Data Breaches: Moving Towards Usable Security through Visualizations

Parsons - The New School for Design

M.S. Masters Thesis

Professor: Christian Sweinheart

Student: Suzanna Schmeelk

Table of Contents

Data Breaches: Implications for Usable Security

Researchers around the world are working on security problems. One of the hardest challenges is finding the sweet spot between a secure system and a usable system. Research can be novel and published but completely unusable. A system can be encrypted to the point it will take over a lifetime to decrypt. Is this novel? Perhaps. Is this security usable? Not in this lifetime!

Many things can be novel but only a small subset of novel things can be usable. Unfortunately, all too often we have to sacrifice the usability because it is the best the security field has to offer.

According to Butler Lampson, a Technical Fellow at Microsoft Research, “Security is not about perfection. In principle we can make secure software and set it up correctly, but in practice we can't, for two reasons: [Bugs and Conflicts].” In a presentation given at an OWASP meeting by Tobias Christen (2009) further elaborates that one risk to usable security is complexity. He emphasizes that simplification is a remedy for the risk. One way to improve the understanding of complex security topics is through the use of data visualization.

People are aware of the need for understanding usable privacy and security. According to recent courses at CMU and University of Maryland, the crux of usable security is in understanding Human Computer Interaction (or HCI). A CMU course, which has been running since 2006 and initially taught by Lorrie Cranor, Michael Reiter and Jason Hong, conveyed the HCI concepts to students, “5-899/17-500 Usable Privacy and Security.” In a similar Coursera course, taught by Jennifer Golbeck (2017) who is the Director of the UMD Human-Computer Interaction Lab, HCI is a key element to understanding what it means to have usable security.

Traditionally, computer programming, algorithm analysis, and compiler construction have been taught without discussing fundamental security principals. This may be part of the traditional teaching paradigm emphasizing that when the students finally become teachers they only teach what they know and understand. In this perspective, the courses they took were good enough, so let us just repeat the cookie-cutter model with their own students.

As such, still in 2017, students can graduate with a degree (e.g. B.A, B.S, M.S., DPS, SciDoc, Ph.D.) related to computer engineering without ever being exposed to basic security principals or even out-of-the-box creative thinking. The repetition in instruction objectives, for example using the same book (but different versions) for years and years, is one cause for repetitive mistakes being seen in the field at large as show by NIST (2017) and MITRE (2017) where fundamental and traditional mistakes in engineering are being recreated every day over and over. One could liken this traditional computer science instruction methodology to the metaphor of giving matches to children, testing the children on lighting the matches, patting the children on the back at graduation, saying good luck to you at your new job and walking away from the children!

As we are seeing by NIST (2017) and MITRE (2017), security professors were asked about studying the problem in research. The security professors say that these problems are well understood and uninteresting for computer security research. We can liken this response with a metaphor, of a new smallpox outbreak. If researchers see an outbreak of the plague and just say that smallpox is known and extremely uninteresting so let us not research the problem, then our global community is at risk to becoming re-infected. It is arguable whether the current attitude from computer security researchers in the field is correct. Should we continue to ignore repetitive problems from a research perspective or should we try to understand why the problems are being reproduced over and over again? Clearly there is a misalignment of viewpoints surrounding the computing field.

In 1987, the United Nations published the sustainability report, "Our Common Future: Report of the World Commission on Environment and Development." This report is commonly known as the Brundtland Report since Gro Harlem Brundtland, the first female Prime Minister of Norway, was commissioned to put it together. Secretary-General of the United Nations, Javier Pérez de Cuéllar, asked Brundtland to lead the effort (United Nations, 1987). Twenty years later, in 2007, the United Nations revisited the report to analyze global progress (United Nations, 2007). Soon, in 2027, will be 20 years again. At that time, we may want to consider (cyber) security as an element worth measuring in our global common future together.

Ask the Expert: An Interview with David Curry

David Curry is. On Tuesday March 19, 2019, David Curry kindly interviewed with us to answer insights about data breaches and the changes to the security field over time.

Interview Questions – David Curry (Tuesday March 19, 2019 @ 3pm)

1. How did you become interested in technology and cyber security field?

   I grew up in West Lafayette, Indianan, where Purdue University is so in those days you could go over to campus and log in to the university to play games, so that is where it started. I began in horticulture; and, then, I switched to engineering. And, then, I switched to computer science. So I was a Unix system administrator and a programmer and at some point I moved out to California and I worked for a place at Nasa and then I went to work for SRI International which use to stand for Stanford Research Institute before spinning off in the 1970s. We had army contracts and we did stuff with Fort Bragg and Fort Lewis. One of the thing I did was communications in Fort Monmouth, New Jersey. They had had their systems get broken into; and, so I put together as part of my job a 50-60 page document on security at that point. That is kind of where I got into it. You can find that paper on the internet (INSERT LINK HERE). And, then I got married and moved back to Indianan; and, went to work for Perdu doing security for the engineering schools there then I moved out to IBM. So, I've been doing security ever since. At some point, I wrote a book on it (INSERT LINK HERE) which was expanding the SRI paper. For the silly trivia, apparently the paper from SRI which that book grew out of I used the word firewall. Apparently, I am the first person to use the word firewall in print. I did not invent firewalls. I do not take credit for inventing firewalls. But, when this book came out, about the same time as the first version of Practical Unix & Internet Security, which is the Garfinkel and Spafford which came out before the internet was a thing. I was on the phone at that time with some of the guys who invented firewalls, for example DEC SEAL, so I picked-up the term and threw sheer luck of the draw was actually the first person to put it on a piece of paper. So, when you get those job interview which say "tell us something unique about you" that is my story of there is something you don't know about me. I got this email out of the blue from someone doing research on the topic, I that is how

I found out. I then started searching around and sure enough, everyone was calling it a secure gateway, packet-filtering gateway…. All the things that it is. I picked up the word firewall from somewhere. I certainly did not coin the term.

2. Has there been significant changes to security, auditing, laws, and policy as data breaches are becoming more common?

No. Yes and no. So much of security is about the same things that is has always been which is controlling access to stuff; being careful about where you send it, encryption, …. And none of that has changed. What has changed is more the environment that you have to do these operations in. It used to be you had a computer on your desk or data center and that is where it was. Now you have everything in the cloud, which is just someone else's computer and someone else's datacenter. So, now you are at the mercy of whatever they have done as well as whatever you are responsible for. Depending on how you purchase your cloud services, you may be responsible for your own security. In Platform as a Service, they give you the tools, but you are responsible for turning them on and setting them up. In Software as a Service, where we using a cloud-based application, we are mostly at mercy of the application configuration. We have some control over who can access what inside the system, but in some sense we are taking on faith that the rest actually is secure. We have phones, laptops, tablets and USB drives all over. One of the things that has changes is the interconnectedness of suppliers. For example, some of the famous breaches show that the vendors were the source of the breach, not the company. It is more policy, process, and procedure, than just about technology.

There are differences in laws. There are different data breach laws in the different states. They are all the same and yet they are all different. They all focus on personally identifiable financial information. Typically, name, social security number, and about financial data. They all require the breach to notify someone in the state government within nearly the same amount of time. If you have a breach over multiple states, one of the hardest parts it to put together this whole spreadsheet of breach process across the states. And, the breach can cause a different response in each state. The different state breach laws are similar to the older GDPR directive where different countries had different laws doing the same thing in somewhat different ways. California just passed the CCNA, which takes into effect next year. It is very similar to the GDPR in California.

Policy is the same over time. Most of it is federal government. New York State has some additional laws on financial regulation. HIPAA only applies to covered entity, which is connected to the way billing is performed. Smaller university health centers may only be covered under FERPA since FERPA and HIPAA have mutual clauses. HIPAA was designed to protect electronic medical records. PCI regulations is industry standard. PCI shifts liability to merchants, so that the merchants must upgrade their equipment.

