I recently read an article that brought to mind the old expression, “Tar and Feathers.”

It appears that a laptop belonging to a Sheriff’s office in the Seattle area was stolen from an undercover officer’s private vehicle (the link to the article “Stolen laptop containing info on victims, suspects, witnesses and police” may be found in News Ripped From The Headlines on page 4 of this newsletter.)

Unfortunately, the police department was just now implementing encryption on their computers. Of course, they had not made it to this one, yet.

As one who is both “paid to be paranoid” and sometimes volatile, my first thought was, “ARE YOU STUPID???? I mean, really!

As anyone who shops during the holidays probably knows, leaving items out in your vehicle (in this case a truck) is just begging for some nefarious individual to go shopping in your vehicle. Shouldn’t an undercover deputy in a Sheriff’s office know this? Yes, read the article.

As IA professionals we run into this type of laxness all too often. Unlike what usually happens in our world, the detective is “facing discipline.”

Now, what is happening with the information on the stolen devices. Thankfully, in most cases like this, the drives are wiped and the systems are resold on the black market. Is that what is happening with this? Don’t know. We can only hope for the best.

Oh, yeah. One more thing. This wasn’t the first data spill like this for this department.

Okay, I feel better now.

Enough of me ranting. That’s not why you are reading this newsletter.

There is an interesting “alternative history” article (also call counter-factual history) about finding Paul Revere using Metadata.

Continuing with the history theme, you’ll see an article on the dangers of a cashless society and when the first program was electronically stored and run (a lot longer ago than I thought.)

I’ve also included articles on cyber attacks against medical devices, the Pentagon five-year cybersecurity plan, how technical skills are not important for future CISOs, digital forensics, one final article on Bitcoin, the IT-User disconnect, and other items that I hope tweak your interest.

Don’t forget that I always include a schedule of upcoming ISSA-COS Chapter meetings and training.

I also hope that you check out the website (www.issa-cos.org) periodically.

Any suggestions for the newsletter, website, how the chapter functions, etc. are always welcome.

Finally, this coming December there will be elections for upcoming Chapter Board positions (including mine.) Stay tuned for additional details.

Don Creamer

The ISSA Colorado Springs Newsletter incorporates open source news articles as a training method to educate readers on security matters in compliance with USC Title 17, Section 107, Paragraph a.

The views expressed in articles obtained from public sources within this newsletter do not necessarily reflect those of ISSA, this Chapter or its leadership.
"Perhaps I should not say "terrorists" so rashly. But you can see how tempting it is. Anyway, look—there he is again, this Mr. Revere! Very interesting."

By Kieran Healy, Kieran-HealyBlog, June 9, 2013

London, 1772.

I have been asked by my superiors to give a brief demonstration of the surprising effectiveness of even the simplest techniques of the new-fangled Social Network Analysis in the pursuit of those who would seek to undermine the liberty enjoyed by His Majesty’s subjects. This is in connection with the discussion of the role of “metadata” in certain recent events and the assurances of various respectable parties that the government was merely “sifting through this so-called metadata” and that the “information acquired does not include the content of any communications”. I will show how we can use this “metadata” to find key persons involved in terrorist groups operating within the Colonies at the present time. I shall also endeavour to show how these methods work in what might be called a relational manner.

The analysis in this report is based on information gathered by our field agent Mr David Hackett Fischer and published in an Appendix to his lengthy report to the government. As you may be aware, Mr Fischer is an expert and respected field Agent with a broad and deep knowledge of the colonies. I, on the other hand, have made my way from Ireland with just a little quantitative training—I placed several hundred rungs below the Senior Wrangler during my time at Cambridge—and I am presently employed as a junior analytical scribe at ye olde National Security Administration. Sorry, I mean the Royal Security Administration. And I should emphasize again that I know nothing of current affairs in the colonies. However, our current Eighteenth Century beta of PRISM has been used to collect and analyze information on more than two hundred and sixty persons (of varying degrees of suspicion) belonging variously to seven different organizations in the Boston area.

Rest assured that we only collected metadata on these people, and no actual conversations were recorded or meetings transcribed. All I know is whether someone was a member of an organization or not. Surely this is but a small encroachment on the freedom of the Crown’s subjects. I have been asked, on the basis of this poor information, to present some names for our field agents in the Colonies to work with. It seems an unlikely task.

If you want to follow along yourself, there is a secret repository containing the data and the appropriate commands for your portable analytical engine.

Here is what the data look like.

The organizations are listed in the columns, and the names in the rows. As you can see, membership is represented by a “1”. So this Samuel Adams person (whoever he is), belongs to the North Caucus, the Long Room Club, the Boston Committee, and the London Enemies List. I must say, these organizational names sound rather belligerent.

Anyway, what can get from these meagre metadata? This table is large and cumbersome. I am a pretty low-level operative at ye olde RSA, so I have to keep it simple. My superiors, I am quite sure, have far more sophisticated analytical techniques at their disposal. I will simply start at the very beginning and follow a technique laid out in a beautiful paper by my brilliant former colleague, Mr Ron Breiger, called "The Duality of Persons and Groups." He wrote it as a graduate student at Harvard, some thirty five years ago. (Harvard, you may recall, is what passes for a university in the Colonies. No matter.) The paper describes what we now think of as a basic way to represent information about links between people and some other kind of thing, like attendance at various events, or membership in various groups. The foundational papers in this new science of social network analysis, in fact, are almost all about what you can tell about people and their social lives based on metadata only, without much reference to the actual content of what they say.

