THE HUMAN VULNERABILITY

Why the cybersecurity industry has been fighting the wrong battle for 20 years—and how we can reclaim the surrendered ground

by Chris Pogue
Senior Vice President, Cyber Threat Analysis

nuix
Simple. Powerful. Precise.

CONTENTS

PREFACE

We are engaged in an information war; a battle to control data in every aspect of our lives. Over the past 20 years, organizations have spent billions of dollars and expended countless hours to protect our most critical information assets.

If all that effort and expenditure had been effective, I would never have built a 15-year career as a penetration tester and computer crimes investigator. In that time, I worked on or oversaw thousands of security assessments and investigations.

This white paper is the culmination of more than six months of research. It has been a labor of love to find a credible answer for that most elusive of questions: why. Why had an entire industry with some of the most intelligent people on the planet fallen so short of its objective? Why are we so consistently defeated by cybercriminals?

Why? All the time I spent in the trenches, all the lessons I learned as a result of the work I performed taught me an undeniable truth: Cybersecurity is not a technology problem; at its heart, it's a people problem. For two decades we've been designing security technology to solve technology problems; in essence, we've been fighting the wrong battle. If technology has a role, and I sincerely believe it does, it must be to help solve people problems.

I joined Nuix in 2014 with a singular focus—to help more people. Working at Nuix has made it possible to integrate the intelligence and lessons I learned from all these investigations into a software platform. And not just me—Nuix has hired security professionals with all kinds of skills and experience complementary to mine and incorporated their knowledge into its technology. Together, we are creating a true intelligence multiplier, the likes of which the cybersecurity market has never seen. In short, it's a game changer.

By merging field knowledge with the power of the Nuix engine, we will give our users an unparalleled capability to deflect, detect, react, respond to, and recover from cybersecurity incidents. This is the missing link that will enable security professionals to reclaim the precious ground we have surrendered to cybercriminals.

Shifting direction, after two decades, will be far from painless for security practitioners and the industry. It is my sincere desire that after reading this work, the industry understands what needs to be done to stem the tide of data breaches, and summons the courage to take action.

I leave you with the words of the 28th President of the United States, Woodrow Wilson: "You are here in order to enable the world to live more amply, with greater vision, with a finer spirit of hope and achievement. You are here to enrich the world."

Let's do this!

EXECUTIVE SUMMARY

Over the past 20 years, organizations have expended billions of dollars' worth of time, energy, and intellectual property pursuing the elusive "next big thing" in cybersecurity. At countless security conferences around the world, vendors have touted their technological achievements and proposed their solutions to scores of hopeful attendees. Despite the collaborative efforts of the entire cyber-industrial machine, very little progress has been made. In fact, by all accounts, the threat landscape has actually gotten worse.

A cursory web search will identify article after article describing data breaches, system hacks, and security faux pas. These incidents happen every day, in every industry, on every continent, targeting every type of data that conceivably holds monetary value. It does not take a brain surgeon to see that whatever the cybersecurity industry has been doing for the past two decades has, very simply, failed. This fact is illustrated in Figure 1 showing the numbers of reported breaches and exposed records in the United States over the past ten years.[i]

Continuing along this path is obviously a fool's errand, in lockstep with what Albert Einstein so accurately defined as insanity. Instead, I took a step back and asked that most important of all questions: why? Why have so many very smart people spent so much money and effort and made such little progress?

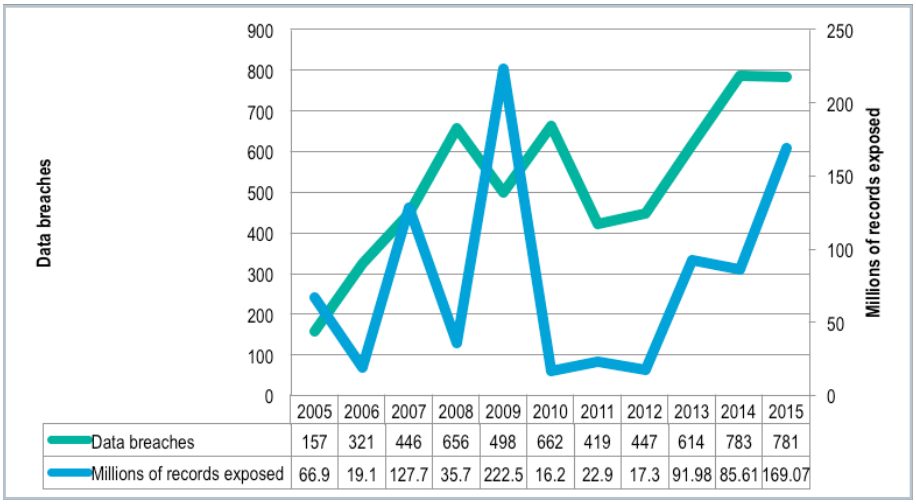
This prompted me to completely reassess the way I was thinking about cybersecurity and start to research the subject in a very different, non-linear manner. I looked outside of the technology industry to see if any other industries had faced similar problems in the past. If they had, how did they solve them?

For approximately six months, I devoured any literature on the subject I could get my hands on—books, industry reports, and news articles on business problem solving, specifically focusing on how organizations identified problems, which approaches were successful and which ones failed, and how long it took to move from identification to definition and ultimately resolution.

My research revealed one industry that faced and solved similar problems, and one whose creative journey to address a dissimilar problem gave me valuable insight that I could apply to the cybersecurity industry. These industries are manufacturing and world healthcare—specifically, the fight against communicable diseases.

In this white paper, I will define the problem facing the cybersecurity industry. I will show that insufficiently defining and therefore inappropriately addressing the problem is the reason for almost two decades of failure. I will then clearly lay out a more comprehensive strategy to address the evolving threat landscape and how the cybersecurity industry can reclaim much of the ground that it has surrendered.

In short, we have all been fighting the wrong battle with the wrong weapons and wondering why we're not winning the war. So hang on and keep reading; that's all about to change.



	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
Data breaches	157	321	446	656	498	662	419	447	614	783	781
Millions of records exposed	66.9	19.1	127.7	35.7	222.5	16.2	22.9	17.3	91.98	85.61	169.07

Figure 1: Annual number of data breaches and exposed records in the United States from 2005 to 2015.

nuix

THE CEREBRAL VULNERABILITY

The human brain consists of about 200 billion *neurons*—nerve cells that are linked together by trillions of connections called *synapses*. As the tiny electrical impulses that make up brain activity shoot across each neuron, they have to travel through these synapses, each of which contains about 1,000 different switches that route each electrical impulse. In total, one human brain contains hundreds of trillions of these neural pathways. This enables our brains to be capable of an amazing 1,016 complex processes per second, which makes them far more powerful than any computer currently in existence. Pretty cool, huh?

