Positioning Analytics in Information Technology Security

A good story can engage the listener and build on the power of our belief. Our goal here, as we talked about in the first chapter, is to build our beliefs on the feedback we collect from our environment. Fortunately, we don’t have to reinvent the wheel here, there have been generations of people attempting to the exact same thing and they’ve place a label on it: Statistics.

Before we dive into this topic (and we won’t dive deep), we understand that the word “statistics” can cause even the bravest of tech warriors to reach for the nearest pitchfork. Data and statistics are often abused and misused (and in some cases flat out made up) for the sake of serving an ulterior motive. However, we are in a different situation. We are sitting on a mound of data and we need to understand the stories lying therein. We cannot afford to ignore the work of honest and hardworking stats-geeks that have already found dozens of methods that don’t work. The quickest way to be fooled by data is through the avoidance of statistics. But let’s not rush in headfirst because the second quickest way to be fooled by data is to use statistics. [this is a huge point that I’m failing to hit on the head] This chapter will help the reader take a big first step towards making sense of data by introducing some simple methods of seeing into data: arithmetic, buckets and comparisons. But before we get to that we need to take a step back and build a foundation.

As we were discussing our plans for this book, we talked about taking the reader on a statistical journey. We could begin with some descriptive statistics, cross the river into inferential statistics (maybe blather on about the strengths and weaknesses of regression analysis) and end the journey pointing to the horizon of machine learning and data mining. We quickly realized that wasn’t the path we should take. Not only would this section be at risk of becoming a sleeping aide, it wouldn’t be solving the first problem we have which is some rather strong cases of analutophobia.

The ABC’s of data analysis

So you’ve got mounds of data and you’d like to know how to make sense of it and possibly learn something.

The world is changing. We are moving from a world of “experts” pushing their knowledge through analogies, to a world where knowledge may be pulled directly from the data. to to a world data, where knowledge is acquired by doing a job for years to a world urrently moving from a world in which we try to do the right thing to a world where we can know what the right thing is to do. think we know what we’re doing to a world where we can know what to do.

Certain areas of information technology and most of information security has been built on So you’d like to step into the world of data analysis and visualization and you’re wondering where to start. Just as a warning, this book will lay out the road in front of you and As a fair warning, it’s a long road and it’s full of setbacks and, assumptions want to move into the world of data? Sure, it’s nice to be able to do generate a random forest on Arithmetic, Buckets and Comparing.

Overcoming Analutophobia

Analutophobia (from the Greek words “analutos” meaning “solvable”, and “phobia” meaning “fear”) is a psychological condition in which a person experiences excessive anxiety about the application of data and analytic techniques to solve real world problems currently being solved without data and analytic techniques. There are many reasons for this condition (some of which are valid), but the root cause of this particular phobia is a general lack of understanding of the role of data analysis, what it is and what it is not.

Analytics and numbers are abused and misused everywhere we turn. Every politician keeps a suite of “supporting” statistics at the ready, marketing efforts use numbers that end up being “mostly accurate” and the media sensationalize analysis to stretch headlines well beyond the conclusions of scientific research. These statistics are intended to influence but are misused so often that any presentation of statistics may illicit analutophobic responses in otherwise normal and healthy individuals. But….

There is also a fear that these cold, heartless statistics will replace free thought as if the two cannot possibly exist in the same analysis. As one statistician put it, “To most people statistics means plugging numbers into an advanced calculator that spits out values, without much thought involved. Those people don’t work with data.” (“a life in statistics: Nathan Yau”, significance magazine). In fact the opposite is true, the data rarely speaks clearly and rarely goes to the extremes. Most of the time the data is ambiguous

. <calculator reference here?>

(ludicrous) or that the analysis will create a false sense of confidence and we’ll be blinded to the reality of the situation (not so ludicrous) or that

overpromise, under-deliver, sales cycles, marketing, -- within our industry, thrown statistics at us by vendors, juniper 2.5 months ago, claiming value, but was

data analysis replaces human intelligence, (I offer no value), (the data is something and it’s something than - challenging conventional intelligence.

treatment: persistence, small battles, showing small victories.

not all forms of analutophobia are treatable, sometimes it just cannot be overcome.

“waste of time” - sometimes we just want to make a decision,

data analysis can draw spurious conclusions

problems typically solved without data, we’re getting by without statistics now

Arithmetic, Buckets and Comparisons.