Read the rest here:
The Privacy Dangers of a Cashless Society Were Clear Over 40 Years Ago

By Matt Novak, Paleofuture, 11 June 2013

Your bank and credit card companies have quite a file on you. They know how often you go out to eat, how often you drink, how often you fill up your gas tank, along with the time and location of all these activities. Cash is all but dead, and with that comes a digital trail of all your purchases watched over by private companies who don’t exactly have the best security record. But we can’t say nobody warned us.

In 1968, Paul Armer of the RAND Corporation testified in front of a U.S. Senate subcommittee about his concerns for privacy in the future. Specifically, Armer was concerned with the computerized ability to look into the lives of Americans as we entered an age where people no longer used cold hard cash.

Back in 1968 the U.S. was far from a cashless society, so Armer tried to paint a picture of what that world might look like:

*Literally, it means a society without cash or checks. In this extreme, all financial transactions, even the purchase of a newspaper, the tipping of a doorman or passing through a highway toll station, would take place via some mechanism not involving a check or cash.*

The doorman's tips may still be that rare case when cash reigns supreme, but with newspaper boxes now taking credit cards and electronic highway toll systems now the norm, this future has certainly arrived.

Armer outlined three major reasons that the computer would destroy privacy in coming years:

*The first is that computer technology is introducing order-of-magnitude reductions in the cost of collecting, transmitting, and processing information. Second, centralization of data is usually a concomitant of computer use. The payoff to successful snooping is much greater when all the facts are stored in one place. Though most of the data to complete a dossier on every citizen already exists in the hands of the government today, it is normally so dispersed that the cost of collecting it and assembling it would be very high. The third factor is that computer systems with remote terminals can permit, unless proper safeguards are provided, remote browsing through the data with a great deal of anonymity.*

Read the rest here: http://paleofuture.gizmodo.com/the-privacy-dangers-of-a-cashless-society-were-clear-over-40-years-ago

The First Ever Electronically Stored Program Ran 65 Years Ago

By Jamie Condliffe, Gozmodo, June 21, 2013

Sixty five years ago, in a cluttered lab in Manchester, UK, three scientists changed the world of computing forever. Working with a machine they’d built and nicknamed Baby, they ran the first ever program to be stored electronically in a computer's memory.

Put together by "Freddie" Williams, Tom Kilburn and Geoff Tootill, the computer—officially called the Manchester Small Scale Experimental Machine—was 5 meters long, weighed a ton, and was a testbed for the experimental Williams-Kilburn tube. That was a newly proposed means of storing bits of data using a cathode ray tube, and if it worked, it looked set to provide the first ever means of storing and flexibly accessing information in electronic form.

It did work, supplying Baby with what amounted to the earliest form of RAM—of which it had just 128 bytes. (The computer you’re using now has billions of times more, but you already knew that.) And that's what allowed the computer to be the first to run a program electronically stored in its memory—a huge turning point in the world of computing.

Read the rest here: http://gizmodo.com/the-first-ever-electronically-stored-program-ran-65-years-ago
News Ripped From the Headlines

**June 6, The Register** – (California) **Police ‘stumped’ by car thefts using electronic skeleton key.** Police in California have reported an unknown electronic device being used by thieves to unlock vehicles and steal their contents. Police are reaching out to manufacturers and mechanics to try and identify the devices. Source: [http://www.theregister.co.uk/2013/06/06/electronics_skeleton_key_has_police_stumped/](http://www.theregister.co.uk/2013/06/06/electronics_skeleton_key_has_police_stumped/)

**June 6, The Register** – (International) **Microsoft and FBI storm ramparts of Citadel botnets.** Microsoft and the FBI have disabled around 1,000 of the estimated 1,400 botnets created by the Citadel botnet malware that have stolen more than $500 million. Microsoft also filed suit against the alleged controller of the botnet, and the FBI is working with law enforcement in various countries to identify the botmaster and 81 bot herders. Source: [http://www.theregister.co.uk/2013/06/06/microsoft_feds_breach_citadel_botnets/](http://www.theregister.co.uk/2013/06/06/microsoft_feds_breach_citadel_botnets/)

**June 8, Softpedia** – (International) **McAfee says it made a mistake, Koobface worm not on the rise.** McAfee acknowledged that it made a mistake in reporting that the Koobface worm has been on the rise, when instances of it have in fact decreased. Source: [http://news.softpedia.com/news/McAfee-Says-It-Made-a-Mistake-Koobface-Worm-Not-on-the-Rise-359553.shtml](http://news.softpedia.com/news/McAfee-Says-It-Made-a-Mistake-Koobface-Worm-Not-on-the-Rise-359553.shtml)

**June 14, Softpedia** – (International) **Flash Player clickjacking flaw allows hackers to hijack your webcam.** A researcher discovered a vulnerability in Adobe’s Flash Player that can be exploited to access a user’s webcam and microphone if the user is using the Mac version of Chrome, Linux, Chromium, and possibly other configurations. Source: [http://news.softpedia.com/news/Flash-Player-Clickjacking-Flaw-Allows-Hackers-to-Hijack-Your-Webcam-360980.shtml](http://news.softpedia.com/news/Flash-Player-Clickjacking-Flaw-Allows-Hackers-to-Hijack-Your-Webcam-360980.shtml)

**June 18, The Register** – (International) **Robbing a bank? Carberp toolkit now available for just $5k.** The source code for the Carberp banking trojan was found for sale on underground forums for $5,000, the first time that the full toolkit has been made available. Source: [http://www.theregister.co.uk/2013/06/18/carberp_trojan_source_code_sale/](http://www.theregister.co.uk/2013/06/18/carberp_trojan_source_code_sale/)