3. Since data breaches are happening across the globe at an unprecedented rate, are there any insights for future changes in technology as related to data breaches? (e.g. training, technology, administration, legal, auditing, etc.)

Training is always a problem. You can train people are you want, but at the end of the day, many of these breaches are targets of opportunity. Depending on what organization is involved, there are different targets. Organizations have different threats. Some threats to smaller organizations are on accessing computer resources for themselves to do one of two things---either to use the systems as a jumping off place to attack other things or use them for the current trend of starting up cryptocurrency. For those purposes, if they happen to break into a system that has sensitive data in it they will probably steal that data, too; however, the primary reason for breaking into the system initially was to hijack some resources. Most of the security issues in smaller organizations are around innocent mistakes without malicious intent. Sometimes you will see employees who want to work from home upload their information into their personal cloud storage provider drive box. These personal accounts do not have the proper contractual protections in place; and, they are, thus, not allowed by policy. Many places have people that are too busy to sit through training; and, is the training effective? You can sit through it or click through it. There are certain roles where for example require more extensive training for example on GDPR. Technology marches on, there are all kinds of solutions that the vendors keep coming up with. The vendors do not talk to each other and the services are painfully expensive. Most technology are outside many organizations budgets; and, many services have dubious value. Some organizations, which are under many security laws, have half million-security budgets. Someday the US may have their own GDPR in place in the United States. The breach laws came in around the 2000s and then the other states have followed over the last 18 years. There have been discussion about having national data breach laws. Banks on the other hand are subject to national data breach laws. There is a national data breach law with HIPAA. There is a smaller national data breach law under FERPA. Under FERPA, you have to notify the Department of Education; but you do not have to notify the students. Auditing. There used to be something called the SAS70 put out by the AICPA. The SAS70 was structured around you the customer to hire this CPA to come around and be an auditor. You would put together this statement of ‘this is what we do’ and they would come in and verify it. There were a couple of levels of that. One was that they would read your documentation and say ‘yep, you are good to go.’ And, then, there was a second type where they would read your documentation and then they would go out and look to see ‘if you are actually doing what you are saying you are doing.’ Around ten years ago, the AICPA realized that security was becoming a huge concern so they came out with the SOC—SOC1, SOC2, and SOC3. SOC2 Type 2 is the one that has is the strongest from a security perspective. It has a piece on security, a piece on privacy, a piece on disaster recovery, a piece on high availability, etc. There now is a set criteria of things to be audited on. SOC2 Type 2 is good when there is a SAAS provider, which is handling a lot of personal data. The SAAS needs to provide smaller organization with their annual findings and their plans for remediation. Also, an alternative is to be certified for ISO27000/1 or ISO27000/2 (there are a few other certifications). There are generally two types of auditing: (1) where they come in and audit you against your own policies; and (2) where they come in and audit you against set criteria.

4. I am building a M.S. Thesis in Data Visualization around data breaches--specifically HIPAA. (For example, I am bringing two posters that I recently designed which will be incorporated into the thesis.) Are there any data breach material (perhaps HIPAA related at the health center) which the New School could benefit from posting or distributing? (e.g. Posters, Handouts, Specialized Visualizations) It would be a huge benefit for part of the thesis to turn into an immediate product for a customer.

Yes. Nice poster. The quote is accurate; we do not care about the cost of the device. About phishing, during a recent phishing attack, we could see that the hackers ran scripts, which ‘tried’ different events. They were attacks, which were just run across schools. Ponemon is pretty good for their statistics.

Preparing for the phishing tests are interesting. Many of the phishing tests are caught by the Google spam filters; and, the Google spam filters learn.

5. Are there any specific additional insights about security and data breaches which you'd like to discuss?

I speak only on behalf of my personal professional experience and not the entire school If you would like, you can take our security training. Suzanna – Thank you very much for your time, David Curry! I will to complete the thesis.

What is Security?

Two recent large-scale ransomware attacks in 2017, Wannacry and Petya, have reminded the world that cyber security is essential for both global e-health as well as the people that rely on e-data and e-communications. The Wannacry ransomware recently effected hundreds of thousands of people globally by potentially exploiting a vulnerable external facing buffer and then using old-school worm techniques (e.g. generating random IP addresses) to spread and infect across the network (Brenner, 2017). Petya, according to Thomson (2017), appeared to mine administrator credentials out of memory and then use the stolen credentials to spread (i.e. worm in) to other machines in the network where the administrator has permissions.

In the following sections, we review categories around securing and protecting data. We speak about current technology trends and news stories. Our discussion brings forth topics in usable security such as current weaknesses and requirements. Our discussion ends with findings on current trends on visualizing cyber security related topics. Finally, we dive into ideas behind data breaches and cyber security issues such as traditional training and lack of ethics training in engineering curriculums.

Administrative Safeguards

Administrative safeguards involve the human interaction with technology. Traditionally, administrative safeguards include: a security management process, security personnel, information access management, workforce training and management and evaluation.

In specifically the security management process is ways an organization identifies and analyze potential risks to the organizational data and the security measures it implements to reduce risks and vulnerabilities to a reasonable and appropriate level.

Security personnel are designated security officials in an organization who are responsible for developing and implementing the security policies and procedures in an organization.

The information access management limits the use and disclosure of protected data to the minimum necessary based on implemented policies and procedures for authorizing access to protected data only when such access is appropriate based on the user or recipient's role (role-based access).

The workforce training and management traditionally provides for appropriate authorization and supervision of workforce members who work with protected organizational data. Organizations should train all workforce members regarding its security policies and procedures and should have and apply appropriate sanctions against workforce members who violate its policies and procedures.

Finally, evaluation involves a periodic assessment of how well its security policies and procedures meet the requirements of general security requirements (e.g. Financial Security Requirements and the Security Rule in HIPAA).

Security Management Process.

The Security Management Process examines the role of how security is manage in an organization. If an organization is retroactive, not keeping up-to-date or has any other form of week security management, there could be elements of the organization which are left completely unprotected from a cybersecurity perspective.

One recent example where a security management process had gaps was in the Office of Personnel Management (OPM) breach where over 22 million United States Citizens data was exposed to cyber hackers. Chappellet-Lanier (2017) wrote an article about a recent OPM audit that found the organization, "decided to extend authorizations for systems that had expired and those that were set to expire through fiscal 2016." Extending authorizations without going through proper controls can increase the risk of data loss, exploited vulnerabilities and breaches. Scyoc (2017) wrote a similar article titled, "2 Years After Massive Breach, OPM Isn't Sufficiently Vetting IT Systems" which summarized a recent audit of the OPM information technology systems. The audit found four major concerns: (1) LAN/WAN system security plan (SSP) was missing, (2) deficiencies in the security control testing, (3) security weaknesses detected during the LAN/WAN authorization were not appropriately tracked, and (4) critical authorization elements were missing. The complexity of the systems requires an adequate security management process.

In 2017 Consultancy.uk published an article titled, "Workload needed for Sarbanes-Oxley (SOX) compliance continues to rise." Their data shows that companies are investing more hours in ensuring compliance with SOX in the European Union (EU). Their data shows that each year companies are spending more hours working towards SOX compliance. According to a survey given, companies are seeing the increase in hours due to the following: (1) "increase in the requirements for process control documentation for high risk areas," (2) "entity-level controls classified as key controls has increased," (3) "workload resulting from increased scrutiny from external auditors has gone up," and (4) "organizations are also upping their internal testing efforts to ensure compliance." The Sarbanes-Oxley EU law relates, in part to, the United States Health Insurance Portability and Accountability Act (HIPAA) law of 1996.

