SECURITY LETTER™

A private monthly Letter – plus supplements and data services – on issues of corporate planning and protection

166 East 96th Street, New York, NY 10128 – 212-348-1553 –

December, 2014
New York, NY, Vol. XLIV, No. 12
Part I, Index Included

HOLLYWOOD HACKERS PUT ALL EMAIL USERS AT RISK. How it would be if your CEO and CFO's private email were hacked and shared with the entire world? This hypothetical occurrence takes place despite the fact that the workplace has a high level of cybersecurity. Choosing judiciously those emails could result in a corporate crisis. Result: disaster.

The embarrassment at Sony Entertainment has gone global. Email messages between producer Scott Rudin and Sony co-chair Amy Pascal have bruised the egos of A-listers. The exchange between the two related to the temperament and capacity of performers, their compensation, as well as trite comments about Pres. Obama.

The significance of the breaches goes far beyond the fluff of the entertainment industry. The Sony email breach is a major event that must raise concerns for every workplace. Why? Because Sony had cyber safeguards in place. They weren't good enough. Further, the hackers remain unknown, but clues suggest that the intruders were from North Korea, perhaps wanting to threaten a Japanese firm.

Also in this Letter....

Email is discoverable? Years ago we offered the analogy that cellphone calls were like messages over a radio station. If people knew how to tune in, they could listen without discovery. In a way emails are even more vulnerable: They are stored, perhaps forever somewhere. Hackers who can never be traced or arrested can use the info to their own advantage if they know how to break the security.

Clearly, that has been done. If the North Koreans presumably have these skills, hackers elsewhere will be able to do the same. Perhaps they have already. Security practitioners have an urgent task: Warn employees that cellphone and email communications **must not be used** for sensitive materials. Other options are available—the use of proprietary codes and better encryption, for example.

WHAT'S GONE WRONG WITH POLICING? KNOWING FOUR LEVELS OF SECURITY. In recent days three black unarmed males have been killed by police officers, mostly white. It seems like a racial thing. Yet, public affairs writer Heather Macdonald has observed that far more black inner city residents have had their lives saved by white cops than have lost them.

The security spectrum has four parts. English jurist Boris (Leo) Brasol wrote: "Naturally, safeguarding society against criminality is the foremost duty of the state." We'd suggest removing two words: "Naturally, safeguarding society is the foremost duty of the state." The first level of protection comes from the military—to protect against threats from abroad. The next is law enforcement—protecting against criminality and maintaining general order. Then comes private security—to protect people and property. Finally, individual initiatives provide one's own security at home, work, and in the community.

The problem with some police depts. is that chiefs and officers are thinking, acting, and being outfitted like soldiers. This is inappropriate. It leads to regarding citizens like adversaries.

CAREERS: TORTURE PRACTICES HURT JOB PROSPECTS FOR CIA RETIREES. Security is a favorite second career for many mid- and high-level federal protection personnel. Ex-FBI special agents,

Editorial staff: Robert D. McCrie, PhD, CPP. Contact: rmccrie@verizon.net Luis A. Javier. Circulation manager: Fulvia Madia

Secret Service personnel, and execs. from various DHS units occupy some of the most important positions in protection mgmt. NSA personnel have done well as entrepreneurs and CTOs with their advanced cyber-security know-how. Some feel that nothing is more agreeable than earning a double pension.

Senior security personnel also include those fascinating ex-spies from the CIA. In candor, your editor has acted favorably toward The Agency. As a dept. chair at a university, I supported began an agent-in-residence program that brought serving CIA agents to the campus to teach courses. The program was a great magnet. Some students were later recruited by the Agency.

However, current CIA retirees face a public perception mess in seeking employment in the private sector. The Report of the Senate Select Committee on Intelligence is devastating for CIA agents over the past 13 yrs. The Agency has gone amok in appalling, cruel physical attacks on detainees. Then they tried to cover it up from the exec. branch and the Congress.

Understanding how the Agency operates. The CIA has two major divisions. One is intelligence gathering and analysis. This is the unit where retirees often have a second career in the private sector. Retirees can make a true contribution in protecting intellectual property. Now some will be blocked from opportunities by their colleagues' actions in the other unit. Clandestine operations conduct a wide variety of activities on its own or through contractors. These activities fight terror, intl. drug trafficking, and global political risks. Retirees from this unit take life easier or work for contract security groups.

Former CIA dirs. George Tenet and Michael Hayden refused to provide documents to Congress and lied to Congress during testimony. Otherwise, the Agency is depicted as cruel and clueless. Despite the unquestionable torture, no significant intel came as a result. It was pure sadism.

The culture of the CIA has veered out of control. They turned to two unproven psychologists who directed the torture, created their own reports of its effectiveness, and then charged $81M for services to their tiny enterprise. The CIA at the highest level approved this behavior in early post-9/11 years.

