Right Brain Sekurity

The Journal of Physical Security

Volume 8(2), 2015

JPS

THIS ISSUE...

Editors Comments

M Gill & C Howell, "Single Service or Bundle: Practitioner Perspectives on What Makes the Best Security", pages 1-14

GD Curry, JJ Leflar, M Glasser, R Loyear, B Grey, T Jordan, L Ong, W Preining & JM Sobron, "How Social Media is Transforming Crisis Management and Business Continuity", pages 15-36

RG Johnston, "The New ASIS Standard on Risk Assessment", pages 37-38

S Hunt, "Why I Hate Security", pages 39-41

Albuquerque Journal, "WIPP May be the Best Place for Weapons-Grade Waste", pages 42-43

L Coney, "The IoT and the Ability to Defend Against the Silent Intruder", pages 42-53

Table of Contents

Editor's Comments, pages i-xv

M Gill and C Howell, "Single Service or Bundle: Practitioner Perspectives on What Makes the Best Security", pages 1-14

GD Curry, JJ Leflar, M Glasser, R Loyear, B Grey, T Jordan, L Ong, W Preining, and JM Sobron, "How Social Media is Transforming Crisis Management and Business Continuity", pages 15-36

RG Johnston, "The New ASIS Standard on Risk Assessment", pages 37-38

S Hunt, "Why I Hate Security", pages 39-41

Albuquerque Journal, "WIPP May be the Best Place for Weapons-Grade Waste", pages 42-43

L Coney, "The IoT and the Ability to Defend Against the Silent Intruder", pages 42-53

Editor's Comments

Welcome to volume 8, issue 2 of the *Journal of Physical Security* (JPS). In addition to the usual editor's rants about security (and other things) that appear immediately below, this issue has research papers on single service vs. bundled security, and on social media impacts on emergency response and business continuity. There are also 4 viewpoint papers. These include a review of the new ASIS International Risk Assessment Standard, an essay on why you should hate security, an editorial on the storage of high-level nuclear waste, and what the Internet of Things and a new IEEE standard for wireless privacy and security may mean for physical security professionals.

Papers are peer reviewed unless otherwise noted.

Past issues of JPS are available at http://jps.rbsekurity.com, and you can also sign up there to be notified by email when a new issue becomes available.

JPS is hosted by Right Brain Sekurity (RBS) as a free public service. RBS (http://rbsekurity.com) is a small company devoted to physical security consulting, vulnerability assessments, and R&D.

As usual, the views expressed in these papers and the editor's comments are those of the author(s) and should not necessarily be ascribed to their home institution(s) or to Right Brain Sekurity.

*****

Germy Biometrics

Every human walks around surrounded by a cloud of millions of microbes that represent a unique "fingerprint" that can potentially be used to identify or verify a person's identity, even after he or she has left the room. For information, see: http://www.theatlantic.com/health/archive/2015/09/inside-the-germ-cloud/406591/

*****

Be Still My Heart

Bionym has developed a wristband that uses an electrocardiogram (EKG) sensor to identify the unique cardiac rhythm of the wearer. A Bluetooth or NFC connection is used to, for example, use the biometric to log onto a computer. For more information, see https://www.washingtonpost.com/news/innovations/wp/2014/11/21/the-heartbeat-vs-the-fingerprint-in-the-battle-for-biometric-authentication/

*****

Defeating Biometrics

Researchers at the University of Alabama at Birmingham have demonstrated how to spoof voice-based user authentication software with electronic voice impersonation. See http://www.uab.edu/news/innovation/item/6532-uab-research-finds-automated-voice-imitation-can-fool-humans-and-machines. (Thanks to Indir Jaganjac for pointing out this work.)

Most biometrics can be fairly easily counterfeited—and it would be surprising if the Microbial and Heartbeat Biometrics discussed above were any different. What is often overlooked is that most biometric hardware is also vulnerable to simple physical/electronic spoofing, such as man-in-the-middle attacks, not just counterfeiting or copying of the biometric signature. These MiM attacks can be done very quickly at the factory, vendor, during shipment, on the loading dock, or before or after installation. It can be quite difficult to detect such attacks—examining software or checking if the device operates normally is of little value in determining if it has been compromised.

There needs to be a secure chain of custody right from the factory, effective tamper-detection built into the biometric devices, and independent and imaginative vulnerability assessments conducted. All of these things are almost universally lacking for biometrics devices—indeed, for almost any kind of security device.

*****

Piss and Vinegar

New research suggests that people are better liars when they have a full bladder. It is not immediately clear how to apply this to security. For more information, see: https://www.newscientist.com/article/dn28199-the-lies-we-tell-are-more-convincing-when-we-need-to-pee/

*****

MLB Authentication

Major League Baseball (MLB) has an authenticity program for sports memorabilia. Official authenticators are on hand for every MLB game. Their job is to try to maintain a visual chain-of-custody on game-day items, such as a baseball involved in a record-breaking play, that are of interest to sports memorabilia collectors. The authenticators attach what MLB calls a "tamper-resistant" authentication hologram—though it isn't particularly tamper-resistant—and assign the item a unique ID number. (Sometimes these tags are called "tamper-proof", which is even worse terminology.)

"Lifting" these kind of pressure-sensitive adhesive holograms, i.e., moving the sticker from one item to another without leaving evidence is usually not very difficult to accomplish, especially in the first 48 hours before the pressure-sensitive adhesive has fully set up. Moreover, the authenticators are often attaching the stickers to dirty baseballs, dusty bats, and sweaty jerseys that are less than ideal adhesion surfaces. Lifting, however, isn't of prime interest to counterfeiters because it leaves them with an authentic item that lacks a hologram. What is more useful for the bad guys is to counterfeit the hologram, or merely mimic it, which is even easier. The counterfeiting or mimicking of embossed, metalized holograms is especially straightforward.

Typically the holographic sticker only has to fool a visual inspection by a non-expert. It is thus mostly Security Theater. The true security in the scheme—if indeed there is any—is in the visual chain-of-custody during the ballgame, and the unique ID that can theoretically be used to verify authenticity. It is not clear how secure the MLB chain-of-custody is after the game, or what kind of insider threat mitigation is in place for authenticators and item handlers.

It is also not clear if the MLB call-back scheme to check on the unique ID number is effective. Virtual Numeric Tokens can indeed be a powerful tool for anti-counterfeiting, but only if implemented intelligently. Otherwise, this, too may just be Security Theater—like so many other approaches to product counterfeiting.

You can see an interesting video at http://mlb.mlb.com/mlb/authentication/ that explains the MLB authentication process. Note in the video that one of the authenticators leaves his roll of "tamper-resistant" holograms briefly unattended during the ballgame. So much for a secure chain-of-custody!

To MLB's credit, they at least take the visual chain-of-custody issue seriously during the game. On October 13, 2015, the Cubs' Kyle Schwarber hit a towering home run at Wrigley Field during the National League Division Series (NLDS) that went over the top of the main video board but then disappeared. Later that night, a ball was spotted sitting at the top of the video score board. This ball was not eligible to become an official MLB souvenir, however, because it had left the sight of the MLB authenticator. This was the case even though the ball had the appropriate NLDS printing that differs from regular season and practice balls, and almost certainly had to be Schwarber's home run ball.

*****

Anti-Counterfeiting?

NEC is reportedly developing a product anti-counterfeiting technology that uses a smartphone to check unique surface markings on high-end products. See http://blogs.wsj.com/digits/2014/11/12/nec-smartphone-tech-can-spot-fake-bling/

It is difficult to believe that product counterfeiters would have any problem duplicating surface patterns or morphology, as this is typically quite easy to do, even down to the microscopic level. If counterfeiters knew the location of where the checking was to be done—as we would have to assume they would—the task of duplicating a surface pattern should be relatively simple. But, like a lot of anti-counterfeiting technology, it probably will never be subjected to a serious vulnerability assessment that investigates subtle (as opposed to knucklehead) attacks.

*****

Security Theater

The TV show "Adam Ruins Everything" on truTV takes on examples of Security Theater in a very entertaining but totally valid way. See the Security Theater episode at: **http://www.trutv.com/shows/adam-ruins-everything/blog/adams-sources/adam-ruins-security.html**

*****

Chip and Pin

The new "smart" credit cards are out with the embedded microchip. These cards are complaint with the EMV Standard, long in use in Europe. ("EMV" stands for Europay, MasterCard, and Visa).

These smart cards should reduce credit card fraud. When they were introduced in France, Canada, and the UK, there was a drop of more than 50% in lost or stolen credit card fraud. We can expect credit card fraud to now move more onto the Internet.

In the United States, we will be mostly using a "Chip and Signature" approach, where a signature is used instead of the more secure personal identification number (PIN). Credit card companies fear Americans would be too annoyed or forgetful if they had to produce a PIN, as is often done in Europe (or in the U.S. for debit cards). Signing your signature at the point of sale rather than using a PIN is largely Security Theater, as pointed out in the TV show "Adam Ruins Everything" discussed above.

The EMV standard is a big deal for small businesses because—starting last month—if your business accepts and processes a counterfeit EMV card transaction on an old, non-EMV terminal, the liability for the transaction is yours—no longer the credit card company's.

Only 59% of US retail stores are expected to be EMV-compliant by the end of this year, and only 1 out of 3 small businesses (according to a Javelin study) is even aware of this switch in liability.

*****

Gambling Cheats

Here is a really interesting website about 10 individuals who "cheated" casinos: http://listverse.com/2010/01/24/10-gamblers-who-beat-the-casino/ Not everything these people did was necessarily illegal.

Perhaps the most intriguing character is Tommy Glenn Carmichael who came up with numerous, clever inventions to beat slot machines. He dutifully paid income taxes on his illicit winnings, however. Carmichael went on to become a consultant for casinos and gambling security.

Also, did you know that a century ago, many of the companies that made playing cards sold a variety of different kinds of "advantage tools" which allowed card players to cheat? These included "card pricks", "poker rings", "punches", and "peggers" to mark cards with a very subtle indentation. There were also "holdout machines" that let you keep a card out of circulation—under a table or up your sleeve—until you needed it in the game. See http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.134.1119&rep=rep1&type=pdf

*****

Art and Anarchy

Two books worth reading:

1. *The Art of Forgery* by Noah Charney. This is a breezy and highly entertaining tour through the history of art forgery (and other kinds of forgery). Charney convincingly makes the point that money is not the prime motivator for most art forgers, at least initially: "Testing and demonstrating one's genius and ability, revenge against the art establishment that has slighted you, and acclaim are more common reasons forgers initially try their hand." In art forgery, as in a lot of security attacks, disgruntlement is a huge motivator for insider attackers.

My favorite forgery discussed in the book involves the theft of Matisse's *Odalisque in Red Trousers* from the Caracas Museum of Contemporary Art in Venezuela. An FBI sting operation recovered the stolen painting in 2014. The burglars had replaced the original painting with a somewhat amateurish forgery. (Charney points out that this MO—stealing the original and replacing it with a fake—is actually fairly rare in the world of art theft.)

It took 2 years before anybody even noticed the switch. The fake had fooled all the curators, staff, art experts, guards, and visitors at the museum for two years. The forgery was in place and unrecognized in September 2000 when a proud President Hugo Chavez was photographed standing in front of what was supposed to be the museum's most prestigious piece. A total of 14 other works were later found to be missing from the museum.

As countermeasures to art and artifact forgery, Charney recommends independent evaluations devoid of conflicts of interests—just as is needed for other kinds of security such as risk assessments or vulnerability assessments. Auction houses, museums, art connoisseurs, and "discoverers" who have an economic, reputational, or ego interest in the found art or artifact being authentic are simply too easy to fool. Charney also believes the public and news media should stop making Robinhood-like heroes of art forgers and art thieves. He calls for laws that prevent forgers from benefiting economically from any sale of art or artifacts after conviction. He would like to see more careful analysis of provenance evidence/documents, more skepticism, and more scientific forensics where practical.

2. *Immigrants Against the State* by Kenyon Zimmer. This is a scholarly discussion of American anarchists in the late 19th and early 20th centuries, especially Italian and Yiddish-speaking immigrants who were major players in the anarchist movement.

People tend to forget today that the anarchist movement was a source of very serious terrorist attacks in the United States and Europe, including bombings, assassinations, bank robberies, and IEDs mailed to prominent people and government leaders. U.S. President William McKinley was assassinated in 1901 by an anarchist sympathizer.

American anarchists had complicated, sporadic connections with socialists groups and various labor movements and unions, but tended to have a philosophy of their own. This often involved rejecting some or all of government, tyranny, regulations, capitalism, exploitation of the working class, war, misogyny, and religion. The majority of anarchists were non-violent; those that were violent tended to think of their terrorism as legitimate political or social violence they called "propaganda of the deed".

Anarchist violence largely ran out of steam in the 1920s on its own. The repressive and extreme measures taken by governments against anarchists—think Patriot Act and McCarthyism only a lot worse—were mostly ineffective. The anarchism movement itself gradually gave way to other methods of trying to deal with perceived social injustice such as labor movements, labor and anti-trust legislation, social welfare programs, the progressive movement, socialism, and communism, as well as various feminist, suffrage, and civil rights movements. Many immigrants also became somewhat better integrated into American society. Anarchists are still around today, of course, but they are almost entirely non-violent and are not dominated by immigrants.

*****

Growth Industry

According to the November 6, 2015 issue of *The Week*, private security was a $202 billion industry in 2013, and is projected to be at $282 billion by 2020. This is compared to a mere $52 billion in 1990.

Of the 5 fastest growing security companies, 3 primarily work in the area of physical security, rather than cyber security and had growth rates well in excess of 1000% from 2011 to 2014.

*****

Run Away from Danger?

The National Nuclear Security Agency (NNSA) has been criticized for issuing a name-brand solicitation in February 2015 for 5 top-of-the-line Woodway treadmills. (See https://www.fedconnect.net/FedConnect/?doc=DE-SOL-0008095&agency=DOE.) The model NNSA is seeking costs over $10,000, with upgrades adding up to $3,900 per unit. NNSA plans to "utilize the treadmills to qualify Federal Agents on the running requirements established by the NNSA …"

Good quality treadmills of the kind used in your neighborhood fitness center can be had for around $4,000.

Presumably, NNSA personnel need to be fleet of foot to keep up with elderly, pacifist nuns who penetrate deeply into nuclear facilities. For an interesting take on this, see http://www.newyorker.com/magazine/2015/03/09/break-in-at-y-12.

*****

I Hate When That Happens

Almost 50 years after a horrendous nuclear accident in Spain, the cleanup is not complete. On January 17, 1966, a B-52 bomber and a KC-135 refueling plane crashed into each other mid-air above the small town of Palomares in Spain. A total of 7 crewmembers died, and 4 nuclear weapons fell to Earth. One fell into the Mediterranean and was eventually recovered after considerable effort. Two of the three bombs that hit the ground burst open when their conventional high-explosives went off, and this caused the release of plutonium into the surrounding area.

The casings of two of the recovered nuclear bombs involved in the Palomares incident are on display at the fascinating National Museum of Nuclear Science and History in Albuquerque.

U.S. Secretary of State John Kerry recently signed a new agreement in Spain, pledging continued U.S. assistance with the cleanup of contaminated soil from the Palomares accident. The plutonium-contaminated soil may be shipped to the United States for permanent storage. See *The Day We Lost the H-Bomb* by Barbara Moran (2009) as well as http://www.cnn.com/2015/10/20/europe/spain-us-palomares-nuclear-accident-cleanup/?iid=ob_article_footer_expansion&iref=obnetwork

There have been numerous other accidents and mishandlings of nuclear weapons over the years—many that are true head shakers and far too ridiculous to put into the plot of a bad paperback spy novel. There will be more amazing nuclear bungling incidents in the future.

*****

Culture of Denial

A new study by think tank Chatham House concludes that nuclear power plants are extremely vulnerable to cyber attacks and that a "culture of denial" is getting in the way of good cyber security. See http://www.ft.com/cms/s/0/b5f0df54-6aa1-11e5-aca9-d87542bf8673.html#axzz3pVEmcPiZ

*****

The Plastic Internet of Things

A new Barbie doll, named "Hello Barbie" is now available. A joint venture between Mattel and ToyTalk, Hello Barbie is a wi-fi connected playmate that can carry on a conversation with the doll's owner. When children talk to Hello Barbie, there conversations are recorded and sent back to ToyTalk's servers so that Barbie can "remember" details of the child's likes. Privacy advocates have called this feature "creepy". There are supposedly some strong parental controls built in.

