistence** and vigilance minimize the impact of risk events. Total risk prevention is no longer feasible, thus rapid response, facilitated by contingency planning in the form of detection and containment, can reduce the impact of security breaches when they do happen. Although the growing trends in readiness calls for frequent tests, simulations and drills, the Pulse Survey suggests that these tactics do not have widespread acceptance and integration into club operating procedures. But, the results suggest clubs may be nearing a tipping point with roughly one out of three clubs reporting that “what-if” scenarios and other procedural walk-throughs are now being utilized.

**4. Protection** is increasingly possible in the form of risk transfer. Insurance, security contracts and cooperative partnerships are increasingly used by organizations. As the range and severity of risks increases to include cyber attacks and other potential business disruptions, new and innovative products and services can reduce or otherwise contain such threats. Many clubs now transfer significant cyber risk to the cloud—servers, records, membership data, email services and software now reside in a more secure and remote environment and one in which usage and abuse can more readily be detected.

Several clubs surveyed also report sensitive financial

## Active Shooter Drills



With active shooter incidents being reported across the country, including private clubs, employees should be trained for rapid response. You can watch a video developed by Homeland Security at: [youtube.com/watch?v=5VcSwejU2D0](https://youtube.com/watch?v=5VcSwejU2D0)

data such as members’ credit card information is no longer collected nor does it reside on POS systems. Third party specialists handle risk related to electronic payments. Clubs are applying similar scrutiny to staff and personnel records. Many clubs report partnerships and cooperative agreements with local police forces. Residential communities frequently have separate entities that manage security and clubs co-located will frequently coordinate and cost share a range of security arrangements, including physical monitoring. These security forces have their own trade association, the Gated Community Security Managers Association, which does training and shares knowledge and best practices.

### REMAIN VIGILANT

*Club Trends’* interview with Saracino points to the importance of club leaders undertaking basic initiatives of education and assessment. But precisely because the security scene is highly dynamic and rapidly evolving, these initial steps must be followed up by the further acquisition of tools, technology, expertise and finally the perspective and managerial judgment to apply them. Like all organizations, club have limited resources, so the best managers will endeavor to apply these ultimately scarce resources precisely where they will deliver the greatest return: the safety and satisfaction of club members. ♦

## Risk Management Trends

Deloitte recently published “The Future of Risk: New game, new rules,” in which they identified key trends shaping this area. Here are several key trends that relate closely to the private club industry. The full report is available at <http://bit.ly/2hBXOkr>.

**Reputation risks accelerate and amplify.** To survive in a hyper-connected world dominated by mobile devices, social media and evolving expectations from society, leaders will proactively address accelerated, amplified risks to their organizations’ reputations.

**Disruption dominates the executive agenda.** The constant threat of disruption resulting from emerging technologies, business model transformations, and ecosystem changes will force executives to make significant strategic choices to drive organizational success.

**Controls become pervasive.** In a sensor-enabled, hyper-connected environment, organizations will deploy pervasive controls as part of their products, services and business models to monitor and manage risk in real time.

**Vigilance and resilience complement prevention as leading practices.** Organizations are realizing that 100 percent risk prevention is not feasible, so investment in vigilance (detecting risk events as they happen) and resilience (containing and reducing the impact of risk events) will increase.

**Risk transfer broadens in scope and application.** Risk transfer instruments, such as insurance, contracts and financial instruments will increasingly be used by organizations to protect them from a wider range of risks—cyberattacks, climate change, geopolitical risks, terrorism, business disruptions and more.



# Managing Risk

## An Interview with Joseph Saracino, Jr.

**C**lub Trends sat down recently with Joseph Saracino, Jr., CEO of Cino Limited Companies, which provides cybersecurity, risk management and education services. The private club industry is an important segment of the broader market that Cino serves.