For example, researchers in Japan used almost 83,000 processors of one of the world's most powerful supercomputers, the Fujitsu K, to connect 1.73 billion virtual nerve cells to 10.4 trillion virtual synapses (with 24 bytes of memory in each synapse). In total, this added up to around one petabyte of memory, which is the equivalent of about 250,000 standard personal computers. Even with all this technology, the researchers were able to mimic just one percent of one second's worth of human brain activity. Their experiment still took 40 seconds replicate the amount of human brain activity that occurs in the time it takes you or me to blink.

Even though our brains behave so much like supercomputers, they are far from perfect. Philosophers, scholars, and behavioral psychologists have tried for millennia to understand the brain's nuances and unravel the mysteries of why we make the decisions we make. For example:

- Why does the same set of factors drive one person into action but another to do nothing?
- How can a group of people all see the same event yet each individual walk away with a different interpretation of what happened?
- What drives one person to risk their life for people they have never met and another to take life from those they love?
- Why do some people give freely from what little they have and others take greedily to grow their increasing surplus?

The human brain is fascinating, complex, and powerful, but clearly nowhere close to being perfect.

Cognitive Biases: Bugs in Our Brain Software?

One of these imperfections is a group of cerebral deficiencies known as *cognitive biases*. A cognitive bias is a limitation in our brain's ability to process information sufficient for us to make conscientious decisions. Some psychologists believe our cognitive biases help us process information more efficiently, especially in dangerous situations, so our instinctive fight-or-flight mechanism has an advantage. While these biases may be useful in, say, avoiding being eaten by a bear, they also sometimes lead us to make grave mistakes, in many cases without our ever being aware of what we are doing.

Cognitive biases also refer to a systematic pattern of deviation from normal or rational judgment, whereby we draw illogical inferences about other people or situations. Individuals create their own *subjective social reality* from their perception of the input they receive. An individual's construction of social reality, not the objective input, dictates their behavior in the social world. Thus, cognitive biases may sometimes lead to perceptual distortion, inaccurate judgment, illogical interpretation, or what is broadly called "irrationality."

Some cognitive biases also enable us to make faster decisions when timeliness is more valuable than accuracy. An example of this is *heuristics*, rules that people use to make decisions without necessarily knowing all the facts. Other cognitive biases come about because humans lack the appropriate mental mechanisms to process certain types of information (bounded rationality) or don't have the capacity to process it in large volumes.

In the world of computers, we call this a *vulnerability*.

Philosophers, scholars, and behavioral psychologists have tried for millennia to understand the brain's nuances and unravel the mysteries of why we make the decisions we make

WHAT IS A BREACH?

In calculating the number of data breaches recorded in the United States in any given year, the Identity Theft Resource Center defines a breach as "an incident in which an individual name plus a Social Security number, driver's license number, medical record, or financial record (credit/debit cards included) is potentially put at risk because of exposure."[ii]

Similarly, the Ponemon Institute's 2015 Cost of Data Breach study, sponsored by IBM, defines a breach as "an event in which an individual's name plus a medical record and/or a financial record or debit card is potentially put at risk—either in electronic or paper format."[iii]

To put it simply, a data breach is any unauthorized party gaining access to protected information for the purposes of benefiting from the theft and subsequent utilization or manipulation of that information.

Every data breach, regardless of the complexity of the attack or the environment in which it occurs, can be broken down into four stages: infiltration, propagation, aggregation, and exfiltration (see Figure 2).

To put this into non-technical terminology, let's use the example of a bank robbery. A criminal who wants to rob a bank needs to do four things:

- Break into the bank
- Move from the point of entry to the location of the money
- Put the money in a bag
- Make their getaway.

If the criminal fails to perform any one of those actions, the robbery fails.

A data breach is no different. In every data breach, the attacker must:

- Gain access to the target environment *(infiltration)*
- Move from the point of entry to the location of the targeted data *(propagation)*
- Harvest the data *(aggregation)*
- Move it from a system controlled by the victim to a system the attacker controls *(exfiltration)*.

Many aspects of a breach are arguably more complex, but overall, that is how it works. It's pretty simple, and something that has come to be commonly referred to as the *breach breakdown*.

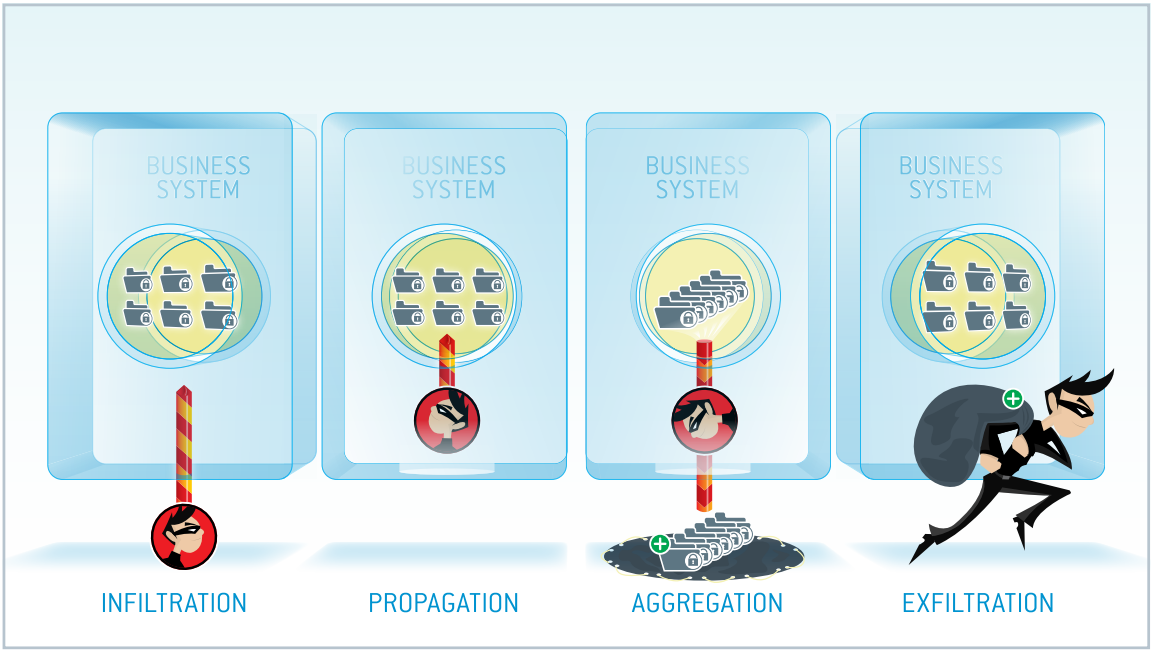


Figure 2: The four stages of a data breach.