Playing with human intuition

In a 2010 presentation to statistics students at the University of Kansas, Bill James said these words: “In my view, anyone who imagines that he can anticipate what will happen next in any area of life is delusional, and people who think that “experts” should be able to do this are children and fools.”

[ “Battling Expertise with the power or ignorance” 4/13/2010 from <http://vimeo.com/16538462> retrieved 3/26/2013 ]

This quote comes across as confusing for anyone who knows anything about the life and work of Bill James (or has seen the movie “Moneyboall” where his work is portrayed). He has spent years trying to anticipate what wins baseball games by collecting and analyzing data. So what or who is delusional here? What he is describing is a flaw we have as people who think we can figure out to anticipate a very complicated system simply by showing up and paying attention, which is a long-winded to say, “relying on our intuition.”

Everyone knows that relying on our intuition can be a very powerful thing. On one hand, most of us choose to get out of bed in the morning because we anticipate our day will be better out of bed then in it. Some of us shower because we anticipate it will feel better (and that we’ll smell better) then if we didn’t. We don’t need to record data and apply a statistical model to tell us these things: they were intuitive and by all accounts, good decisions. Just by living our lives, we have learned to make many valid decisions based on nothing but gut-feel and intuition. But (and this a really big but), there is a limit to these judgments. We wouldn’t want to take a good long look at the sky and attempt to predict the weather for the day no matter how many days we’ve looked at the sky in the past. According to the work of Bill James, we also cannot simply watch baseball and intuitively deduce the true value of a fast player or when bunting is a good strategy. Somewhere between the simplicity of getting out of bed and showering and the complexity of weather forecasting and building a winning baseball team there is a tipping point. At some point, the world quietly becomes too complex to understand by simple observation. What’s more is we may not realize it until either the pain of being wrong or the benefit of being right outweighs our apathy.

We may not realize that we’re being fleeced by complexity because our helpful brains fill in any confusing gaps with familiar stories[[1]](#footnote-1) (remember the power of stories?). We make sense of the world by drawing upon our own experiences (or the experiences of others) to conjure a seamless logical flow. When the world is relatively simple this mechanism serves us well. We can make valid comparisons and connections between the qualities of our day in and out of bed. But when the world becomes more complex, familiar stories may be too simple or worse, completely inapplicable and inaccurate.

Back in the late 1990’s, I was working as an I.T. consultant and felt lucky to be surrounded by some very talented and clever people. One of those people was Alan, a seasoned 30-something system administrator who taught me a lot during our time together. During one engagement, we were hired by a medium-sized organization to test their computer security by trying to break in, something now commonly called “pentesting” (penetration testing). We spent several weeks mapping their network and gaining access through various exploits and hacks. Even though this was being done without the knowledge of their I.T. admin (yes their one admin), Alan had come to respect this guy as we played an advanced game of cat and mouse with him. It seemed for every complex combination of attacks we’d throw at the systems, this sysadmin would fire back with something to prevent our attempts. We triumphed in the end though and we prepared for our final presentation. Alan was actually a little nervous about meeting his nemesis face to face. Would he be upset that we had bested him on the field of battle? Would he show us the same respect we had for him? I will never forget the look on Alan’s face when the system administrator walked into the meeting. Alan’s nemesis turned out to be a high-school student working a summer job. He had no idea what the meeting was about and responded with indifference when we described pitched battles we had just fought. Turns out that all of the obstacles we found were just the random effect of a complex environment. But we (probably in order to save face), incorrectly attributed our set backs to an intelligent adversary. We crafted this story in our minds because that’s what made the most sense and what made us comfortable.

Our intuitive explanations for our setbacks were completely wrong, but in this case it didn’t matter much. The consequence of being wrong in this case was completely tolerable. We wasted time and effort avoiding the system administrator, but in the end we still delivered a good report.