Both laws are related to the protection of people’s personal identifying information (PII) from exposure and misuse.

Security Personnel.

Every organization which touches the internet in some form, even as basic as an employee checking a free email account or internet browsing, needs some level of cybersecurity protection. At the very least, phishing, still shown to be the number one risk to end users (Thubron, 2017), can transpire from anyone browsing the web or checking any kind of email account. Most organizations appoint some security personnel to oversee the diffusion of cybersecurity within an organization.

In 2015, an AT&T data breach resulted in AT&T to hire senior compliance managers (Chabrow, 2015). AT&T was fined $25million by the FCC for “call center employees in Mexico, Colombia and the Philippines accessing personally identifiable information from some 278,000 customer accounts without authorization (Chabrow, 2015).” The information collected was given to “unauthorized third parties who appear to have trafficked in stolen cell phones or secondary market phones that they wanted to unlock. (Chabrow, 2015)”

Chabrow (2015) writes, “the FCC is requiring AT&T to improve its privacy and data security practices by appointing a senior compliance manager who is a certified privacy professional, conduct a privacy risk assessment, implement an information security program, prepare appropriate compliance manuals and regularly train employees on the company's privacy policies and the applicable privacy legal authorities. AT&T will file regular compliance reports with the FCC.”

A press release issued by the HHS (HHS, 2016) reports that Care New England Health System (CNE), based on their actions, must pay a fine and agree to a comprehensive corrective action plan to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules. CNE’s lost two unencrypted backup tapes from its covered business associate, with whom it had a business associate agreement, Woman & Infants Hospital (WIH) of Rhode Island from two of its facilities. CNE provided WIE with corporate support, technical support, and information security. Part of the CNE settlement with the OCR involved establishes processes and policies within CNE such as immediately reporting security incidents to internally designated Privacy/Security Officers.

Information Access Management.

Information comes with very different security level requirements. In fact, basic information that we read from a Newspaper requires some level of assurance for the integrity of the information. Typically, information can be grouped into different severity levels. There is very little information which if modified will not affect end users. People with access to information can come with different modification privileges such as the standard Linux model of read, write and execute. Therefore, people with information access need management best practices to assure that the information upholds: availability, integrity and confidentiality.

Lenovo recently settled with the Federal Trade Commission (FTC) $3.5 million to be spread among 32 states for preinstalling hijacking software into their pre-shipped laptops in late 2014 to early 2015 (Weise, 2017). Up to 750,000 laptops were sold in the United States with the embedded hijacking software. According to Weise, “the VisualDiscovery program caused pop-up ads to appear on the user's screen whenever his or her cursor hovered over a similar-looking product on a website.” The users’ security was compromised in order to deliver ads.

As mentioned before, a press release issued by the HHS (HHS, 2016) reports that Care New England Health System (CNE), based on their actions, must pay a fine and agree to a comprehensive corrective action plan to settle potential violations of the HIPAA Privacy and Security Rules. Part of the corrective action plan requires all personal to sign the policies and procedures around interaction with

PHI. CNE must not allow any individual who does not agree to proper protections of PHI to interact with the data.

Workforce Training and Management.

"Securing the human" (SANS, 2017) is one of the most effective ways to lower risks to an organization. The more the human at the end of technology is aware of the risks, current threats and technical limitations when using the technology the better off people, their data and their organizations will be as the risks are lowered.

In early 2017, the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) announced a HIPAA settlement with the MAPFRE Life Insurance Company of Puerto Rico related to impermissible disclosure of electronic protected health information (ePHI) (Metzger, 2017a). Part of the misconduct indicated by the HHS OCR was a "failure to implement a security awareness and training program for all workforce members (Metzger, 2017a)." Metzger (2017a) indicates that part of the settlement requires MAPFRE to pay a $2.2M fine as well as institute a corrective action plan.

TJMAX Companies reached one of the largest databreach settlements in 2009, according to Kent (2017), which was $9.75m. This breach caused the credit card companies to issue a report from the Payment Card Industry Security Standards Council and subsequently enforce PCI compliance fines since credit cards were used (Zetter, 2009). Zetter's article indicates that the 33-page report included guidelines which are the product of the PCI-SSC working group composed of more than 40 entities – banks, network security companies and point-of-sale vendors. According to Zetter (2007), "TJX failed to notice thieves moving 80 gigabytes of data on its network." An estimated 96 million customers are estimated to have been effected by the breach which started in 2005.

An early 2005 audit, "of TJX's network found 'high-level deficiencies' in its security practices (Zetter, 2007). TJX was found to be non-compliant with 9 of 12 requirements established by the payment card industry for secure card transactions, according to Zetter (2007). The audit showed that, "problems included a misconfigured wireless network, improper anti-virus protection, weak intrusion-detection, use of user names and passwords that were easily cracked, and improper patch procedures and log maintenance (Zetter, 2007)." The TJX credit card breach was the largest in United States history until the Target breach in 2013 (Kent, 2017).

According to Stone (2009), the Justice Department has indicated that Albert Gonzalez, 28, of Miami and two unnamed Russian conspirators made off with more than 130 million credit and debit card numbers from late 2006 to early 2008 which included the credit card information collected at TJX.

Periodic (Re)Evaluation.

Software can change over time. Every time someone installs a new system, installs updated software update, changes the data they put into the technology or changes the architecture of their systems, risks may change. As risks changes, technology and processes surrounding these technologies should be (re) evaluated so that the risks can be understood. Similarly to building a house or making changes to a house, someone needs to evaluate the plans to ensure that undue risk is not being added into the house and subsequently the family living within.

Metzger (2017b) writes, "HIPAA Risk Analysis Lapses Lead to OCR Enforcement: How Is Your Security Management Process?" In the article Metzger wrote that the "Metro Community Provider Network (MCPN), a HIPAA covered entity (CE), agreed to pay a $400,000 resolution amount and enter into a corrective action plan (CAP) after workforce members fell victim to a phishing scam that resulted in unauthorized disclosures of protected health information." According to the Metzger article the MCPN had "not conducted an assessment of risks and vulnerabilities to ePHI before the phishing incident, and therefore, had not instituted a plan to appropriately reduce existing risks and vulnerabilities. Further, MCPN did not conduct a risk analysis until several weeks after the phishing attack, and OCR determined that this analysis was insufficient to meet HIPAA Security Rule requirements."

According to an article by Katten Muchin Rosenman (2016), the "Feinstein Institute for Medical Research (FIMR), a nonprofit research institute, will pay $3.9 million and enter into a three-year corrective action plan to settle charges it violated HIPAA, following its breach when an employee's unencrypted laptop containing patient information of 13,000 individuals was stolen." As part of the three-year corrective action plan the organization must "conduct an organization-wide risk analysis and develop a corresponding risk management plan, develop a process for evaluating environmental or operational changes to the security of ePHI, revise its policies and procedures for privacy and security, and provide extensive training and reporting."

Technical Safeguards

Traditionally, technical safeguards involve technology constructs to protect a system such as access control, audit control, integrity control and transmission control.

Access control are implement technical policies and procedures that allow only authorized persons to access protected organizational data.

Audit controls are implemented hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use protected data.

Integrity controls are implemented policies and procedures to ensure that protected data is not improperly altered or destroyed. In such cases, electronic measures must be put in place to confirm that protected data has not been improperly altered or destroyed.

Finally, transmission security requires the implementation of technical security measures that guard against unauthorized access to protected organizational data that is being transmitted over an electronic network.