**Club Trends (CT):** *What trends are you seeing in the cyber security space?*

**Joseph Saracino (JS):** Compliance issues. Many states have agencies focused on compliance. Here in New York, the Department of Financial Services has just enacted privacy and data compliance mandates as of the first of March, which means that all of the banking industry that deals in New York state—all the banking industry, real estate agents, mortgage brokers, financial brokers, insurance companies, agencies and agents—all come under the Department of Financial Services. They now have compliance standards that require them to demonstrate that their data is being protected. There are certain processes that everyone has to perform in order to make sure and then attest to the fact that they are doing the necessary things that come under this compliance regulation. Vulnerability assessment is now part of the compliance. People need to know what level of security they are at and where they stand as an entity.

**CT:** *Does your firm go into clubs and conduct a vulnerability assessment?*

**JS:** Yes, we do this for many clubs. A vulnerability assessment is our first step to let you know where you stand.

As part of the assessment, we have our own hacking teams that are certified ethical hackers (the good guys) that do what's called a live penetration test. They launch an attack on your system, as a hacker would, identify vulnerabilities and then we explain/brief the results.

**CT:** *Most private club websites are password protected. Would your team of hackers see if they could breach that first layer?*

**JS:** Yes. We do that not only externally, but we also conduct an internal penetration test, and internal scanning. In our vulnerability assessment program, we examine the entire environment.

**CT:** *What do you mean "internally"?*

**JS:** Let's say you have a disgruntled worker who wanted to get into the administrative sectors or financial sectors of your organization. There are ways to do that because they often have administrative rights and email access. We test vulnerabilities to determine if there are weaknesses that an internal worker could get to. We want to expose that.

**CT:** *At my university we must change passwords every six months. We also use two-factor authentication. Is that a best practice?*

**JS:** Passwords should be changed more frequently than every six months. We recommend every 90 days. I call this the inconvenience of cybersecurity.



Two-factor authentication is definitely a best practice. We look at a range of best practices from NIST (National Institute of Standards and Technology) (cybersecurity framework) and ISO (International Organization of Standardization), (27001,27002), two leading resources for managing information security. There are a lot of agencies that have set up best practices, and we take a cross section of those so we can keep on top of that experience curve. The landscape on cyber changes every day.

**CT:** *What about physical security?*

**JS:** That's part of our assessment as well. We always look at the environment—the access points. We look at what organizations are doing, including how they shred paper and position cameras.

There are a lot of different elements. For example, you must have good camera equipment. Some people just do it for appearances, what we call security theater. Security theater is essentially saying, "Well, we got them up there, so it looks pretty good, and we've covered that base." But it doesn't really do the job. You have to make sure you're able to capture a clear image because if you can't see it, then what's the sense?

**CT:** *What else do you consider in assessing physical security?*

**JS:** We look at people—obviously the end user—whether it's an employee at a desktop or an employee that's coming in and out of the liquor cabinet. You always have to look at who you're hiring and how you're hiring. Most clubs see the value of background checks and do that on a fairly consistent basis. Drug testing is increasingly part of the rules and regulations related to how you set up club HR policies.

**CT:** *What about facilities and grounds?*

**JS:** Access is important. We will look closely at access roads, whether or not you have a guarded facility or security measures using access control cards. We see biometric systems that identify individuals that should or should not be on the premises. Arming security guards is now on the table.

**CT:** *With so many issues at play, where does a club start or continue to move forward?*

**JS:** The key is to address them on a consistent basis as part of the fabric of club life. Club safety should be addressed or assessed periodically—at the very least once a year. The costs are often more affordable than what clubs expect. Our own CCSA (Cino Cyber Safeguard Advantage) program was created for that purpose. I would rather have someone start somewhere, than never start because they feel it's out of reach because of cost or they didn't know where to start. As a veteran-owned organization we take pride in what we do and protecting of our family of clients including their data is our first priority.

For more information, visit [cinoltd.com](http://cinoltd.com).