In the book ghost map, Dr. John Snow is quoted as talks about the prevailing intuitive approaches to an ongoing cholera epidemic in 1854:

…the scientific method rarely intersected with the development and testing of new treatments and medicines. When you rest through the endless stream of quack cholera cures published in the daily papers, what strikes you most is not that they are all, almost without exception, based on anecdotal evidence. What's striking is that they never apologize for this shortcoming. They never pause to say, "Of course, this is all based on anecdotal evidence, but hear me out." There's no shame in these letter. No awareness of the imperfection of the method, precisely because it seemed eminently reasonable that the local observation of a handful of cases might serve up the cure for cholera, if you looked hard enough.[[2]](#footnote-2)

Snow is appalled at not just the lack rigor being applied to this problem, but the apparent apathy in the overall approach. This is much different then our pentest where the consequence of being wrong isn’t some wasted effort on a consulting engagement, it’s death.

How we can improve on this? Where do we find better answers? Before we can answer these questions, we have to get something out of the way first…

Being less wrong versus being right

Information technology is built on deterministic systems. We can produce highly complex systems and given the same input, we can very precisely predict the output. For a variety of reasons, I.T. people have a belief that if something is possible it much be accounted for and uncertainty and There is a certain expectation that if something

still expect absolutely perfect execution. Engineering principles are built on striving for perfection. The world of statistics on the other hand, is built entirely on the world of probability. There is never a right answer in statistics, there is only an answer that is probably more wrong then another.

Simple, most people can connect the keyboard, monitor and mouse to a computer and turn it on.

But there is an obvious limit to that predictive ability and that’s what Bill James was talking about, in a complex environment (human performance in a competitive sport like baseball) our intuitive judgment can fill in the gaps with some wildly crazy stories and through compounding factors becomes conventional wisdom, one of the most dangerous things to get to a complex environment.

Our ability to predict depends on many things, but a couple of things influence greatly: the underlying complexity of patterns in the environment and two, our ability to make sense of those patterns. Our desire to be right (or avoid consequences of being wrong) and how predictable the environment is, that is how well we can observer and learn from the environment. The relatively simple physics of hitting a ball with a bat is observable and understandable by children, but predicting how a complex system of circuitry and software will fail next is not as easily observable.

Our ability to make intuitive prediction is directly and inversely related to the complexity of the environment.

The debate against “algorithms versus intuition” has a simple answer: intuition excels at both speed and accuracy in simple environments and algorithms consistently outperform intuition in complex environments. There is no blanket statement of one is better then the other and to further stop the bickering, they are not exclusive. Algorithms support intuition.

and the next failure will occur in a computer system composed of some of the most complex hardware and software we are capable of making may not be as predictable.

Patterns and Randomness

Randomness is a funny beast. There was once a statistics professor (statistics is filled with stories about statisticians by the way) having her students flip a coin 500 times by hand and writing our the results on a piece of paper. When the students brought in their homework, the professor amazed her class by quickly flipping through the results and announcing who had faked their coin flips and who hadn’t. How’d she do that? She relied on the fact that humans are very poor random number generators and they underestimate the probability of patterns within randomness. Turns out that when a fair coin is flipped 500 times, it’s highly unlikely (less then 2% chance) to not have at least 7 consecutive results (heads or tails) in a row. So the professor would perform magic by scanning through the records looking for these missing consecutive results as a sign of cheating.

Humans are not just poor random number generators, but we are also naturally poor at intuitively understanding the patterns that can occur randomly.

Nathan Yau: “To most people statistics means plugging numbers into an advanced calculate that spits out values, without much thought involved. Those people don’t work with data.” (“a life in statistics: Nathan Yau”, significance magazine)

this is not to say that we are unable to learn with-feel is worthless.

build expertise simply by showing up with our eyes open. learn anything if we just hang around it long enough. A good baseball scout is someone who has been around the game for a while.

We can figure out how

“I don’t really know much of anything about the workings or applications of statistical methods. I could not describe myself as a statistician because I could not meet the standards that people in this room would expect of a professional statistician”

“Experts are people who claim to know things or claim to understand how things works.”

Expertssay that baseball players are in their prime 28-32 - it turned out that this is “totally, wildly and completely untrue, it doesn’t match the data in anyway shape or form”

“large shared body of expertise”

“bunting doesn’t increase the number of runs the team can expect to score or their chance scoring a single run.

speed is not the key element of success of baseball teams

runner on first, no one out, bunt

“There was a great deal of misunderstanding, they thought that I as trying to supplant the experts, or anti-expert. or anti-scout.

speed was important.

experts good starting pitcher would draw a few thousand fans.