**June 20, V3.co.uk** – (International) **Anonymous OpPetrol hacking campaign targets oil and gas sectors.** Symantec urged oil and gas firms in the U.S. and worldwide to be vigilant for cyberattacks after a hacker group announced their plans for attacks on energy companies beginning June 20. The group promised to use distributed denial-of-service (DDoS) attacks, deface social media accounts and Web sites, steal sensitive information from systems and post it online, as well as infect networks with disk-wiping malware. Source: [http://www.v3.co.uk/v3-uk/news/2276288/oil-and-gas-sector-warned-of-anonymous-oppetrol-hacking-campaign](http://www.v3.co.uk/v3-uk/news/2276288/oil-and-gas-sector-warned-of-anonymous-oppetrol-hacking-campaign)


**June 26, Help Net Security** – (Washington) **Stolen laptop containing info on victims, suspects, witnesses and police.** Nearly 2,300 potential victims were notified June 21 of a theft after a laptop and personal hard drive belonging to an undercover officer from a Seattle sheriff’s office was taken from her truck. Social Security numbers, drivers license numbers, and case files containing personal information about crime victims, suspects, and police officers were all unencrypted on the devices. Source: [https://www.net-security.org/secworld.php?id=15144](https://www.net-security.org/secworld.php?id=15144)
Feudal Security

By Bruce Schneier, Schneier on Security, June 13, 2013

Facebook regularly abuses the privacy of its users. Google has stopped supporting its popular RSS feeder. Apple prohibits all iPhone apps that are political or sexual. Microsoft might be cooperating with some governments to spy on Skype calls, but we don't know which ones. Both Twitter and LinkedIn have recently suffered security breaches that affected the data of hundreds of thousands of their users.

If you've started to think of yourself as a hapless peasant in a Game of Thrones power struggle, you're more right than you may realize. These are not traditional companies, and we are not traditional customers. These are feudal lords, and we are their vassals, peasants, and serfs.

Power has shifted in IT, in favor of both cloud-service providers and closed-platform vendors. This power shift affects many things, and it profoundly affects security.

Traditionally, computer security was the user's responsibility. Users purchased their own antivirus software and firewalls, and any breaches were blamed on their inattentiveness. It's kind of a crazy business model. Normally we expect the products and services we buy to be safe and secure, but in IT we tolerated lousy products and supported an enormous aftermarket for security.

Now that the IT industry has matured, we expect more security "out of the box." This has become possible largely because of two technology trends: cloud computing and vendor-controlled platforms. The first means that most of our data resides on other networks: Google Docs, Salesforce.com, Facebook, Gmail. The second means that our new Internet devices are both closed and controlled by the vendors, giving us limited configuration control: iPhones, ChromeBooks, Kindles, BlackBerry PDAs. Meanwhile, our relationship with IT has changed. We used to use our computers to do things. We now use our vendor-controlled computing devices to go places. All of these places are owned by someone.

The new security model is that someone else takes care of it -- without telling us any of the details. I have no control over the security of my Gmail or my photos on Flickr. I can't demand greater security for my presentations on Prezi or my task list on Trello, no matter how confidential they are. I can't audit any of these cloud services. I can't delete cookies on my iPad or ensure that files are securely erased. Updates on my Kindle happen automatically, without my knowledge or consent. I have so little visibility into the security of Facebook that I have no idea what operating system they're using.

There are a lot of good reasons why we're all flocking to these cloud services and vendor-controlled platforms. The benefits are enormous, from cost to convenience to reliability to security itself. But it is inherently a feudal relationship. We cede control of our data and computing platforms to these companies and trust that they will treat us well and protect us from harm. And if we pledge complete allegiance to them -- if we let them control our email and calendar and address book and photos and everything -- we get even more benefits. We become their vassals; or, on a bad day, their serfs.

There are a lot of feudal lords out there. Google and Apple are the obvious ones, but Microsoft is trying to control both user data and the end-user platform as well. Facebook is another lord, controlling much of the socializing we do on the Internet. Other feudal lords are smaller and more specialized -- Amazon, Yahoo, Verizon, and so on -- but the model is the same.

To be sure, feudal security has its advantages. These companies are much better at security than the average user. Automatic backup has saved a lot of data after hardware failures, user mistakes, and malware infections. Automatic updates have increased security dramatically. This is also true for small organizations; they are more secure than they would be if they tried to do it themselves. For large corporations with dedicated IT security departments, the benefits are less clear. Sure, even large companies outsource critical functions like tax preparation and cleaning services, but large companies have specific requirements for security, data retention, audit, and so on -- and that's just not possible with most of these feudal lords.

Feudal security also has its risks. Vendors can, and do, make security mistakes affecting hundreds of thousands of people. Vendors can lock people into relationships, making it hard for them to take their data and leave. Vendors can act arbitrarily, against our interests; Facebook regularly does this when it changes peoples' defaults, implements new features, or modifies its privacy policy. Many vendors give our data to the government without notice, consent, or a warrant; almost all sell it for profit. This isn't surprising, really; companies should be expected to act in their own self-interest and not in their users' best interest.

Read the rest here:
http://www.schneier.com/blog/archives/2013/06/more_on_feudal.html
The Game-Changing Legislation That No One is Talking About

By Jon-Louis Heimerl, SecurityWeek, June 07, 2013

Well, it is probably not quite game-changing yet, or people would be talking about it more. But the Omnibus Rule (PDF) that updated the Health Insurance Portability and Accountability Act (HIPAA) has the potential to be a game changer because of the things it says in writing, as well as some of the things that it doesn’t say.