For more information, and to read various views about Hello Barbie, see: http://pixelkin.org/2015/09/11/why-hello-barbie-is-not-as-creepy-as-she-sounds/ and http://www.dallasnews.com/business/retail/20150328-hello-barbies-critics-using-mattel-doll-to-wage-privacy-fight.ece

*****

Secret Computing: Beyond Playing Video Games at Work

The *IEEE Spectrum* has an excellent article on concepts for keeping data encrypted during computations and database processing. This can greatly increase the security and privacy of the data. See "How to Compute with Data You Can't See", http://spectrum.ieee.org/computing/software/how-to-compute-with-data-you-cant-see

*****

The Prison Problem

It is widely believed that the reason there are so many Americans in prison is due to drug arrests. David Brooks in the New York Times questions this assumption. He points out that only 17% of inmates in state prisons are there for drug related offenses, with the percentage continuing to decrease.

Mandatory sentences are also not the cause of having so many people in prison. According the Brooks, the reason we have so many prison inmates may primarily a combination of prosecutors wanting to seem tough on crime by avoiding plea bargaining, and the fact that many inmates with mental illness who would have been sent to mental institutions in the past are now warehoused in prison. To read the editorial, see http://www.nytimes.com/2015/09/29/opinion/david-brooks-the-prison-problem.html?_r=0.

*****

Nobel Peace Prize?

According to BleacherReport.com, the National Football League (NFL) recently went an entire calendar month (September) without any of its players getting arrested. This is the first time that has happened since 2009.

*****

We Are Safer

According to researcher David Finkelhor at the University of New Hampshire, the physical abuse, sexual abuse, and neglect of children declined by 55, 64, and 13 percent respectively, between 1992 and 2011. Abduction by strangers is also sharply down. The Centers for Disease Control (CDC) says that the death rate for children 12 and under declined by 43% in the last decade. See http://www.unh.edu/ccrc/pdf/_Updated%20trends%202013_dc-df-ks-df.pdf and http://nymag.com/scienceofus/2015/03/we-live-in-an-age-of-irrational-parenting.html

An under-appreciated statistic is that, according to the FBI, the U.S. homicide rate in 2013 (the most recent year for which statistics are available) was 4.5 per 100,000 people. This is approximately the same as in 1962 and less than half the rate of 1993. This is among the lowest rates since the end of World War II.

*****

Scandinavia

According to the *Independent* (UK) newspaper, Norwegian police fired their guns only twice in 2014, injuring or killing nobody. In Norway, police are usually unarmed and only carry guns in special situations.

On the other hand, Sweden has the second highest reported rate of rapes in the world, about 3 times higher than the United States. Some of this is due to changes in how rape statistics are reported there. See https://en.wikipedia.org/wiki/Rape_in_Sweden

*****

Sis-Boom-Bah

The October 18, 2015 issue of *The Chronicle of Higher Education* has an excellent article on the history, challenges, and controversies of college and university policing. See Scott Carlson, "Campus Cops' Contested Role", pages A18-A21.

In the same issue is a story about a study of college exam cheating. The investigators recommend randomly assigning seats to students during exams as a countermeasure to copying. See Kate Stoltzfus, "To Stop Exam Cheats, Economists Say, Try Assigning Seats", page A15.

[Incidentally, the classic college cheerleading chant "sis-boom-bah" was around in 1867, and may go back to 1858 or earlier. It is meant to mimic a skyrocket: "sis" for the launch, "boom" for the explosion, and "(b)ah" for the crowd reaction. For more on the history of this cheerleading chant, see http://esnpc.blogspot.com/2014/05/skyrockets-transatlantic-cable-and-pre.html.]

*****

TSA Follies

USA Today reports that the Transportation Security Administration (TSA) has paid about $3 million over 5 years for claims that airport security screeners broke, lost, or stole luggage and/or its contents. The TSA settled by making payments in about one-third of the 50,000 claims filed from 2010 to 2014. The number of claims filed were down about 35% from 2010 to 2014. Since 2003, the TSA has fired more than 500 TSA officers for theft. The story can be found at http://www.usatoday.com/story/news/2015/07/02/tsa-damage-tops-3m/29353815/

Bruce Schneier asks in a recent editorial why we are spending $7 billion dollars on ineffective or unnecessary efforts by the TSA:
http://www.cnn.com/2015/06/05/opinions/schneier-tsa-security/

Josh Noel in a June 19, 2015 article in the *Chicago Tribune* notes these TSA failings:

- More than 1,500 TSA badges used by TSA employees to access airport security areas are lost, missing, or stolen.
- The TSA failed to identify 73 airport workers with potential terrorist links.
- In a recent test, DHS agents were able to get banned items past TSA airport screening 95% of the time.

Part of what I think is the problem with the TSA—a problem shared by many other organizations, including NNSA, DOE, DoD, IAEA, and NRC—is a failure to perform frequent imaginative, independent vulnerability assessments (VAs) to find security weaknesses.

It is common to confuse VAs with threat assessments, risk assessments, design basis threat, security surveys, security audits, fault or event tree analysis, data analytics, "red teaming", and penetration testing. While these things are definitely worth doing, they are not a good substitute for a holistic, imaginative VA done by people thinking like the bad guys. If you want to predict how the bad guys might attack, you need to think like they do. Bad guys don't do threat assessments, risk assessments, design basis threat, etc. They do VAs.

For more discussion of the myths and misconceptions surrounding vulnerabilities and VAs, see: "Vulnerability Assessment Myths", *Journal of Physical Security* **7**(1), 31-38 (2014) and "Why Security Fails", *Journal of Physical Security* **8**(1), 37-39 (2015), both at http://jps.rbsekurity.com. Also see, "The Fear of NORQ", *Homeland Security Today* **11**(4), 39-41 (2014), http://www.nxtbook.com/nxtbooks/kmd/hst_20140607/#/40.

*****

3-D Printing and Keys

A group of lock-picking and security hobbyists demonstrated how to duplicate a lock key from an online picture of the key. Anyone with a 3-D printer can use the resulting CAD files to make a copy.

The keys in question were the master keys that TSA uses to open their "approved" luggage locks—which are not high security locks.

In one sense, this is nothing new. Talented locksmiths have supposedly been able to read the pattern of cuts in a key at a distance when the key is flashed in a parking lot, then make a duplicate key without ever having handled the key. The advent of 3D printing just makes this easier. Bottom line: do not show your keys in public or let them get photographed!

For more information on the 3-D printer hack see:
http://www.wired.com/2015/09/lockpickers-3-d-print-tsa-luggage-keys-leaked-photos/

*****

Fly the Friendly Skies

According to the Chicago Tribune, 4/20/2015 on page 13: United Airlines stopped a prominent security researcher, Chris Roberts, from boarding one of its planes after he had posted a suggestion online that the airline's onboard system could be hacked. He was on the way to speak at a major security conference.

This is a good example of **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 maxim is named for the physicist Richard Feynman. During the Manhattan Project, when he pointed out physical security vulnerabilities, he was banned from the facility, rather than having the vulnerabilities dealt with (which would have been easy to do).

*****

Bully For You

A new study suggests that abusive bosses often bring their abusive behavior into the workplace because of problems at home. The study also found that supervisors and mangers are more likely to engage in (non-physical) abuse of employees if they felt their organization would let them get away with it. (Many do.)

While only 14% of U.S. employees report being the victim of a (non-physically) abusive boss, the security risks that abusive bosses create are substantial for the insider threat—not to mention the impact on employee performance, productivity, morale, turnover, and recruitment. An organization's reputation can also be harmed.

To read about the study, see http://newsroom.niu.edu/2015/09/24/bosses-unhappy-at-home-wreak-havoc-at-work/

*****

Performance Anxiety

The large consulting firm Accenture is eliminating annual performance reviews and rankings for all its 330,000 employees. The company believes the annual review process is too time-consuming and expensive, and the benefits are minimal. Accenture will now do more timely feedback from managers on an *ad hoc* basis.

Microsoft did something similar in 2013. Instead of annual performance reviews, Deloitte now encourages team leaders to check in with each team member once a week,

and to focus on future performance, rather than obsessing about issues from the past. Other companies now hold quarterly or monthly reviews or conversations, rather than annual ones.

Multiple studies (and common experience) have shown that the traditional annual performance reviews often causes enormous amounts of employee annoyance, resentment, and disgruntlement. Supervisors and managers who write the reviews often have no idea what they are talking about or what their employees really do. Annual performance reviews can damage morale and aggravate the insider risk. They do not effectively motivate employees, but rather waste time, money, and energy. The year-long delay in feedback makes the review nearly useless as a metric and for improving employee performance.

Vauhini Vara had an excellent article on this issue in the *New Yorker*. See http://www.newyorker.com/business/currency/the-push-against-performance-reviews

*****

JPS Peer Review

The *Journal of Physical Security* uses a blind peer review process. This means that the reviewer(s) are anonymous but the author(s) are not. Reviewer anonymity means that they can feel freer to offer commentary without issues of attribution. Some journals—though not many—use a double blind review process where both the author(s) and reviewer(s) are anonymous.

One disadvantages to a double blind review process is that the reviewers can typically guess the authors' identities from the references, acknowledgements, past work, or other hints in the paper. It can be very difficult to remove such clues. Moreover, the identity and affiliation of the author(s) is often useful to single-blind reviewers in identifying any conflicts of interest, and determining if the author(s) have sufficient resources and approvals to conduct their research and analysis.

Of course, there are disadvantages to single-blind reviews, too. Reviewers can hide behind their anonymity when offering lazy or unnecessarily snarky reviews. Conflicts of interest on the part of the reviewers are not publicly obvious. To a considerable extent, however, a good editor can at least partially mitigate these disadvantages.

JPS usually has 2 anonymous reviewers for Research Papers, and 0, 1, or 2 reviewers for Viewpoint Papers, depending on the topic and content. Reviewers are not compensated for their efforts. As editor, I have been very gratified by the careful thinking and hard work reviewers put into their reviews, and for their willingness to serve the physical security community without being able to receive any public recognition (or money!) in return. These are true security professionals.

If you think you would be interested in serving as an anonymous reviewer, contact the editor at http://jps.rbsekurity.com. Be sure to indicate your credentials and area(s) of expertise.

*****

The Limitations of Peer Review

Actual product reviews on Amazon.com:

This carbon monoxide detector saved my son's life. I give it 4 out of 5 stars.

Review of the movie, "Captain America: the First Avenger": WE HAD BARBEQUE. We invited family and friends over to watch this on blu-ray. When it ended, they got up and left. 2 out of 5 stars.

Review of the movie, "Rocky III": ARE YOU KIDDING? I have colleagues who might read this so even if I did enjoy this film, I could not admit to it on this quasi-public site. I am in enough trouble just for responding. 1 out of 5 stars.

Review of the movie, "Rise of the Planet of the Apes": There is no way an orangutan can ride a horse without crushing it. 2 out of 5 stars.

Review of Herman Melville's novel, *Moby Dick*: A complete rip-off of the movie "Jaws". 1 out of 5 stars.

Review of *Anna Karenina* by Leo Tolstoy: Parts of the book were discussing political views nothing to do with Anna. It appeared there were many main characters not only Anna. 2 out of 5 stars.

Review of the book, *Where is Baby's Belly Button: A Lift-the-Flap Book*: This book is completely misleading. The entire plot revolves around finding Baby's belly button; the title makes this much clear from the beginning. However, there is no mystery. There is no twist. Baby's belly button is right where it's suppose to be, on Baby's stomach. Right where it clearly SHOWS you it is on the COVER OF THE BOOK. This plot is a complete mess as a result of it's reliance on the mystery of where the belly button is; everything falls apart the second you realize that the belly button was in plain sight all along. There is no conflict, there is no character development, and there is scarcely any plot. Whoever wrote this book must have a serious error in judgment, because you would have to be an infant to not immediately understand where Baby's belly button is. This is one of the worst pieces of literature I have ever read. 1 out of 5 stars.

*****

The Study of Stupid

Research on stupidity may have some lessons for security, as stupidity seems to be involved in a lot of security blunders. Interesting research of this type is discussed in the following article: Roberto A. Ferdman, *Washington Post*, October 19, 2015, http://www.washingtonpost.com/news/wonkblog/wp/2015/10/19/how-to-act-less-stupid-according-to-psychologists/.

*****

Scary Lucy

In 2009, a 400-pound bronze sculpture of actress Lucille Ball (1911-1989) was erected in a park in her hometown of Celoron, NY. The statue has been described as having zombie-like eyes with a deranged toothy grin, and is considered particularly scary at night. (You can see a photograph at http://www.washingtonpost.com/news/morning-mix/wp/2015/04/07/in-lucille-balls-hometown-scary-lucy-haunts-her-memory/) The statute will eventually reside in the National Comedy Center, though the sculptor has promised to redo it.

*****

Glad You Warned Us!

I know I have been traveling too much when I read the snack wrappers handed out on airplanes. The packet of "Honey Roasted Peanuts" you get on Southwest Airlines, which lists peanuts as the number one ingredient, warns us in small print on the back that the contents are "produced in a facility that processes peanuts…".

-- Roger Johnston
Oswego, Illinois
November, 2015

Journal of Physical Security 8(2), 1-14 (2015)

Single Service or Bundle: Practitioner Perspectives on What Makes the Best Security

Martin Gill and Charlotte Howell

Perpetuity Research & Consultancy International Ltd
11a High Street
Tunbridge Wells, Kent, TN1 1UL
United Kingdom

Abstract

The aim of this paper is to discuss the relative advantages and disadvantages of providing security services as either a single service or as part of a bundle. It is based on one-to-one interviews with 72 respondents, 44 from client organizations (and including security and facilities managers) and 28 suppliers (including representatives from security only providers and facilities management companies). While there are supporters of supplying security both as a single service and as part of a bundle, the arguments used to support each are based on experience and perception rather than evidence. This study is presented as a first step in identifying key issues that pertain to the deployment/integration of security alongside other facilities management services. There is a need for more evaluative research.

Key words: security services, bundled services, client/supplier relationships

Context

It has long been recognized that there are different ways of outsourcing and a variety of frameworks are in evidence (McIvor, 2005; 2008; Varadarajan, 2009) for a variety of different facilities management services. The motive is often highlighted as an economic one although this is but one of many possibilities (see, McIvor, 2008; Shekar, 2008); much depends on the type of outsourcing model being discussed, and there are many. Willcocks et al. (2007; 2009) helpfully identify four options which they term sole supplier, prime contractor, best-of-breed, and panel.

- Sole supplier: This is where all the services are supplied by a single supplier, sometimes considered to be Total Facilities Management (TFM).
- Prime contractor: This is where one supplier is responsible for a contract but may subcontract where it lacks expertise.
- Best-of-breed: This is where potentially a range of services are managed by the client.
- Panel: This is where a preferred group of approved suppliers compete for contracts.

In reality, there are a variety of ways of classifying services (see also, BIFM, 2007; 2012), and since outsourcing is complex (see, Nordin, 2006), 'ideal type' models often disguise wide variations and overlaps in practice (see, Oshri et al., 2011; Willcocks et al., 2009b). A number of key points, though, are in evidence and are relevant to this paper. The first is that the decision on which model to choose rests with clients (see, Jain and Natarajan, 2011), and at least part of the influence on their decision will be their own capability for managing the different options (Willcocks and Lacity, 2011; 2012). The extent to which they understand the potential barriers to implementing their chosen strategy (if they have one) will have important implications for how successful it is likely to be (Nordin, 2006). A second issue is that single service provision is typically viewed as less complicated, and that the scope for outsourcing in some sort of bundled way comes with experience and requires greater expertise (BIFM, 2007; Willcocks et al., 2009), not least in turbulent environments (Momme and Hvolby, 2002). Third, the scope for moving to some type of bundled provision depends in part on expertise emerging amongst suppliers (Oshri et al., 2011; Feeny et al, 2005; Willcocks and Lacity, 2009).

Fourth, there are a range of advantages and disadvantages of different models in different sectors, albeit that many of these are not tested by independent research (see, BIFM, 2007; Willcocks et al., 2007; Willcocks et al., 2009; Interserve and Sheffield Hallam University, 2012). Indeed, some evidence suggests that not only will the effects of outsourcing be different for different functions, but that there is a danger that internal skills and knowledge that are lost by outsourcing will need to be meditated by effective management strategies (Agndal and Nordin, 2009). Fifth, there is a lack of research on the pros and cons of different models in different facility management service areas. Both security management (Gill, 2014) and facilities management (Drion et al., 2012) are relatively new areas of study where the body of knowledge about what works and what doesn't is still evolving. Indeed, despite research on the outsourcing of various areas of facilities management, such as business processing (Whitaker et al., 2010); engineering (Burdon and Bhalla, 2005); information services (Petry-Eberle and Bieg, 2009); and property management services (Yam, 2012), there has been little research on security services (but see, Hassanain and Al-Saadi, 2005). It is against this background that our research took place.

