Editor's Comments

Welcome to volume 6 of the Journal of Physical Security. This issue has papers about Fukushima implications, lock bumping, tamper-indicating seals, election security, stresses on windows for explosions vs. projectiles, and private security in Serbia and in Nigeria.

As usual, the views expressed by the editor and authors are their own and should not necessarily be ascribed to their home institutions, Argonne National Laboratory, or the United States Department of Energy.

*****

An intriguing article by Charles Kenny in *Bloomberg Businessweek*, entitled "Airport Security is Killing Us" makes several interesting points. Of the 150,000 murders in the U.S between 9/11 and the end of 2010, Islamic terrorists were responsible for fewer than 36. Outside of Iraq and Afghanistan, the total number of deaths due to Islamic terrorism was 200-400 worldwide in the same time period, about the same number that die *each year* in bathtubs in the U.S.

U.S. Government spending on homeland security between 2002-2011 was about $580 billion (not counting wars in Iraq and Afghanistan) vs. an estimated $123 billion economic impact of the attacks on 9/11.

While not a single terrorist has been caught trying to board an aircraft in the U.S. by airport screeners, hundreds of Americans have died since 9/11 because they drove in motor vehicles (much more dangerous than flying) to avoid onerous personal and baggage screening at airports.

For more information see http://www.businessweek.com/articles/2012-11-18/how-airport-security-is-killing-us.

*****

The controversy early this year on whether to block the publication of research on how to mutate H5N1 bird flu viruses into more pathogenic forms was certainly an interesting issue in physical security. For more information, see http://www.bbc.co.uk/news/health-17914706

*****

Want to spoof DNA biometrics? Check out the 1997 science fiction movie *Gattaca*. Or for $599 you can replicate DNA on a Mac, Windows, or Linux platform in a few hours. The OpenPCR or "Personal PCR Machine" (http://openpcr.org) automatically runs through the various heating and cooling cycles that are part of the Polymerase Chain Reaction (PCR) process routinely used by biologists and forensics experts to turn a very small DNA sample into a (relatively) large sample of identical DNA. *Wired* magazine gave the device mixed reviews (January 2012 issue, page 48).

A biometric that almost anybody can easily replicate is not much of a biometric! Unfortunately, we're somewhat in the same situation with most (all?) other biometrics.

*****

Sociologist and political scientist James Q. Wilson (1931-2012) died earlier this year. Wilson helped to advance our understanding in a number of areas of interest to physical security. His 1975 book, *Thinking About Crime*, put forth the theory that criminals might not be deterred by longer sentences, but that putting them behind bars could ultimately reduce crime simply by getting them off the streets.

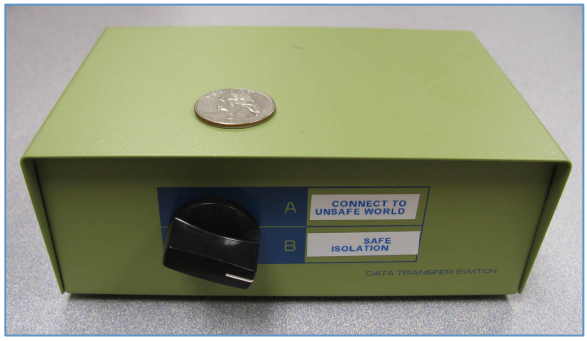
Wilson, along with George L. Kelling, devised the "broken window theory" that became the foundation for CPTED—Crime Prevention Through Environmental Design. The original concept appeared in their article, "Broken Windows" in the March 1982 edition of *The Atlantic Monthly*.

Then in 1989, Wilson wrote the classic tome *Bureaucracy*, a topic many physical security professionals are intimately familiar with. *Bureaucracy* was a kind of anthropological—and ultimately pessimistic/depressing—study of bureaucrats and bureaucracies.

Wilson's critics claimed he underestimated in his work the importance of civil liberties and civil rights. There is no doubt, however, that he was an original thinker who changed the mental landscape of how people view government, society, and security.

*****

Want to double your computer security for under $12? Get a RJ45 AB switch box. This makes it easy to disconnect from the Internet when you don't need to be connected, and instantly re-connect when you do. No fumbling with cables or software to disconnect/reconnect the Ethernet port. (Of course this doesn't address wifi or Bluetooth connections, nor help all that much if you are being personally targeted by hackers, but it can potentially cut down on opportunities for mischief.)