Ocean Reef Club

## *Our Safe Haven*

# The Growing Importance of Club Safety

By Frank Vain

***Members want their club to be a safe and secure environment. Are you prepared to provide it?***

**O**n a recent tour of private city and country clubs in Bogota, Colombia, security personnel and procedures were a palpable part of the experience. When entering the wonderful city club, El Nogal, members and guests pass through magnetometers like you find at airports. Every vehicle entering their garage undergoes a thorough search. Most of the club's supplies are received at a remote commissary to eliminate the need for delivery trucks to come on site. This is the aftermath of a terrible bombing the club experienced in 2005, when anti-government rebels attacked it as a symbolism of capitalism and the huge wealth disparity that exists in the country. More than a decade later, security has a noticeable impact on the membership experience and consumes about 5 percent of the club's annual budget.

Fortunately, America is not Colombia, but at the same time, it isn't the country it was in the 1950s. There is greater uncertainty and less cohesion. The historically high-income gap between the haves and have-nots has amplified tensions in the U.S. and globally, which makes places where the affluent gather targets of opportunity. Additionally, members want their club to do more for them, further complicating things. For example, there is a clear preference among younger and prospective members for their club to entertain and even take care of family members. That clearly raises the bar, as it challenges the club with protecting their members' most precious and vulnerable asset, their children.

It can be downright scary to think of all the threats to the

safety and the security of a club's assets and personnel and members and their personal belongings. It could come in the form of a disgruntled employee looking to get even with someone, hackers who want access to privileged information, the petty thief running a smash and grab on a vehicle or the disenfranchised wanting retribution from those who have more. It's a dangerous world, and, let's face it, private clubs are soft targets. They exist to create a drop-in, home-away-from-home environment, not put themselves in a castle behind moats and walls. Creating a sense of security is clearly a part of hospitality—people can't be comfortable and threatened at the same time—but they can also work at odds with one another. Don't you feel both better and on edge when you go through a security line at the airport or at a concert or a ballgame? On the one hand, you're thankful for the protection, but on the other, you are reminded of the bad things that could occur.

## **SAFETY AS AN AMENITY**

In the landmark 2013 NCA-McMahon Group study, "Navigating the Future," 90 percent of respondents, which included club executives, members, board members, consultants and legal experts, agreed with the statement, "Clubs will increasingly appeal to people as a safe and secure environment." Surveys of purchasers in gated real estate communities consistently find safety and security as one of the top three reasons for purchasing a home there. People join clubs in search of other people with similar values and interests, but they are also there because the membership vetting process produces known parties, creating an environment where trust and looking out for others is commonplace.





The trick for club leaders is to make their members and guests secure, but not intimidated. As with many issues affecting clubs, your location and type of club plays a role. Most city clubs adopted stronger security protocols years ago when the urban core began to deteriorate. They have evolved these practices even as their environment has improved with the resurgence of the American city. With mostly vertical structures, they have fewer entrances than a horizontal clubhouse or the campus-style layout of a country club. They also tend to have larger memberships and more traffic through their buildings, so diligence is required.

## THE MODEL FOR CLUB SAFETY

The gated community club has a natural culture of security. To the delight of their security detail, many presidents have visited Ocean Reef Club (ORC) in Key Largo, Fla. Surrounded on three sides by water and accessible by a single, lengthy access road that leads to a gated entry, the club has been described by the United States Secret Service as one of the most secure communities in the country. Entry by land, sea and air is strictly monitored and only members and their guests pass through the gates. Because the club has hosted so many dignitaries, stringent, but not oppressive security has become second nature at ORC.

The secure environment at ORC is treasured by their special guests and regular members too. In the club's annual survey, more than 90 percent of the members indicate they place great value on and have high satisfaction with the club's security program. Through the Ocean Reef Public Safety program, residents and their guests are assured of a seldom-equalled level of security. The tranquil setting, billed as a unique way of life, is greatly enhanced by the peace of mind the security systems create. Each member of the ORC private security force is certified as a paramedic, emergency medical technician (EMT) or firefighter. Several are certified in all three specializations. Most also have law enforcement training. There is a presence of each trained skill on every shift, around the clock.