THE INFILTRATION CAUSATION

The vast majority of cybersecurity activity is focused on preventing the first stage of the breach breakdown: infiltration. (There are plenty of things we can do to make the other three stages harder for cybercriminals, but that's a whole other discussion.) What makes infiltration possible?

According to the 2015 Ponemon Institute study, "Hackers and criminal insiders cause the most data breaches. Forty-seven percent of all breaches in this year's study were caused by malicious or criminal attacks." The study further indicated that 25% were caused by human error.

Let's do the math: 47% + 25% = 72%. That means the remaining 28% were caused by *system glitches*. Well, what's a system glitch?

The report defines a system glitch as a failure of IT and business processes. So it's not a human being actively making a mistake (because that would be a human error), but neither is it a random and unpreventable event. True, power outages, internet service provider issues, hardware failures, and natural disasters happen and can have unpredictable downstream effects on a computing environment. However, the study is talking about process failure. Presumably, those processes that failed were developed and implemented by humans. Computers are stupid—they do exactly what humans tell them to do. The more logical explanation for these glitches, therefore, is a human being failing to tell the computer to do the right thing.

Let's face it—that 28% attributed to system glitches simply isn't accurate.

Additionally, let's think about who is making these assertions that data breaches were the result of systems failures. It is most likely someone within the organization who knows how the systems are supposed to work and what failure looks like. More than likely, these are the same individuals responsible for some aspect of their company's cybersecurity posture, if not all of it. To admit that the system didn't work as planned would mean admitting personal failure, since they are likely responsible for security design or implementation, or both. Humans are very bad at admitting fault, a phenomenon called *externalization*.

Internalizing Success, Externalizing Blame

When something good happens to someone, their natural response is to internalize the responsibility for that thing as something they caused. "Look what I did," or "Look at how great I am." I may be paraphrasing, but you get the idea.

You will probably not be shocked to learn that the natural human response to something bad happening is the exact opposite—externalization rather than internalization. When something goes wrong in our lives, we tend to look for some way to project blame onto somebody or something else. Obviously, we are far too skilled and wise to commit such an error, so therefore there must be another party to blame. It's not *MY* fault, it's *YOURS*. *I* didn't do this, *THE COMPUTER* did.

One of the key findings of my research is that technology is rarely the cause of data breaches. In the more than 2,500 breaches I have investigated, I can count exactly zero that were caused by a random, non-human-initiated system failure.

I am not saying they never happen, just that a basic application of Occam's razor tells us the cause is much more likely to be elsewhere. (Occam's razor, or the law of parsimony, is a concept attributed to a 14th century Franciscan friar named William of Occam.[iv] This principle states that when you must choose between several potential scenarios, the one that requires the least number of assumptions is most likely to be correct.) When presented with the two possibilities of complex system glitches or a simple human error, Occam's razor leans pretty heavily towards human error.

Since there are only a few human-machine hybrids in all the world,[v] I am going to go out on a limb and make what I believe to be the logical assumption that 100% of hackers, malicious insiders, unknowing insiders, and IT and business personnel are human beings. Whether they are attackers (internal and external) seeking to do damage or employees simply making mistakes, 100% of breaches are the result of human behavior.

One of the key findings of my research is that technology is rarely the cause of data breaches—in the more than 2,500 breaches I have investigated, I can count exactly zero that were caused by a random, non-human-initiated system failure

THE INFILTRATION CAUSATION cont

On Becoming the Underdog

Success or failure is not something binary, a one or a zero, the presence of a charge or the absence of it. There is something else that drives success or failure apart from simple ability and skill. That "thing" represents the essence of what make us human: desire, motivation, drive, and the relentless pursuit of a goal.

If skill and ability were all it took to be successful, sports teams with the most skilled and highly rated athletes would always win. But that's not the case, is it? Sports history is littered with talented teams who fell to underdogs that figured out a way to work together and achieve victory. This is one of the most compelling reasons to watch sports.

In 1969, the New York Mets had not placed higher than ninth in their first seven seasons as a Major League Baseball team. The odds of them winning the World Series that year were 100-1. Nonetheless, the Mets won more than 100 games that season and went on to be the unlikely World Series champions.

The United States Winter Olympic hockey team in 1980 was seeded seventh in a field of only 12 teams. After upsetting a superior Czechoslovakian team en route to a 4-0-1 record in bracket play, the Americans came to face the Soviet Union in the semifinals of the first medal round. Earlier that year, the same team had lost 10-3 to the Soviets and they were not expected to do much better in this tournament. Yet somehow, the "Miracle on Ice" team of amateurs found a way to win 4-3 against the "best" hockey team in the world at the time. The US then went on to beat Finland 4-2 in the gold medal game, completing an impossible championship run.

So what is the connection between cybersecurity and sports? This is really important. Just like in sports, the success of an organization's cybersecurity program relies on more than the technical skills of the people who are responsible for the plan. If all that mattered was technical skill, it would simply be a case of knowing that you had to segment the network, deploy firewalls, and use dual factor authentication (for example), and WHAM … you'd be secure.

But it doesn't work that way, does it?

We are human beings, and we have flaws in the way we think, in the way we interact with other human beings, and in the emotional substance of our decision-making process. Understanding these flaws, and identifying the human aspect of the workplace, is the first and arguably one of the most critical steps we can take in ultimately overcoming them; becoming the underdog and beating the superior opponent.

The Missing Link

Over the past 20 years, the security industry has focused on technology to solve its complex problems. Yet despite decades of research and the myriad security vendors, products, and technological advancements that have emerged year after year, the threat landscape is stronger today that it has ever been, with no signs of abating.

Since no problem is unsolvable, we're compelled to wonder what critical information has eluded cybersecurity companies and prevented them from stemming the tide of data breaches. I believe this *missing link* to be human beings.

As I mentioned earlier, I've conducted or overseen more than 2,500 data breach investigations during my career. The overwhelming majority were not the result of failures in technology, but of poor decision-making by the people responsible for the victim organization's security program. Decisions such as using weak or default passwords, leaving open remote access, improperly configuring firewalls, not segregating networks, and using poorly designed or coded applications. These remain among the primary attack vectors cybercriminals use to infiltrate their targets.

In each of these scenarios, the attacks were 100% preventable; the knowledge and the technology existed to prevent the breach from ever taking place. A human being was either ill-informed as to the steps that were required to implement adequate security controls, or simply made the choice to not implement them.