Front

Back

*****

Security professionals often must make difficult hiring decisions. Unfortunately, choosing good employees is still very much an art, rather than a science.

I was reminded of this by looking at the (surprisingly weak) correlation between an individual's success in professional football and how high he was chosen in the NFL draft. Now there are always injuries and unexpected situations that can limit a football player's career, but one would think that given all the quantifiable data on a football player (speed, strength, jumping ability, college career stats, etc.), plus all the intensive attention given to draft candidates that it would be fairly easy to predict who will succeed. But according to the Sporting News, less than a third of the 319 supposedly "can't miss" prospects selected in the first round of the last 10 NFL drafts have been selected to even one Pro Bowl—an acclaimed (though admittedly somewhat flawed) measure of football success. Only 17% went to multiple Pro Bowls. (See http://aol.sportingnews.com/nfl/story/2012-04-22/nfl-draft-2012-first-round-disappointments.)

Another Internet site (http://www.advancednflstats.com/2009/04/career-success-by-draft-order.html) shows that Pro Bowl selection *does* correlate with order chosen in the draft, as does years ultimately played as a starter, but these correlations are not nearly as strong as one might expect. Moreover, the authors of the site argue that being chosen high in the draft is something of a self-fulfilling prophecy. Teams spend huge amounts of money on high draft picks and tend to do anything possible to justify the funds spent and the players chosen. Players who are high draft picks tend to get lots of playing time and extra coaching assistance because they are expected to succeed; indeed, it is embarrassing to the team if they do not. Thus, high draft picks have something of an unfair advantage that skews the statistics.

The bottom line: if NFL "hiring" experts—with tens of millions of dollars at stake, who choose from among highly scrutinized candidates for which reams of rigorous data are known, in an endeavor where success is fairly easily measured (winning

games)—can't reliably choose outstanding performers, what chance do you have to pick good employees?

*****

Here's another Human Resources issue that might be of interest to security managers: Baby Boomers were born between 1946 and 1964. Generation X are those that followed the Baby Boomers. Millennials are the generation born between 1982 and 1999. Each generation, it is claimed, has its own characteristics. Millennials supposedly tend to have trouble dealing with conflict and lack the ability to deal effectively with confrontation. Their communication style is quite different from earlier generations. According to Linda Gravett with the HR consulting firm Gravett & Associates, Millennials tend to work more effectively when paired with Baby Boomers than with Gen Xers who are, after all, near the age of their parents and may invoke ingrained parent-child conflicts.

*****

Increasingly, courts, government, and society as a whole are grappling with issues of rights, responsibilities, and liabilities of private security officers. There was an interesting court case here in Illinois recently. In *Poris v. Lake Holiday Property Owner's Association*, the Appellate Court ruled that the private security officers hired by the homeowners association of the Lake Holiday subdivision in LaSalle County, Illinois do not have the legal authority to stop, detain, or inspect the driver's license of persons violating association rules (as opposed to Illinois laws). The court also ruled that the security officers could not use flashing amber lights in the process of making such a stop, but that the use of video recording equipment (if openly reported) and radar to measure vehicle speed was permitted. For more information, see http://www.illinoisrealtor.org/drlegalnews/Mar2012/casestudies.

Update 1/25/2013: The Illinois Supreme Court overturned this lower court ruling on both the stop/detain issue and the flashing lights. The plaintiff, former DuPage County prosecutor, Ken Poris asserted that this new ruling "…is going to have possibly some real serious consequences". For more information, see the *Chicago Tribune*, January 26, 2013, page 4.

*****

The curse of auto spell checkers: In February of this year, a college student in Oakwood, Georgia texted a friend that he would be near the West Hall High School. He meant to text, "Gunna be at West Hall this afternoon." But his smart phone's spell checker changed "Gunna" to "Gunman". Then he sent the text to the wrong phone number. What resulted was a lockdown at the high school and general chaos.

*****

Also, in the news: Officials with Prince George's County in Maryland are having to install security cameras to monitor their speeding cameras. Seems six of the speeding cameras have been burned, vandalized, and shot at by angry motorists. No word yet on when security cameras will be installed to monitor the security cameras monitoring the speeding cameras.