The aim of this study was to identify practitioner perspectives on the relative merits of single service as opposed to bundling in one specific area that has received very little coverage in the facility management (FM) literature, that of security. The word 'security' in practice covers a wide variety of activities that often bear little relation to each other (for example locksmithing, security guarding, alarm installation). There is a tendency to discuss security in terms of personnel services (such as manned guarding and close protection) and technical services (such as alarms and CCTV), the approximate equivalent to soft and hard facilities management. (For a discussion of the security sector, see Gill, 2014.)

The approach in this work was to identify and interview a wide range of individuals using the different models in practice to help understand the key issues involved in single service and bundling (these terms will be defined later in this paper) which involves

security. A snowball sampling strategy was used. This involves using contacts and word of mouth to identify relevant people to take part in the study. An advantage of this method is that it allows access to members of the population who may be difficult to identify and engage by other means. Moreover, it allows for potentially more valuable responses, as those taking part are more likely to be knowledgeable about the research. Indeed, one of the early findings was that knowledge about the benefits and drawbacks of providing single service or bundling security was not clear-cut. Against this, however, snowballing is a non-random form of research sampling and it is therefore unlikely that the sample is representative of the total population, which should be kept in mind. The interviews typically lasted thirty to sixty minutes, and semi-structured interview schedules were used. An advantage of a semi-structured schedule is that it gives the flexibility for interviewers to probe the issues raised.

A total of 72 individuals took part in telephone interviews, mostly from the UK, but also from Australia (7), Canada (4), Europe (3) and a respondent working in the Middle East. Table 1 provides further information on the role of individuals taking part.

Table 1: Breakdown of interviewees (n=72)

Interviewee	**Type**	**N**
Clients (n=44)	Security Managers	27
	Facilities/Property Managers	14
	Consultants	2
	Procurement Specialists	1
Suppliers (n=28)	Bundled service provision	10
	Single service provision	9
	Combination of bundled and single service provision	7
	Advisory role	2

Clearly, the sample was not intended to be representative, rather we sought to engage participants who were involved in different aspects of security—both single service and bundled—to better understand the pros and cons of different types of security service purchase and delivery. It provides a foundation on which further studies may build.

Findings

Thinking about terminology

One of the early findings was that there remains widespread confusion in the terminology used (see, Varadarajan, 2009). This included what was meant by single service, since some referred to a type of security as single service (say manned guarding) while some companies offering a variety of different services (including personnel and technical) considered this a single service because it was all related to security, when in

fact it is best described as 'bundled security'. Indeed, it was possible to identify the following types of security delivery that do not fit easily into the four categories noted above:

- *in-house*: security provided in-house
- *single service security*: just one type of contract security provided
- *bundled security*: different types of contract security provided
- single service security supplied with a limited number of FM services
- bundled security supplied with a limited number of FM services
- single service security supplied with all other relevant FM services
- bundled security supplied with all other relevant FM services
- single service security supplied with a limited number of FM services with integration between them
- bundled security provided with a limited number of FM services with integration between them
- single service security supplied with all FM services with integration between them
- bundled security provided with all FM services with integration between them

This list reflects the somewhat complex array of arrangements that exist. Moreover, there was a belief that the further down the list one reads, the more complex the delivery. Just to add to this, sometimes there was a mixture of delivery approaches across sites or countries. In this short paper, it is not possible to examine the different risks and opportunities these arrangements present—a laudable aim though that would be. Rather, the focus here is to compare the relative merits of offering security on its own (whether single or a security bundle) compared to security combined with other FM services. The focus has been on other facility management services, but of course security is sometimes provided alongside an even broader range of services such as those focussed on safety and emergency management, such as managing natural disasters; this provides another potential field of enquiry.

The case for bundling security

There were three overarching reasons why clients and suppliers said they favored bundling. The first and most widely commented upon was that it offered cost savings for clients. There were a number of dimensions to the ways in which these could be achieved. Some noted there were lower overheads, which resulted from such factors as having to deal with fewer contracts (and under Total Facilities Management [TFM] or Integrated Facilities Management [IFM] models a single point of contact); less insurance and legal costs; having to manage fewer invoices and be involved with fewer accounts teams and such. Some argued that there was a need for less management and supervisory personnel in the contracted service, and others noted that as a consequence, there was less need for oversight in the client organization when services were managed collectively. Thus:

> *Sometimes (we) bundle security with facilities management, security and cleaning … That brings economies of scale … in the management, one account manager managing both.*
>
> *Senior Regional Facilities Manager, Property Management*

> *Straight away you will get economies of scale, you won't be getting margin on margin or management on management.*
>
> *TFM Director, Facilities Management*

Reducing the number of contractors also meant that the profits each individual supplier had to make could be consolidated; a supplier involved in offering a range of services would be more amenable to reducing its profit margins in return for a larger slice of the available business. Some noted that in a bundle, one service might be charged out at cost in order to generate a profit in other areas, and at least one supplier had this under consideration. Manned guarding was seen as a prime contender here because the margins were so slight that some wondered whether there was a viable future for a single manned guarding service in the mass market in the absence of a change in buyers' behavior.

A second point, and one that implied cost savings but accrued other benefits was the opportunity that bundling provided for improved management practices. Some here pointed to the benefits of instilling a specific corporate style to the provision of services across sites, which becomes especially possible with one or fewer suppliers. In a different way, bundling was perceived as being good for facilitating cooperative working, and this had a number of dimensions. The opportunity to avoid the restrictions implicit in a silo mentality was considered important by providing a platform, via joint management, of encouraging service lines to work together where appropriate. There has been a major emphasis in recent times in various types of collaboration with a range of buzz words to depict various types of co-operation including integration (BSIA, 2007; De Toni and Nonino, 2009), convergence (Hunt, 2010; Willison et al., 2012), and partnerships (Prenzler and Sarre, 2012; Yang and Wei, 2012) to name but a few. Amongst both buyers and suppliers, there was widespread agreement that there was confusion about what these terms meant, but for the purposes of this study, the fact that some type of collaboration was typically a good thing as far as effective security was concerned generated support for bundling.

On the people side, integration typically involved multi skilling individuals, or at least in engaging them with a more varied set of duties. This was seen as an opportunity to build teams with different service lines supporting each other. It provided more varied work for staff, enhanced their commitment and reduced turnover. This applied to management, too, in being able to take on new opportunities with greater responsibility than might otherwise exist. And on the technology side, a number of suppliers (in particular) identified the potential for systems to provide for better integration, and specifically for security systems to enable the better functioning of other systems, more cost effectively and with more benefits than if the services were provided separately. Moreover, it was argued that the integration of technological systems, security with non-security, and security technology with security people facilitated innovation. For suppliers, this was

especially important. Many lamented the growing power of procurement within organizations, which was seen to drive prices and profits down. Some felt that the only way margins could be protected was by being afforded the opportunity to combine technology with manpower.

> *(There are) economies of scale in teams helping out in other areas, multi – cross skilling, if done right, with the right training and skills (means you can) utilize labor better.*
>
> *Security and Operations Manager, Event Centre*

> *Cleaners can be on the look out for any problems and help reduce crime by noticing who should not be in places … On the security side, guards pick up papers as they walk around.*
>
> *General Manager, Security, Shopping Centres*

There was a third major influence behind the move to bundling, and that was the growing expertise of both clients to understand their needs and develop a bundled response, and of suppliers to deliver a range of services under one umbrella. Indeed, some clients noted that they had been drawn to bundled services by developments in the supplier market, and interestingly, some interviewees from overseas (and especially outside major conurbations) lamented the lack of multi service providers to meet their needs. One client noted:

> *Actually, opportunity is the biggest factor here. I have a provider able to provide the solution that drives this largely, and were my contractor not providing this solution, we wouldn't have adopted it.*
>
> *Head of Security, Bank*

> *Security providers were one-trick ponies, just [offering] guards or cameras or intrusion alarms. [Now] more and more companies are becoming a bit of a supermarket, they are moving from [being a] specialism to [a] master of [all] trades. So it makes sense: one source for all or most of services required.*
>
> *Security Advisor, Energy Provider*

Bundling was rarely argued to provide a better quality of security delivery than single service, however, suggestions that quality would be sub-standard in a bundle were refuted; proponents of bundling argued that a good procurement process and effective management can ensure that the quality of service provision is maintained. It was also noted that bundling could facilitate the standardization of processes which improved efficiency and helped to ensure consistently high quality delivery.

<u>The Case for Providing Security Single Service</u>

A major reason why single service was advocated was because it was viewed as a 'best in class' service. This was enabled by security being provided by a specialist security

company and by the service, often the management, not being 'diluted' by the engagement of non-security specialists. Some corporate security managers felt that by first outsourcing and then by placing a Facilities Manager in charge of a company they lost direct control of security operations. This was not always the case; it in part depended on how it was structured and the skill sets of the facilities manager's point of contact. Some corporate security people saw advantages in security being accountable to operational business units rather than them personally, but for many, the distancing of oversight was viewed as a further dilution of security expertise. Some typical comments on this issue from both buyers and suppliers included:

> *I have to say that from a security operational perspective … I see potential for compromise on security delivery and degradation of security … The drive for incorporated FM into a single contract is due to cost, not security efficiency.*
>
> *Head of Security, Telecommunications*

> *I was trying to raise security standards but in an FM bundle there is no focus on one service—jack of all trades—you don't get the buy-in on what you are trying to achieve. I think things have moved on—some reputable companies have been bought out by FM and try to keep (the) specialism but you see them start to be eroded by the FM.*
>
> *Head of Security, Finance Company*

> *Security is a specialist business and it needs a security expert and if you don't value security as a specialist skill, then you won't value us as a security expert.*
>
> *Chief Executive, Security Company (security only)*

> *A FM manager has a different outlook, so his priority is almost certainly not security. Plus that manager may not have security experience first hand so may not have a good idea of risk management.*
>
> *Regional Security Director, Manufacturer*

A second reason why some said they preferred single service was because it led to management efficiencies. Some saw managing the link between security and other facility management services, not least where it involved anything approaching integration, as a complex one. Some suppliers noted that finding good partners was often a challenge, and finding staff that could multi skill (or wanted to) was a challenge. One supplier manager felt that the opportunity to manage a multi skill team had enabled him to develop personally and provided a welcome career fillip, but felt that many others would not feel the same. Moreover, it sometimes meant a dilution of services, as staff were asked to take on additional duties or be deployed in ways that rendered security less of a priority and, at least, involved less focus on security related tasks. In a different way, management of single service was seen to be easier in general because there was a longer tradition of this type of delivery and specifically because there was a direct relationship between the corporate security manager and the security supplier. Some lamented that with suppliers

of multi services, there was a tendency to subcontract some services, and there was always the danger that this might result in a poorer quality service especially if they were focused more on costs than quality, and subcontracting the service area in question was not their specialist expertise. Furthermore, some were against employing one company to undertake a variety of roles, and that was because it entailed 'putting all your eggs in one basket'; in short, this amounted to poor risk management. Finally on this issue, some clients admitted that they were not geared up for anything other than single service, and some suppliers in order to promote their security expertise, were keen to steer clear of any type of service that was not their specialism and in which they were not experts:

> *We use different suppliers for guards, and the contractor who does systems is different contractor and different again for fire. We go with the experts, rather than find a one company fits all.*
>
> *Senior Manager, Facilities, Medical Systems Company*

> *There are merits for buying security alongside waste, cleaning, but we had separate companies. The risk of one company doing it all, is that they generally try to subcontract and so you don't know what you get. But it is cheaper. Specialists really know more about the topic.*
>
> *Operations Services Manager, Blood Service*

A third reason why some buyers and suppliers stated they preferred single service over bundling was because it was more cost effective. They were rarely referring to the price paid here, more in relation to the risks involved in leaving security to a non-specialist company, or overseen by non-security experts noting that the consequences of a security failure can cause unlimited reputational damage and result in lasting and even devastating consequences for the client. It was noted that security experts are better placed to monitor the changing risk landscape and keep abreast of new measures and different ways of working as they evolve. Single service suppliers in particular also noted that cost savings that are perceived to come with bundling could in fact often be achieved by looking at security holistically and relating mitigation measures to risk, and looking imaginatively or innovatively at the use of people and technology. Some argued that this not only avoided a dilution of security, it also afforded an opportunity for clients to make cost savings and suppliers to protect margins:

> *There is a perception that bundled brings huge cost benefits, because it takes away the inefficiencies of multiple managers, sharing back office resources, economy of scale etc. This is a misconception because on larger contracts, if the customer works with you, you … can save cost on single if provider works innovatively with customers.*
>
> *MD, Security Company*

The points that those favoring single service made was that it protected the organization from a dilution of expertise, and suppliers especially promoted the case that if done so imaginatively could be achieved cost effectively and generated management efficiencies.

Suppliers in particular felt the benefits of co-operation implicit in bundling can also be achieved by 'partnerships' and 'joint working arrangements' without diluting expertise.

The point is more important than saving jobs; it was argued that both the status and the effectiveness of security in organizations is enhanced where there is a security specialist or expert on both the buyer and supplier side.

Determining the Strategy and Whether it Works

While it has long been recognized that there can be a variety of influences on strategy (see, Burdon and Bhalla, 2005), in this study, 7 key factors emerged as important. First was the policy of the organization towards outsourcing, and whether there was a well developed strategy that guided policy (see, Nordin, 2006). Some companies had a way of providing services dictated or directed from the center, and this meant there was a reference point for how things should be done, although it seems that most often, even where a strategy/policy did exist, it was flexible (at least as far as security was concerned). Second, some clients recognized that they were only geared-up for single service, and others felt they had developed sufficiently to bundle security. The skill sets of the client are crucial. A third factor was the skill sets of the suppliers and, as noted above, some clients were led towards bundling (both of security and with facilities management) by the competence of suppliers, and some refrained from heading this way because of what they saw as the lack of availability of services to meet their needs in the market. Others had tried bundling and stopped because the service levels were short of their requirements. Where there was a single point of contact—a key benefit of bundling—the competence of that contact could characterize how it was perceived. It is important to note that there are a range of features that combine to make bundling work, including the ability to multi skill or integrate, the ability to find staff including managers who can multi skill and keep them, and to structure the business so that internal competition does not undermine collaboration.

A fourth key factor was the status of the head of the security function, and not least his or her relative status to that of the head of facilities management and procurement. Where security was of a lower status to facilities management, it would often (but not always) reflect an emphasis on bundling compared to single service in outsourcing arrangements. The role of procurement was generally seen to have a major impact, and where procurement was seen to be of a higher status, which is not unusual (Gill and Howell, 2012) then that could lead to a greater emphasis on cost rather than quality. A fifth factor, somewhat following on from this, is the importance of security to the organization. There was a tendency for security to be provided as a single service where it was crucial to the organization, perhaps because of regulatory requirements or because of persistent or serious threats. A sixth factor was the role of security within an organization. Some suppliers, who favored single service noted that they did not see bundling as a problem where there was some form of accountability to, or second best, engagement with a security specialist in the client organization. Many suppliers and some security experts felt the quality of security was diluted where there was a break in the link between internal security and security contractor. A seventh and final point, was the nature of the contract

and whether the focus was primarily on delivering an excellent service or on reducing costs to the maximum extent.

The findings revealed a clear tendency for corporate security directors to favor single service and facilities managers to favor bundling. On the supplier side, specialist security companies generally favored single service and facility management companies bundling. Although this was to be expected, it was not a hard and fast rule. Similarly, there was a tendency for clients and suppliers to highlight different features. So while clients said they favored bundling because of cost savings, efficiencies in delivery, the growing competence of the market, and the opportunity for standardization across sites, suppliers focussed on cost savings, followed by innovation, the benefits of multi skilling staff, and the opportunities for technology. This evidence would suggest that there was more to be done to bring clients' attention to potential benefits. With regards to single service, clients highlighted the value of security as a specialism which should not be diluted, the greater ease and experience of managing single service (in providing a more efficient form of management and a less risky one), and in saving costs in terms of incurring less risk. Suppliers largely agreed, also noting that a focus on security as a specialism additionally protected internal jobs.

Discussion

Security is but one element of facilities management. When asked whether security was different in any way to other services, answers reflected the relative importance of security to the organization. Some felt it was just the same. Where it was different, it was noted that it was regulated (in some countries at least), was a 24-hour requirement (in some cases), and that if it went wrong, it could lead to catastrophe. Others noted that security staff not turning up for work would be less noticed by staff than caterers not providing food, or the air conditioning or company server not working; in short, it varied. And security covers a wide variety of activities. On the technology side, integration is less intellectually problematic to understand (although in practice it is far from commonplace), but the integration of people represents a real challenge, which only some claim was managed effectively.