Access Control (e.g. authentication)

Not everyone should be able to access all data. Certain data is for certain people. Therefore, good technology should have developed adequate access control mechanisms to prevent unauthorized people from retrieving the private data. There are many types of access control including two factor, biometrics and plain old password systems. Passwords should not be sent to the user in plaintext as there is no basic email encryption protection globally in place. Encryption is something the endpoint people and their systems must put in on top of email.

In the news, Andy Greenberg published an article on Wired.com where University of Tulsa researchers (one named Jason Staggs) performed penetration tests on five different wind farms and found many cyber security vulnerabilities. In fact, the article quotes Staggs, “They don’t take into consideration that someone can just pick a lock and plug in a Raspberry Pi.” The researchers simply picked the turbine tumbler lock on the metal door in less than a minute and opened the unsecured server closet inside where they plugged in a Rasberry Pi and in three of five cases took over the wind farm.

In May 2017, Goodin wrote an article about the Greyhound.com website. According to the article, the website will not let users change passwords and, in fact, emails the users in plain text. The plaintext email can be sniffed off the network but the fact that it email the entire password in plaintext indicates that it may be stored in plaintext on the Greyhound server. If the server is ever compromised all emails and passwords will most likely rest there in plaintext, too. Storing data in the cloud can be quite beneficial but it comes with risks much like trusting your friend with your keys to your house.

Audit Controls.

Activity monitoring is extremely important. When grades change or system configuration changes, we need to have an audit trail of who and how these items were changed. These audit controls provides a methodology to confirm that a system is running correctly. These audit data can be used during real life audits from entities such as the Office of Civil Rights (OCR), Internal Revenue Service (IRS), Federal Bureau of Investigations (FBI), etc.

Geller (2017), writes that Colorado, “will become the first state to regularly conduct a sophisticated post-election audit that cybersecurity experts have long called necessary for ensuring hackers aren't meddling with vote tallies.” According to the article, “Colorado enacted the audit requirement in 2009 but delayed its implementation to allow counties to test different methods.”

According to Cave and Difuntorum (2017), the National Highway Traffic Safety Administration (“NHTSA”) issued cybersecurity best practices that promote a layered approach to vehicle cybersecurity. The #6 best practices (Cave and Difuntorum, 2017) requires cars to, “document the details related to the cybersecurity process to allow for auditing and accountability.”

Integrity Controls.

How can we ensure that the data we have stored and are using has not been tampered with or changed? How can we ensure our records remain accurate so that when we visit our online bank system that it correctly reflects the state of our account? How can we ensure our medical records have all the correct data about the medications embedded into them? Integrity controls, such as checksums, ensure that the data at rest *adds up* to what is should add up too. Checksums are different than encryption since encryption only provides confidentiality but does not guarantee that what is encrypted is accurate to begin with. Integrity is very important for information and system reliability.

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT, 2017e), issued an advisory for Hyundai Motor America Blue Link (ICSA-17-115-03) for two vulnerabilities: man-in-the-middle and use of hard-coded cryptographic key. According to ICS-CERT, “successful exploitation of these vulnerabilities may allow a remote attacker to gain access to insecurely transmitted sensitive information, which could allow the attacker to locate, unlock, and start a vehicle associated with the affected application."

According to ICS-CERT (2017b), the Philips' DoseWise Portal (DWP) has vulnerabilities which have been identified with hard-coded credentials as well as the clear text storage (i.e. non-encrypted) of sensitive information in the DWP web application. Philips had to update their product documentation and produce a new DWP version that mitigates these vulnerabilities. According to ICS-CERT (2017b), "Successful exploitation may allow a remote attacker to gain access to the database of the DWP application, which contains patient health information (PHI). Potential impact could therefore include compromise of patient confidentiality, system integrity, and/or system availability."

Transmission Security.

Transmission security ensure that data is as secure as possible when being transmitted across a network. Transmission security is not necessarily a given when using *HTTPS*. The secure HTTP (*HTTPS*) protocol transmission relies on encryption keys, domain certificates and actual additional transmission protocols such as TLSv1, TLSv0, SSLv3, SSLv2, etc. If there is a weakness in any parts of this system, the entire transmission of data is compromised. For example, using SSL any version is considered bad practice since it is easily broken.

Recently the United States Department of Homeland Security (DHS) and ICS-CERT (2017a) has warned of eight new vulnerabilities in several popular medical syringe infusion pump models which could allow a remote hacker to alter how they work (Muncaster, 2017). One of these types is Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump (ICS-CERT, 2017a). According to ICS-CERT, "Successful exploitation of these vulnerabilities may allow a remote attacker to gain unauthorized access and impact the intended operation of the pump."

According to ICS-CERT (2017f), St. Jude Merlin@home transmitter has a vulnerability where "successful exploitation of this vulnerability may allow a remote attacker to access or influence communications between Merlin.net and transmitter endpoints." St. Jude Medical has validated the vulnerability and produced a new software version that mitigates this vulnerability.

Secure Code Development Improvements

Secure code development is not only considered best practice, it is actually a requirement for developers to undergo secure code development training annually to maintain their PCI-Compliance development credentials. PCI-Compliance is what is enforced by the credit card and banking industry to ensure that financial data is being treated correctly.

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT, 2017c), issued a warning about BMC Medical and 3B Medical Luna CPAP machines. According to ICS-CERT, "MedSec has identified an improper input validation vulnerability in BMC Medical's and 3B Medical's Luna continuous positive airway pressure (CPAP) therapy machine. For devices released after July 1, 2017, this vulnerability has been addressed. For devices released prior to July 1, 2017, BMC Medical and 3B Medical offer no mitigations." According to ICS-CERT, "Successful exploitation of this vulnerability could allow an attacker to cause a crash of the device's Wi-Fi module resulting in a denial-of-service condition affecting the Wi-Fi module chipset. This does not affect the device's ability to deliver therapy."

Hikvision Cameras has been show with ICS-CERT (2017d) and advisory (ICSA-17-124-01) that their the have two major vulnerabilities: improper authentication and the system password is housed in the configuration file. The impact indicates that "successful exploitation of these vulnerabilities could lead to a malicious attacker escalating his or her privileges or assuming the identity of an authenticated user and obtaining sensitive data."

Physical Safeguards

Physical safeguards traditionally are how e-technology and e-communications are safeguarded physically. Two ways to examine physical safeguards are through he facility access and control and through workstation security and device security.

Facility access and control requires the limitation to physical access to its facilities from unauthorized parties while ensuring that authorized parties access is allowed.

Security of workstations and devices ensure that an organization or entity has implemented policies and procedures to specify proper use of and access to workstations and electronic media. For example, an organization should have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of protected organizational data.

Facility Access and Control.

The physical storage of equipment is just as important as the technical and administrative use of equipment. If for example a confidential server is left in the middle of the street, then the risk of exposing the data and functionality of the system becomes high. Many organizations, such as the Yahoo! paranoids, have members on their security team visit all offices globally to check the security of their international systems. Simple problems arise such as the way the door is place on the frame (e.g. externally exposing the hinges, placing the door release sensor too close to the door so that someone from the outside can spoof the opening of the sensor by passing a card through the top of the door, etc.).

In the news, it has recently been shown that locked doors can be fooled into being opened from the outside by triggering internal motion sensors using e-cigarettes (TODO, cite). The e-cigarette may trigger the system fire response software to unlock the door.

Ben-Gurion University of the Negev (BGU) researchers have demonstrated that security cameras infected with malware can receive covert signals and leak sensitive information from the very same surveillance devices used to protect facilities (Phys.org, 2017).

Workstation and Device Security.

Devices need to be maintained over time. Similar to maintain a card or license, devices need to be (re)evaluated so that they do not expose weaknesses into systems and networks. Computer devices are not being manufactured to be bought, installed and left unattended indefinitely.