HIPAA was ahead of its time by defining regulations not only to enable better use of electronic records, but to improve both privacy and security of protected healthcare information (PHI). The Health Information Technology for Economic and Clinical Health (HITECH) Act made considerable changes to HIPAA. In terms that security geeks care about, like security and privacy, HITECH added better definition of fines, and better enabled enforcement, along with laying out definitions for “willful neglect”. HITECH’s additions for unauthorized uses and breach notification were significant changes and enhancements, as was guidance that Business Associates had some direct responsibilities to safeguard PHI (under HIPAA, this responsibility was primarily passed to a BA under terms of their contract). But by now, HIPAA is “old news” and HITECH is getting there.

Does the recently passed HIPAA Omnibus Rule really change things? We don’t know yet, partially because so much counts on how the rule will be enforced, but it has the potential to.

The obvious question is “what is so profound about the Omnibus Rule?” Realistically, the Omnibus Rule includes many more things than are included here, and some of those things may have substantive impacts on healthcare organizations. But I am a security geek, not a healthcare practitioner, so these are the updates that, as a security geek, I consider the most likely to be “game changers”.

The general deadline for compliance with the Omnibus Rule is September 23, 2013. This should not be a terrible surprise for anyone who has been reading HITECH, the interim rule, and associated updates, but this is ONLY a little over three months away from the time of this article. Security is often as much about organizational culture as it about technical controls, and organizational culture does not evolve overnight. In the world of integrating requirements into your security program that is no time at all. In other words, you should already be started or you may very well be too late.

Enhanced Patient Privacy

There are numerous updates to patient privacy requirements. To simplify, the Omnibus Rule expands patient rights and notification requirements. The point is that there are changes from the interim rules, so a healthcare organization needs to update their privacy policies and notifications in meaningful ways.

Business Associate Responsibility

Under HIPAA, BAs were pretty much obligated to do the things they had promised to their Covered Entities (CEs) in contractual language. In practical terms, if it was not in the contract, you did not “have” to do it. Under HITECH, BAs became responsible to directly meet the requirements of HIPAA and other pieces of HITECH. With the Omnibus Rule, BAs and any subcontractors who have access to PHI are directly liable for compliance with the HIPAA Security and Privacy rules. In fact, the same is true of subcontractors and vendors of the BA. Just as the CE absorbs responsibility to ensure that the BA has an appropriate security program, the BA now absorbs responsibility to make sure that subcontractors and vendors have appropriate security programs. Everyone in the chain can now be audited and assessed civil and criminal penalties for violations. And this is regardless of any contractual agreements that they may already have in place. The fact that a BA is truly responsible for HIPAA and HITECH compliance is not completely new, since it was in the interim rules, but BAs should pay heed to the fact that their requirements have now been formalized in the final Omnibus Rule.

CEs are also now required to get proof from the BAs that the BA is taking appropriate action to protect PHI, just as the BA is required to get this proof from any subcontractors. Previously, the CE and the BA could rely on their contractual language to isolate themselves from any liability for lack of performance. This is no longer the case. It is now incumbent on the CE to know whether or not the BA is behaving. If the CE does not have this proof, and the BA gets popped, the CE is no longer able to isolate their selves from liability by pointing to the BA.

Read the rest here:
Pentagon five-year cybersecurity plan seeks $23 billion

By Tony Capaccio, Bloomberg News, June 11, 2013

A Pentagon cybersecurity budget outline calls for spending almost $23 billion through fiscal 2018, as efforts are expanded on initiatives from protecting computer networks to developing offensive capabilities.

The Defense Department already has proposed $4.65 billion for such programs in the fiscal year that begins Oct. 1, an 18 percent increase from the $3.94 billion budgeted this year. The five-year “cyber-expense” budget obtained by Bloomberg News calls for spending to remain elevated from past levels.

Defense Secretary Chuck Hagel this month cited “the growing threat of cyber-intrusions, some of which appear to be tied to the Chinese government and military.” His predecessor, Leon Panetta, said last year that “a cyber-attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack of 9/11.”

The budget outline shows “increased investment will be made in protecting critical infrastructures,” cyber-attack capabilities “for use against our adversaries and enhancing overall security of DoD networks and systems,” Harry Raduege, chairman of Deloitte LLP’s Center for Cyber Innovation in Washington, said in a statement.

Increased U.S. spending on computer security may benefit defense contractors, including SAIC Inc. (SAI) and Northrop Grumman Corp. (NOC), in a time when other Pentagon spending is declining, according to data compiled by Bloomberg Government.

YEARLY FUNDING

The Pentagon plans to request $4.72 billion in fiscal 2015, declining to $4.61 billion in 2016 and $4.45 billion the next year, then rising to $4.53 billion in 2018, according to the budget document.

Among national-security documents disclosed last week, the U.K.-based Guardian newspaper reported that President Barack Obama issued a directive in October saying “Offensive Cyber Effects Operations” can provide “unique and unconventional capabilities to advance U.S. national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging.”

Read the rest here:

Technical Skills Not Important for Future CISOs Declares Forrester

By InfoSecurity, 10 June 2013

In a session titled ‘Becoming the Future CISO’ at the Forrester Forum for CIO’s in London, England, June 6 2013, Andrew Rose declared the current role of CISO a dying breed.

Based on research carried out with 60 current CISOs and Forrester’s observation of the industry, Andrew Rose - principal analyst at Forrester Research - announced that the role of CISO as we know it today will “fall from under our feet”. The choice it leaves, he said, is to either step up to be the corporate information risk manager, or to step down to a support-based role, as a technical expert for example. “CISOs need to think about their career path because they can’t stay where and as they are”, he advised.

“Being a CISO is a tough job. There are too many problems to balance and too many vendors shouting at you”. Rose recalled the evolution from the tecchie CISO in 1998 “who always said no” to today’s CISO who is focused more on business, delivery and engagement. “The role will evolve even more radically between now and 2018”, he advised. “CISOs are needed more than ever, as security is becoming more important”, he said.