Certainly the arguments presented in favor of single service, principally that it is best in class, are being challenged by those facilities management providers who believe that multi skilling and integrated services offers a better form of security. On the other hand, the claims of supporters of bundling that it is more cost effective is challenged by single providers who argue the real costs of increased risks and the opportunity for more efficient ways of working offer an alternative perspective. The inclusion of different types of security services in bundling arrangements is not new, but it has received relatively little attention. Although some interviewees claimed that they had noticed a trend towards more bundling over single service, the research approach taken meant that this needs to be substantiated by future studies. However, if it is true, it raises the question as to whether this reflects a structural change in the way services are delivered or is more cyclical and a reflection of the current priorities clients are attaching to cost over risk in choosing how

security is provided. The evidence from this study highlights the lack of a common language to describe outsourcing arrangements, and the paucity of evidence to support arguments for and against different options; there has been little independent evaluation of the claims being made. The aim of the research was not to develop a fact-based model to guide decision-making, a laudable aim though that would be. Hopefully this study has provided a more informed foundation for assessing the implications and potential effectiveness of different models of security service delivery. The benefits and drawbacks of different service options seem finely balanced and need to be better understood if organizations and suppliers are to combine to provide the most effective security.

References

Agndal, H. and Nordin, F. (2009) 'Consequences of outsourcing for organizational capabilities: Some experiences from best practice', *Benchmarking: An International Journal*, Vol. 16:3, pp. 316-334.

British Institute of Facilities Management (2007) *The Good Practice Guide to FM Procurement,* Redactive Publishing Limited.

British Institute of Facilities Management (2012) *FM Categories* (http://www.bifm.org.uk/bifm/knowledge/resources/Categories).

BSIA (2007) *A Guide to Integrated Security Management Systems*, BSIA.

Burdon, S. and Bhalla, A. (2005) 'Lessons from the Untold Success story: Outsourcing Engineering and Facilities Management', *European Management Journal*, Vol. 10:5, pp. 576-582.

De Toni, A.F. and Nonino, F. (2009) 'The Facility Management: Non Core Services Definitions and Taxonomy', in De Toni A.F., Ferri A., Montagner M., *Open Facility Management: a New Paradigm for Outsourced Service Management*, pp. 3-28, MILANO: IFMA.

Drion, B., Melissen, F. and Wood, R. (2012) 'Facilities Management: Lost or Regained?', *Facilities*, Vol. 30:5/6, pp. 254–261.

Feeny, D., Lacity, M., and Willcocks, L. (2005) 'Taking the Measure of Outsourcing Providers', *MIT Sloan Management Review*, Vol. 46:3, pp. 41-48.

Gill, M. (ed) (2014) *The Handbook of Security: Second Edition*, Basingstoke: Palgrave.

Gill, M. and Howell, C. (2012) *The Security Sector in Perspective*. Leicester: Perpetuity Research.

Hassanain, M. and Al-Saadi, S. (2005) 'A Framework Model for Outsourcing Asset Management Services', *Facilities*, Vol. 23:1/2, pp. 73-81.

Hunt, S. (2010) *Convergence: The Semantics Trap,* Online article: CSO Online (available at: http://www.csoonline.com/article/560063/convergence-the-semantics-trap)

Interserve and Sheffield Hallam University (2012) *The Changing Shape of Facilities Management Procurement,* Interserve. (available at: http://www.interserve.com/docs/default-source/Document-List/sectors/commercial/the-changing-shape-of-facilities-management-procurement-march-2012.pdf?sfvrsn=10)

Jain, R.K., and Natarajan, R. (2011) 'Factors influencing the outsourcing decisions: a study of the banking sector in India', *Strategic Outsourcing: An International Journal*, Vol. 4:3, pp. 294-322.

McIvor, R. (2005) *The Outsourcing Process: Strategies for Evaluation and Management*, Cambridge: Cambridge University Press.

McIvor, R. (2008) 'What is the Right Outsourcing Strategy for your Process?', *European management Journal*, Vol. 26, pp. 24-34.

Momme, J. and Hvolby, H-H. (2002) 'An outsourcing framework: action research in the heavy industry sector', *European Journal of Purchasing and Supply Management*, Vol. 8:4, pp. 185-96.

Nordin, F. (2006) 'Outsourcing services in turbulent contexts: lessons from a multinational systems provider', *Leadership and Organization Development Journal*, Vol. 27:4, pp. 296-315.

Oshri, I., Kotlarsky, J., & Willcocks, L. (2011) *The Handbook of Global Outsourcing and Offshoring: Second Edition*, Hampshire: Palgrave Macmillan.

Petry-Eberle, A. and Bieg, M. (2009) 'Outsourcing information Services', *Library Hi Tech*, Vol. 27:4, pp. 602-609.

Prenzler, T. and Sarre, R. (2012) 'Public-Private Crime Prevention Partnerships', in Prenzler, T. (ed) (2012) *Private Security in Practice: Challenges and Achievements*, Basingstoke: Palgrave.

Shekar, S. (2008) 'Benchmarking knowledge gaps through role simulations for assessing outsourcing viability', *Benchmarking: An International Journal*, Vol. 15:3, pp. 225-41.

Varadarajan, R. (2009) 'Outsourcing: Think more Expansively', *Journal of Business Research*, Vol. 62:11, pp. 1165-1172.

Whitaker, J., Mithas, S. and Krishnan, M. (2010) 'Organizational Learning and Capabilities for Onshore and Offshore Business Process Outsourcing', *Journal of Management Information Systems*, Vol. 27:3, pp. 11–42.

Willcocks, L. Cullen, S., Lacity, M. (2007) *The Outsourcing Enterprise: The CEO's Guide to Selecting Effective Suppliers.* Logica in association with the LSE Information Systems and Innovation Group. pp. 10.

Willcocks, L. & Lacity, M. (2009) *The Practice of Outsourcing: from IT to BPO and Offshoring*, Palgrave: London.

Willcocks L, Oshri, I & Hindle J (2009) *To Bundle or not to Bundle? Effective Decision-making for Business and IT Services,* Accenture.

Willcocks, L., Oshri, I., & Hindle, J. (2009b) *Client's Propensity to buy Bundled IT Outsourcing Services*, White Paper for Accenture.

Willcocks, L and Lacity, M. (2011) 'What Suppliers would tell you if they Could', *Outsourcing*, Issue 6, Autumn. pp. 6-14.

Willcocks, L and Lacity, M. (2012) 'What Suppliers would tell you if they Could 2', *Outsourcing*, Issue 8, Spring. pp. 28-34.

Willison, J., Kloet, F., & Sembhi, S. (2012) *Security Convergence and FMs: the Learning Curve*, Online article: Ifsec Global (available at: http://www.ifsecglobal.com/security-convergence-and-fms-the-learning-curve/)

Yam, T. (2012) 'Economic Perspective on Outsourcing of Property Management Services', *Property Management*, Vol. 30:4, pp. 318-332.

Yang, C. and Wei, H. (2013) 'The Effect of Supply Chain Security Management on Security Performance in Container Shipping Operations', *Supply Chain Management: An International Journal*, Vol. 18:1, pp. 74–85.

About the Authors

Professor Martin Gill is a criminologist and Director of Perpetuity Research which started life as a spin-out company from the University of Leicester. He holds honorary/visiting Chairs at the Universities of Leicester and London. Martin has been actively involved in a range of studies relating to different aspects of business crime, including the causes of false burglar alarms, why fraudsters steal, the effectiveness of CCTV, the victims of identity fraud, how companies protect their brand image, the generators of illicit markets and stolen goods, to name but a few. Martin has been extensively involved with evaluation research and with the offender's perspective, looking at how they target certain people and premises and aim to circumvent security measures. He has published 14 books including

the second edition of the 'Handbook' of Security' which was published in July 2014. Martin Gill is a Fellow of The Security Institute, as well as a member of the Company of Security Professionals (and a Freeman of the City of London). He is a member of both the ASIS International Research Council and the Academic and Training Programs Committee and a Trustee of the ASIS Foundation. In 2002 the ASIS Security Foundation made a 'citation for distinguished service' in 'recognition of his significant contribution to the security profession'. In 2009 he was one of the country's top 5 most quoted criminologists. In 2010 he was recognised by the BSIA with a special award for 'outstanding service to the security sector'. In 2015 IFSEC placed him in the top 10 most influential fire and security experts in the world.

Charlotte Howell is Research Manager at Perpetuity Research. She has conducted a wide range of projects on crime and security including consulting with offenders, victims, security professionals and the police. Charlotte also manages the running of the Secured Environments accreditation—a police accreditation run by Perpetuity Research on behalf of the Association of Chief Police Officers. Charlotte holds a first class LLB (Hons) in Law and an MSc in Criminology.

Journal of Physical Security 8(2), 15-36 (2015)

How Social Media is Transforming Crisis Management and Business Continuity

Gerald D. Curry, James J. Leflar, Marc Glasser, Rachelle Loyear,
Briane Grey, Tim Jordan, Leonard Ong, Werner Preining, and Jose Miguel Sobron*

ASIS International Crisis Management and Business Continuity Council

Key Words-
Social media, emergency operations, crisis management, emergency management, disaster

Terminology-

Social Media: an aggregate term for networking sites, messaging sites, texting, and other web-based or mobile technologies that support social interaction. Examples include Facebook, YouTube, Twitter, Instagram, Google+, LinkedIn, Plus, Tumblr, email, etc.

Emergency Operations: this term was selected to encompass the many similar terms such as emergency management, crisis management, business continuity, disaster management, disaster recovery, and emergency planning. The differences between these terms is often discipline- or industry-driven, but the differences do not justify using all of the terms when describing emergency operations. Emergency operations are the managerial functions charged with creating the framework that helps organizations, communities, and individuals reduce vulnerability to hazards, and cope with disasters.

---

* All of the authors are active members of the ASIS International Crisis Management and Business Continuity Council. This study, conducted as a Committee project of the Council, was unfunded and is free of any known conflicts of interest.

The American Society for Industrial Security (ASIS) International is a prominent professional security organization with Chapters and Councils. The Crisis Management and Business Continuity Council promotes crisis management, business continuity, and organizational resilience standards and best practices worldwide. More information about ASIS International is available at https://www.asisonline.org/Pages/default.aspx.

Author affiliations:
Gerald D. Curry, DM, Environmental Management Office, Safeguarding and Security, Department of Energy.
James J. Leflar, Jr., MA, CPP, CBCP, MBCI, Senior Physical Security Consultant, Zantech IT Services.
Marc Glasser, MS, CPP, Managing Director, Resilience Management LLC.
Rachelle Loyear, MBCP, MBCI, PMP, Enterprise Director, Business Continuity Management, Time Warner Cable.
Briane M. Grey, Senior Vice President, Director of Corporate Security, City National Bank.
Tim Jordan, B.A., AMBCI, Senior Consultant, Automation Consulting Group, GmbH.
Leonard Ong, CPP, ASIS International Information Technology Security Council.
Werner Preining, CPP, ASIS International, Chapter Chairman, Austria Chapter 107.
Jose Miguel Sobron, Department of Safety and Security, United Nations.

Abstract

The purpose of this paper is to investigate social media usage in crisis management planning, response, and recovery activities. Social media usage during an emergency event to gather immediate information has been demonstrated as an alternative when traditional forms of communication have been less effective. Most of the messages transmitted using (or through) social media are from non-traditional media sources, and the medium has become an expected source for traditional news agencies, as every cellular smart device user in the world has the potential to be an information broadcaster. This research survey explores the role social media is having on crisis management for security professionals. Survey participants consisted primarily of ASIS International members.

Introduction

Social media is being leveraged across global disciplines or industries, and according to an overwhelming majority of ASIS International security professionals who participated in this study, an established practice has been laid in emergency operation planning. The purpose of this paper is to explore and report the varying means by which social media is being used by practicing professionals for generating alert messages, confirming personnel and other asset accountability, and keeping key stakeholders—including the general public—informed on crisis events.

This study uses a mixed methods (quantitative and qualitative) research design to analyze the survey results. The qualitative section of this paper identifies thematic topics that point to the depth of social media frequency and the quality of its use. Several questions were asked of 154 participants who confirm their acceptance of this tool as an information channel. Additionally, the survey addresses the future of how social media will be used to help security professionals achieve their protective responsibilities.

This paper uses a traditional research model and format in discussing the highlights of the survey. The qualitative section sets the foundation for this paper, as the survey participants help the reader to better understand the reasons and rational of "how" and "why" social media is being incorporated into emergency management, including preparedness and mitigation planning. The data collected are rich in critical information for discovering new social media techniques as it pertains to contingency operation planning, and for determining the depth to which social media is currently being utilized. The qualitative research methodology offers the opportunity to review the data from a shared perspective, by reducing limits and potential research barriers.

We did not develop a particular theory, but rather offer security-practitioner perspectives on how social media is being utilized in emergency management. Additionally, the results will reveal how social media is being used throughout the emergency operations industry by expediting alert messaging. This study offers new insights on the tremendous possibilities for the use of social media platforms in emergency management.

The quantitative section of this paper summarizes the depth of this study by reviewing the strength of social media's application in real world scenarios. However, it was not enough to gather data on whether or not social media is saving lives. Also needed was an examination of how is it being used, and at what frequency. These questions were all important, and helped to direct the research to a stronger, more applicable conclusion.

The sample size for this research was 154 participants. The majority of participants were ASIS International members. This study provides an in-depth description of the social media domain within the dealings of these security professionals.

This study leverages quantitative methods to determine statistical results and qualitative research to explore social media's usage, in hopes of developing a comprehensive understanding. We hope this study will serve to inspire future studies on this subject.

Our study divided the analysis of questions into qualitative and quantitative in order to explore the full spectrum of inquiry. Social media has received significant societal attention. Social media has also completely changed the way people engage one another and. more importantly, how businesses connect with potential clients and customers. Social media has become the one common denominator that the world's citizens understand and use on a daily basis. The preferred online applications may change from country to country, but the basics of being able to reach mass numbers of people quickly has been accomplished through social media.

Purpose of the Study

The purpose of this study was to document established ASIS International security professionals' social media processes, identify frequency of social media use, and help provide a global perspective to improve contingency operations. Additional research opportunities are identified later in this paper; these will lay the foundation for security professionals to identify and potentially benefit from further social media benefits applicable to security professionals worldwide.

Social media has rapidly become a societal norm (Kaplan, 2012), and it is important for security professionals to assess its use. The Department of Homeland Security's Federal Emergency Management Agency (FEMA) reports that, "Social media is a new technology that not only allows for another channel of broadcasting messages to the public, but also allows for two way communication between emergency managers and major stakeholder groups." (FEMA, 2015, paragraph 1). The social media technology is still considered to be in its infancy and thus requires dedicated exploratory research.

This study examines the utility of social media in emergency management by security professionals, so industry leaders can predict its current and long-term applicability. Often, new technology comes and disappears just as quickly as it arrives. Social media seems to be significantly different; this study concludes that many security professionals around the world are using some aspect of social media for emergency notification, keeping

stakeholders engaged, and making critical documents more accessible. Our study aims to expand the conversation on social media being used in emergency management.

Literature Review

There is an enormous amount of literature on social media and its increased utilization in emergency management. This study leveraged the closest and most relevant resources to expand the narrative pertaining to this important topic. The survey was used to better understand and identify the professional pervasiveness of the platform, assess if the tools are embedded in current policy, and explore future possible applications of social media. The literature used in this study aims to better understand these three tenets, and confirm the research results.

Kaplan (2012) offers an overview in his "Social Media In Emergency Management: A Quick Look," and suggests social media can be used as a means for public service announcements, a dependable resource for information for emergency responders, and can provide immediate feedback for all stakeholders through its crowdsourcing capabilities. Additionally, Kaplan (2012) validates the fact that social media has quickly become the subject of vigorous academic and professional studies. In fact, FEMA Administrator Craig Fugate uses his Twitter application to converse with industry professionals and the general public.

Su, Wardell, & Thorkildsen (2013, page 1) in their work simply titled, "Social Media in the Emergency Management Field, 2012 Survey Results," announces that "…76% of adults responding to a 2012 American Red Cross survey expected help to arrive in less than three hours if they post an emergency-related request on social media." The study solidifies the fact the public has a psychological expectation that once they post an emergency message in social media, the official authorities will acknowledge it and respond appropriately. Su, et al. (2013) shares the finding that social media has created an expected demand by the public, and an additional platform for emergency management professionals.

One critical question this survey asks is, "How knowledgeable are emergency management agencies regarding social media?" In Su, et al. (2013, page 2) the researchers do not stop there however; they continue to examine the issue by identifying the governance, technology, data/analytics, and processes that must be used to fully embrace social media.

DHS (2012) uses their "Next Steps: Social Media for Emergency Response, Virtual Social Media Working Group and DHS First Responders Group," to navigate the future of social media in emergency management. The DHS report recognizes that many United States government officials are turning to social media technologies to share information and connect with citizens during all phases of a crisis. In response to the global attention social media has drawn, the U.S. Department of Homeland Security's Science and Technology Directorate (DHS S&T) has established working groups to provide guidance and suggest best practices for emergency preparedness and the response community. The DHS study concludes by highlighting six steps DHS needs to focus on: (1) Choosing the right

technology and application; (2) Developing strategy, policy, and procedures; (3) Setting and managing expectations; (4) Engaging the community; (5) Managing misinformation; and (6) Addressing challenges to adoption, including concerns related to privacy, public comment, record retention, public disclosure, health information, human resources, information technology, and security.