Perhaps the weakness here is in non-creative education. Professors tend to teach what they know and test students on the current or past trends in industry. The tests are simply put in place as superficial legal boundaries, which, in many cases, are simply recycled repeatedly every semester so that professors do not have to spend too much time developing a new test. Professors rarely train students to think about the big picture and to think about the future. Encryption techniques change over time. Transmission security changes over time. Integrity technology changes over time. Cryptographic protocols change over time. Biometrics change over time. Testing students on recycled current trends makes students nearly outdated and organizationally useless when they graduate. Professors are not worried about this issue it seems; they are predominately worried about their own paycheck at the expense of society. Developers are being unleased into society without an adequate understanding of how their research fits into a bigger picture, if it even fits in at all. Research importance is still primarily based on feelings about a student rather than any other factor. Research is mainly being done as a perfunctory exercise for tenure rather than true novel and useful research. These trends are scary and can leave to a bankrupt society where time and money become exhausted for exercises that focus on the wrong elements.

McGee (2017a) writes about how a ransomware attack effects 500,000 patients through a provider of oxygen therapy and home medical equipment. The quantity of effected data make the attack the second largest health data breach posted on the federal Office of Civil Rights 'Wall of Shame.' Information that was breached included patient names, addresses, birth dates, telephone numbers, diagnosis, the type of service providing and their health insurance policy numbers.

McGee (2017b) discusses that "under the HIPAA Breach Notification Rule, the theft or loss of encrypted computing or storage devices is not considered a reportable data breach." However, the article discusses an incident at the Bowling Green, Kentucky-based Med Center Health, where an employee "allegedly obtained patient information on an encrypted CD and encrypted USB drive, 'without any work-related reason to do so.'" Data that was leaked included billing information comprised of patients' names, addresses, Social Security numbers, health insurance information, diagnoses codes, procedure codes and charges for medical services. This data breach may be followed-up with OCR fines.

Privacy

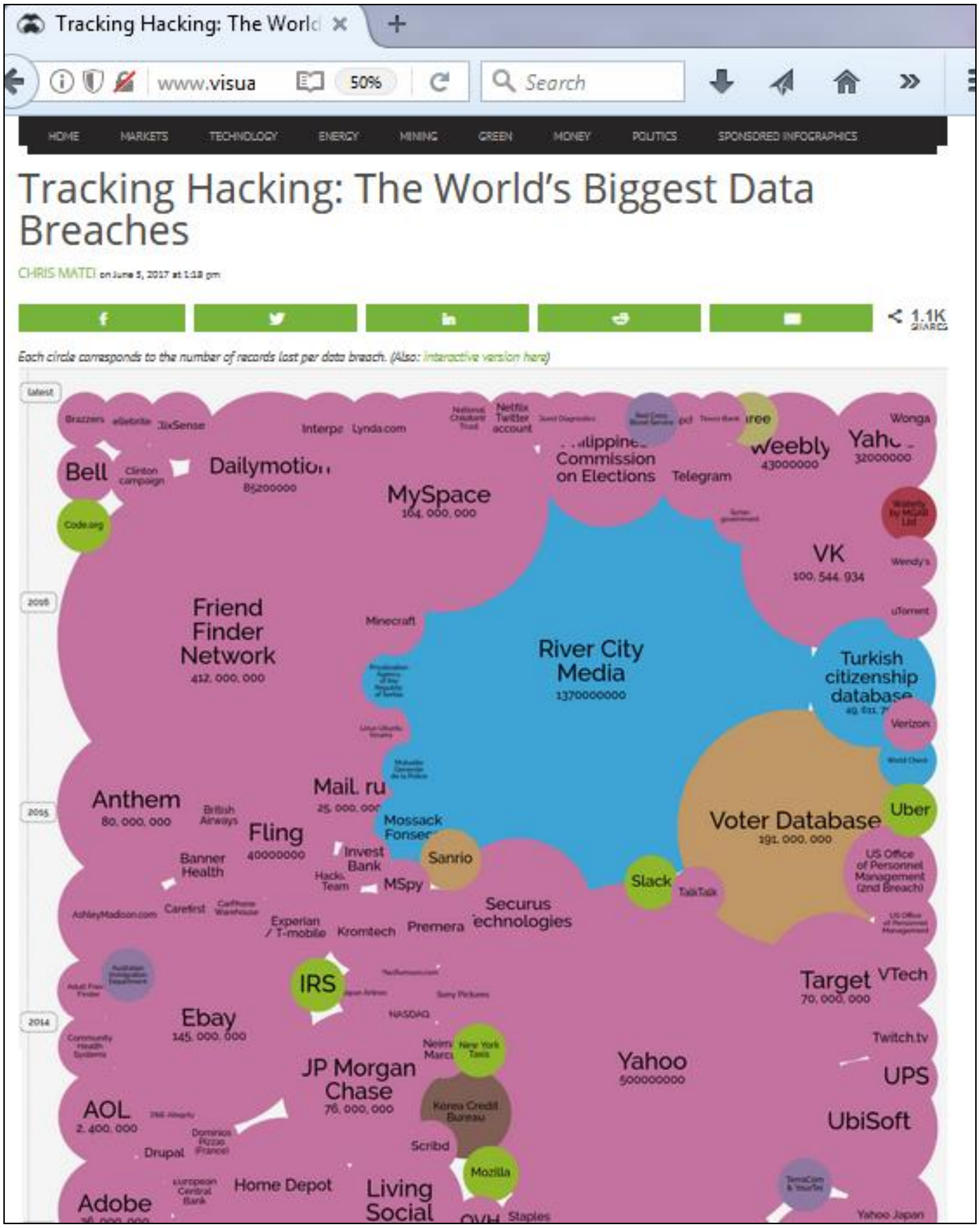
The HIPAA Privacy Rule complements the HIPAA Security Rule (HHS, 2003). An organization can have a Chief Security Officer as well as a Chief Privacy Officer. According to the summary, "The Privacy Rule standards address the use and disclosure of individuals' health information—called "protected health information" by organizations subject to the Privacy Rule — called "covered entities," as well as standards for individuals' privacy rights to understand and control how their health information is used." At the Federal level, within United States Department of Health and Human Services (HHS), the Office for Civil Rights (OCR) has the responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties. At the state level, the State Attorney General (SAG) has the responsibility for implementing and enforcing the Privacy Rule at the State Level.

Visualization of Security Issues

Visualization of security issues and usable security is very important. Visualization can be used to show public data loss, security events and health security events. Matel (2017) plots the data breach size over time in his visualization in Figure 1. This type of visualization is a bit misleading since it does not indicate information importance.   A further visualization could add a 3rd dimension to the plot based on data importance.

Data Breach size as compared to Time

An interesting visualization can be the size affected by a data breach during time as seen below by Matei (2017). The Equifax data breach of 2017 would now need to be added to the below diagram. Another interesting study would be of the people names affected by the various data breaches. How many letters has any one person received as notice that their data was lost in a databreach?