To enable a smooth transaction into the future CISO, “we need to get angry, fight, and keep innovating.” Neither staffing challenges nor third-party supplier challenges are going away, argued Rose. “Technology is becoming more pervasive, customer expectations are increasing and new business transactions are taking off.” The ‘internet of things’ and big data will also pose great challenge for tomorrow’s CISO according to the Forrester analyst.

The 2013 CISO is focused on five areas in the below order:

Read the rest here:
http://www.infosecurity-magazine.com/view/32858/technical-skills-not-important-for-future-cisos-declares-forrester/
US warns of cyber attacks on medical devices

By Agence France Presse, June 14, 2013

US authorities on Thursday warned makers of medical devices and hospital networks to step up efforts to guard against potential cyber attacks.

The US Food and Drug Administration said implanted devices, which could include pacemakers or defibrillators, could be connected to networks that are vulnerable to hackers.

An FDA warning notice was sent to medical device manufacturers, hospitals, medical device user facilities, health care technical staff and biomedical engineers.

It said the agency has recently "become aware of cybersecurity vulnerabilities and incidents that could directly impact medical devices or hospital network operations."

"The FDA is recommending that medical device manufacturers and health care facilities take steps to assure that appropriate safeguards are in place to reduce the risk of failure due to cyberattack," the warning said.

These devices or systems could be compromised "by the introduction of malware into the medical equipment or unauthorized access to configuration settings in medical devices and hospital networks," the FDA said.

"This may sound like it is out of a science fiction movie, but the threat is conceivably a serious one," said Jon Ogg at 24/7 Wall Street.

"Can you imagine a device being retooled maliciously, like an inserted pacemaker/defibrillator? Or imagine if a robotic surgery system was maliciously recalibrated in even a slight manner for surgeries.

"The list of threats is endless."

The FDA said it was "not aware of any patient injuries or deaths associated with these incidents" nor does it have any specific information on targeted devices.

The FDA said it had been working with other federal agencies as well as manufacturers, which it said are "responsible for remaining vigilant about identifying risks and hazards associated with their medical devices."

Among the measures that should be taken, the FDA said, are limiting unauthorized device access, "particularly for those devices that are life-sustaining or could be directly connected to hospital networks."

Original article here:

---

Is the Xbox One a Covert Surveillance Device?

By InfoSecurity, 28 May 2013

When details about Microsoft's new games console, the Xbox One, first began to emerge, privacy campaigners were immediately concerned: is the Xbox One an intrusive but covert surveillance device?

Three aspects raise concerns. Firstly the device requires connection to the internet (although not apparently, the continuous connection originally thought). Secondly, it does require continuous connection to Kinect. And thirdly, Kinect is always on. These three aspects mean that anything in front of the device can be recorded, both sound and video, and can be transmitted back to Microsoft over the internet while it is connected.

Germany's federal data protection commissioner for Berlin, Peter Schaar, gave his concerns to Spiegel Online: "The Xbox continuously records all sorts of personal information about me. Reaction rates, my learning or emotional states. [These] are then processed on an external server, and possibly even passed on to third parties. Whether they will ever [be] deleted, the [user] can not influence." (Google translation)

Tim Vines, director at Civil Liberties Australia, is equally concerned. "Microsoft's new Xbox meets the definition of a surveillance device under some Australian laws," he told GamesFIX, "so they need to be upfront and tell customers whether anyone else can intercept their information or remotely access their device."

Microsoft for its part has been quick to dispel fears. "Microsoft has very, very good policies around privacy," corporate Vice President Phil Harrison told EuroGamer. "We're a leader in the world of privacy, I think you'll find. We take it very seriously. We aren't using Kinect to snoop on anybody at all. We listen for the word 'Xbox on' and then switch on the machine, but we don't transmit personal data in any way, shape or form that could be personally identifiable to you, unless you explicitly opt into that."

Read the rest here:
Bitcoin Hits the Big Time, to the Regret of Some Early Boosters

The first major conference for the digital currency suggests it is gaining legitimacy, but in a manner disappointing to some early enthusiasts.

By Tom Simonite, MIT Technology Review, May 22, 2013

This past Sunday, Doug Scribner took out five $100 bills and began feeding them into what looked like a small, white ATM in San Jose Conference Center in California. The machine swallowed the bills smartly and credited him with an equivalent value in bitcoins, an intangible, digital currency that is backed by not gold or any government, but by math.

Scribner was one of an estimated 1,100 people who attended Bitcoin 2013, a weekend-long event in the heart of Silicon Valley and the first large conference dedicated to Bitcoin. Unsurprisingly, all those present seemed certain that the cryptocurrency was set to upend the world of finance, perhaps more. But the event also offered something new: evidence that Bitcoin is gaining traction outside its existing community of enthusiastic early adopters.

Bitcoin’s origins are mysterious. It was created by an unknown individual or individuals who used the pseudonym Satoshi Nakamoto. Cryptographic operations and oversight from a peer-to-peer network of people running Bitcoin software process transactions and protect against counterfeiting without the need for a central authority (see “What Bitcoin Is and Why It Matters” http://www.technologyreview.com/news/424091/what-bitcoin-is-and-why-it-matters/).

Commercial enterprises based on Bitcoin are gaining momentum in part thanks to people like Scribner, who, after buying large numbers of bitcoins early in their short history, has seen them soar in value and is in a position to invest.

"I’m going to buy one of these and put it in Mall of America," Scribner told me after using the dollar-gobbling machine, which has a $4,000 price tag. He described a plan for a small booth that would offer passing shoppers Bitcoin literature and the opportunity to exchange greenbacks for bitcoins on the spot. Scribner, who works in teleconferencing near Minneapolis-St. Paul, Minnesota, could probably afford to do it. He says that he bought his first 100 bitcoins when they were just $3 each, and then steadily amassed more at relatively low prices. A single bitcoin today now sells for just over $120.