TECHNOLOGY I: INNOVATIVE BIOMETRIC SYSTEM OFFERS HIGH AUTHENTICITY. Security practitioners know—with deep regret—that past procedures for identification won't make it in the years ahead. The three-factor mantra is that authentication is established by something one knows (password), something one has (card or token), and something of one's self (a biometric feature). Sounds good, doesn't it? But it is not good enough going forward. Multiple biometrics could work for now.

A new system gaining attention is Biometric (dynamic) Signature ID. The user authentication solution is beguilingly simple. Like all systems, the authorized user has to be registered first. That requires someone to write four letters, numbers, or symbols of one's own choosing into a format. That's all. Than repeat the four characters to gain access. Independent research showed that 98% of enrollees in BioSig-ID found the system easy to use. This gives new secure flexibility for BYOD use.

Try it yourself. BioSig-ID was created by Biometric Signature ID, Louisville, TX. You won't see it at any security conference or read an ad in an industry publication so far. But BioSig-ID claims to have over 3M users in over 70 countries. CEO Jeff Maynard says federal funds have helped establish its use to deter online identity fraud, among other apps. Here's one example:

> Colleges and the federal govt. can be defrauded by a simple ruse. A student receiving a Pell Grant may be offered, say, $5K. The college may keep $1K and the student keeps $4K for expenses—if the student remains enrolled. But if students are not verified, they can pocket the money and disappear. Improper Pell Grants are a nine-digit direct loss. BioSig-ID verification and attendance reporting can monitor student enrollment making fraud less likely.

BioSig-ID can be scalable from a small organization to an application involving many thousands of users—all with the same high level of confidence. The system can be tried easily and free of charge. Perhaps a lucky reader will spoof the system and win a prize. (Not likely.) Instead of four letters or numbers, only three are needed. Try your luck at www.biosig-id.com and let us know the outcome.

TECHNOLOGY II: WILL SECURITY OFFICERS USE WEARABLE VIDEO CAMERAS? The NYPD is in the process of providing body cameras to patrol officers as a way to create a sense of transparency and accountability. It's not just a local issue. About $75M in federal funds is being sought to provide 50K body cameras to police nationwide. If the funds are provided, less than 7% of the nation's sworn police officers will have the technology available. But that's a good start.

If the police are supplied with such cameras, will the private sector be far behind? Body cameras are likely to have a limited role in security, like it or not. The use of image collection on police vehicles has been valuable in resolving issues that could have been lingering disputes. But wearing something on one's chest or shoulder is a different situation. The person wearing the camera might just move slightly and the image is lost. Training will make the cameras useful for police, prosecutors, and security.

The concept has problems. Just because the individual has live video to record an event does not mean that the info is conclusive. NYC has been in the thrall of the Eric Garner case. Garner died from a chokehold placed by an arresting police officer. Allegedly, the arrestee called out 11 times before he died, determined partially to be related to asphyxiation. The action was not caught by a body camera, but a nearby pedestrian's cell phone. Still, the grand jury voted not to indict the police officer in the incident.

Improving performance. The real payoff from wearable cameras is on police performance. They are more careful in dealings with the public. In Rialto, CA (pop. 100K), the PD had 24 complaints against officers in 2011, including for excessive use of force. The next year a partial rollout of cameras began and complaints dropped to 3; then 4 last year. Police behavior arguably improved. Equally arguable is the fact that the public might have behaved better as well. According to the Police Executives Research Fdtn. potential benefits of body-worn cameras offer "largely out-weight the potential drawbacks."

The private sector faces different issues and will not need wearable cameras as much as police. Yet, some situations will call for them. We expect security programs to start using such technology soon.

One source: VIEVU which offers two models: VIEVU^2 which streams video RT to a smartphone. Cost: $350. And LE3 used by police which provides cloud storage of images. Cost: $900 or $25 per month www.vievu.com Also, Taser Intl.'s Axon Flex body cameras capture images in a buffer for 30 sec. without recording them until it's switched on. Cost: $600. www.taser.com

CAMPUS SECURITY: ENFORCEMENT MUST CHANGE TO CUT DRINK INCIDENTS. Colleges have been in the news a lot recently—and not always for good reasons. An article by the magazine *Rolling Stone*, described a brutal gang rape of a freshman woman in 2012 at the elite Univ. of VA. The facts were not right. The locale where the fraternity party occurred had no such social event on the day of the alleged incident. Other facts in the article were false. A partial retraction has occurred.

Yet other incidents involving campus security have received attention at the same time. According to Beth McMurtrie in the *Chronicle of Higher Education*, more than 1,800 students die each year of alcohol-related causes. More than 600K are injured while drunk. And almost 100K students become victims of alcohol-influenced sexual assaults. That's why the UVA article was quickly perceived as credible, though the facts were incorrect as published and the article should have been killed.