## HOW CLUBS CAN BETTER PROTECT THEMSELVES

Most private communities don't have the resources of an Ocean Reef, but it serves as a model of ideal procedures. For

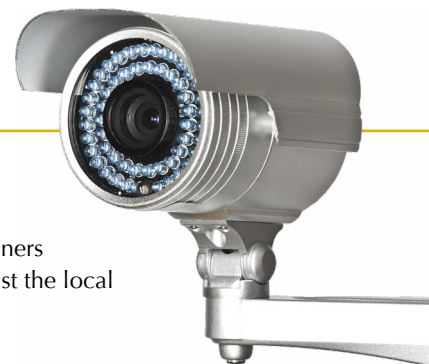
most clubs, security starts with a fully equipped and staffed entrance gatehouse. This is important to seniors looking for retirement options and one of the top reasons they choose to move to a gated community. The responsibility and cost for security measures is typically shared with the homeowners association, easing the burden for everyone. Of course, many clubs and communities employ security staff to protect their members, but cameras aimed at the key access points and high-profile spaces, like the golf shop, locker rooms and parking lot increasingly augment this.

Conversations with club leaders indicate the freestanding country club is the category with the most difficult security challenge. Often spread across 125 to 150 acres, some parts of which may be bounded by walls or vegetation while others are wide open. They have multiple buildings and activity centers and much of it was planned in a lower threat environment. There are often multiple doorways into the clubhouse, and with tighter payrolls, it is increasingly common to see unmanned reception desks.

Security gates, once a fixture only at gated community clubs, are becoming increasingly common at freestanding clubs. As with many aspects of security, impressions matter, so an un-manned gatehouse can reduce intrusions and crime without the personnel costs. Even fully automated gates activated with code entry can help prevent unauthorized traffic through the grounds. Cameras and other forms of electronic surveillance are increasingly available and they should be mounted at all key access points. Manned entrances with receptionists are well worth the expense and new tools like RFID chips, near field communication devices and beacon technology make it much easier to keep tabs on who is entering the grounds and monitor where they are in the club.

Another key aspect of creating a safe club is to get the employee element correct by building a strong human resources department that runs background checks on all hires and structures training exercises and emergency preparedness drills. Finally, the financial arm must protect your data through the latest cyber security technology, and for that ever-possible breach, cyber insurance.

No matter what the setting, every club needs a plan to create a secure and safe environment. Threats come in all shapes and sizes, and clubs that have been through an event cite how valuable their planning proved at the time of crisis. Properly structured and communicated, a solid plan can be priceless in times of need and an asset in your membership and marketing plan. ♦



## Safety Idea

An Automatic License Plate Reading (ALPR) Camera Contribution Campaign brought together homeowners associations and the Round Hill Country Club in Alamo, Calif., to fund cameras to deter crime and assist the local sheriff with apprehension of criminals.



# Peace of Mind at Desert Highlands

By Bridget Gorman Wendling

Photos courtesy of Desert Highlands

**D**esert Highlands in Scottsdale, Ariz., established in 1983, was the first private residential community built around the nucleus of a country club. The gated community has become the prototype for subsequent developments and has set a standard for excellence in many facets of such communities' operations. Providing a sense of security, privacy and comfort to its members and staff is integral to the Desert Highlands lifestyle and experience.



Spread out amongst 850 acres of lush Sonoran Desert at the foot of Pinnacle Peak, homes at Desert Highlands are designed to harmonize with the natural landscape. This peaceful enclave has world-class amenities including an 18-hole Jack Nicklaus Signature Championship golf course, an 18-hole putting course designed by Gary Panks, an award-winning Racquet Club with 13 courts, a 7,000-square-foot Wellness Center and more than 500 distinctive residences.

We spoke with Terra Waldron, CCM, CCE, ECM, the Vice President/COO of Desert Highlands Association and the Association's Director of Security, Nick Ciliento, CPP, about how they approach the issues of safety and security for both members and staff in their unique community.