Tracking Hacking: The World's Biggest Data Breaches

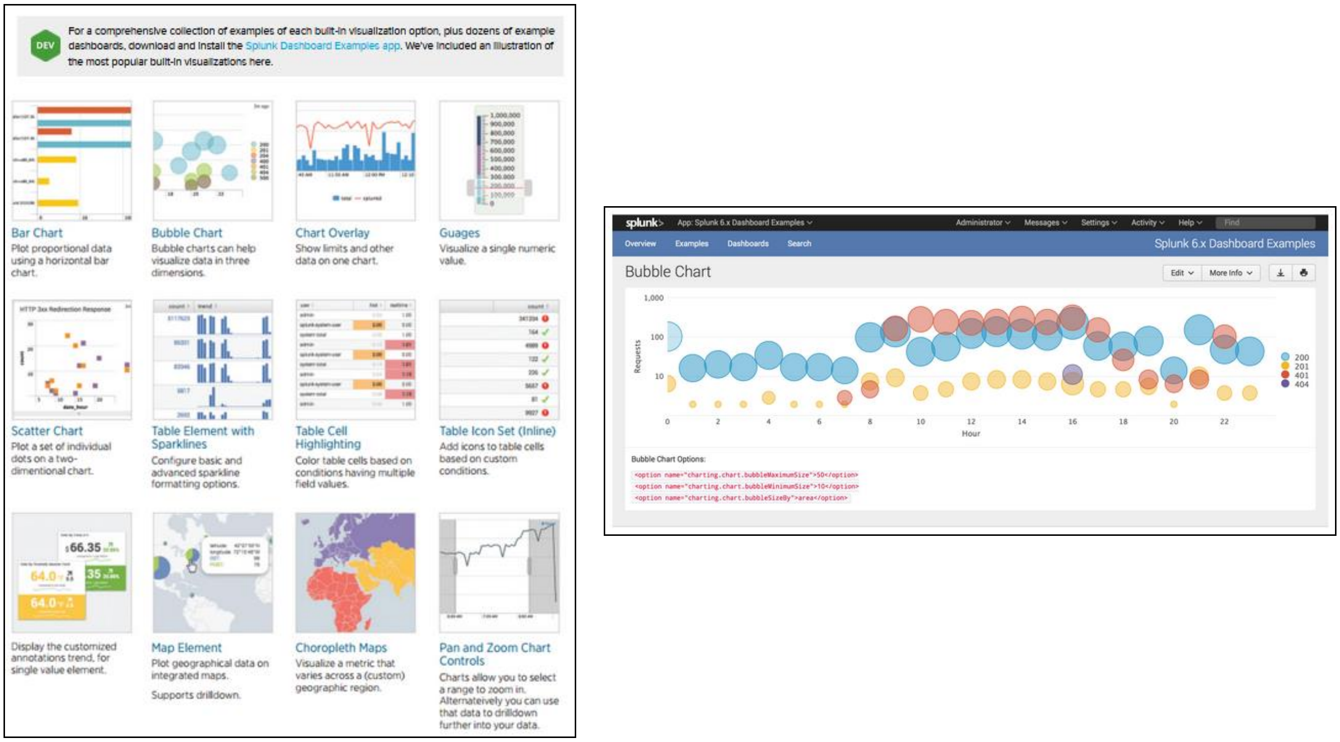
CHRIS MATEI on June 5, 2017 at 1:18 pm

Each circle corresponds to the number of records lost per data breach. (Also: interactive version here)

Figure 1. Chris Matei (2017)

Security Events

Splunk is a popular log aggregation tool useful for visualizing events occurring in the logs. The figures below show some of the Splunk visualization charts given on their online content (Splunk, 2017) as follows: Bar, Bubble, Overlay, Gagues, Scatter, Table, Table Cell Highlighting, Table Icon Set, Map, Choropath, Zoom and Customized. The tool is proprietary but it helps users quickly visualize events occurring in the logs to recognize and pinpoint certain activities.



For a comprehensive collection of examples of each built-in visualization option, plus dozens of example dashboards, download and install the Splunk Dashboard Examples app. We've included an illustration of the most popular built-in visualizations here.

Bar Chart
Plot proportional data using a horizontal bar chart.

Bubble Chart
Bubble charts can help visualize data in three dimensions.

Chart Overlay
Show limits and other data on one chart.

Guages
Visualize a single numeric value.

Scatter Chart
Plot a set of individual dots on a two-dimentional chart.

Table Element with Sparklines
Configure basic and advanced sparkline formatting options.

Table Cell Highlighting
Color table cells based on conditions having multiple field values.

Table Icon Set (Inline)
Add icons to table cells based on custom conditions.

Display the customized annotations trend, for single value element.

Map Element
Plot geographical data on integrated maps.
Supports drilldown.

Choropleth Maps
Visualize a metric that varies across a (custom) geographic region.

Pan and Zoom Chart Controls
Charts allow you to select a range to zoom in. Alternateively you can use that data to drilldown further into your data.

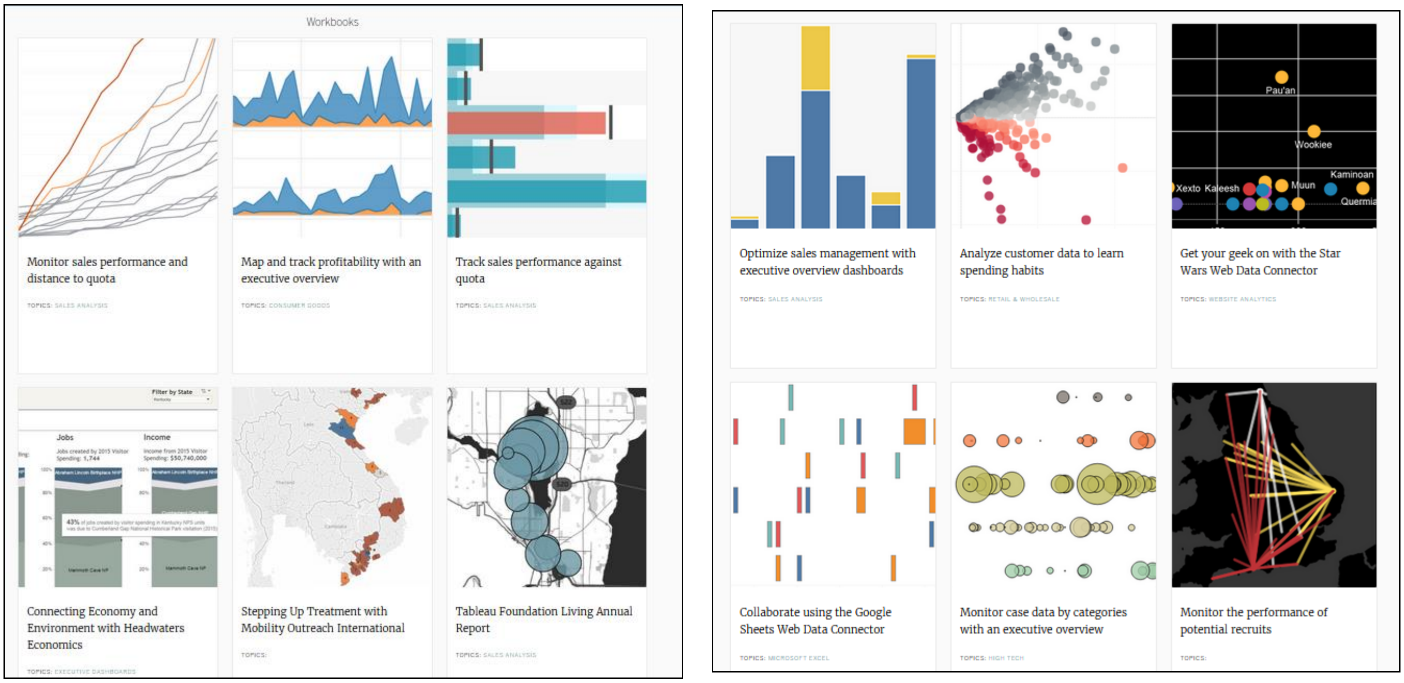
Bubble Chart Options:

```
<option name="charting.chart.bubbleMaximumSize">50</option>
<option name="charting.chart.bubbleMinimumSize">10</option>
<option name="charting.chart.bubbleSizeBy">area</option>
```

Figure 2. Splunk (2017)

Health Care Events

Tableau (Tableau, 2017a) is another popular system to visualize event data (Tableau, 2017). It is comprised of a proprietary language and visualization package. It is a language traditionally not taught in an academic setting but is quite popular across the globe in industry. The figure below shows some of the proprietary dashboards as Tableau has posted for the public on their website (Tableau, 2017b).