The USDE/REMS (2013) presentation accurately sums up the progress made to protect school children and teachers. The presentation provides an understanding of the benefits and challenges associated with employing social media in school crises. It builds on the traditional four phases of emergency management: prevention-mitigation, preparedness, response, and recovery. The presentation notes that in the aftermath of the Columbine High School shooting, and other horrific events that have occurred, social media use is gaining traction. The presentation confirms that 96% of young adults ages 18-29 own a smart device of some kind, and 73% of online teens (age 12-17) use social networking sites. The report highlights the fact that teens from lower income families are more likely to use online social networks (4 in 5).

Lindsay (2011) starts his discussion by confirming that social media is playing an increasing role in emergencies and disasters. His report cites research from Information Systems for Crisis Response and Management (ISCRAM) and the Humanitarian Free and Open Source Software (FOSS) Project, both groups that are exploring related linkages. The author shows how social media is being used in one of two ways: first, to disseminate information and receive feedback, and second, as a systematic tool to conduct emergency communications, such as issue warning messages, receive victim requests for assistance, monitor activities, establish situational awareness, and create damage estimates. Social media has created a broad platform for emergency management professionals. Lindsay's report summarizes how social media is being used by management officials.

Hiltz, Kushma, and Plotnick (2014) offer a very unique opportunity of semi-structured interviews of U.S. public sector emergency managers to determine the use, and potential barriers to using, social media. They point out three barriers to social media use, which are (1) a lack of personnel time to work on social media, (2) a lack of policies and guidelines, and (3) concerns about trustworthiness of collected data. While these barriers or challenges are very real, social media usage continues to grow to epic proportions.

One significant point Hiltz, Kushma, and Plotnick make is that even with the millions of people who are flocking to social media sites, the government has yet to establish an emergency management platform. Additionally, they cite Kavanaugh (2012) who reported that social media is not being used in a particularly thoughtful or systematic way (Hiltz, Kushma, & Plotnick, 2014, page 602). The Hiltz, Kushma, and Plotnick (2014) study focuses solely on two important questions: (1) what problems or barriers do these managers perceive in terms of using social media, particularly for gathering and acting upon real-time disaster posts in them?; and (2) what is their reaction to several potential types of tools that might enhance their use of social media? This research concludes that the lack of trained personnel is the primary reason the government has not fully embraced social media (Hiltz, Kushma, & Plotnick, 2014). This technology is dependent on

professional security managers and leaders who have the technical know-how to enhance operations internally, externally, and with key stakeholders.

Methodology

The ASIS International Crisis Management and Business Continuity Council (CMBC) developed a 17-question survey and received answers from 154 security professionals from across the globe who occupy security positions in federal, state, local, and private company positions. See the Appendix for the survey questions. The web-based survey was available from July 6 to September 1, 2014, via Survey Monkey. The survey team published the link to CMBC members, who in turn shared the link with ASIS Chapter members and business colleagues who are associated with ASIS International.

We believe the survey received a fairly wide distribution within the limited ASIS related population, but there is no indication of the total number of recipients. We estimate at least several hundred recipients, and likely many more. The recipients and participants had some relationship to ASIS International, either as members or as professional colleagues of the research team, but there is no way to know the identities of the participants. The participants were anonymous, and the survey was completely voluntary. Participants were assured that any personal identifying information they provided would be kept confidential, and the final responses would be presented in aggregate form. We cannot make any claims concerning the participant's representativeness of security professionals within a general population.

The participants consisted of 118 ASIS International members and 35 non-members. It should be noted that the 35 non-member participants who engaged in the study are security professionals, just not members of ASIS International. Approximately 91.9% of the participants have been members of ASIS International for over five years, and 100% actively worked in a security or crisis management position as their primary profession.

Interestingly, 58.3% held a professional certification such as the Certified Protection Professional (CPP), Certified Business Continuity Professional (CBCP), Master Business Continuity Professional (MBCP), or Certified Emergency Manager (CEM). 59.3% described their profession as security (non-data). This classification of security becomes interestingly important because it is used as an umbrella term, and translated to capture several security disciplines. Almost all participants held some level of college education, 84.2% held a bachelors, masters, or doctorate degree.

The qualitative section asked 5 open-ended probing questions to better understand the progress that has been made in emergency operations by adjusting to the society demand for social media. These questions very purposefully explored the depth of each participant's professional involvement, including their participation in drills and exercises that leveraged social media. As with any survey, some participants failed to answer all questions, so we cannot determine or remark upon their responses to those questions. Several themes were garnered from the written responses that were provided, and these will be discussed in the next section.

The quantitative section explored each participant's online application preference, and then shifted the inquiry to examine their exposure to social media being used in emergency operations practical applications. Discovering the depth and frequency of social media use is important in understanding the professional commitment to adapting policies by localizing procedures. This quantitative exploration validates the critical impact social media is having on how society views official authoritative response and recovery operations.

Denise Rousseau's Psychological Contract helps us understand when and how an individual's belief in mutual obligations between that person and another party, such as an employer or agent of the government, is expected (Rousseau, 2000). This expectation of mutual obligations can be easily illustrated in the federal response to Hurricane Katrina. The citizens in the region held an expectation that it was the government's responsibility to provide for those individuals stranded in New Orleans and the impacted surrounding area.

The mixed methods process of using a qualitative and quantitative approach allows this research to explore social media usage in emergency operations applications. Additional details are offered throughout this study to expand on the use and future applications of social media. In the analysis section of this paper, more emphasis is placed on the importance of communication and the need to hear feedback from citizenry. Social media has become prevalent in society by becoming the preferred method for connecting with people, and for government agencies connecting to people within their jurisdiction of responsibility.

Qualitative Summary

Previous generations witnessed technological advances resulting in the progression from direct, limited, interpersonal communication (word of mouth, lectures or speeches, and town criers) to more remote or extended forms of transmitting information (print, telegraph, radio, cinema, and television.) As technology has increased in complexity and capability, the time needed to send a message to an audience has reduced significantly. The Internet and social media platforms in particular have allowed a message from any individual to reach millions of people around the world almost instantly. Social media via the individual (as in-person) has become firmly entrenched in modern society as a primary method of communication and has helped decrease the time needed to inform a society of an event. This individual or personal ability to become a reporter of news information has dramatically changed the way large audiences receive their current events information.

When reviewing the data gathered in this survey, strong evidence shows unique themes from the participant's responses. Question 13 was: Based on your experience as an emergency professional, have you participated in emergency risk operations using social media? The reason for this question was to explore the participant's familiarity of using social media first hand, and not relying on things they heard, read, or perceived from other agency's participation. It was important to have authentic experiences in using social media on a daily basis or routinely.

One participant commented that social media was used as the primary way to communicate during the Japanese Tsunami, as well as leveraging global geolocation online applications to identify victims in need. Another confirms that social media was used during Hurricane Sandy's recovery operations. It is apparent from the data that social media has found a significant use in emergency operations, and is used routinely as appropriate.

The qualitative (open-ended) questions were developed to elicit more information from the respondents concerning their respective experience and opinions with social media usage in conjunction with an emergency event. There are 154 respondents to the survey, but approximately 35% of the respondents skipped the qualitative questions. Since there is no way to know the reasons for skipping the questions, those "skipped" responses have been deleted from the total. Allowing such unanswered or meaningless data to remain as part of the total responses would skew the distribution. Removing the "skipped" respondents provides a more accurate and meaningful interpretation of the data, but also creates a slight inequality in the totals for each question. The total number of respondents for each question does not equal the same amount; the totals range from 95 – 105, with the median equal to 98.

Table 1 - Responses to Open-Ended Opinion Questions

Response Categories	Participant Response
Q13: Based on your experience as an emergency professional, have you participated in emergency risk operations using social media? Please explain its use.	
Never used social media for an emergency event	52%
Used social media for general warnings notifications	22%
Q14: Based on your experiences, do you believe social media should receive more of a priority in preparing for emergency risk operations?	
Positive desire to develop social media as a priority	32%
Develop and establish more controls to vet information, develop infrastructure stability, and organizational controls for reliability	22 %
An efficient method of disseminating information	13 %
Q15: Based on your experiences, do you think social media can	

enhance or cripple emergency risk operations?

Enhancement	60%
Of those indicating enhancement, respondents claim excellent situational awareness and dissemination tool	29%
Of those indicating enhancement, emergency risk operations if properly managed with appropriate policies and coordination by the organization	28%
Will cripple emergency risk operations	5 %
As to enhancement or cripple, it depends on the quality and tone of the messages	30%

Q16: Based on your experiences, do you think more demands will be placed on emergency managers if social media is applied to emergency risk operations? Please explain why or why not.

Will see fewer demands on their time	14%
Will be an increase in work demands	61%
Of those indicating an increase in work demands, the increase will level off and become a routine part of the emergency manager's job	6%

Q17: What recommendations do you have for emergency managers desiring to use social media?

Organizations should embrace social media as part of the official organization with policies and procedures to support the effectiveness of social media usage	35%
Researching and following the lessons learned from other organizations has value	18%
Social media usage should be an integral part of the organization managed by a specially trained team or department such as Corporate Communications	23%

Of the respondents indicating a preference to the question of social media use during an emergency, 52% have never used social media for an emergency event. 22% indicated they have used social media for general warnings or notifications.

When asked for an opinion on establishing social media as a priority resource during emergency risk operations, 32% of the respondents indicated a positive desire to develop social media as a priority. 22% expressed a desire to develop and establish more controls to vet information, develop infrastructure stability, and organizational controls for reliability. 13% responded that social media was an efficient method of disseminating information.

When asked to comment on whether social media usage will enhance or cripple an organization during an emergency, 60% indicated enhancement and only 5% clearly indicated that social media will cripple emergency risk operations. 30% responded that it depends on the quality and tone of the messages. Of the 60% indicating social media will enhance capabilities during an emergency, 29% believe it is an excellent situational awareness and dissemination tool, and 28% expressed the opinion social media will enhance emergency risk operations if properly managed with appropriate policies and coordination by the organization.

Whereas 14% of respondents for question 16 indicated emergency managers will see fewer demands on their time if social media is integrated into emergency risk operations, 61% believe there will be an increase in work demands. The increase in demands involves a management responsibly for the integration of social media into emergency operations, as well as ensuring the accuracy of the information. Of the 61% indicating an increase in work demands, 6% believe the increase will level off and become a routine part of the emergency manager's job.

When asked for recommendations to managers wishing to use social media, 35% indicated that organizations should embrace social media as part of the official organization with policies and procedures to support the effectiveness of social media usage. 18% suggested that researching and following the lessons learned from other organizations has value. According to 23% of the respondents answering Question 17, social media usage should be an integral part of the organization managed by a specially trained team or department such as Corporate Communications.

This study confirmed that social media is establishing its place in emergency operations planning and execution. Undoubtedly, communication efforts have improved with emergency alert messaging, offering feedback to local citizens, potential victims, and other stakeholders who may be impacted by the event. Emergency operations professionals may require additional training to learn how to best create alert messaging, and ensure communication lines are established with citizens before, during, and after the crisis event. Approximately 25% of the participants have not used social media. It will prove interesting to track this trend over the coming years to determine if social media use among emergency operation professionals is increasing or decreasing.

Summary

This study is constructed using a sampling of ASIS International security professionals and related colleagues. We distributed the survey to professional associates and ASIS Chapter members. We promoted a wider distribution of the survey to any emergency operations professionals. In the analysis section, we attempt to make sense of the collective summary of both areas.

The questions selected for this quantitative review were purposefully designed to be more objectively structured, rather than the more discussion-based (subjective) format experienced in the qualitative section. The following section will emphasize the analysis of data that will combine the qualitative themes and the quantitative statistical analysis of the findings.

The following are the results of the respondent's responses. The average score for each question is calculated based on a scale of 0 to 4, where 4=Strongly Agree, 3=Agree, 2=Disagree, 1=Strongly Disagree, and 0=Not Sure. The scale is 0 to 3 for Yes (3), No (2), Potentially (1), and Not Sure (0).

Table 2

Question 1 Responses: Social Media Will Increase Efficiencies in Emergency Risk Operations, Average Score = 2.97

Answer Choices	Responses	Participants
Strongly Agree (4)	33. 6%	50
Agree (3)	51.0%	76
Disagree (2)	4.0%	6
Strongly Disagree (1)	2.0%	3
Not Sure (0)	9.4%	14
Total	100%	149

Table 3

Question 2 Responses: Use of Social Media During Emergency Risk Operations, Average Score = 3.07

Answer Choices	Responses	Participants
Strongly Agree (4)	30.2%	45
Agree (3)	57.1%	85
Disagree (2)	6.0%	9
Strongly Disagree (1)	2.7%	4
Not Sure (0)	4.0%	6
Total	100%	149

Table 4
Question 3 Responses: Participated In an Emergency Risk Operation Event(s) When Social Media Was Used, Average Score = 2.34

Answer Choices	Responses	Participants
Yes (3)	47.0%	70
No (2)	43.0%	64
Potentially (1)	7.3%	11
Not Sure (0)	2.7%	4
Total	100%	149

Table 5
Question 4 Responses: Social Media Requires Emergency Managers Embrace New Processes, Average Score = 2.50

Answer Choices .	Responses	Participants
Yes (3)	75.2%	112
No (2)	2.0%	3
Potentially (1)	20.8%	31
Not Sure (0)	2.0%	3
Total	100%	149

Table 6
Question 5 Responses: Social media will revolutionize emergency risk operations, Average Score = 2.80

Answer Choices	Responses	Participants
Strongly Agree (4)	26.2%	39
Agree (3)	55.0%	82
Disagree (2)	4.0%	6
Strongly Disagree (1)	2.0%	3
Not Sure (0)	12.8%	19
Total	100%	149

We found the quantitative data to be most useful in illustrating the depth of social media usage, and deciding future applications. This study would be incomplete if a quantitative process was not included. There are significant common strands of data extracted from the participants that are of interest. The data structure used in this study compliments the interpretation of various types of data, and offers a platform for future studies.

Analysis

The data collected in this research illustrate that social media is still in a developmental stage, and that technology has not yet been fully exploited to fulfil its potential (Dantas,

Seville, Nicholson, 2006/Field, 2010). This understanding offers an introduction into the application of social media worldwide, confirming that social media is playing a significant role in all phases of emergency management planning, mitigation, response, and recovery. Social media's application has found a permanent home in contingency planning, yet still needs further development. This invention continually provides a forum for people from all walks of life to connect globally in real-time. For example, emergency planners have the opportunity to explore new ways of standardizing notification protocols, deepen response coordination, and confirm evacuation reporting.

The data validate security professionals' view of social media as a communication tool. The majority of the participants reported that stricter usage controls are needed in order for social media to have an effective role in contingency management. In the qualitative section, several themes evolved from the participants: (1) Social media expedites citizen notifications and enhances community awareness; (2) Solid guidelines are needed to ensure message consistency and reliability; (3) Privacy safeguards are necessary to ensure technology platform trustworthiness. Each of these themes is critically important to creating an industry foundational approach to social media policy governance. Resilience and consistency in social media application and execution will yield tremendous results as technology evolves.

Also found in the survey results was a reluctance from many of the participants to completely embrace social media. Several participants expressed the need to hold onto the "old" ways of doing things, because everyone does not have access to social media or newer technology. This hesitancy is prudent in the sense that it is taking some communities decades to firmly find their way with newer technology applications. Managers should be mindful of duty-of-care responsibilities towards employees during an emergency and ensure that advances in technology are included in procedures and processes. Collaborative techniques are required and building partnerships will require new alliances to be successful.

Another element that surfaced in the data is that maintaining the ability to manage information was viewed as paramount. According to survey participants, while crisis managers cannot control individual citizens input, the messages being relayed from authoritative sources must be consistent and reliable. Most importantly, it must be trustworthy. Multiple resources are needed to combine data streams that will ultimately improve data management. Creating in-depth feedback protocols will be necessary to understand developments and concerns from residents actively being impacted by the crisis.

Emerging Trends

Social media is well established and significant. Various new online applications are being released daily, to ease public access to important information and establish linkages to people and data. One of the toughest dilemmas society has is balancing the ability to process huge amounts of data with determining the trustworthiness of that data (Cullen, 2010). As technology increases, the amount of data will surely increase. Emergency

managers will need to create social media platforms they intend to use, and then popularize those sites for the public to use in times of crisis.

Several social trends and business patterns are developing due to interest in social media. Today, more people are connected together than ever before. Social media appears to be the mechanism for linking together people from various cultures from around the world, where learning is taking place in complex industries such as medicine, science, technology, politics, and various forms of academia. Progress in these industries cannot occur without considering advancements made in emergency operations. Social media allows people to become familiar with one another on various levels.