The Desert Highlands Security Department is an in-house operation that consists of 15 highly-trained officers who operate 24 hours per day, seven days a week. Although they

are unarmed, some of the officers have law enforcement backgrounds. Once hired, members of the team must maintain CPR/AED/First-Aid certification. The team participates in other ongoing safety and security training, such as Active Shooter response

## PHYSICAL SECURITY

Nine miles of walls surround the entire property, with a main gate that is manned by a security team member at all times. All visitors entering the property receive screening and must be authorized by a homeowner or staff member to proceed. A secondary gate (West Gate) is only manned if necessary; however, Desert Highlands' access control software enables the security department to remotely verify all visitors and vendors who are attempting to enter the property. Homeowners receive individual gate passes that are mounted on their windshields, which activate the gates for automatic entry and exit. Additionally, management must approve any individual wishing to visit with a staff member to gain access, which minimizes social visits and serves to protect the employees from unwanted visitors.

## CAMERAS

The club utilizes an extensive surveillance system to monitor activity. They installed 39 cameras around the property including the entry and exit points at the two gates. There are



infrared sensors and cameras installed along the perimeter of the property that alert the security team if action is required. The footage is retained about two months, and records over itself when its data limit fills. The team has shared footage with the police department on a number of occasions.

## KEY CONTROL

Most of the homeowners leave a set of their keys with the security department so that the team can access the property in their absence if necessary. Many service vendors work on homes when the owners are not there, but they must sign the keys out and sign them in again upon returning them. If there were to be an emergency when a vendor is in a home, the security team has a separate set of keys to gain entry.

## HOME ALARM SYSTEMS

Desert Highlands has an agreement with ADT to provide home security systems in the community, and more than 300 of the residences in Desert Highlands use ADT. The security department shares access to a software program that mirrors alarm signals emitted from community houses and allows the on-site security team to quickly respond as well.

## COMMUNICATIONS PROTOCOL

When an emergency or crisis occurs, effective communication helps to minimize damage, communicate facts and risks, update members and staff, and move toward a resolution. The Desert Highlands Security Department and management have an emergency communications plan in place, which includes an emergency paging system for homeowners and protocol for staff to send alerts either via text message or voicemail.

Desert Highlands management maintains a close relationship with local law enforcement and first responders. The security team is able to contact the chiefs of these organizations on their cell phones as opposed to going through published office numbers. As a private property, Desert Highlands security staff does its own patrols, and the police department only comes on property when summoned.

## CYBER AND DATA SECURITY

In addition to physical security considerations, Desert Highlands is vigilant in protecting the security of its data and information systems. In an effort to prevent the possibility of a data breach—under the purview of the communications



manager and the CFO—Desert Highlands has taken very aggressive, multi-tiered measures to protect their data.

A SonicWall firewall provides real-time cyber defense to prevent the infiltration of ransomware or encrypted threats that could compromise data. Desert Highlands maintains complete control of ports open to the outside world while ensuring that data is accessible remotely, such as through the SSL VPN.

Another layer of protection is the use of Gateway antivirus software, which checks for viruses at the application layer using a web-based scanning service to ensure that intrusions are prevented and content is secure.

Although access to Wi-Fi seems ubiquitous these days, and offering complimentary Wi-Fi is standard in the hospitality industry, it does introduce security risks that need to be addressed. Desert Highlands has adopted formal Wi-Fi segregation and access policies.

Yet another layer focuses on malicious email, virus attacks and spam threats. Using Barracuda Spam Firewall protects sensitive information from being destroyed or lost through an attack via the email server as well as against threats that can slow the network and hinder employee productivity. The firewall also checks for internally tainted email to prevent the spread of viruses that don't access the email gateway.

Also, Symantec Endpoint Protection antivirus software is installed on all desktops, workstations and servers. This product prevents unapproved programs from running, and applies firewall policies that block or allow network traffic. The software has a centralized administrative console that allows management to modify security policies, monitor activity, receive alerts and update the products.

Desert Highlands also uses best practices in network access control, which include enforced protocol and policies on user names and passwords, user group folder access and internet access policies.