*****

The Vulnerability Assessment Team (VAT) at Argonne National Laboratory hosts and edits the *Journal of Physical Security* as a free, public service. Part of what we get out of it (other than getting to read some really interesting papers about physical security) is a chance to shamelessly plug our own work and views from time to time. Here are some recent news stories about the VAT. (The first two are also very good general reviews on the subject of election security.)

Victoria Collier, "How to Rig an Election", *Harper's Magazine* **325**, 33-41 (November 2012), http://harpers.org/print/?pid=225772

Laura Spadanuta, "Machine Politics", *Security Management* **56**(10) 50-57 (September 2012), http://securitymanagement.com/article/machine-politics-0010437?page=0%2C0

"How Your Vote Can Be Hacked", http://money.cnn.com/video/technology/2012/10/31/ts-voting-machine-hack.cnnmoney/index.html?iid=HP_River

"How Reliable is Electronic Voting in the US Election", BBC Click Radio Program, http://www.bbc.co.uk/programmes/p0104hxr

Wolfgang Stieler, "Wahl Ohne Kontrolle", *Heise Technology Review*, http://www.heise.de/tr/artikel/Wahl-ohne-Kontrolle-1733733.html

RT News live interview, http://www.youtube.com/watch?v=Ksvd7FJtNuU&list=UUczrL-2b-gYK3l4yDld4XlQ&index=5&feature=plcp

Eric Parizo, "Researcher Details Findings on Spoofing GPS, Malicious Insiders", http://searchsecurity.techtarget.com/video/Researcher-details-findings-on-spoofing-GPS-malicious-insiders

Eric Parizo, "Vulnerability Researcher on Layered Security Plan Mistakes", http://searchsecurity.techtarget.com/video/Vulnerability-researcher-on-layered-security-plan-mistakes

*****

As vulnerability assessors, we frequently encounter denial from security managers and bureaucrats about security flaws, or even are the targets of their fear and anger that would more productively be directed at their true adversaries. The latter phenomenon is predicted by **Feynman's Maxim**: An organization will fear and despise loyal vulnerability assessors and others who point out vulnerabilities or suggest security changes more than malicious adversaries.

The name for this maxim comes from the entertaining book, *Surely You are Joking, Mr. Feynman!*, published by W.W. Norton in 1997. During the Manhattan Project, when physicist Richard Feynman pointed out physical security vulnerabilities, he was banned from the facility, rather than having the vulnerability dealt with—which would have been easy. (A total of 120 more security maxims can be found at: http://www.ne.anl.gov/capabilities/vat/seals/maxims.shtml.)

Oliver Burkeman recently published an interesting essay in the *Wall Street Journal* (http://online.wsj.com/article/SB10001424127887324705104578147333270637790.html) that reminds us of the power of negative thinking, specifically the "premeditation of evils".

As Burkeman points out, the ancient Greek and Roman Stoic philosophers advised people to periodically think about the worst thing that could happen as a way of chilling out when facing risks and uncertainties. As modern psychologists know, mentally focusing in detail on the worst that can happen has (somewhat counter-intuitively) an amazing ability to make the future seem a lot less scary to people with fears and anxieties. Interestingly, thinking about the worst that can happen is also a very good security strategy. Thus, by focusing on the negative, you can have better security AND stop freaking out!

Failure to consider the worst that can happen may make you the victim of **Mahbubani's Maxim**: Organizations and security managers who cannot envision security failures, will not be able to avoid them. This maxim is named for scholar and diplomat Kishore Mahbubani. He meant to apply this general principle to politics, diplomacy, and public policy, but it is also applicable to security.

*****

We always try in this journal to introduce fresh approaches to thinking about security. Bad poetry is one possible approach that has been inexplicably ignored by other security journals. So here we offer some bad haiku poetry about security.

English haiku is an English language version of the Japanese haiku poetic tradition of terse, fragmentary poems that paint a verbal picture. Each English haiku poem typically consists of 3 lines of 5, 7, and 5 syllables, respectively. Thus…

Security fights:
evil, denial, conceit.
The dismal science.

Over-Confidence.
Denial. Wishful Thinking.
The real enemies.

Primitive methods
often overcome high-tech.
So don't get dazzled!

If you're happy with
your security. Well, then...
so are the bad guys.

Tamper Detection
is only as good as your
Seal Use Protocol!

gruntled employees
much safer than disgruntled
treat everybody well!

Insiders attack.
Many different reasons.
But revenge burns hot.

-- Roger Johnston
Argonne National Laboratory
December 2012