The college years are supposed to be for studying and self-growth, not getting drunk or stoned every weekend. Kevin Carrey, New American Ftdn., writes: "If students have time to get drunk, colleges aren't doing their job." With popular movies from *Animal House* (1978) to the more recent *Neighbors* and *21 Jump Street*, Carrie writes: "Our culture provides a detailed instruction manual for undergraduate alcohol abuse, and students comply with something close to obligation."

How about getting tougher? Colleges do enforce alcohol policies at intercollegiate sporting events (57%), at dorm parties (44%), and at fraternity events (32%), according to a study. Over 20 yrs. the percentage of students who say they binge drink has slightly dropped from 43.8% to 40.2% in 2013.

Campus security and safety officials have to enforce existing policies better. The problem also is a wider one. Bars near campuses offer cheap drinks and attractions to lure students despite the risk of violating dram laws. Monitoring is needed to avoid abuses. Solutions also have to be state-wide. Maryland banned extreme-strength alcohol sales this year. See our annual survey on campus safety: Part II.

RETAILING: SHOPLIFTERS & DISHONEST WORKERS GROWING AS CONCERNS. For 26 years Jack L. Hayes Intl. has conducted a survey of retail workplaces on losses. This year's report shows a moderately worsening condition. The database comes from 23 large retailers with $660B sales last year. Apprehensions grew: almost 1.2M dishonest shoppers and workers, up 2.8% from the previous year.

The goods recovered grew almost 4.5% to $144M. An additional $100M was recovered where no apprehension was made. In 2013, the shoplifter was apprehended with an average of $130.89. As always, dishonest employees are in a much higher category: average case value: $706.21. Retail theft "is stealing retailers' profits," says Mark R. Doyle of Hayes. See www.hayesinternational.com

PRE-EMPLOYMENT SCREENING: WHAT IF THE APPLICANT HAS A RECORD? Eddie Sorrells, COO, DSI Security Services, Dothan, AL, makes the case for checking applicants' criminal backgrounds. About one-in-three adults has had an arrest. Many of these are for minor incidents which do not lead to convictions. What's an employer to do? Quoted in the *Wall St. J.* (Dec. 13-14), Sorrells says the process of reviewing applications takes hundreds of hours.

Public policy is to ignore arrest records in employment consideration. This policy is enforced by the EEOC. The federal ban-the-box prohibits asking about a criminal record through a check-off. Advice: Consider the whole candidate and determine his/her applicability. Then at the end of the process check to ascertain if a relevant police record exists. Sorrells says applicants with felony records deserve employment somewhere, but not in the security industry. We agree.

ISAIAH BERLIN'S "MESSAGE TO THE 21ST CENTURY." Isaiah Berlin was regarded as one of the greatest intellectuals of the 20th century. Twenty years ago he received an honorary degree from the Univ. of Toronto. His message for the future: "Security, and indeed freedoms, cannot be preserved if freedom to subvert them is permitted. Indeed, not everyone seeks security or peace, otherwise some would not have sought glory in battle or in dangerous sports."

BOOK: *CONFLICT MANAGEMENT FOR SECURITY PROFESSIONALS*. When private security personnel engage with the public in enforcement activities, the situation is adversarial. If security officers can turn a dicey situation into a partnership, the community is likely to be willing to follow directions. That's the theme in this book by Andrew A. Tufano, a security trainer and consultant.

Yet "verbal-only" conflict resolution is ineffective when behavior becomes assaultive or a physical threat occurs because "that person's behavior can no longer be managed; it has to be stopped." Such situations are uncommon and, if they do occur, police should be called, the author advises. Workplaces should create a safety pr program highlighting what security personnel do. Conflict resolution strategies can be learned. Failure to do so can lead to dire results.

The author might have provided a more detailed discussion on conflict resolution training. Still, ample info is given drawn from the author's experience. One industry myth: "Law enforcement training or experience *naturally* prepares individuals for private security employment." Pub. by: Butterworth-Heinemann, www.elsevier.com 150 pp.; $29.96.

INDUSTRY BRIEF. G4S divests its extensive govt. services unit, G4S Government Solutions. The biz served some of the nation's largest contracts such as the Kennedy Space Ctr. It recently was awarded a contract to provide security at Guantanamo Bay Naval Base in Cuba.

But more than a dozen federal contracts required a level of costly bureaucracy for a parent, G4S, domiciled in the UK. The acquisition was made by Alvarez & Marsal, Greenwich, CT, known as workout specialists, for $135M including debt. The new name: Centerra Group, Palm Beach Gardens, FL.

SEASON'S GREETINGS

Robert McCrie
Editor