Waldron is proud of the Desert Highlands team and its reputation, noting that several people have moved into the neighborhood because of the security department's stellar reputation and the peace of mind it provides. She comments, "The department is unique in that, in addition to being trained in protection, it is also very much like a concierge service." ♦





# Physical Security at the Club

## CANOE BROOK COUNTRY CLUB

By Bridget Gorman Wendling

Photos courtesy Canoe Brook Country Club

Canoe Brook Country Club, located 20 minutes from New York City in Union County, N.J., was founded in 1901 and has a rich history as a family-oriented club with two championship golf courses and an array of sporting facilities and activities. Catering to an active membership of approximately 3,000 men, women and children, the club's 250-acre campus is bustling year-round with social gatherings and sporting events for members of all ages.



Part of Canoe Brook's property is adjacent to The Mall at Short Hills, a large upscale shopping complex. Because of its proximity to the mall and a major thoroughfare, the club has experienced isolated security incidents over the years—auto theft, locker room theft, trespassing and a car jacking at the mall—that prompted the club to examine its safety and security measures. Historically, the club's approach to security emphasized discretion. That philosophy has changed, and the security team now has unique uniforms, identifiable marked vehicles and a visible presence at the club and throughout the grounds. The membership seamlessly embraced this shift in thinking and enjoys a friendly rapport with the security staff.

### THE SECURITY TEAM

The club's 12 to 14 person security team is comprised of active or retired law enforcement officers, corrections personnel and fire fighters (eight or nine off-season) who report to Richard Bickel, director of security and a standing member of the club's Security and Safety Committee. Because the club added guest rooms that enable members to be on the grounds overnight, the security team is now a 24/7 presence.

General Manager Albert Costantini, CCM, CCE, notes that melding security and hospitality and providing a safe environment in a friendly, low-key yet thorough manner helps provide

peace of mind for Canoe Brook's members. Although the security team is unarmed, having law enforcement, corrections or fire fighting training and practical experience under their belts enables them to assess risks, implement safety and security measures and provide protection and assistance for the well-being of both members and staff.

Bickel and Costantini outlined some of the measures the club takes to ensure the safety and security of its members, guests and employees:

**Entrance and Exit.** Bickel says that the 250-acre campus is fenced in and there is one entry point and one exit with a parking gate, but the club looks forward to building a gatehouse in the future where staff can greet members and monitor access. The staff routinely monitors vehicles as they enter and depart and they use a color-coded decal system on vehicles. Additionally, the staff is required to have photo ID badges.

**Surveillance System.** Canoe Brook Country Club uses a closed-circuit TV system that monitors all points of entry and exit. There are cameras installed in several areas in and around the clubhouse and surrounding buildings that are monitored in the security office. There is a fine line between ensuring members feel safe and having them feel like their privacy is being invaded, so it is important to avoid the perception that members' and guests' behavior is being monitored. Cameras are used to protect the staff, members and guests. If, for example, there is suspicion that an employee or member is pilfering inventory, the recorded surveillance footage can be very useful in assisting the management in identifying who is responsible or, better yet, in exonerating innocent parties.

**Training and Checks and Balances.** Because of the policy to hire only security personnel with experience in law enforcement or the military, the staff is well-equipped to respond to any conceivable safety and security incident at Canoe Brook. Over the years, the team has handled a variety of issues



(Left to right) Albert Costantini, GM/COO, Richard Bickel, Director of Security, Michael McNany, Security Supervisor and Tom Balke, Security Officer

including administering CPR, responding to medical emergencies, dealing with a bear on the golf course, reporting and resolving traffic incidents, handling vandalism and investigating and preventing theft.

The team maintains appropriate certifications and regularly attends pertinent professional development training. Richard Bickel and his staff developed a comprehensive Emergency Response Plan that has been formally adopted by the club as protocol for dealing with various safety and security concerns. Bickel completed an Active Shooter Response training program, which he is integrating into the response plan and will introduce to the team this summer.

Costantini affirms their proactive approach, stating, “As managers of an operation this large in scale, the best preparation method one can apply to remain safe is scenario-based training, not only for the security team but for all club staff. Taking a class is one thing, reacting to situations in a calm and professional manner is altogether different.”