We've established that data breaches are the result of human activity. It's clear that the technology and security knowledge exists to prevent successful breaches. The next logical question is: "Why would someone who knows better make such a poor decision?"

As I sought to find an answer to this question, my research led me identify several factors that play a part in formulating the overall solution. Each has to do with the way we think and act as humans. I don't think cybersecurity will progress in any meaningful way until we confront and address these issues.

COGNITIVE BIASES

As I've discussed earlier, cognitive biases are tendencies formulated in our brains that can lead to illogical decision making or poor judgement. For many years, psychologists have studied how these biases affect business and economic decisions, interpersonal relationships, and geopolitical relations. Through introspection, training, and role playing, it is difficult (but not impossible) to retrain our brains to behave differently.

Psychologists have identified scores of biases and broken them down into categories including decision making, belief, behavioral, social, and memory error biases. For the purposes of my research, I have focused on five decision-making biases that appear to have the greatest impact on cybersecurity professionals. I believe these are the primary obstacles preventing us from making better choices, ultimately leading to the degraded protection of critical information assets in our care.

Normalcy Bias

If a plumber fixed a leaky pipe in your home, would you expect him to test his work, making certain the leak was fixed before calling the job complete? If you took your car to a mechanic to have your air conditioning serviced, would you expect that he would check to make sure cold air was blowing before saying the job was done? Of course you would! In just about every aspect of business, there is a logical expectation that once services have been performed, there is a mechanism in place to ensure that things are running the way they should.

In many instances during my tenure, I have seen organizations spend hundreds of thousands of dollars on defensive countermeasures and then fail to test them adequately once they were in place. In the rare instances where they performed some testing, it was usually automated or trivial, designed to test specific features against a canned data set rather than to evaluate strategic enhancements to the organization's security posture. This sort of post-deployment testing, which is increasingly common, in no way adequately represents a realistic attack.

It has always baffled me that behavior which would never be acceptable in any other line of business is almost universally accepted in cybersecurity. Why?

Normalcy bias drives our brains to believe that since something catastrophic, such as a data breach, has not happened in the past, it will not happen in the future. We therefore illogically minimize the possibility of a breach and its potential impact on the organization.

History has shown (and I have said many times) there are really only three types of organizations: those that have **been** breached, those that **are** breached, and those that are **about to be** breached. This is the reality of the current threat landscape.

However, as a result of normalcy bias, we dismiss important tasks such as security technical testing of defensive countermeasures. We postpone vital steps such as creating an incident response plan, testing that plan, conducting realistic response training scenarios, and providing companywide security awareness training—or we take them off the security roadmap entirely in favor of other, more bottom-line-related activities.

Neglect of Probability

Neglect of probability, similarly to normalcy bias, leads decision makers to disregard the probability an incident occurring; we ignore or largely overlook risks and ignore the continuum of the extremes.

You don't have to be a computer scientist (I'd like to see a rocket that works without computers) to realize that data breaches occur every day despite our seemingly best efforts. It is logical to assume that if your organization stores, processes, or transmits any data of value, it will be a target for attackers—if it hasn't already become so. I believe many key decision makers fail to accept this fact because of this bias.

While the exact probability is difficult to calculate, it should be obvious by now that just about every type of organization with computing resources will suffer a significant security incident in the foreseeable future. Multiple reports (including the Verizon Data Breach Investigation Report, the FireEye Threat Intelligence Reports, the IDT911 ITRC Data Breach Report, The Experian Industry Forecast Report, and the Ari Kaplan Advisors Defending Data report—see "References and Further Reading" on page 19) indicate that data breaches are on the rise on every continent and in every business vertical. Not accepting this reality is foolish and inappropriately optimistic. It will happen.

COGNITIVE BIASES cont

The Ostrich Effect

The ostrich effect refers to the common (albeit false) belief that an ostrich, when faced with danger, will hide its head in the sand—if it can't see the danger, it doesn't exist. This cognitive bias refers to the similar tendency humans have to ignore problems in the hope that they will go away. Unfortunately, bad guys do bad things and bad stuff happens, whether our heads are in the sand or not.

The truth is that bad things happen to good people; in relation our specific set of circumstances, it does not matter if you are a non-profit providing drinking water to poor children in Africa or an online pornography vendor. If you store process or transmit data that has a black market value, you will be targeted. The sooner everyone everywhere realizes this, the sooner they can start preparing accordingly. Pull your head out (of the sand). This is for real.

Parkinson's Law of Triviality

When I first began to read about Parkinson's Law of Triviality (sometimes referred to as bike-shedding), I immediately felt like it applied to cybersecurity professionals. However, I didn't want my research to be impacted by my own cognitive biases, so I wanted more than a feeling. It wasn't until I attended the 2016 RSA Conference in San Francisco, California, that it made sense. (To be fair, the RSA conference is not the only place this phenomenon is present but it was on my mind while I was there.)

This bias is that humans assign a disproportionate weight to things they understand, and much less to things they don't understand, totally independently of how important those things are.

Here is an easy example. I have had countless conversations about cybersecurity that focus on antivirus (AV), firewalls, and intrusion detections systems (IDS) as the "magic trio" of countermeasures to thwart ne'er-do-wells (I had to work that word in somehow). There is no question those technologies should be part of every organization's defensive posture, but they are nowhere near comprehensive. Many organizations that suffered data breaches had all those technologies in place, so logically their mere presence is not enough to stop attackers. What gives?

The explanation is that most people can wrap their heads around linear solutions such as AV, firewalls, and IDS, while they struggle with more dynamic concepts of vulnerability management, defense in depth, strategic countermeasures, and threat simulations. So instead of tackling the larger, more complex issues, Parkinson's Law of Triviality drives them to focus on the smaller, less complex issues and to think that they are more important than they really are.

CURSE OF KNOWLEDGE

I found the curse of knowledge to be one of the most interesting biases for a variety of reasons. Its mere existence provides a glimpse into the human psyche is that simultaneously illogical and yet completely logical—a cerebral paradox if you will.

When an individual amasses expertise in a certain field, it is understandably the result of many years of research, study, and practical experience; this knowledge is the summation of all of their efforts. However, as their knowledge grows, so does the potential for hubris directed at others who do not have the same level of expertise. They become disdainful of the traits they worked so diligently to overcome.

There is a fine line between confidence and arrogance. During my career, I have often contemplated where this line resides, and how to navigate it in such a way that I am just confident enough to do my job. If I am too confident, then I am arrogant; not confident enough, then I appear to be weak. It is a challenge to be certain, but not an insurmountable one.