Workbooks
Filter by State
Jobs
Income
43% of jobs created by visitor spending in Kentucky NPS units was due to Cumberland Gap National Historical Park visitation (2015)
Mammoth Cave NP
Pau'an
Wookiee
Kaminoan
Xexto
Kaleesh
Muun
Quermia

Monitor sales performance and distance to quota

TOPICS: SALES ANALYSIS

Map and track profitability with an executive overview

TOPICS: CONSUMER GOODS

Track sales performance against quota

TOPICS: SALES ANALYSIS

Connecting Economy and Environment with Headwaters Economics

TOPICS: EXECUTIVE DASHBOARDS

Stepping Up Treatment with Mobility Outreach International

TOPICS:

Tableau Foundation Living Annual Report

TOPICS: SALES ANALYSIS

Optimize sales management with executive overview dashboards

TOPICS: SALES ANALYSIS

Analyze customer data to learn spending habits

TOPICS: RETAIL & WHOLESALE

Get your geek on with the Star Wars Web Data Connector

TOPICS: WEBSITE ANALYTICS

Collaborate using the Google Sheets Web Data Connector

TOPICS: MICROSOFT EXCEL

Monitor case data by categories with an executive overview

TOPICS: HIGH TECH

Monitor the performance of potential recruits

TOPICS:

Figure 3. Tableau (2017b)

Hospitals need data visualization (O'Dowd, 2017). They are one of the largest Tableau customers (McCarthy, 2016). They can quickly develop applications to visualize their data. Interestingly, any academic graduates would have to learn Tableau to get a job requiring Tableau since it is not taught in academia. Here is another example of how academia is not keeping up with current industry demands or futuristic trends.

Visualizing Security Products

Security products weaknesses and strengths can be visualized using techniques such as SWOT analysis or Gartner's Magic Quadrants.

Data Visualization for Teaching Security Concepts

Other visualizations include research on teaching visualizing access control (Wang et al., 2014; Heitzmann et al., 2008).

Conclusion

This research has explored many requirements for ethical treatment of data. The findings include current known trends in visualizing security-related topics for the ethical treatment of data which effects many people since all collected data belongs to someone (Gitelman, 2013).

Recently, the Army created a reserved guard cyber task force (Tomkins, 2017). These trends are showing us there are new needs in society to address these concerns. Our society is moving more and more towards interconnection. We are implicitly trusting each other when we buy devices and bring them into our home (Gitelman, 2013). Should devices blindly be trusted off the shelf?

References

Bill Brenner, Deconstructing Petya: how it spreads and how to fight back. 28 Jun 2017 6 Malware, Ransomware, Security threats, SophosLabs. https://nakedsecurity.sophos.com/2017/06/28/deconstructing-petya-how-it-spreads-and-how-to-fight-back/

Kristen V. Brown. (2017) DARPA's Brain Chip Implants Could Be the Next Big Mental Health Breakthrough—Or a Total Disaster. Retrieved from: https://gizmodo.com/darpa-s-brain-chips-could-be-the-next-big-mental-health-1791549701

Bryan Cave and Ashlee Difuntorum (2017). Cybersecurity Issues of Self-Driving Vehicles. Retrieved from: http://www.jdsupra.com/legalnews/cybersecurity-issues-of-self-driving-27237/

CBC. (2017). University of Regina Engineering grades hacked Dean. Retrieved from: http://www.cbc.ca/news/canada/saskatchewan/university-of-regina-engineering-grades-hacked-dean-1.4368984

Eric Chabrow. (2015). Insider Breach Costs AT&T $25 Million. Retrieved from: https://www.bankinfosecurity.com/insider-breach-costs-att-25-million-a-8089

Tobias Christen. (2009) CTO. DSwiss / DataInherit. Usable Security. The OWASP Foundation. OWASP-Italy Day IV. Milan. Retrieved from: https://www.owasp.org/images/e/e0/UsableSecurity.pdf

Consultancy.uk (2017) Workload needed for Sarbanes-Oxley (SOX) compliance continues to rise. Retrieved from: http://www.consultancy.uk/news/13688/workload-needed-for-sarbanes-oxley-sox-compliance-continues-to-rise

Lorrie Cranor, Michael Reiter and Jason Hong. "5-899/17-500 Usable Privacy and Security" http://cups.cs.cmu.edu/courses/ups.html

Tajha Chappellet-Lanier. (2017). Audit: OPM still faces information security weaknesses 2 years after breaches. Retrieved from: https://www.fedscoop.com/opm-security-audit-2017/

Ryan J. Foley. (2017). High-tech cheating scheme prompts charges at University of Iowa. Retrieved from: http%3a%2f%2fwww.press-citizen.com%2fstory%2fnews%2feducation%2funiversity-of-iowa%2f2017%2f10%2f27%2fhigh-tech-cheating-scheme-prompts-charges-university-iowa%2f808335001%2f

The United States Department of Health and Human Services (HHS). (2003) Summary of the HIPAA Privacy Rule. Retrieved from: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

Eric Geller. (2017). Colorado to require advanced post-election audits. Retrieved from: http://www.politico.com/story/2017/07/17/colorado-post-election-audits-cybersecurity-240631

Lisa Gitelman. (2013). "Raw Data" is an Oxymoron. MIT Press.

Andy Greenberg. (2017) Researchers Found They Could Hack Entire Wind Farms. Wired.com Retrieved from: https://www.wired.com/story/wind-turbine-hack/

Dan Goodin. Risk Assessment — Meet Greyhound.com, the site that doesn't allow password changes Greyhound allows four-digit PINs and stores them in plaintext. 5/1/2017, 1:28 PM. https://arstechnica.com/security/2017/05/when-it-comes-to-password-security-greyhound-com-is-truly-awful

Jennifer Golbeck. (2017) Director Human-Computer Interaction Lab. Created by the University of Maryland, College Park. Usable Security. Coursera. Retrieved from: https://www.coursera.org/learn/usable-security

Christal Hayes (2017). UCF boosts safeguards of grading program after hack, arrests of 2 students. Retrieved from: http://www.orlandosentinel.com/news/breaking-news/os-ucf-student-grade-change-20170725-story.html

HHS. (2016) HIPAA settlement illustrates the importance of reviewing and updating, as necessary, business associate agreements – September 23, 2016.Retrieved from: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/wih

Alexander Heitzmann, Bernardo Palazzi, Charalampos Papamanthou, and Roberto Tamassia. 2008. Effective Visualization of File System Access-Control. In *Proceedings of the 5th international workshop on Visualization for Computer Security* (VizSec '08), John R. Goodall, Gregory Conti, and Kwan-Liu Ma (Eds.). Springer-Verlag, Berlin, Heidelberg, 18-25. DOI=http://dx.doi.org/10.1007/978-3-540-85933-8_2

ICS-CERT. (2017a) Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump Vulnerabilities. Advisory (ICSMA-17-250-02). Retrieved from: https://ics-cert.us-cert.gov/advisories/ICSMA-17-250-02

ICS-CERT. (2017b) Philips' DoseWise Portal Vulnerabilities. Advisory (ICSMA-17-229-01). Retrieved from: https://ics-cert.us-cert.gov/advisories/ICSMA-17-229-01