More significantly, the conference also showed that Bitcoin has begun to attract the backing of conventional technology industry investors, who have sunk millions of dollars into a handful of Bitcoin startups. “What’s going on right now is a transformation from stage one, supported by the purists that are devoted to the idea, to a period where we are asking ‘What does this do for global commerce?’ " Chris Larsen, CEO of OpenCoin, told me at his company’s booth, one of about 20 in the conference’s exhibition space.

Larsen previously founded two conventional finance companies, E-Loan and Prosper; his new company runs a service called Ripple that offers easy transactions between conventional currencies, bitcoins, and a math-backed currency of the company’s own design. OpenCoin is backed by Silicon Valley venture funds Lightspeed Venture Partners, Andreessen Horowitz, and Google Ventures (see “Big-Name Investors Back Effort to Build a Better Bitcoin” http://www.technologyreview.com/news/513606/big-name-investors-back-effort-to-build-a-better-bitcoin/). Bitcoin businesses have been started before, but OpenCoin and a few others now have access to funds, expertise, and contacts that allow a more significant, lasting assault on the status quo. The U.S. Treasury helped strengthen investor interest in March, when it clarified which financial crime regulations apply to virtual currencies.

CoinBase, the media sponsor of the San Jose event, received the largest venture investment in a Bitcoin business to date earlier this month. The company, which originated in the incubator Y Combinator and helps individuals and businesses use bitcoins, received $5 million from Union Square Ventures, a fund better known for backing Tumblr and Zynga. In San Jose, I also met the founders of BitPay, which enables online stores—including those hosted by Amazon—to take Bitcoin payment. Bitpay recently received $3 million from Founders Fund, led by Facebook’s first major investor, Peter Thiel.

BitPay CEO Tony Gallippi told me that Thiel invested because he saw how the company could help ease online commerce across borders; the company already handles $5 million in transactions each month and says the figure is growing. “Traditional payments such as credit cards don’t even work in half the world, so companies just choose to not service international customers,” Gallippi said. “That leaves a big opportunity.” He plans to take further investment later this year but told me it will be more for reasons of making strategic contacts than a need for cash, since he and his cofounders have significant Bitcoin holdings.

Read the rest here:
Attempts to destroy digital evidence are common. Such attempts can be more or less successful depending on the action taken, time available to destroy evidence, as well as the type of storage device (magnetic hard drive, flash memory card, or SSD drive).

Deleted Files

Important evidence often ends up in the recycle bin. This is especially true for Windows PCs. Thus, deleted files can often be successfully retrieved by analyzing the contents of the Recycle Bin, a temporary storage they’re placed in before being erased.

If deleted files do not show up in the Recycle Bin, there is still a good chance to recover them by using one of the many commercial data recovery tools. The principle of deleted file recovery is based on the fact that Windows does not wipe the contents of the file when it’s being deleted. Instead, a file system record storing the exact location of that file on the disk is marked as “deleted.” The disk space previously occupied by the file is then advertised as available, but not overwritten with zeroes or other data (we’ll discuss the issue of SSD drives in a minute).

By analyzing the file system and/or scanning the entire hard drive looking for characteristic signatures of known file types, one can successfully recover not only files that were deleted by the user, but also discover evidence such as temporary copies of Office documents (including old versions and revisions of such documents), temporary files saved by many applications, renamed files, and so on.

Read the rest here:
http://www.dfinews.com/articles/2013/06/destroyed-evidence-deleted-files?et_cdid=3316969&et_rid=454841830&location=top

By Jacob Goodwin, GSN Magazine, June 14, 2013

Sometimes, when a computer forensics expert is dissecting a suspect’s computer, the most important question to answer is this: “Am I looking at the original hard-drive, with all of its incriminating evidence, or has that drive been swapped out surreptitiously for a new drive, which will not contain the evidence that I’m hoping to find?”

In a significant breakthrough in the world of computer forensics, a small forensics company, CynanLine LLC, has discovered a little-known feature of most major hard-drives -- buried deep within their operating systems -- that can reveal to computer forensic experts the exact number of times that the examined hard-drive has been turned “On,” and the exact number of hours that the specific hard-drive has been used inside the computer.

These two pieces of information can be found in what is known as the Self Monitoring Analysis Reporting Tool, nick-named SMART, which was developed by hard-drive manufacturers for a completely different purpose -- to help an owner assess the physical “health” of his or her disc drive. In fact, most computer users have no idea that SMART even exists on their hard-drive, and can only access the information it presents if they download and use a separate piece of free software.

Those two vital pieces of forensic data -- how many times a hard-drive has been turned on, and for how many hours it has been used -- have not been readily available to forensic investigators, can help crack a case wide open.

Steven Branigan, a forensic scientist and the president of CynanLine, in an exclusive phone interview with Government Security News on June 13, recalled two instances in which this crucial data about a laptop’s hard-drive turned out to be pivotal.

In one case, CynanLine was working with a private investigation firm that had been retained to examine a laptop computer surrendered under a court order by a man suspected of leaking insider information. The accused was suspected of creating new online identities for himself to disguise the discussions he was conducting over the Internet about specific publicly-traded companies.

Read the rest here:
http://www.gsnmagazine.com/node/30055?c=cyber_security
Phew, NSA Is Just Collecting Metadata. (You Should Still Worry)

By Matt Blaze, Wired, June 19, 2013

We now know that every day, U.S. phone companies quietly send the government a list of who called whom and when — “telephony metadata” — for every call made on their networks, because of a secret order by the Foreign Intelligence Surveillance Court. It turns out that this has been going on for seven years (and was even reported by USA Today then); the difference now is that the government — uncharacteristically for such a secret intelligence operation — quickly acknowledged the authenticity of the leaked order and the existence of the metadata collection program.