Over the years I have come across many people who, for whatever reason, do not share in my understanding or efforts. This failure to understand and control one's intellectual maturity acts as a firewall for any ideas that are not self-generated. I believe this bias is directly responsible for many of the poor decisions we see during cybersecurity incidents.

The most common manifestation of this bias takes form in statements such as "Don't tell me how to do my job," and "I've been doing this for 15 years, I know what I'm doing." These statements reveal the curse of knowledge cognitive bias at work, as well as a certain degree of emotional immaturity.

The realm of cybersecurity is so multidimensional, it is simply not plausible to think that any one person know enough to be competent in every possible area; it's madness really.

Think of an inverted pyramid (see Figure 3) whereby the more the individual learns, the more he realizes what he doesn't know. The curse of knowledge is exactly the opposite in the mind of the impacted individual. They think they know so much but in truth they don't know enough to even realize how much they don't know.

Figure 3: The curse of knowledge

THE FAILURE OF THE HUMAN SYSTEM

Data breaches are almost always framed as technical failures. If you read enough media statements issued by organizations that suffered data breaches, you will see a common script: The breaches were the result of super-sophisticated attackers who exploited a completely unknown vulnerability to gain access to the highly protected target systems. All these organizations overstate the technical complexity of the breach, while understating its impact. In just about every instance, they never mention the potential for or presence of human failure.

For further evidence, think about the checklists used in governance, risk, and compliance (GRC) régimes. They all contain volumes of technical security controls dictating how to configure systems, what types of passwords to use, how to deploy firewalls, etc. None of them contain guidance on decision making, staffing, or security strategy. This makes sense if everyone believes we are facing a technical problem; technical solutions solve technical problems. Right? Wrong!

Data breaches are human failures. I refuse to believe that in the past two decades an entire industry full of very smart people has completely failed to develop technology sufficient enough to prevent systems from being compromised.

In fact, the 2015 Defending Data Report found 93% of respondents thought human behavior was the biggest threat to their organization's security.[vi] The Experian 2015 Data Breach Industry Forecast Report says "Employees and negligence are the leading cause of security incidents but remain the least reported issue."[vii] Finally, the 2015 BakerHostetler Data Security Incident Response Report found "human error is most often to blame" in the clients the firm sampled.[viii] Specifically, 37% of the breaches the firm litigated in the year leading up to the report's publication were the direct result of human error.

We are clearly facing a human problem that our industry has been unwilling or unable to address for over 20 years. So my research led me to look outside the cybersecurity industry to see if others had experienced similar human problems and how they solved them.

Two examples were instructive:

- The way the World Health Organization (WHO) combats the threats of communicable diseases
- The way the industrial manufacturing industry has addressed machine-related accidents on assembly lines.

The Ebola Epidemic

In 2013 the World Health Organization was called on to combat the largest and most complex Ebola outbreak on record, in West Africa. By the time the WHO declared the epidemic over, on November 29, 2015, it had identified more than 28,000 cases of Ebola resulting in more than 11,000 deaths.

Colin McIff, Health Attaché to the US Mission to the UN in Geneva, told me the major challenge WHO faced was not a breakdown in medical science—after all, the organization has been handling the spread of communicable diseases for years. Rather, this particular instance was a breakdown in human behavior.

"Depending on the disease, human behavior change can be the most important factor in getting it under control," he said. "Ebola in West Africa was exactly that situation as a person is actually most infectious just after they died. Local customs for both Christians and Muslims required elaborate burial rituals that brought people in close contact with the highly infectious loved one (very sad really).

"WHO has been rightly dinged for their slow performance in response and this is one of the key factors—they didn't have anthropologists and local community experts in the loop soon enough to help with the messaging and outreach and it cost us."

We are clearly facing a human problem that our industry has been unwilling or unable to address for over 20 years

THE FAILURE OF THE HUMAN SYSTEM cont

Theories of Accident Causation

In 1931, Herbert William Heinrich first published his book *Industrial Accident Prevention: A Scientific Approach*.

In a famous diagram (see Figure 4), Heinrich summarizes that *management* controls *man failure (knowledge, attitude, fitness, and ability)* which causes or permits *unsafe acts of persons* and *unsafe mechanical or physical conditions*, which cause *accidents*. Heinrich's "domino theory" argued that injuries resulted from accidents; accidents from unsafe acts; which in turn occurred from the faults of people; which had their origin in the social environment.

He theorized that:

- 88% of workplace accidents were caused by unsafe acts (usually by the injured person)
- 10% of workplace accidents were the result of unsafe equipment or conditions
- The remaining 2% were unavoidable.

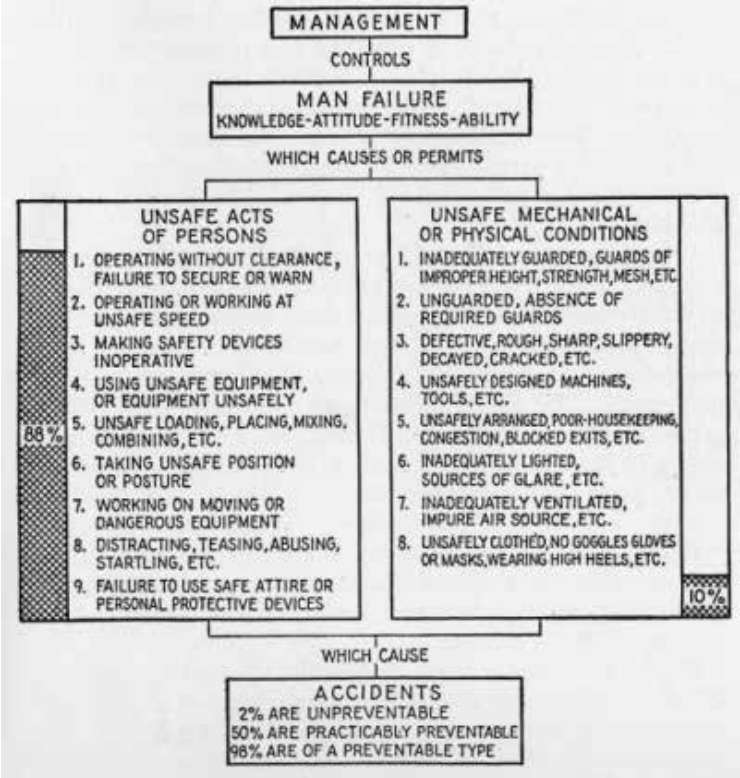


Figure 4: Chart of direct and proximate accident causes from Heinrich's *Industrial Accident Prevention: A Scientific Approach*.

Nine items make up the unsafe acts that cause 88% of accidents as shown in the Figure 4.