The majority of the initial evidence used to prosecute the defendants in the Boston Marathon bombing case was received from various everyday citizens who took YouTube videos, tweeted on Twitter, and leveraged footage from surveillance cameras (Crumpacker, 2014). Disasters are being captured on individual smart devices by those closest to the event while it is occurring. There is an abundance of 9-1-1 calls received in a timely manner because of people's access to smart devices. Social media and computer technology have completely changed the emergency operations industry, and it has modified the behavior of emergency managers and the public. People are connecting with public officials by sending files when an event occurs, and expecting emergency operation agencies to be just as responsive by returning feedback or a response if something adverse is reported.

Individuals in the public, private, and non-profit sectors are using social media as a common tool. Social media is being leveraged by police departments to hunt down criminals by reviewing their online profiles. According to the International Association of Chiefs of Police (IACP) in their 2014 report on emerging technologies, approximately 55.8% of police departments surveyed actively use social media in the performance of their duties (IACP, 2014). First Responders are using social media to determine the propensity of a company or person's actions, while conducting mitigation planning. It is estimated that by 2030, every living adult human (worldwide) who is capable will have a smart device equipped with online access and emergency alert applications (Su, 2013). This smart device availability will increase crisis event reporting, as well as periodic updates when adverse activities occur. The entire spectrum of situational awareness will surely overwhelm existing protocols and communication systems, unless deliberate actions are taken now or in the near term to improve and increase functionality in the long term.

Conclusion

Social media is a developing phenomenon and useful platform that is securing its place in society by connecting people from various walks of life. This research emphasizes that social media has a permanent place in helping security professionals achieve effective contingency planning, orchestration, and crisis management. According to the participants in this study, more can be done on various levels, starting with establishing stricter guidelines governing the use and application of social media.

Security professionals realize that additional learning will be required to fully embrace and exploit social media online applications. Approximately, 75.2% agreed that more knowledge is required to expand social media to a wider audience in emergency operations. 81.2% either agreed or strongly agreed that social media has the ability to revolutionize emergency risk operations. In an effort to move the professional initiatives forward with social media in emergency operations, a deliberate strategy is required to properly advance. Participants agreed that more needs to be done, but whose responsibility is it? ASIS International has a legacy of leading the way by establishing professional security certifications and international training opportunities for a broader audience. It is advisable that ASIS International or a similar security organization work to promote social media guidelines for use in emergency operations.

Social media has found its place in emergency management, and the research participants view social media as a communication tool, but feel more controls in respect to confidentiality and privacy need to be established. This study confirmed purposeful educational programs are necessary if social media is to be used wholesale in emergency management. Additionally, social media offers the ability to receive instant feedback from those most impacted by the event. This new level of public access will apply new pressures on emergency management professionals not experienced before (Hiltz, 2014).

Over 100 participants in the study requested new tools to effectively manage social media. These tools included mobile training teams designed to educate communities, communication feedback platforms in the form of online applications, and websites to help collect data. No single initiative or tool was identified as the primary focus to improve social media applications. It was apparent that social media is having a tremendously positive impact on emergency managers, but there was a clear reluctance to accept social media protocols wholesale.

Social media offers real-time information that can be processed immediately, and contribute value to the overall operations. The question of social media saving lives was not answered in this study, but if the right platforms are created and fully exploited (e.g., the Internet of Things), it may be possible. Incident Commanders (i.e., Emergency Managers) require critical information, and it is possible for social media to expedite the amount of information they receive. The emergency operations industry should have a responsibility and a business opportunity to create new methodologies, applications, and data strategies that will enhance overall contingency operations.

This research study addressed several critical elements and current practices within emergency operations as it applies to social media. The participants in this study were all professionals who actively contribute every day to the safeguarding and security of people and property. Their participation in this study is appreciated as they help educate colleagues worldwide. More research in this area is necessary, and it was the aim of this study to begin a meaningful conversation. Social media is making a positive difference in emergency operations, yet still has a way to go before being completely transformed into common practice.

References

Bamberger, M. (1999). Integrating quantitative and qualitative research: Lessons from the field. Washington, DC: World Bank.

Bertot, J., Jaeger, P., Grimes, J. (2010) Using ICT to create a culture of transparency: e-government and social media as openness and anti-corruption tools for societies. Government Information Quarterly, Science Direct. Available from http://www.elsevier.com/locate/govinf

Callahan, M.E. (2010). Haiti social media disaster monitoring initiative, Office of Coordination And Planning, Department Of Homeland Security. Washington DC: Government Publishing Office.

Cameron, M.A., Power, R., Robinson, B and Yin, J. (2012). Emergency situation awareness from Twitter for crisis management. Proceedings of the WWW 2012- SWDM '12 Workshop, Lyon, France, ACM, 695-698.

Coombs, T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. Corporate Reputation Review, 10, page 163-176. Retrieved from http://www.palgrave-journals.com/crr/journal/v10/n3/full/1550049a.html

Crowl, T. K. (1996). Fundamentals of educational research (2nd ed.). Chicago, IL: Brown & Benchmark Publishers.

Intelligence Community, Central Intelligence Agency, Department of Justice, Department of Homeland Security, (2014). Unclassified summary of information handling and sharing prior to the April 15, 2013 Boston Marathon bombings. Washington, DC: Government Publishing Office. Retrieved from http://www.justice.gov/oig/reports/2014/s1404.pdf

Cullen, J. (2010). When bloggers and tweeters attack! Social media and the organizations reputation. Retrieved from http://www.theicor.org/art/present/art/ARCMC00067.pdf

Dantas, A., Seville, E., Nicholson, A. (2006). Information sharing during disaster: Can we do it better? Retrieved from Resilient Organisations Research Report: http://www.resorgs.org.nz/images/stories/pdfs/information_sharing_during_disaster_resorgs_06_02.pdf

Department of Homeland Security (2012). Next steps: Social media for emergency response. Virtual Social Media Working Group and DHS First Responders Group, Science and Technology Group. Retrieved from http://www.ghinternational.com/docs/DHS_VSMWG_Next_Steps_Social_Media_Strategy_Formatted_May_2013_FINAL.pdf

Department of Homeland Security. (2014). Using social media for enhanced situational

awareness and decision support: Virtual Social Media Working Group and DHS First Responders Group. Retrieved from http://www.firstresponder.gov/TechnologyDocuments/Using Social Media for Enhanced Situational Awareness and Decision Support.pdf

Federal Emergency Management Agency (2015) IS-42: Social media in emergency management. (Emergency Management Institute, Independent Study-42). Retrieved from http://training.fema.gov/is/courseoverview.aspx?code=is-42

Field, T. (2010). Social media: What every senior leader must know: Interview with Prof. Sree Sreenivasan of the Columbia Graduate School of Journalism. Retrieved April 15, 2013, from the CU INFO SECURITY website: http://www.cuinfosecurity.com/social-media-what-every-senior-leader-must-know-a-2421

Fraenkel, J.R., & Wallen, N.E. (1996). How to design and evaluate research in education (3rd ed.). New York: McGraw-Hill.

Gonzales-Herrero, A., Smith, S. (2008). Crisis communications management on the web: How internet-based technology are changing the way public relations professionals handle business crises. Journal of Contingencies and Crisis Management, 16 (3), 143-153. Available from http://onlinelibrary.wiley.com/doi/10.1111/j.1468-5973.2008.00543.x/abstract;jsessionid=1686BDD5693F10317EE456BC1E947AC0.f03t04

Goolsby, R. (2010). Social media as crisis platform: The future of community maps/crisis maps. ACM Transactions on Intelligent Systems and Technology, 1(1), Article 7. doi:10.1145/1858948.1858955.

Hiltz, S.R. and Gonzalez, J.J. (2012). Assessing and Improving the Trustworthiness of Social Media for Emergency Management: A Literature Review, in: V.A. Oleshchuk (Ed.) Proceedings, NISK, AkademikaForlag, Trondheim, Norway, 135-145.

Hiltz, S., Kushma, J., Plotnick, L. (2014). Use of Social Media by U.S. Public Sector Emergency Managers: Barriers and Wish Lists, The 11th International USCRAM Conference-University Park, Pennsylvania, USA, Retrieved from http://www.iscramlive.org/ISCRAM2014/papers/p11.pdf

IACP (2014). International Association of Chiefs of Police 2014 Social Media Survey Results. Retrieved on January 22, 2015, from http://www.iacpsocialmedia.org/Portals/1/documents/2014SurveyResults.pdf

James, E., & Wooten, L. (2009). Leadership in turbulent times: Competencies for thriving amidst crisis. Working Paper Series, Paper No. 04-04, Darden Graduate School of Business Administration, University of Virginia. Richmond, VA. Available from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=555966

Kaplan, E. (2012). Social media in emergency management: A quick look. Homeland Security Studies & Analysis Institute, Retrieved from: http://www.homelandsecurity.org/docs/reports/RP11-01.01.05-01_A Quick Look_30Nov12.pdf

Kavanaugh, A. L, Fox, E. A., Sheetz, S.D., Yang, S., Li, L.T., Shoemaker, D. J., Natsev, A. and Xie, L. (2012). Social media use by government: From the routine to the critical. Government Information Quarterly, 29, 480-491.

Krigsman, M. (2009). IBM: IT failure and social media disaster. Retrieved April 15, 2010, from ZDNet website: http://www.zdnet.com/article/ibm-it-failure-and-social-media-disaster/

Lindsay, B. (2011). Social media and disasters: Current uses, future options, and policy considerations. (CRS Report for Congress, 7-5700, R41987). Retrieved from Congressional Research Service website: https://www.fas.org/sgp/crs/homesec/R41987.pdf

McKinney, K. (2011). Quantitative analysis and reporting: Telling a story with numbers. Assessment Institute, Chicago.

McMenamin, J. (2015) Social media during disaster response: A lawyer's perspective. Retrieved March 10, 2015, from the Disaster Resource Guide website: http://www.disaster-resource.com/index.php?option=com_content&view=article&id=856:social-media-during-disaster-response-&catid=9:crisis-response

Owyang, J. (2008, December 1). How municipalities should integrate social media into disaster planning {Web log post}. Retrieved from http://www.web-strategist.com/blog/2008/12/01/how-municipalities-should-integrate-social-media-into-disaster-planning/

Palen, L. (2008). Online social media in crisis events. EDUCAUSE Quarterly, 3, 76-78. Retrieved from https://net.educause.edu/ir/library/pdf/eqm08313.pdf

Ray, A. (2008). Social media disasters (or how not having a social media strategy can hurt). Retrieved April 15, 2010, from the Social Media Today website: http://www.socialmediatoday.com/content/social-media-disasters-or-how-not-having-social-media-strategy-can-hurt

U. S. Department of Education (2013). Social media in school emergency management: Using new media technology to improve emergency management communications. Retrieved from U.S. Department of Education, Office of Safe and Healthy Students, Readiness and Emergency Management for Schools (REMS) Technical Assistance (TA) Center website: http://rems.ed.gov/docs/Training_SocialMediaInEM.pdf

Rousseau, D. (2000). Psychological contract inventory technical report. Retrieved from

http://vodppl.upm.edu.my/uploads/docs/dce5634_1298965643.pdf

Su, Y. S., Wardell III, C. and Thorkildsen, Z. (2013). Social media in the emergency management field: 2012 survey results. (IPP-2013-U-004984/Final report). Retrieved from CAN website:
https://www.cna.org/sites/default/files/research/SocialMedia_EmergencyManagement.pdf

Sutton, J., Palen, L., Shklovski, I. (2008). Backchannels on the front lines: Emergent uses of social media in the 2007 Southern California Wildfires. Proceedings of the 5th International ISCRAM Conference – Washington, DC. Retrieved from
https://www.cs.colorado.edu/~palen/Papers/iscram08/BackchannelsISCRAM08.pdf

Vila, S. (2010). NGOs must harness social media beyond disaster relief. Retrieved April 15, 2014 from the PBS Media Shift website:
http://www.pbs.org/mediashift/2010/02/ngos-must-harness-social-media-beyond

Wagstaff, K. (2014) The Internet and the World Wide Web is Not the Same Thing, NBC News, Retrieved October 18, 2014 from http://www.nbcnews.com/tech/internet/internet-world-wide-web-are-not-same-thing-n51011

York, B. (2010). Advertising age: McDonald's names first social-media chief: Hire of Rick Wion, Founding Member of Digital Task Force, comes after a year spent devising strategy. Retrieved April 15, 2014 from the Advertising Age website:
http://adage.com/article/digital/marketing-mcdonald-s-names-social-media-chief/143248/

Appendix

The following survey questions were used to develop the data in this study:

1. Are you a current member of ASIS International?
   Yes
   No, please go to question 3.

2. How long have you been a member of ASIS International?
   Less than 1 year
   1 – 5 years
   6 – 10 years
   11 – 15 years
   More than 15 years

3. What is/are your main duties? (Select all that apply)
   Security Management (inclusive of Business Continuity)
   Security Management (exclusive of Business continuity)
   Business Continuity Management/COOPS
   Crisis Management
   Physical Security
   Others (Please specify) _____

4. Do you hold any of the following certifications? (Select all that apply)
   Certified Protection Professional (CPP)
   Certified Business Continuity Professional (CBCP)
   Master Business Continuity Professional (MBCP)
   Certified Emergency Manager CEM)
   Other relevant certification (please specify) _____
   No

5. How do you describe your professional discipline? (Please select the primary choice)
   Security (non-data)
   Disaster Recovery
   Business Continuity/COOPS
   Crisis Management
   Security (data or network)
   Others (Please specify) _____

6. Do you hold any of the following degrees? Please indicate your highest, completed degree.
   Bachelor degree
   Graduate/Master degree
   Post-graduate/Doctorate degree
   Professional Certificate
   Others (Please specify)

7. What social media platforms do you use (either for personal or work)?
   LinkedIn
   Twitter
   Facebook
   Instagram
   Blog websites (e.g. Bloggers, Wordpress, etc.)
   Private platform
   Others (please specify) _____

(Quantitative Questions)

Number	Question Text	Potential Responses
8	Based on what you know or have experienced, social media will increase efficiencies in emergency risk operations.	4—Strongly Agree 3—Agree 2—Disagree 1—Strongly Disagree 0—Not Sure
9	Do you agree or disagree with using social media during emergency risk operations?	4—Strongly Agree 3—Agree 2—Disagree 1—Strongly Disagree 0—Not Sure
10	Have you participated in an emergency risk operations event(s) when social media was used?	3—Yes 2—No 1—Potentially 0—Not Sure
11	Will social media require emergency risk operations managers to embrace new processes?	3—Yes 2—No 1—Potentially 0—Not Sure
12	Social media has the ability to revolutionize emergency risk operations.	4—Strongly Agree 3—Agree 2—Disagree 1—Strongly Disagree 0—Not Sure

(Qualitative Questions)

Q13: Based on your experience as an emergency professional, have you participated in emergency risk operations using social media? Please explain its use.
Q14: Based on your experiences, do you believe social media should receive more of a priority in preparing for emergency risk operations?
Q15: Based on your experiences, do you think social media can enhance or cripple emergency risk operations? Please explain why.
Q16: Based on your experiences, do you think more demands will be placed on emergency managers if social media is applied to emergency risk operations? Please explain why or why not.
Q17: What recommendations do you have for emergency managers desiring to use social media?

Viewpoint Paper

The New ASIS Standard on Risk Assessment*

Roger G. Johnston, Ph.D., CPP
Right Brain Sekurity

The new ASIS International standard for Risk Assessment is out. (ANSI/ASIS/RIMS RA.1-2015.) Here is my take on it.

Like a lot of ASIS "standards", this is less of a technical standard or set of suggestions than an intelligent mapping out and general discussion of the subject area. There is the usual multitude of bland platitudes and mundane shopping lists. Also like many other ASIS standards, there is an obsession with scope, documentation, and establishing complicated business "programs" for security, rather than focusing on practical advice about how to engage in the necessary actions. Effective risk management involves subjective value judgments, but this is given somewhat short shrift.

The standard seems to underemphasize the role of vulnerability assessment in the risk assessment/management process. For example, "threat analysis" is defined in the list of terms but not vulnerability analysis or assessment. The discussion in Section 6.4.4.1.3 of Vulnerability/Capability Analysis is somewhat confused about what a vulnerability assessment is about. It focuses more on threats, assets, and consequences than vulnerabilities, and encourages letting the existing security thinking, strategy, and infrastructure define the vulnerabilities. Unfortunately, the bad guys get to do that.

Risk itself is rather oddly defined as the "effect of uncertainty on the achievement of strategic, tactical, and operational objectives." Uncertainty isn't what causes harm, the threat does. Under this definition, worries within an organization about possible security shortcomings—which might be very healthy—would be considered risk.