To ensure that the security team doesn’t inadvertently neglect

**Canoe Brook Country Club has the utmost respect for law enforcement and first responders.** As a community outreach endeavor and a way to thank these members of the community, Costantini began hosting a complimentary “Battle of the Badges” golf outing between the two police departments that service the property. He looks forward to incorporating all emergency response departments from the towns in the next couple of years. Costantini reflects, “Although we truly intended the event to solely be a way to thank our emergency response community, we also have developed a better rapport with these departments. This type of outreach is crucial in developing better relationships between the club and the community.”

a part of the property, the club installed an electronic guard system that monitors the security staff’s adherence to a scheduled property tour. This electronic key box system confirms the time of the security team’s presence in each area of the property and is monitored by the director. Having checks and balances in place provides an extra layer of protection and confirms that the security team is moving about the property.

**Contact/Communications Systems.** Costantini and Bickel emphasize that the relationship the club fosters with the local police forces (they are covered by two police departments) and first-responders has been enriching and positive. They’ve instituted a direct contact system with one of the local police departments; the adjacent mall experiences regular shoplifting incidents and the perpetrators often flee the area by coming on to club property. The police department directly contacts the Canoe Brook Security Team to alert them of potential danger and get their assistance in apprehending the suspect. In addition to fostering a spirit of cooperation, it helps to avoid or minimize potential threats to Canoe Brook’s members and guests on the course.

The club is working with a consultant to develop an app that they will use to alert members and employees of emergency situations, security issues or special updates. The app will have the ability to send push notifications for all types of issues, like course rain/frost delays or pool weather-related issues. It will also allow the club to send emergency notifications in the event of any type of security issue to inform members who are either on property or planning to come to the club. Until then, members are apprised as necessary of security initiatives via e-mail blasts, website postings and newsletter articles and are very supportive of the department and the club’s efforts to ensure that everyone enjoys a safe environment. A documented “use of force policy” is in effect and communicating policy, procedure and protocol ensures that members empower the team to employ the necessary means to fulfill their duties. ♦



## MEMBERS ONLY!

# Case Studies on Security and Control

*By Jim Fisher, Ph.D.*

One persistent challenge that managers face in operating a club is to make sure that club's facilities are not subject to unauthorized access. There are many variations on this problem:

- A non-member resident in proximity to a country club golf course may ease onto the back nine and play a few holes without authorization.
- At peak hours in a bustling city athletic club, non-members might swim a few laps and use the gym with no one noticing.
- For yacht clubs in particular, access from the sea is yet another route to enter into places non-members are not permitted.
- Some bona fide members may utilize services and facilities that their membership status does not entitle them to.

Thus far clubs have struggled to find solutions that are not either prohibitively expensive in the implementation or heavy-handed in their execution. Also, club managers and their staffs typically pride themselves in knowing and recognizing members. Personalized service takes as its very premise that a member is made to feel welcome and accommodated with service that is frequently customized to fit his or her individualized tastes and requirements.

In the face of these high expectations, staff may understandably be uncertain as to the best course to take when an unrecognized individual is encountered. Maybe someone who has recently joined? A guest? Perhaps someone whose use is infrequent or focused on other parts of the club? Other staff members may just suffer from that occupational hazard shared with preachers and teachers: everybody looks familiar. Safety and security is a top priority, but so too is the wish not to offend.

Many clubs have looked to technological innovation for a solution. These have taken various forms: access cards, entry fobs, codes keyed into locking systems, even touchpads that recognize a fingerprint (now common on smartphones). These show promise, but are not without drawbacks or limitations.

Keys or codes can be separated from the authorized user. Systems that integrated with club personnel, such as database look-up or identity confirmation are sometimes slow or compete for attention that might otherwise be focused on members.

One technology that shows promise uses facial recognition as part of a larger access control system. We offer two case



The Granite Club



studies of clubs that have recently implemented these comprehensive identity management systems: The Bel-Air Bay Club in Pacific Palisades, Calif., and The Granite Club in Toronto.