After reading these components, I thought for a long time about how these findings could map to the failures we see in cybersecurity. My mappings are in the table below:

	CAUSES OF INDUSTRIAL ACCIDENTS	CAUSES OF CYBERSECURITY INCIDENTS
1	Operating without clearance, failure to secure or warn	Operating without sufficient technical knowledge
2	Operating or working at unsafe speed	Failure to use the system as it was intended
3	Making safety devices inoperative	Failure to properly use prevention mechanisms
4	Using unsafe equipment, or equipment unsafely	Failure to follow documented procedures
5	Unsafe loading, placing, mixing, combining, etc.	Failure to implement appropriate configuration settings
6	Taking unsafe position or posture	Failure to take a proper defensive posture
7	Working on moving or dangerous equipment	Unnecessary interaction with critical computing assets
8	Distracting, teasing, abusing, startling, etc.	Failure to understand the severity of the situation
9	Failure to use safe attire, or personal protective devices	Failure to implement proper security controls

THE FAILURE OF THE HUMAN SYSTEM cont

Changing Behavior to Prevent Accidents

Heinrich argued that the best way to prevent injuries was to stop accidents from happening. Since the immediate cause of accidents was unsafe acts, eliminating these was the most effective focus of injury prevention programs.

This is the premise of behavior-based safety (BBS) and other industrial safety programs: changing workers' behavior is the principal means of reducing the number and severity of workplace accidents.

Behavior-based safety applies the science of behavior change to real-world problems. It analyzes what people do and why, then uses an intervention strategy to change that behavior.

A successful BBS program must include all employees, from the CEO to the frontline workers, contractors, and sub-contractors. Achieving changes in behavior requires changes in policy, procedures and systems. These require buy-in and support from all involved in making those decisions.

BBS is not based on assumptions, personal feelings, or common knowledge; it must be based on scientific knowledge.

However, regulators such as the US Occupational Safety and Health Administration do not necessarily focus on the behavioral aspects of the job. One commentator I read accused OSHA of being "all about compliance and findings" and "more comfortable with problems it can see on a clipboard."[ix]

The Connection to Cybersecurity

I found this aspect of BBS programs eerily similar to something security experts have identified and echoed for many years: A successful security program must be holistic. It is a business issue, not an IT issue. Without top-down commitment, evangelization, and support acceptance, ultimately integration at the lower levels of the organization will be impossible.

As with a successful BBS program, a successful cybersecurity program must keep everyone—the CEO down to the newest intern—in lockstep, myopically focused on the singular goal of making the organization safer.

This is also very similar to the way the US military trains during peacetime. I served in the US Army for 13 years in the Field Artillery and Signal Corps. Our primary mission was to remain combat ready at all times.

We trained as if we would be deployed tomorrow, giving rise to the concept *train as you fight*. We drilled our minds and our bodies each day for one singular purpose: going to war. Likewise industrial manufacturing operators should perform their duties as if a safety incident were just around the corner and cybersecurity professionals should prepare their organizations as if a breach was going to take place at any moment.

The (All Too) Common Causes of Accidents

Digging deeper into BBS programs, I spoke to Rob Caillet, Environmental Health & Safety and Security Manager at a General Electric facility in Fort Worth, Texas that manufactures large locomotive engines. When I asked him what he observed to be the primary social factors present during and after accidents, he told me accident victims usually said something like:

- "I've worked on this equipment for 15 years. I know what I'm doing."
- "What could happen? I'm only working on X."
- "All that safety stuff is for other people."
- "This kind of thing won't happen to me."
- "That accident has never happened before."

There it is!

The main cause of failure in the WHO's handling of the Ebola epidemic and in workplace accidents was exactly the same as the one I identified in the cybersecurity industry. Not medical science, not mechanical failure, not gremlins or system glitches, but human beings who experience the same cognitive biases no matter what job they do and regardless of their physical or intellectual capacity.

I also noticed a very clear correlation between OSHA's compliance-driven approach and that of GRC regimes such as the Payment Card Industry Data Security Standards, the Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes–Oxley. The manufacturing industry figured out the hard way that checklists and process guidelines will not solve the underlying problems of safety and security because human behavior is the common denominator. Try as you might, you cannot simply provide a checklist and expect people to change.

Like it or not, we are the problem.

THE PATH BEFORE US

Now we can see that this is a human problem, the logical conclusion is that we need a human solution.

This is where it gets tricky.

Do we keep trying the same things we've been trying for close to 20 years with no visible impact? Or do we take a lesson from WHO and the manufacturing industry, and implement a solution that has proven to be successful? Specifically, should we stop trying to solve the problem in a linear, technical manner and shift to a more human-centric approach?

Consistent with Heinrich's theory, I believe we should engineer out as many manual intersection points as possible. By reducing the number of times human beings need to make a decision, we minimize the opportunity for mistakes. Then, for those areas where human interaction is inevitable, provide comprehensive training and simulations to better prepare individuals to make those decisions.

This would foster a marriage of human intelligence and technology in a manner that the cybersecurity industry has not adopted to any significant degree.

In my experience, network and security operations centers (NOCs and SOCs) use mechanisms such as AV, IDS, or security incident event management (SIEM) solutions to look across huge numbers of alerts. As a result, actual malicious activity is frequently buried under the volume of false positives.

In most cases, the configuration settings of these monitoring solutions have not been adjusted during an actual threat scenario. (Often these systems remain at their default settings or have nominal adjustments made by the vendor at disparate intervals). This means the tools are not configured to spot an actual attack in progress. In my experience, this capability is vital for an organization to defend itself during an attack and to conduct comprehensive investigations afterward.

In addition, many of the individuals working in these centers have never been trained on correlating the alerts they see with actual human activity; creating a widening knowledge gap that prevents them from being truly effective.

Even if their tools were configured properly, performing as intended, and displaying alerts of actual, no-kidding attacks, the humans sitting in the SOC or NOC lack the knowledge to understand what they are looking at, why it's important, and what to do about it. There are organizations that are doing this really well today, but the rest are spending vast sums of money on tools and technology in the hopes of protecting their critical data. Unfortunately, they are falling short of that goal by failing to implement the most important component of their defensive posture: trained people.

Escalation of Commitment

Changing the course we have been on for a long time houses its own bias: *escalation of commitment*. This bias is the pattern of behavior in which humans continue to rationalize their decisions and behavior, even when they cause clearly negative outcomes, rather than alter their course. As we look back on all of the time and money we spent fighting the wrong battle, there will naturally be some resistance to change.