Should we be worried? At least “nobody is listening to our telephone calls” (so the president himself assured us). People breathed a sigh of relief since first learning of the surveillance because surely there’s nothing to worry about when it comes to such seemingly innocuous information — it’s just metadata, after all. Phew!

Unfortunately, metadata still leaves a lot to be concerned about. There’s more to privacy than just the sounds of our voices: Content may be what we say, but metadata is about what we actually do.

And unlike our words, metadata doesn’t lie.

The Metadata Is the Message

With today’s communications technology, is metadata really less revealing than content? Especially when we’re dealing with metadata at the scale that we now know the NSA and FBI are receiving?

Because at such a scale, people’s intuition about the relative invasiveness of content and metadata starts to fail them. Phone records can actually be more revealing than content when someone has as many records and as complete a set of them as the NSA does.

Voice content is hard to process. It ultimately requires at least some human analysis, and that inherently limits the scale at which it can be used, no matter how much raw material the NSA might have. Intelligence agencies are famously backlogged in translating and analyzing even high-priority intercepts. More content only makes the problem worse.

Metadata, on the other hand, is ideally suited to automated analysis by computer. Having more of it just makes it the analysis more accurate, easier, and better. So while the NSA quickly drowns in data with more voice content, it just builds up a clearer and more complete picture of us with more metadata.

But that’s not the most revealing thing about metadata, or the only reason to be concerned about the privacy implications of a massive call records database. Metadata ultimately exposes something deeper, far more than what a target is talking about.

Metadata is our context. And that can reveal far more about us — both individually and as groups — than the words we speak.

Context yields insights into who we are and the implicit, hidden relationships between us. A complete set of all the calling records for an entire country is therefore a record not just of how the phone is used, but, coupled with powerful software, of our importance to each other, our interests, values, and the various roles we play.

The better understood the patterns of a particular group’s behavior, the more useful it is. This makes using metadata to identify lone-wolf Al Qaeda sympathizers (a tiny minority about whose social behavior relatively little is known) a lot harder than, say, rooting out Tea Partiers or Wall Street Occupiers, let alone the people with whom we share our beds.

It is, in effect, a National Relationship Database.

Is This Legal? Can We Opt-Out?

We might reasonably wonder how any of this could possibly be legal. Doesn’t electronic surveillance require a warrant based on evidence of wrongdoing?

Yes, but a peculiarity of U.S. surveillance law gives call metadata less protection than call content. There are generally stricter requirements for wiretaps that intercept call content than for those that obtain only transactional data (the who called whom and when).

While the legal rationale for this distinction is complex, it’s important to know that it has its origins in how landline/wired telephones worked and were used in the last century. There’s even a legal theory that while the audio of a telephone call is intended only for the person we’re talking to, the numbers dialed are legally less “private” because they are given voluntarily to a third party: the phone company.

Read the rest here:
http://www.wired.com/opinion/2013/06/phew-it-was-just-metadata-not-think-again/
Ignoring security advice from the pros:  
The IT-user disconnect

By Michael Kassner, TechRepublic, June 17, 2013

Takeaway: IT pros and the general population of users have seemingly different agendas when it comes to security. Michael P. Kassner interviews a noted researcher about the psychology of these two groups.

“The grumpy IT guy,” is the title my fellow employees have bestowed upon me. I don’t think I’m grumpy. When all is said and done though, what I think does not matter; the perception is real in their eyes. How can it not be? An overwhelming number of my conversations, at work, center on some digital thing that is not working right, and it needs to be fixed right away, and no one has any idea what happened.

I know I’m not the only IT person in this illustrious club. When grabbing coffee with colleagues, the conversation inevitably gets to “us versus them” situations allowing for a shared commiseration over latte.

I think I may have a possible explanation of the phenomenon. I met Professor Rose McDermott, through her ACM paper, “Emotion and Security.” During a conversation, I asked Rose, a well-regarded scholar in psychology and behavioral studies, how to convince users of the importance of IT security, and avoid IT-user discord. She did not mince words:

People will listen to a conversation that is vivid, salient, concrete, and emotionally engaging. Abstract, pallid, statistical arguments tend to make people’s eyes glaze over.

Now the “not-mincing words”:

IT-professionals, please don’t take this the wrong way, but the skills that make one good at IT (meticulous attention to detail, ability to process large amounts of data simultaneously, detachment) can make it hard to communicate effectively with the technologically illiterate.

It’s hard to deny what Rose said. Yet, I have faith in my fellow IT professionals that once we understand what Rose proposes in her paper, we’ll be ready for the next IT-user encounter. Maybe I’ll even be able to get rid of my “Grumpy IT guy” moniker.

Kassner: Thank you Rose, I’m not sure I would have figured much of this out without your help.

As I understand, the main idea presented in the paper is that emotions temper our perception of reality — something IT professionals need to understand if they want to truly convince users doing something is in their best interest. Do you have an example?

McDermott: We can feel secure when we are not, just as we can feel insecure even when we are protected. For example, TSA invests an enormous amount of time, money, energy, and resources making us take our shoes and jackets off to go through a screening that is largely performative. It makes people feel secure so they will fly, not actually making anyone more secure.

On the other side, we can feel at risk when we are largely safe; the risk of dying in a shark attack is low, but people feel insecure all summer once they learn about a local shark attack case on the evening news. Psychologically, we are affected more by perception than probability.