Both clubs have opted for biometric security provider, FST Biometrics' in Motion Identification (IMID) technology. Their experience has thus far demonstrated that a number of different benefits can accrue to clubs through the system's application.

## BEL-AIR BAY CLUB

This club draws its membership from some of the most affluent



areas in southern California: Pacific Palisades, Brentwood, Santa Monica and Malibu. The facilities are a perfect match for the sun-drenched, laid-back west coast lifestyles and include a one-quarter mile stretch of Pacific Ocean beachfront.

The club has two clubhouse facilities that are bisected by the Pacific Coast Highway: the Upper Club and then the beachfront's Lower Club, which both has seen a significant influx of activity since its 2007 renovation.

With 850 memberships and more than two thousand people who will potentially enjoy the Lower Club at some time in the extended peak summer season, the club wants to welcome members in both a warm and efficient way, while also keeping any star-gazers or beach interlopers outside the club environs.

Two unobtrusive cameras make for a fast, frictionless member positive identification as the members enter the Lower Club en route for dinner, the bocce courts (15 feet from the edge of the ocean) or one of 104 much sought after cabanas. As the ID is done rapidly and automatically, the staff is free to have more personal and tailored interactions with the club members.

The system has been effectively integrated with the club's membership management system (Jonas Club) and thus also provides the management with information that is useful for purposes both strategic, like leadership development, and

operational, like cabana utilization. The much sought-after cabanas are offered on a use-it-or-lose-it basis. The IMID system verifies that cabanas are indeed inhabited in the peak season on a regular basis.

COO Bill Howard gives the system an enthusiastic thumbs up: "We feel confident in the system, which has proven to be fast, accurate and seamless. Most importantly [it] helps us improve the level of service we provide to our membership, allowing us to truly get to know each and every member by face and name."

## THE GRANITE CLUB

This club is among the premier family, social, recreational and athletic clubs in North America. It is also a big club, which is the nexus of activity for approximately 11,000 members.



With its scale and great variety of offerings, The Granite Club tailors its offerings accordingly. This is the foundation for a user pay system with members electing to use some facilities, activities and services, but not others.

In the past, the club has not strictly monitored usage, instead relying largely upon member compliance using an honor system. But in 2014, with the addition of a new wing and with it a bevy of athletic, fitness and gym facilities and services, more rigorous access control and utilization monitoring system was desired.

The system manages member entry into the two large gym areas in the new wing. Also among the applications that The Granite Club now especially values is the secure and controlled access to its childcare area.

Mary Sullivan, the club's COO, anticipates that the club will continue to expand its access system to eventually cover access to most areas of the club as well as entrance to the overall club facility itself. She sees the club reaching that "next level" whereby a warm and welcoming environment is further enhanced by assurances of safety and security to all members and staff. ♦

## Implementing Facial Recognition Technology

Installation of this technology—FST was the vendor at both The Granite Club and The Bel-Air Bay Club—involves the positioning of cameras (typically two) and then the integration with the various access points. At The Granite Club, this included doors to restricted areas (like the childcare center) or entry gates into more highly trafficked areas like the athletic facilities (see photo on page 20). In the case of Bel-Air Bay Club, installation at the Lower Club required a two-day retrofit and integration with the front desk, which is attended by staff. At The Granite Club the system was put in place when a new wing was added to the larger club facility.

The system requires photographs of all adult club members and their qualifying family members (although children are not included in the registration process). Though the photographing and enrolling takes less than a minute, there remains the logistics and publicity required to build awareness and participation. Both clubs developed communication plans to inform members of the procedures and opportunities for enrollment. Bel-Air Bay Club pushed for enrollment over a one-month period, while The Granite Club, a larger operation, extended its enrollment over several months. Both clubs had overwhelming participation and satisfaction. The facial recognition system integrates with the club membership databases, but the photographs often represent both an update and enhancement.



## **National Club Association**

1201 15th Street NW, Suite 450

Washington, DC 20005

Phone: 202-822-9822 or 800-625-6221

Fax: 202-822-9808

Website: [nationalclub.org](http://nationalclub.org)