“axioms of expertise” to

“My job was to find questions about baseball that have objective answers, that’s all that I do, that’s all that I’ve done for the last 35 years.”

Our theory is that he was addressing his critics. Those who swore it was better to bunt in some situation, or steal bases.

But this isn’t at all what he was describing with that quote. He was describing a flaw we have as humans to not know when our own gut-feel is fooling us.

Intuition (as defined by some fancy researchers) is nothing more than the recognition of patterns in our memory. What Mr. James is saying is that our ability to make a prediction based on just the patterns in our memory is impossible.

ability to the recognize patterns in our memory. of patterns in memorycollection of memories.

project the simplicity of our intuition onto a highly complex world. The “experts” he is referring to are those who collected enough stories and memories that they seem like they are the most worthy of trust. But as James showed in his own work, human gut-feel can be remarkably poor at predicting the future.

But with respect to Mr. James, I knew that prediction was achievable without math and can be much simpler then that. I chose to get out of bed this morning because I predicted my day would be better out of bed then in. I showered because I predicted I’d feel better (and smell better) then if I didn’t. I ate breakfast because I predicted it’d give me energy for the morning. I didn’t need to record data and apply a statistical model to tell me these things: they were intuitive and by all accounts, good decisions. Just by living my life, I’ve learned to make many valid decisions based on nothing but a gut-feel. Day after day, our lives are filled with predictions that are (thankfully) fairly accurate. But (and this a really big but), there is a limit to gut-feel judgments. I wouldn’t want to take a good long look at the sky and attempt to predict the weather for the day no matter how many days I’ve looked at the sky in the past. Somewhere between the simplicity of getting out of bed and the complexity of weather forecasting there is a tipping point when our intuitive judgment ceases to be enough. There is a tipping point in system complexity where our ability to predict based on gut-feel should stop receiving our trust.

Strengths and limitations of statistics

Robin W decided to conduct a longitudinal study on the health among I.T. system administrators. The study followed the lives of 30 system administrators all of which died eventually (which greatly affected their performance at work). Robin ran the numbers and concluded the average proportion of system administrators who eventually die is between 88.6% and 100% (with 95% confidence).

There are two takeaways from that story. First, even though it’s absurd, there is a tiny bit of truth in that story. People see statistics being a mindless activity and can envision a math nerd presenting that conclusion while pushing their glasses up their nose and doing a laugh-snort at the end. Statistics is perceived as blindly shoving data into a magic box of math and getting an answer without any real thought. While we are technically able to calculate a confidence interval on 30 deaths out of 30 people, it doesn’t make much sense in the daylight of reality. Everyone understands the probability of death is 100%.

However, what if during the study, Robin found that 30 out of 30 system administrators developed bad eyesight and required glasses? It’s the same exact proportion (30 out of 30), yet we cannot come to the same conclusion as before. It’d be absurd to jump to the conclusion and pronounce, “All system administrators need glasses!” There is a perception that in order to do statistics you have to turn off all forms of logic, reasoning and common sense. Those people have obviously never actually worked with data.

The second takeaway from Robin’s story is that it conveys a certain amount of uncertainty in the statistical conclusion. This is rather important because another misperception of statistics is that it will provide one clear answer. Again we have the users and abusers of statistics to thanks for this. When statistics are misused, the assumptions, qualification and uncertainty in the conclusions are removed or relegated to a minor footnote. Because we’re not focusing on infographics here, we are much more interested in what we can learn from the data. We want to find the stories within the data and unfortunately most of the data is just a reflection of the uncertainty and variability we intuitively see in the world around us.

Given the uncertainty, it’s easy to form the initial (and incorrect) conclusion that statisticians have got the market cornered on CYA (cover your a-posterior) politics. Think about this statement: “Given that we observed 30 out of 30 system administrators in need of eyeglasses, we conclude, with 95% confidence, that the average (mean) rate of eyeglass usage among system administrators is between 88% and 100%.” Which means if we were to study more system administrators, we could expect the average to be less than 88% once in every 20 groups we look at. But what if we do one more sample and see that an average of 70% of system administrators wear eyeglasses? It could just be 1 of the 20 of groups that we’d expect and we’ve got CYA!

[insert Anscomb’s quartet in this section!]

However, once we can get past the initial wishy-washiness in that particular statement, it turns out to be the best statement (and the most honest) that we can communicate given the data in front of us.