ICS-CERT. (2017c). BMC Medical and 3B Medical Luna CPAP Machine. Advisory (ICSMA-17-227-01). Retrieved from: https://ics-cert.us-cert.gov/advisories/ICSMA-17-227-01

ICS-CERT. (2017d). Hikvision Cameras. Advisory (ICSA-17-124-01). Retrieved from: https://ics-cert.us-cert.gov/advisories/ICSA-17-124-01

ICS-CERT. (2017e). Hyundai Motor America Blue Link. Advisory (ICSA-17-115-03). Retrieved from: https://ics-cert.us-cert.gov/advisories/ICSA-17-115-03

ICS-CERT. (2017f). St. Jude Merlin@home Transmitter Vulnerability (Update A) Advisory (ICSMA-17-009-01A). Retrieved from: https://ics-cert.us-cert.gov/advisories/ICSMA-17-009-01A

Kana Inagaki. (2017) Honda plant hit by WannaCry ransomware attack. Retrieved from: https://www.ft.com/content/a0f5d047-2e20-3db9-b258-565d3be17bba

Ben Johnson and Kristin Schwab. (2017) Why this ransomware attack is more alarming than the last. Retrieved from: https://www.marketplace.org/2017/06/28/tech/why-ransomware-attack-more-alarming

Spencer Kent. (2017). Target to pay $18.5M in largest data breach settlement in U.S. Retrieved from: http://www.nj.com/news/index.ssf/2017/05/target_to_pay_185m_to_settle_massive_2013_data_bre.html

Marianne Kolbasuk McGee. (2017a) Ransomware Attack Affects 500,000 Patients. Retrieved from: http://www.bankinfosecurity.com/ransomware-attack-impacts-500000-patients-employees-a-10057

Marianne Kolbasuk McGee. (2017b) Breach Involving Encrypted Devices Raises Questions. Retrieved from: http://www.healthcareinfosecurity.com/breach-involving-encrypted-devices-raises-questions-a-9789

Butler Lampson. (2009). Privacy and security: Usable security: how to get it. Communications of the ACM 52, 11, 25-27. DOI=http://dx.doi.org/10.1145/1592761.1592773

Chris Matei. (2017) Tracking Hacking: The World’s Biggest Data Breaches. Retrieved from: http://www.visualcapitalist.com/worlds-biggest-data-breaches/

Kimberly C. Metzger. (2017a). $2.2 Million HIPAA Settlement Emphasizes the Importance of a Security Management Process. Retrieved from: https://www.icemiller.com/ice-on-fire-insights/publications/2-2-million-hipaa-settlement/

Kimberly C. Metzger. (2017b). HIPAA Risk Analysis Lapses Lead to OCR Enforcement: How Is Your Security Management Process? Retrieved from: https://www.icemiller.com/ice-on-fire-insights/publications/hipaa-risk-analysis-lapses-lead-to-ocr-enforcement/

Jack McCarthy. (2016). Tableau Software lays down product roadmap for enhanced data analytics. Retrieved from: http://www.healthcareitnews.com/news/tableau-software-lays-down-product-roadmap-enhanced-data-analytics

MITRE. (2017) Common Weakness Enumeration. Retrieved from: https://cwe.mitre.org/

Phil Muncaster. (2017). Alert Over Bugs in Medfusion Syringe Pumps. Retrieved from: https://www.infosecurity-magazine.com/news/alert-bugs-medfusion-syringe-pump/

National Institute of Standards (NIST). (2017). National Vulnerability Database. Retrieved from: https://nvd.nist.gov/

Elizabeth O'Dowd. (2017). Advanced Visualization Critical to Health IT Data Analytics. Retrieved from: https://hitinfrastructure.com/news/advanced-visualization-critical-to-health-it-data-analytics

Office for Civil Rights (OCR). (2013) Summary of the HIPAA Security Rule. Retrieved from: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

phys.org. (2017). Security cameras are vulnerable to attacks using infrared light: study. Retrieved from: https://phys.org/news/2017-09-cameras-vulnerable-infrared.html

Katten Muchin Rosenman (2016). OCR Kicks Off HIPAA Audits After Issuing Two Major Settlements. Retrieved from:https://www.kattenlaw.com/OCR-Kicks-Off-HIPAA-Audits-After-Issuing-Two-Major-Settlements

SANS. (2017). Securing the human. Retrieved from: https://securingthehuman.sans.org/

Scyoc, Mark Van. (2017) 2 Years After Massive Breach, OPM Isn’t Sufficiently Vetting IT Systems. Retrieved from: http://www.nextgov.com/cybersecurity/2017/07/two-years-after-massive-breach-opm-isnt-sufficiently-vetting-it-systems/139321/

Splunk. (2017) Dev. Visualizing data. Retrieved from: http://dev.splunk.com/view/dev-guide/SP-CAAAE3C

Brad Stone. (2009). 3 Indicted in Theft of 130 Million Card Numbers. Retrieved from: http://www.nytimes.com/2009/08/18/technology/18card.html?mcubz=0

Sydney.edu.au. (2017). The TJX Data loss and security breach case. Retrieved from: http://sydney.edu.au/engineering/it/courses/info5990/Supplements/Week07_Malware&Security/Supp07-4TJXCaseDetails.pdf

Tableau. (2017a) Homepage. Retrieved from: https://www.tableau.com

Tableau. (2017b) Data Visualization. Retrieved from: https://www.tableau.com/solutions/topic/data-visualization

Iain Thomson. (2017) Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide. This isn't ransomware – it's merry chaos. Retrieved from: https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/

Rob Thubron. (2017) Google: data breaches responsible for most stolen credentials, but phishing is biggest threat. Retrieved from: https://www.techspot.com/news/71843-google-data-breaches-responsible-most-stolen-credentials-but.html

Richard Tomkins. (2017). National Guard activates cyber-security task force. Retrieved from: https://www.upi.com/National-Guard-activates-cyber-security-task-force/7571503078722/

United Nations, (1987) Our Common Future - Brundtland Report. Oxford University Press.

United Nations, (2007) Framing Sustainable Development. The Brundtland Report – 20 Years On. Retrieved from: http://www.un.org/esa/sustdev/csd/csd15/media/backgrounder_brundtland.pdf

U.S. News (2017). 2018 Best Engineering Schools. Retrieved from: https://www.usnews.com/best-graduate-schools/top-engineering-schools

Man Wang, Steve Carr, Jean Mayo, Ching-Kuang Shene, and Chaoli Wang. (2014) MLSvisual: a visualization tool for teaching access control using multi-level security. In *Proceedings of the 2014 conference on Innovation & technology in computer science education* (ITiCSE '14). ACM, New York, NY, USA, 93-98. DOI: http://dx.doi.org/10.1145/2591708.2591730

Elizabeth Weise. (2017). FTC settles with Lenovo over a built-in snooping software, $3.5 million fine. Retrieved from: https://www.usatoday.com/story/tech/2017/09/05/ftc-settles-lenovo-over-built-snooping-software-scanned-users-computers/632775001/

Mará Rose Williams. (2017). Easy-to-get hacking device puts KU professors' information in student's hands. Retrieved from: http://www.kansascity.com/news/local/article178522396.html

Will Yakowicz. (2017) Ex-NSA Analyst: Hackers Can Use E-Cigarettes and Whiskey to Get Your Most Sensitive Data. Inc.com. Retrieved from: https://www.inc.com/will-yakowicz/hackers-use-e-cigarettes-whiskey.html

Kim Zetter. (2009). 4 Years After TJX Hack, Payment Industry Sets Security Standards. Retrieved from: https://www.wired.com/2009/07/pci/

Kim Zetter. (2007). TJX Failed to Notice Thieves Moving 80-GB. Retrieved from: https://www.wired.com/2007/10/tjx-failed-to-n/