The standard endorses the use of Gap Analysis, but I have always found this kind of approach to be dangerous because it engenders binary thinking about security. Security is actually a continuum, not a matter of gaps or no gaps.

On the plus side, the standard's call for outside, independent risk assessors with no conflict of interests is specific and praise-worthy. The recognition of the detrimental effect that cognitive bias has on risk management is surprising and welcome. There is a strong

---

* *This viewpoint paper was not peer-reviewed. The author participated in a minor way in the early stages of the standard development. ASIS International is the American Society for Industrial Security, a trade group of security professionals.*

and appropriate emphasis on identifying and documenting assumptions. Overall, the discussion is well organized and fairly well-written (both of which are difficult to do by committee), and covers many important points.

At $135, the 138-page standard is expensive to order, but much less expensive by a factor of 2-8 than many shorter and less thoughtful standards issued by other organizations. Moreover, ASIS International members can download one copy of the standard for free.

Despite its problems and limitations, the Risk Assessment standard is a significant contribution to thinking about security, and well worth a read.

About the Author: Roger G. Johnston, Ph.D., CPP was the head of the Vulnerability Assessment Teams at Los Alamos National Laboratory (1992-2007) and at Argonne National Laboratory (2007-2015). Currently he is editor of the Journal of Physical Security, and CEO of Right Brain Sekurity (http://rbsekurity.com), a company devoted to creative security solutions.

Viewpoint Paper

Why I Hate Security*

Steve Hunt, CPP, CISSP

Hunt Business Intelligence
http://www.huntbi.com

These criticisms are nothing new. You've heard them all before, or muttered them under your breath. If you are a business executive, you've shaken your head when you've seen it. And if you are a security professional, you're guilty of more than one:

- "I hate security."
- Much of what passes as security is no more than window dressing, or, as Bruce Schneier has called it, “Security Theater”, with its posturing, phony controls and security guard bravado.
- Not a week goes by that a CIO or other executive hears a pitch from a security vendor, whose eyes are bugged out as their words ooze fear, uncertainty, and doubt (FUD).
- Security directors, including some of the most esteemed CISOs, can be seen from time to time running the halls, arms flailing overhead, screeching, "The sky is falling! The sky is falling!"
- Risk management experts talk for hours about the "fuzzy logic" of measuring impact and likelihood, using game theory, and generally talking until the audience goes numb.
- And when the big one happens, when the big data breach hits, as it inevitably does, security pros and business executives alike point fingers at budgets, and internal politics, and vendor missteps for blame.

So I am here to give you the straight dope. To address all of these complaints once and for all. To put the discussion to rest so we can all move on.

Security is all those things. Security is often mere theatrics. Vendors do commonly sell

---

* *This viewpoint paper was not peer-reviewed. It is reprinted from an essay posted on LinkedIn.*

FUD in place of value. Risk management experts do often employ pseudo science "to definitively calculate" intangible and unknown risks. CISOs do sound like Chicken Little when they predict the things we simply aren't prepared for and need more budget for. And security pros do like to find a scapegoat.

All of these things are true, and security deserves its criticism.

Personally, though, I look at it differently. Security is something special to me. For example, when I see a CISO work his or her way out of a messy data breach by responding quickly, limiting impact, and recovering smoothly—it gives me a very satisfied feeling. Moreover, when I think of my own career as a security professional, I think of the truly costly and damaging attacks that we've avoided by working hard to improve continuously.

In the early 1990s, I worked at a financial institution in Chicago. We got hacked—before we even had the word "hacked." The bulletin board server was fine yesterday, but today it isn't, and the audit log is gone. As we scratched our heads an ol' timer leaned over us and said, "Looks like you got a security problem with your computer."

I was stunned. I had never considered security and computers in the same thought before. My father was a locksmith, and I had worked my way through college and grad school at the University of Chicago with my own locksmith company and building PC clones on the side. So when I heard those words, a light bulb went on. I thought to myself, I know security, and I know computers. Right then I began retooling for a career in computer and network security. Right place. Right time.

So security gave me an entree into the world of the fledgling Internet, and into the world of creating value for the business in ways I never could have imagined before that fateful day, seated cross-legged on the floor, under a desk, staring blankly at the back of a bulletin board server.

Security also did much more than that. It solved real problems. From the script-kiddies of the '90s to the state sponsored hacking of the 2000s, security gave hundreds of professionals an opportunity to fight in very foreign territory—guerrilla IT warfare. We created a new way of operating the Internet, and we opened doors permitting businesses to create value and revenue in new ways. For example, the security community put its collective head together, limiting loss sufficiently to make online commerce (once called e-commerce) a reality.

Converged approaches to physical and cyber security for the decade beginning 2001 created an amazing new world of inter-networked security cameras, intrusion detection, gates, fences, locks, employee ID badges, laptops, personal devices, and home automation controls. Everything was suddenly networkable because the basic questions of authentication and authorization (who are you?, and what are you supposed to do?) were answered by security professionals.

Today, we are coming up with clever ways to extend the work we did previously and apply it to the Internet of Things (IoT). Soon, we will see alternatives to keys and locks being used widely in the secure networking of any and every common device at home or sensor on a locomotive. Homes will operate more efficiently and businesses will make countless billions in new revenue because of IoT. This is possible because the security industry truly is doing its best.

Does security have its foibles? Is it Security Theater laced with FUD, bad logic and blame? Yes. But does it create value that outweighs its sometime silliness? Yes it certainly does. For me personally, it has provided me many benefits and opportunities, making me a better philosopher of technology, a better technologist in general, a better citizen of the world, a better provider for my family.

So the next time you sit through another ridiculous vendor pitch about all the bad things that will happen if you don't buy their product: use your phone to securely transfer funds at your bank, or buy a gift for your kid on Amazon, or plan the next product launch with confidence that the security pros have your back.

About the Author: Steve Hunt, CPP, CISSP is Principal Consultant at Hunt Business Intelligence (http://www.huntbi.com), which focuses on cyber security, physical security, data analytics and business intelligence.

Viewpoint Paper

WIPP May be the Best Place for Weapons-Grade Waste*

Editorial Board, Albuquerque Journal

There are some important details that don't quite make the talking points of what to do with the nation's nuclear waste, those being:

It has to go somewhere, most of where it is now is not good or safe or responsible, and New Mexicans have offered the only permanent solution.

The nation's more than 70,000 metric tons of used reactor fuel is now kept in temporary facilities in 39 states—some sites adjacent to rivers or on top of water tables. The nation's 55 metric tons of surplus weapons-grade plutonium is kept in bunkers at the Energy Department's Pantex warhead assembly-disassembly plant outside Amarillo, Texas, and in an old reactor building at the Savannah River Site.

Those aren't permanent solutions, and the nation's $15 billion permanent plan, Yucca Mountain, remains the largest, most expensive and emptiest parking garage ever. A close second is the $4 billion incomplete "mixed oxide" fuel, or MOX, facility in South Carolina that would convert the plutonium for use in commercial nuclear power plants. Since its designation in a 2000 arms-control agreement with Russia, the price tag for the MOX facility has ballooned from $1.5 billion to between $7 billion and $30 billion.

So it is important not to blindly follow former New Mexico Gov. Bill Richardson's lead in dismissing the Waste Isolation Pilot Plant (WIPP) as a final resting place for diluted weapons-grade plutonium in favor of a MOX plan that may never happen. MOX was approved when Richardson was U.S. Energy secretary, though now even his former employer, DOE, is looking at storage alternatives including WIPP.

That is likely in part because of the increasing MOX construction price tag, in part because no utility has stepped up to say it will use the MOX fuel, and in part because while WIPP was shuttered after a 2014 truck fire and drum radiation release, there has been serious, ongoing scrutiny to ensure its policies, procedures and contractors are on track.

And it is likely also in great part because southeastern New Mexico has become home to nuclear experience and expertise, with WIPP, the $4 billion Urenco USA uranium

---

* *This viewpoint paper was not peer-reviewed. It is reprinted with permission of the Albuquerque Journal from an editorial by the editorial board printed on September 26, 2015.*

enrichment plant, a proposed $100 million International Isotopes plant to process spent uranium from Urenco, a proposed $280-million-plus Holtec International Inc. underground storage site for used reactor fuel, and a proposed spent-fuel storage facility run by Waste Control Specialists and French firm AREVA Inc. just across the Texas state line.

As Richardson cautions that DOE will make the WIPP facility a high-level waste dump, Carlsbad leaders are welcoming the idea of downblending the nation's weapons-grade plutonium with inert materials so it can be permanently disposed of at WIPP.

Mayor Dale Janway has written to NIMBY Senate Minority Leader Harry Reid, D-Nevada, that "if non-proliferation is your intent, then the clear path forward is disposal in WIPP. This is a national decision, we recognize that. But we are a community of taxpayers, within a state of taxpayers, and we volunteered to host a defense-only deep geologic waste disposal facility that permanently removes risk from the biosphere."

Southeastern New Mexico has done more than any other community, company or government leader to offer a safe, long-term storage solution to the tens of thousands of metric tons of nuclear toys the nation has left lying around. Its weapons-grade proposal deserves serious consideration and, if approved, remuneration.

.

Viewpoint Paper

The IoT and the Ability to Defend Against the Silent Intruder

Lillie Coney
coney.lillie@gmail.com

Chair of the IEEE Par 1912 Privacy and Security Architecture
for Consumer Wireless Devices Working Group

Introduction

A Working Group on Privacy and Security Architecture for Consumer Wireless Devices—based upon the IEEE Project Authorization Request 1912 (P1912)—first met in July of 2015. The purpose of the Working Group is to develop a Standard for Privacy and Security Architecture for Consumer Wireless Devices. The Institute of Electrical and Electronics Engineers (IEEE) is a professional association with more than 400,000 members worldwide. It supports the educational and technical advancement of electrical and electronic engineering, telecommunications, computer engineering, and allied disciplines.

The resulting P1912 architectural standard will establish a common communication protocol to enable relationships among disparate consumer digital wireless technologies and devices. The architecture envisioned by P1912 will permit control over devices, through the use of unique identifiers, which are inherent in wireless technology or can be assigned by individuals, through subnets or private geo/location-proximity fencing protocols. Individuals will be able to establish an array of subnets, among two or more devices, to support the equivalent of private GPS systems within a radius, defined by radial points, bounded interior spaces, or geo-locations.

Where has digital communication been, and where is it going?

The network computing communication environment evolved from rivers and streams of information formed by two-way data flows over coaxial cable or twisted pair connections among networked devices. Later, these rivers and streams formed ponds, pools, or lakes created by wireless area networks. Today, we are on the verge of creating vast oceans of digital data rich environments that will cover a home, office complex, industrial park, city blocks, towns, cities, or nations depending on the resources allocated and the innovations that will be enabled by the Internet of Things (IoT).

We may be fast approaching the verge of a global civilization that would have the capability if not the will to account and chronicle all activity on a micro- and macro-level. The ability to collect detailed bits on a granular level combined with the IoT could enable the collection of many bytes of data regarding human beings at nearly every stage of life.

The projection of the capabilities and qualities of computing into physical space will allow for the collection, retention, analysis, and sharing of information on health, education, abilities and deficits, successes and failures—in short each life could be an open book. The IoT will not only create pools of data that isolate each person's life experiences, but will place those life experiences in the context of places, things, events and other lives both close and distant.

In 2010, a research project funded by the *Wall Street Journal* generated enough topics for the paper to publish a series of stories entitled, *What They Know*. The *Wall Street Journal's* series was made possible by the broad adoption of smartphones, which are the leading wireless personal computing device constantly in the hands of individuals. Smartphones encompass every form of human communication conceivable. Smartphones enable two-way wireless sharing of data, which include audio, video, photographic, text, and visual content.

The study of smartphone usage is revealing the lives of people as they are described through the data on devices, as well as their location and proximity to other devices. These data are further augmented by how smartphone usage changes overtime as well as individual user's reaction to data received or sent. Human relationships observed by researchers with access to moment-by-moment smartphone usage data for both casual and very intimate communications reveal more than most would assume possible.

Those responsible for the physical security of companies engaged in sensitive negotiations; or on the verge of mergers, acquisitions or other major activities should take note. Leaking of sensitive information or the warnings about potential problems may come by many means, including changes in smartphone usage patterns among key employees.

Before the full realization of the IoT, there is already so much data that human beings are unable to process it—which is why terabytes of data are being stored until technology and innovation can catch up. It is inevitable that the terabytes of knowledge collected by IoT fed networks or cloud servers will have to yield analysis, decision-making, and actions to be taken to automation. However, before that day arrives, there is work that must be done to make the IoT secure end-to-end: its applications, firmware, and hardware must be trustworthy, resilient, privacy-centric, and cyber secure—which is the goal of P1912.

How will we know when the IoT age of ubiquitous computing arrives?

The full integration of the IoT in every aspect of daily life will be silent with the exception of glitches or problems that are too public to ignore. There will not be an IoT drum roll, but there will instead be the introduction of once physical tasks being performed by automated processes. Initially the tasks removed from the list of routine human control such as turning on lights or adjusting the temperature of a room may be noticed, but quickly the novelty will fade and future iterations of the technology and innovation will remove the physical controls without much notice. As more functions are taken over that once

performed by maintenance and custodial staff, the only people who may notice are those who work unscripted staff hours.

Municipal governments leading the way on IoT adoption

The pace that municipal governments are moving to invest in ubiquitous wireless access for residents—coupled with the growing number of private and quasi-private wireless networks offered by tourist areas, private venues, and businesses—will continue to expand IoT infrastructure. Some of the first beneficiaries may be the budgets of governments that can remove the cost of paying for meter readers and traffic enforcement officers from the mix, and let the computing functions of automobiles deal with wireless sentries stationed within a jurisdiction when vehicles are illegally parked or exceeding the speed limit. Governments could be attracted to the potential income and the ability to incorporate a more just policy for awarding tickets and fines.

The days of the night watchman may be numbered as well. What company will resist cutting night security personnel for a 24/7 live feed with in a sensor network that is ever present throughout the physical space that is to be secured?

Citizen-consumers will benefit from the IoT as their daily routines can be synchronized to the level of a senior executive working at a large firm, or that of the head of a government department or agency. Individuals can experience the benefits of a minute-by-minute synchronized life as the movements of a bus is tracked and synced with the pre-determined arrival time desired, which movement can be used to adjust when the alarm will sound, when the coffee or tea maker will start its cycle, when the water will be heated for a shower, and when (if necessary) a message is sent to a supervisor updating them on arrival status.

Why is P1912 needed to secure physical space?

The security of physical space is about to inherit many of the security vulnerabilities that plague cyberspace; perhaps some new threats will arise that have not been considered before the existence of a pervasive ever-present wired physical world. The threats posed to computing devices include viruses; worms; Trojan horses; botnet creation, capture, and exploitation; pharming; phishing; denial of service attacks; and other cyber security threats executed by internal and external sources that intend to undermine the proper functioning of physical security that incorporates or relies upon computing devices. These are only the things that people may attempt who intend to do harm, but threats can extend to actions by insiders that cause harm without the intent to do so.

There are a range of threats presented by unintended actions by insiders that include introducing devices into the work IoT environment that carry exploitable vulnerabilities that could be seized upon by opportunistic applications or technology that probe the

environment for stray information to collect and report back to cloud services or networks hosted by data and financial thieves.

Physical security in IoT environments will present challenges because of the number, diversity, and fluidity of digital technology that will traverse physical spaces. Another challenge will be the speed that devices will change; the ability or willingness of manufacturers or providers to update software on every type of IoT device; and to what degree remote actors (such as criminals, nation/states, or intellectual property thieves) may be able to explore potential vulnerabilities in larger, more complex systems by using very simple IoT-enabled technology.

Unfortunately, individual control over the data that may be collected from an insecure router may be limited—this was the argument made after it was discovered that Streetview technology collected data from unencrypted private wireless routers in the homes or businesses on streets it was mapping.

Businesses large and small will adopt IoT technology without hesitation because of the tremendous opportunities for cost savings. Lowering electricity bills based on actual usage; smart light bulbs that reduce output or completely turn off when sensors in a space indicate that it is unoccupied; employee credentials that not only act as a time clock, but a location service while employees are at work; and sensors that regulate the function of everything from water coolers to elevators base on a "just in time delivery" of only what is needed and exactly when it is needed.

This will usher in an opportunity for much of life's reflexive responses to changing conditions in the physical environment to become seamlessly automated: e.g., changing the thermostat or micro-interior climate control features that allow for settings based on the number of occupants in a room or space.

Innovation will move at unprecedented pace, as new physical designs for everyday consumables will be changed to work as a node in the Internet of Things. The same light bulb from the same manufacturer will now have a wireless interface that allows it to send and receive wireless communications. The same is true for the fleet of vehicles large and small that are used by employees on or off the campuses of companies or organizations.