We must also overcome another pesky cognitive bias, conservatism. *Conservatism bias* (as opposed to political or social conservatism) is the tendency for humans to insufficiently revise their beliefs even when they are presented with compelling new evidence. This is the root of the saying (and the bane of my existence) "But we've always done things this way!"

It is going to be a very tough pill to swallow, since humans do not like to admit fault for anything (remember externalization?). Identifying and overcoming our cognitive biases take a tremendous amount of emotional maturity, something technical people (including me) are not the best at, if you believe the stereotypes.

The logical question now is, as an industry are we mentally and emotionally mature enough to push beyond our cerebral programming and alter our destiny? Can we break a decades-old bad habit?

As we look back on all of the time and money we spent fighting the wrong battle, there will naturally be some resistance to change

THE PATH BEFORE US cont

Outthinking our Brains, or, the Way Forward

Economist and social philosopher Adam Smith described it this way in his 1776 book, *The Wealth of Nations*: "It is not from the benevolence of the butcher, the brewer, or the baker that we expect our dinner, but from their regard to their own interest." Do we want to survive, thrive, or simply go gently into that goodnight?

We now know that we are dealing with a cerebral vulnerability that can be "patched," to use technical vernacular. Doing so will require the courage to admit we have been wrong, the strength to alter course, and the resolve to see it through. This is a very tall order, but history has shown if we can do these things, we will be successful and start to take back the ground we have surrendered to the enemy.

Our industry is densely populated with very intelligent, very technical people who want to solve problems through technology. This is not a shortcoming on their part, just how they are naturally wired. They are quantitative thinkers, binary—if there is a technical problem, there must be a technical solution. However, two decades of less than stellar results has proven otherwise.

Bringing the real problem into focus reveals what we have been dealing with all this time: not a shortcoming in technical capability, but the ugly messiness of people.

As a leader and member of highly technical security teams over the past 15 years, I can personally attest to the fact that emotional intelligence and maturity are not highly valued in this field. These teams have included brilliant technical minds who wrote books and computer scripts and programs capable of doing truly amazing things. Their knowledge was vast and impressive—they were true masters of their craft. However, their technical acumen overshadowed their lack of emotional maturity, and rightfully so. They were measured and paid on their ability to solve technical problems.

So, in a sense, the cybersecurity industry has done this to ourselves. We have focused so heavily on technical knowledge and capability that we have created an entire population of workers who are frankly not that great with people. Now, if we do things the right way, we must ask these technical experts to solve a largely human problem.

Do you really anticipate anything other than resistance, futile as it may be?

Bringing the real problem into focus reveals what we have been dealing with all this time: not a shortcoming in technical capability, but the ugly messiness of people

TURNING THE SHIP AROUND

I had a commander in the army who once told me "Don't come to me with problems unless you have a solution." So, in line with my military training, I submit two plans for changing the course we find ourselves on. I have separated this plan into two sections, a Battle Plan, which is a higher level, strategic plan; and an Action Plan, which is a more granular tactical plan focusing on how to execute on the Battle Plan.

THE BATTLE PLAN

1. Admit	Admit there is a problem. This is step one in every recovery program for good reason. You cannot begin to address a problem that you can't or won't admit is actually there.
2. Identify	Identify which cognitive biases are present in your organization. This will take emotional maturity at all levels—to the best of my knowledge, every person at every company everywhere in the world is a human being. Expect tremendous resistance at this stage of the process. Progress here will essentially involve admitting personal shortcomings at various levels, up to and including the CEO. Organizational leadership will face the question, "Which is more important: your ego or the success of your organization?" You can only choose one answer.
3. Automate	Science the %^#& outta it! Engineer out as many human decision points as possible. Technical people get nervous about the word "automation" for good reason. In many instances their job relies on a manual process that, if automated, could mean the loss of employment. It's important to clearly state that you are reducing human decision points, not eliminating them, and that the remaining intersection points will require enhanced decision-making capability from those individuals responsible for them. You should follow this up with extensive, realistic scenario-based training to give people those skills.
4. Learn	Let other people make bad decisions and be happy to learn from them. Seriously, do that! There are so many breaches that can be analyzed that there really is no reason why our industry should not have volumes of post-incident review documentation to learn from. Organizations should implement an after-action review process for all breaches, whether they're publicly disclosed or not. It's true that when you are in the middle of trying to fix an urgent problem, the last thing you have time for is being a case study for someone else. Still, if you think beyond the impact to your own organization about what can be learned from your incident, it will help others avoid a similar situation. That can only benefit everyone involved, including you. So ask yourself: what can we learn from this breach? How can these lessons improve your organization's security posture? If you are dealing with an internal incident, how can you use your experience to help others?
5. Hire	Hire for success. You should seek to employ the right kind of people, rather than the most geographically convenient ones or those with a certain skillset. You will need people who can follow processes and procedures, can take direction, and are less egocentric and more mission focused. Historically, the hiring process for technical jobs has mainly focused on whether or not the applicant already has the technical skills to perform the tasks required for the job. While this may seem logical, we have two decades of evidence to substantiate that it's a very poor hiring strategy. Curse you, pesky evidence!

nuix

TURNING THE SHIP AROUND cont

THE ACTION PLAN

1. Realize there is a problem, and that we are going to do something about it	While step 1 of the Battle Plan is admitting there is a problem, the first step in the Action Plan is to commit to taking action. Think of the difference between saying "I need to start going to the gym" and showing up at the gym on Monday morning. Count the cost, commit, and act!
2. Garner or provide top-down support	Just like a BBS program, a security program cannot be successful without top-down commitment, support, and evangelization. This is absolutely critical; the leadership of your organization must be utterly committed to the security program or it will become an exercise in futility and a colossal waste of money, time, and energy.
3. Identify cognitive biases and implement a mechanism to overcome them	This is going to take some serious mental and emotional maturity within the organization as these biases will be present in every member of the staff, from the CEO down. As you seek to implement this phase, I highly recommend retaining the services of a professional executive coach or organizational change consultant. It will not be easy, it will not be pleasant, and it will very likely cause a lot of political and social upheaval within the company.
4. Understand the return on investment for security	Spending time, energy and resources on security is not a net loss. When weighed up against the costs of post-breach litigation, the fines that regulatory bodies can levy, and the decrease in revenue from losses of customer confidence and market share, there is tremendous wisdom to investing in security.
5. Understand that GRC regimes are only part of the solution	You are kidding yourself if you think you can checkbox your way to a secure environment. If GRC regimes alone could prevent data breaches, payment card breaches would have ceased in 1999 when Visa first released the Cardholder Information Security Program. Compliance will never ever equal security … ever. Now, it can still be a good idea to align your security posture with a compliance régime—or in many cases, a requirement. But you should never expect that compliance alone will make your environment safe from attackers.
6. Look for wisdom in other areas of industry	As this white paper has shown, you can learn valuable lessons from other, older businesses. Do not be so precious as to think our industry is unique. The two examples I chose—the spread of communicable diseases and the manufacturing industry—provided a wealth of knowledge and many parallels. Other areas very likely will have similar wisdom to share. I hope others will do as I have done and write about these nuggets of hidden knowledge.
7. Institute a "train as you fight" security philosophy	Just like the military is myopically focused on going to war, cybersecurity professionals should focus on preparing for a cyberattack. Doing so will put your organization in a much better position to handle a real incident when it happens. And it will happen. Remember the organizations that are breached and don't know it yet? Train as if every day is that day.