Kassner: What you mention reminds me of the term Bruce Schneier coined: “Security Theater.” Beyond that, we must be aware of how users perceive what we are telling them, as it will inform us whether we are making any sense or not.

A bit further in the paper, you drop another bomb — one I’m not sure I comprehend. You say it doesn’t matter whether we raise the flag saying a threat is likely, or whether we lower the flag saying the threat is no longer likely; people are going to be negatively impacted either way. Why is that?

McDermott: We tend to forget about things over time, or push them to the back of our minds. But when the threat is publicly addressed, even as a reduced possibility; it becomes salient again, reminding us there is still something out there we should be afraid of, and this makes people more anxious.

Kassner: Wow, this explains why users are nowhere near as relieved as I am when a security issue is resolved.

You talk about two theories: Probability theory and Prospect theory. Probability theory suggests the bigger the threat, the stronger the response. But that’s not the case. It seems we react more in line with tenets proposed in the Prospect Theory. Could you explain the theory, and what IT professionals should be paying attention to?

McDermott: Sure, Prospect Theory describes how people respond to risk. Basically, people are more accepting of risk when confronting loss than when they are facing gains. Also, people do not respond to probability in a linear fashion.

We give more weight and attention to events that have a low-probability of occurring. Think of all the money we have spent preventing terrorism, when fewer people have died from terrorism in the past ten years than those who have died from domestic gun violence in any one year of the past ten.

Oppositely, we give less weight and attention to moderate and high probability events. For example, few of us eat healthy, and engage in daily exercise in order to reduce the risk of heart disease and cancer.

Read the rest here:
**Article for the Newsletter?**

If you would like to submit an article...

Are you a budding journalist? Do you have something that the Colorado Springs ISSA community should know about? Can you interview one of the "movers and shakers"? Tell us about it!

We are always looking for articles that may be of interest to the broader Colorado Springs security community.

Send your article ideas to Don Creamer at: doncreamer-issa@q.com

Ensure that “Newsletter” is in the subject line.

Looking forward to seeing you in print!

---

**NIST drafts new cloud security policy**

SimplySecurity, June 21, 2013

The U.S. government's Cloud First plan, which is a directive that tells agencies to look to cloud computing solutions first during IT procurement processes, is getting some help from the National Institute of Standards and Technology. NIST is drafting a special publication specifically to help companies define a cloud security architecture. This builds on the previous reference architecture the NIST created, but not the special publication that had been previously released, according to Fierce Government IT.

Michaela Iorga, NIST senior security technical lead for cloud computing, told the news source that the intent is to map out the specific controls necessary for a safe move into the cloud. Many components come from the Cloud Security Alliance’s Trust Cloud Initiative-Reference Architecture, as they address high and mid-level security needs of government agencies. One example given as a high concern is security monitoring service, while mid-level cloud be endpoint monitoring.

"The document's objective is to demystify the process of selecting cloud-based services that best address an agency's requirements in the most secure and efficient manner," Iorga said. "The Risk Management Framework has to be adapted when applying the risk-based approach to applications or systems migrated to the cloud because the implementation, assessment, authorization and monitoring of selected security controls may fall under the responsibility of different cloud 'actors;' for example, consumer, service provider or broker."

As a prescription for a"healthy security lifestyle," Iorga told FierceGovernmentIT that agencies and consumers must think about concerns before any kind of adoption. Requirements should not be compromised once implementation gets underway she said, as there is a responsibility to keep security up to the organization’s standards.

To help users pick out the best possible cloud solution, a case study will be provided to walk agencies through steps for deploying a typical application into the cloud, whether it be email, calendars, document sharing or a cloud-based chatting service.

According to the CDW-G State of the Cloud Report, 73 percent of IT professionals said personal use of cloud applications by employees has influenced their decision to adopt more cloud computing services and applications. Sixty-one percent of users agree that these apps allow their agencies to move faster.

Read the rest here:

 Volunteers Needed

Deborah Johnson is soliciting volunteers for the next ISSA-COS conference committee. Please contact her if you have an interest in helping on this committee. The venue is being narrowed down, but there are other planning tasks that need to be handled as well, such as marketing and publicity, brochures, programs, sponsors, door prizes, etc. so if you would like to take on any of these roles, let her know.

If you are interested in helping please contact her (djohnson@swcp.com).

Thank you in advance!

Training: The next Security + training session will be September 7 at Colorado Technical University. Watch for more information to come via e-mail as we get closer.

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jul 11</td>
<td>5:30 to 7:30</td>
<td>Bambino's Italian Eatery and Sports Bar, 2849 East Platte Avenue, Colorado Springs, 719) 630-8121</td>
</tr>
<tr>
<td>Aug 8</td>
<td>11:00 to 1:00</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Sep 12</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Oct 10</td>
<td>11:00 to 1:00</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Nov 14</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Dec 6</td>
<td>11:00 to 1:00</td>
<td>Carrabba’s North</td>
</tr>
</tbody>
</table>
The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity, and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved. Members include practitioners at all levels of the security field in a broad range of industries such as communications, education, healthcare, manufacturing, financial, and government.

Reclaim Your Privacy With Glowing Glasses That Foil Facial Recognition

By Andrew Liszewski, Gizmodo, June 19, 2013

In a time when it seems like the privacy we all enjoyed was just a smokescreen, it's nice to know there's at least one way to fight back against all the systems designed to keep track of our comings and goings. Developed by Japan's National Institute of Informatics, these glasses include eleven LEDs that blast a privacy curtain of near-infrared light to obscure your face.

Read the rest here: http://gizmodo.com/reclaim-your-privacy-with-glowing-glasses-that-foil-facial-recognition-514256615

Published at no cost to ISSA Colorado Springs by Sumerduck Publishing™, Woodland Park, Colorado