In this fast paced environment, one of the important protections for digital communications may not be available either through design or due to the limited capacity of the IoT device. Password protection may be unavailable for many passive IoT wireless devices and this may further challenge physical security.

Exploitation of weaknesses found in the poor, or inefficient design of software or IoT device security may facilitate broader discussions about its implications for physical vulnerabilities and security threats. The IoT appears to be about to project the power of computing into physical space without much consideration for the totality of the vulnerabilities and threats that may be imposed on once controlled and secure environments.

There will be no barriers within the IoT that will preserve physical security of businesses, government, or personal spaces unless they are created through broad voluntary adoption of standards that work both in theory and practice to address real-world challenges to physical security, privacy, or confidentiality.

Why should the security and privacy of IoT technology matter to physical security?

Physical security relies upon control over who or what can enter or exit a defined area or space. The challenge to physical security posed by the IoT is a lack of security over the wireless communication signals and/or devices that may enter or exit a space. The following are incidents that foreshadow some of the challenges to physical security in a world dominated by the IoT. Security professionals responsible for facilities that rely on industrial control systems should be aware of new paths that may be used to access networks to cause disruptions to threats posed by cyber attacks that can result in physical damage to equipment.

A light bulb exploit

In 2014, it was reported that a LiFX system of wifi remote controlled light bulb designed to work with a smart phone had a security vulnerability. Sensors on light bulbs designed to operate in conjunction with a smart phone offered an opportunity for a breach of other systems. The problem was discovered in the bash shell of applications that translates commands from a device's operating system, in this case the command to a light bulb to turn on or off. The problem is that the bash shell program also queries the device for additional information that it will then automatically collect and take into the operating system interacting with the light bulb. The extra information could include malicious code in the form of a computer virus, worm, Trojan horse, or other code that, once behind the firewall of a computer network, could do harm. This is a real threat and one that has no solution at present, and may be hard to detect if it has been exploited. We may not know for months if thieves have used it and what the outcome in damage might be.

IoT enabled intercom systems (baby monitoring technology)

In September 2015, two years after the first cyber security warning regarding the security vulnerability of baby monitoring technology, it was reported that 9 baby monitor models for top manufacturers remain vulnerable to hacking. There are documented cases of monitors being breached, allowing unauthorized voice communication from hackers over the communication system, and external access to video live feeds from baby's rooms.

Physical security of vehicles is in question

In 2015, researchers gained remote access to a Jeep Cherokee and took control of physical functions such as climate control, windshield wipers, and the sound-system. They could even turn off the engine while the vehicle was in motion. Automobile manufacturers, not just of the Jeep Cherokee, understood that the computing systems of their vehicles could be compromised and took action to close the cyber security risk that had consequences for the physical security of their vehicles and the safety of their customers.

Physical security of industrial control systems

In 2010, Stuxnet—roughly 500 kilobytes of code—became known to computer security experts who identified it as a hybrid computer-worm designed to destroy physical equipment. Its target application was reported to be the gas centrifuges used by Iran to enrich uranium. Stuxnet was released in 2005 and is believed to have caused significant damage to the equipment used by Iran to reportedly enrich uranium based on reports by U.S. and Israeli officials, as well as the Institute for Science and International Security, an independent think tank. Iranian officials acknowledged the Stuxnet worm was founded in industrial software used to operate centrifuges in their Natanz nuclear facility. A report by the Institute for Science and International Security assessed that 1,000 of 8,000 centrifuges at the Natanz nuclear facility had to be replaced, and by November, Iran suspended enrichment due to technical problems with its centrifuges.

According to a September 2010 Symantic report, there were 100,000 Stuxnet-infected computers worldwide of which 60,000 were in Iran. The Stuxnet is stealth, and until some worm is discovered that can do stealth better, it is at the top of the food chain for worm code. Stuxnet moved from system to system through connected and unconnected computing technology using the Microsoft Windows Operating System. If a machine was not connected to a network, sticking a USB drive into an infected machine, then into the uninfected machine was sufficient for Stuxnet to spread. Once Stuxnet is inside of a machine or network, it replicates itself.

Stuxnet also sought out "Siemens Step7" software, which was also Windows-based and used to program industrial control systems that operate equipment. This allowed for the hackers to collect data on the machines operation, and take control of the machine—giving it instructions that in the case of the centrifuges exceeded safe operational parameters.

Researchers who studied the Stuxnet code for months believe its origin is the United States and Israel, while others attribute the source to China. Russia also has the capability to develop the weapon. The lack of attribution by those who released Stuxnet makes it impossible to definitively place blame.

However Stuxnet began, by 2012 United States government officials started to warn of a "Cyber Pearl Harbor". Stuxnet is not limited to harming the function of gas centrifuges used to enrich uranium, but can damage or destroy machines or equipment controlled by industrial control systems used for a range of non-military purposes. The capacity of Stuxnet to destroy equipment or make it unusable poses a threat to physical security.

According to the IEEE Spectrum article, *The Real Story of Stuxnet*, its path into systems took the route of most predatory worms—it exploited one or more vulnerabilities in the host system. In Stuxnet's case, it used 4 "zero day" vulnerabilities, which were previously unknown or were never widely used that could attack or infiltrate Microsoft Windows operating systems. Typically, these types of vulnerabilities are used to steal credit card information, personal identifiable information on customers or clients, intellectual property, or financial transaction data for monetary gain.

In the case of Stuxnet, the zero day exploits were used to implant a stealthy malicious worm program that would cause physical damage to property. In short, Stuxnet was written to damage another nation's critical infrastructure, but it could have been written to damage a competitor's assembly line equipment, a distiller's processing machinery, cloth maker's weaving machinery, any number of food processing or storage processes, water treatment facilities, or electricity generation capacity. The list of potential Stuxnet targets is nearly inexhaustible the more technologically advanced the society.

Once Stuxnet entered the operating systems, it spread to control systems with a specific mission to disrupt or destroy physical equipment by tricking the system into thinking one set of physical facts are true regarding the state or condition of the system, and then the system's computer automated program components took action. The action taken is what caused the damage because the underlying facts accepted by the system as being true were in fact false. In other words: if a convincing lie can be told to an industrial control system, then the system can be tricked into harming itself.

There is one additional worm program addressed in the IEEE article, "Flame," which is about 40 megabytes in size and is believed to be an earlier version of the now infamous Stuxnet. The Flame worm was design to collect data and send that information to its sponsors in small amounts overtime to avoid detection. This spyware worm could exchange data wirelessly with Bluetooth-enabled devices further than the standard communication range up to 2 kilometers if a directional antenna linked a Bluetooth computer. In the days of war driving, a Pringles-can would suffice as an antenna for an unsecure Bluetooth wireless router or hub.

The Flame worm appears to have been introduced through an update to Microsoft's Windows 7 operating system, which is phenomenal because to get Windows Operating system to accept an update it has to authenticate that the request source of the update is legitimate. The only way to get the Windows Operating system to do this is to have the encryption key that Microsoft uses to secure its operating system, which should only be known by Microsoft.

Microsoft would have a secure algorithm and would rely upon a highly secure key that would require significant computing capacity to acquire the key through brute force attack. It would be hard to imagine that Microsoft would not have taken precautions against an insider threat, so that leaves open the question of who would have the resources to expend to get Microsoft's Window's operating system update key.

Stuxnet or Flame worms can be altered to attack a wide range of industrial control systems or critical infrastructure. Stuxnet-derived worm code could be written to damage water treatment and delivery systems, electricity delivery systems, industrial control systems used by food processors, ports operations, or automobile assembly lines.

Laying the ground work for seeking out vulnerabilities to exploit and therefore to defend, Hungarian researchers in September 2011 uncovered "Duqu" a program that was designed to steal data regarding industrial control systems.

What will be the IoT physical security challenges of complex operations?

Thinking about this question gave me pause because the ubiquitous IoT is not yet present to learn what it will mean to have a wireless communication-rich environment without a single entity empowered to control it. Fortunately, there is some research on a major critical infrastructure area of concern for cyber safety and security—deep-water and container ports.

Title 33, Chapter 29, Section 1502 of the United States Code defines a "DEEPWATER" port as "any fixed or floating manmade structure other than a vessel, or any group of such structures, that are located beyond State seaward boundaries and that are used or intended for use as a port or terminal for the transportation, storage, or further handling of oil or natural gas for transportation to or from any State." The definition "includes all components and equipment, including pipelines, pumping stations, service platforms, buoys, mooring lines, and similar facilities to the extent they are located seaward of the high water mark" and cover water ways to depths of 30 feet or more that can manage ships that are the maximum size that the Panama Canal lock systems can handle.

There are also container ports located on land built to manage large volume container cargo, as well as industrial and manufacturer products that comprise high-volume sea commercial imports and exports. Hundreds of millions of twenty-foot equivalent units or containers are processed by ports around the world each day.

The security of deep-water and container ports have been wedded from their earliest beginnings because cargo was personal wealth and nation-state commerce. The volume of activity at deep-water and container ports made innovation and computing necessary for automation of facilities to management port functions. However, no one system manages everything that happens at deep-water and container ports. Arrivals and departures may be managed by one system; loading and offloading by another entity; container management by another provider; employee access by another system; and private companies may track their cargo using proprietary systems.

The number, type, and severity of cyber threats experienced by ports, service providers or port customers are unknown. The preference is not to report incidents and to pay or absorb costs resulting from breaches or thefts. The other reasons for underreporting is likely that companies and ports are unaware that their cyber security has been breached. An October 15, 2014, report by CyberKeel entitled, *Maritime Cyber-Risks*, reported on financial thefts; alteration of carrier information regarding cargo location; barcode scanners use as hacking devices (a variation of the light bulb vulnerability described above); targeting of shipbuilding and maritime operations; cyber enabled large drug smuggling operations; compromising of Australian Custom and Border protection; spoofing a vessel Automated Identification System (AIS); drilling rig cyber attack; vessel navigation control hack; GPS jamming; vulnerabilities in the Electronic Chart Display and Information System; and a Danish Maritime Authority breach.

Man-in-the-middle attack

The financial-based maritime cyber risk is the same in regards to motivation and intent—theft from bank accounts by tricking a legitimate company into paying funds into an illegitimate account held by thieves who are posing as a trusted business partner. The FBI issued a warning in December 2013, using 3 cases as examples that cost $1.65 million in transfers to thieves. These were man-in-the-middle attacks where the thieves inserted software in the e-mail communications of a company and waited for legitimate communications that bank account information had changed for an existing business relationship. At that point, they would insert themselves into the exchange and provide erroneous bank account information after intercepting the communication with the correct bank account change information. They would then confirm the receipt of the change of account information to the source of the change request. When payments were eventually sent, they went to the thieves' account and not the business that should have been paid.

It is important for businesses to note that U.S. financial protection laws that are used to cover personal losses due to identity theft associated with credit cards do not protect thefts from businesses, including for businesses that process EMV credit cards (chip and pin) on non-EMV compliant devices.

Deletion of carrier information

In August 2011, an incident of deletion of carrier information regarding the location of cargo occurred against the Islamic Republic of Iran Shipping Lines. The attack damaged all the data related to cargo ship contents, which meant that no one knew where any containers were or the status of containers—off-loaded, picked up, or still onboard ships. The data was eventually recovered, but the disruption in operation of the business was significant.

Barcode scanner hacking tool

The attack was named "Zombie Zero" and involved malware hidden in the software for barcode scanners of at least 8 different companies. The malware activated when the barcode readers were connected to company networks. When connected, the malware launched a series of automated attacks searching for the location of the financial server. Upon location of the financial server, the malware would compromise the target server to be taken over. One account of this attack had the company's control over their financial server transferred to a server in China. The CyberKeel report stated that, "The manufacturer providing the scanner was also located in the same physical area as the location of the remote control."

Australian customs exploit

A cyber-crime organization breached the cargo system of Australian Customs and Border Protection, which allowed criminals to verify that their shipping containers were viewed as suspicious by the police or customs authorities. This allowed criminals to abandon contraband that would result in arrests or confiscation and focus on what they knew would be released without difficulty.

Spoofing AIS

Automated Identification Systems may be used for entities managing fleets of vehicles, or access cards for employees, but in either case, it is important to understand that if these systems are vulnerable to breach or have been breached they are not trustworthy. In the case of ships, a test in October 2013 by Trend Micro demonstrated that a cargo ship's AIS could be breached using $200 in equipment. This breach would allow modification of the reporting on a ship's position, course, cargo, speed, and name; send false weather information; trigger a false collision warning alert; allow the ability to impersonate marine authorities; create a fake man overboard distress beacon; and increase the frequency of AIS data transmissions which can cause a DNS attack on those receiving that data. With a denial of service attack (DNS), so much data is being sent that the recipient cannot receive the information nor have the capacity to receive AIS information from others.

Drilling rig cyber attack

In 2010, while a drilling rig was being moved from the construction site in South Korea toward South America, its critical control systems were infected by malware that shut it down for 19 days to fix the problem. A similar attack on a rig reported off the coast of Africa caused it to be shut down for a week.

GPS jamming and spoofing

A backpack GPS jammer is legal to obtain and costs $10-20,000.00 with a range of 3-400 meters. People on land, in flight, and at sea rely upon GPS for navigation and for this reason disabling a GPS system can present serious consequences for safety and commerce. The test of one GPS jammer resulted in the failure of the electronics chart display and information system, AIS, the dynamic positioning system, and the ship's gyro calibration system among other systems.

Surreptitious GPS attacks involving GPS spoofing, not just jamming, have been demonstrated. This is where phony time and location is sent to GPS receivers.

These are some of the cyber vulnerabilities known to exist in maritime environments. The chronicling of these vulnerabilities provides a view into a world where good physical security has long been the goal, and the introduction of computing has introduced a new level of threats that are both old and new.

The larger security challenge is not the cataloging and addressing of vulnerabilities introduced by known wireless devices or technologies, but rather the reality that the state of vulnerability will never be static. It will be impossible to control the number and types of IoT technologies that will be in any given space.

Should the IoT be feared?

This paper was meant to raise issues and questions regarding the physical security of industrial control systems, energy efficiency systems, and methods for managing the accounting of products and materials, labor, and resources, among other things. The IoT is

going to change the world of physical security forever. Physical security professionals will need to meet with IT personnel, the CISO, and others to start looking at how to approach physical security of industrial control systems.

Large complex environments such as deep-water and container ports offer the worse set of conditions for cyber security—high probability and high impact situations. Critical infrastructure or vital functions within physical environments should be assessed and classified as low, medium, or high for analysis of the risk of something happening as well as the assigning of a rating of low, medium, or high consequences should a particular event occur.

Where does P1912 fit in the security and privacy of the IoT?

The IoT will force a continuous evaluation and re-evaluation of the societal definition of "what is secure." IoT will drive the security risk moving into physical space, which is an extension of the current Internet's capabilities. The Internet was not built for security, but to make sure that messages get from the sender to the receiver.

P1912 will focus on security and privacy with equal weight. Privacy can be called "confidentiality" in the context of businesses. Privacy assures when, where, why, and how data about an individual are under the individual's control. The smart grid and other advances that bring the IoT into homes and businesses through applications and technology that report on energy consumption every 15 minutes or less will introduce the potential for authorized and unauthorized energy surveillance.

P1912 offers an opportunity to develop a voluntary communication architectural standard to create greater simplicity and ease of use that supports privacy and security. A common communication platform that bridges the communication divide that exists among wireless technology (e.g., RFID, IP, NF or other wireless technology) would create options for users to control access to personal and consumer digital devices. The goal is to use the capacity of the IoT in a physical space to allow flexibility in securing the data and the space from harm, abuse, or misuse by others.

Establishing a common architecture will support end-user ease of use of security and privacy options. The common architecture can support unique device recognition among wireless digital devices and technology. P1912's common architecture will allow development based on this standard for a range of applications and digital technologies. Ultimately, the standard can aid in preventing theft, abuse, or misuse of digital devices and stored information, and can help to increase privacy. At the same time, it will reduce the need to rely on passwords or PINs to establish legitimate access. Adoption of technology requires greater security and ease of securing wireless enabled digital devices. This standard will support flexibility in the methods that may be employed by users to exert control over or access the content on their digital devices.

This standard would provide greater consumer and user control over physical devices and technology, so as to fit them to the unique needs of individual users. Development of the P1912 standard will extend greater control to owners and legitimate users through a common architecture, while supporting innovation and broad adoption of RFID, IP, NP, wireless or other remote communication enabled devices and technology.

About the Author: Lillie Coney serves as Policy Director for a senior member of the House of Representatives. She is also President of Bruce Corporation, a privacy and cyber security consulting company. Ms. Coney chairs the P1912 Working Group discussed in this paper. Formerly, she worked as the Associate Director of the Electronic Privacy Information Center.