But let’s take a more realistic example. Let’s take the problem of phishing emails. Everyone knows what these are, emails that claim to be from some authority or acquaintance and enticing the user to click a link or open an attachment in the hopes of infecting their system. We want to measure just how bad this is so we construct the following email:

Hello Alicia,

I noticed an irregularity in the salary information for your department, could you take a look at the attached list of salaries and see if they match with what you have on record?

Then we send the fake email that looks like it is coming from Human Resources to 100 people in Alicia’s group (or perhaps not in Alicia’s group). The attachment within the email is set to simply record whoever clicks. This enables us to measure who clicks and hopefully get a feel for the success of a real phishing campaign.

Maybe make two/three groups, executive leadership,

Let’s say out of 100 people 18 people click on the attachment. What could we conclude? While the easy answer is to head to a local pub and wishfully think up ways to patch people. The real answer is , to a conclusion that we can’t patch people and hope for the best, in reality we’re going to have some variation but in reality

The problem of course is that within I.T. and engineering we generally seek perfection. And when we don’t see perfection, it’s tossed out as flawed or broken or worthless. We want to know that if we build redundancy into an application that it will work. We confuse measurement with precision instead of accuracy .

get to know statisticians e most wishy-washy folks you could ever imagine.

that the answer. Just because we saw 30 out of 30 system administrators in need of eyeglasses (we’ll stick with that example for now), there will be some natural variation that will occur

Simplification occurs

But before we get into that we should go back to what was brought up at the beginning of this chapter. We are not talking about the type of statistics (or should we say “hype of statistics”) portrayed in the average Infographic. o <http://www.phdcomics.com/comics.php?f=1174> ?)

But thanks in large parts to the science news cycle

Lying with data

It’s easy to focus on the mechanics of mathematics and blame the cold-hard world of numbers for the inaccuracies in our stories. But unfortunately the math is actually the easy part (especially given that most of it done in applications now) and it’s rarely a source of misunderstanding. Most inaccuracies are caused either by the data collection methodology or introduced via error in the preparation and handling prior to any analysis of data has a chance to mess things up.

of data is analyzed.

are caused by the data (typically the collection) itself and not how we handle the data.

Some problems are established before any data are collected. of the problems are either set forth before any bit of data is collected

1. Applying probability to an uncertain world
2. Lying with data
3. Instilling a culture of analytics
4. Planning for analytics
5. Diagnosing & treating analutophobia
6. The role of visualization in data analysis

This breeds the “experts” (and we can toss in “pundits” into that category) that James was referring to. Experts are not those who

When the environment is complex and

unaware s environments we we are trick ourselves into thinking we know how things work when in reality, the system is just too complex.

At some point the pain of being wrong is too great or the benefit of being right outweighs our apathy.

When things become too complex our wonderful brains help us out by projecting stories: droughts are the gods being angry just as much as organizations who suffer a breach must have been idiots. Wearing the same socks during a winning streak in baseball and requiring a new complex passwords every 90 days all become plausible reasons correlations to the patterns we see.

when our intuitive gut-feel ceases to be enough. There is a tipping point in system complexity where our ability to predict based on gut-feel should stop receiving our trust.

The trick to this then is to know when we should become distrustful of a gut-feel approach and start looking for ways to enhance our ability to make decisions. Can we look at enough computer systems to know when there is enough risk present to warrant action just by looking at one more? Better yet, can we identify when not to make something more secure by identifying even though the system isn’t perfect, it is secure enough?

(every decision involving the future is a prediction) machines and mathematics can produce better results, but the challenge is identifying when that is. When do we learn to distrust our gut and learn to trust the data?

Ironically, the answer to that question can only be found accurately with data.

Interesting Quote: “We are shifting from a world in which *we think we know* into a world in which *we know and we can prove it*.” http://blogs.sas.com/content/corneroffice/2013/04/03/q2-2013-intelligence-quarterly-bring-big-data-to-life-with-visual-analytics/

1. There needs to be a citation here, probably to Kahneman, Klein or Gigerenzer [↑](#footnote-ref-1)
2. To see this quote adapted for information security, see http://rud.is/b/2013/03/27/a-wish-for-snow-in-spring/ [↑](#footnote-ref-2)