nuix

TURNING THE SHIP AROUND cont

THE ACTION PLAN

8. Create a culture of security-minded employees	Security is everyone's responsibility. This is not a clever cliché, but a reflection of the current threat landscape. Client-side attacks such as social engineering, spear phishing, and browser-based exploits are among the most common and most effective attack vectors. Every employee, contractor, third party vendor, intern, or volunteer should understand the basics of identifying, deflecting, and reporting these attacks.
9. Realize security is a journey, not a destination	Becoming secure is not something you do, it's something you are. You will not reach the end of a strategic initiative, declare victory, and celebrate your hard work. There is no beginning or end to this journey. It's sort of like getting fit; you don't go to the gym for a year, announce one day that you've achieved fitness, and never run another mile or lift another weight. This is a long-term commitment that will change and evolve or time. Like physical exercise, it will get easier as time goes by, but you will never be done.
10. The marriage of human intelligence and technology is the key to victory	As with the industrial manufacturing industry, the goal is to engineer out as many human intersection points as possible to reduce the opportunity for errors. In those areas where automation cannot replace human interaction, the people in those positions should be extensively trained and equipped with software that will act as an intelligence multiplier. This marriage of technology and human intelligence represents the path forward and what I believe to be the crucial element in reclaiming surrendered ground.

THE CATCH-22

Ok, so this is great: We have identified the problem, we have a Battle Plan and an Action Plan, so now all we need to do is go and implement it, right?

Well, it's not quite that easy (it never is).

Here's the Catch-22—everybody in the cybersecurity industry knows there is a worldwide skills shortage; we have far more openings than we have people to fill them. Organizations are trying to bridge this gap by finding enough bodies that closely align with the skills they're looking for. They've learned to overlook or ignore prospective employees' lack of non-technical people skills.

Remember, though, that technical ability alone is not enough; if it were, breaches wouldn't occur in such great numbers and with such frequency. Now organizations will have to take a very short list of people who have the technical skills to fill their cybersecurity vacancies and try to identify the individuals who also possess the mental and emotional maturity to effectively contribute to this next generation of strategic security solutions.

I realize this may not be realistic in the short term; business needs may require immediate action. However, if organizations become more aware of the need to identify and hire candidates who possess these non-technical skills, they can start the process of hiring for long-term success. In other words, they need to start looking for Mr. or Ms. Right rather than Mr. or Ms. Rightnow.

THE SUMMATION OF THE PSYCHE

> "Excellence is never an accident. It is always the result of high intention, sincere effort, and intelligent execution; it represents the wise choice of many alternatives—choice, not chance, determines your destiny."
>
> **Will Durant, *The Story of Philosophy***

Our brains are supercomputers, but like all computer systems we have vulnerabilities that need to be identified and remediated. Throughout this white paper, I have clearly shown that data breaches are caused by human action or inaction.

The cybersecurity industry has historically thought of data breaches as a technology problem, but all the evidence indicates that they are really a human problem. Based on the lessons learned from WHO and Heinrich, preventing breaches requires changing behavior and reducing the number of opportunities for people to make mistakes.

We now find ourselves at a crossroads where decision makers need to choose the "same ole same ole," or innovation.

Do cybersecurity practitioners have the mental and emotional maturity to overcome the cognitive biases identified in this paper, admit we have been fighting the wrong battle for two decades, and learn from those mistakes?

The cybersecurity industry is in a very interesting place. Our collective experience does not easily lend itself to the situation we find ourselves in. If we are not careful and hyper-cognizant of our decisions, we could very easily be led astray.

L.M. Montgomery, author of the Anne of Green Gables novels, eloquently said, "We all make mistakes, dear, so just put it behind you. We should regret our mistakes and learn from them, but never carry them forward into the future with us."

Our brains are amazingly fast and accurate at recognizing patterns. We collect all sorts of data and we create mental shortcuts to make sense of the world. To illustrate this point, did you know that none of us actually reads the individual letters in words beyond elementary school; rather, we recognize words or word patterns and quickly draw meaning from what we see. This is why we can decipher writing that is jumbled, backwards, or drastically misspelled (see Figure 5).

Whether or not we act on those patterns depends on our emotional maturity, specifically on something called *emotional tags*. These tags provide the framework for us to develop a sense that what we are seeing is a good thing or a bad thing. Put simply, we don't make fact-based decisions; we make emotional choices based on pattern recognition.

Our focus, as we move forward, should be on the patterns and tags associated with the marriage of people and technology. By reducing the number of human decision points through technology, we can dramatically reduce the opportunity for mistakes and failure. Then we can focus our pattern recognition efforts on realistic attack scenarios, provide military style training and education, and conduct ongoing threat simulations. Doing so will enable the individuals at the remaining intersection points to be exponentially more prepared and subsequently more successful than they have ever been.

One final thought: The status quo bias can be summed up with the saying "If it ain't broke, don't fix it." This bias takes the current reference point and views any sort of deviation as a perceived loss. Do we have what it takes to outsmart our own brains and stop ourselves from repeating the mistakes of the past? Hopefully we can set ourselves up for the next 20 years and we can get serious about security, start addressing the real human vulnerability, and start reclaiming surrendered ground.

THE PAOMNNEHAL PWEOR OF THE HMUAN MNID. Aoccdrnig to a rscheearch at Cmabrigde Uinervtisy, it deosn't mttaer in waht oredr the ltteers in a wrod are, the olny iprmoatnt tihng is taht the frist and lsat ltteer be in the rghit pclae. The rset can be a taotl mses and you can sitll raed it wouthit porbelm. Tihs is bcuseae the huamn mnid deos not raed ervey lteter by istlef, but the wrod as a wlohe.

Fgirue 5: Can you raed tihs?

References and Further Reading

BakerHostetler, *Data Security Incident Response Report 2015*, May 2015

Michael Carroll, "Part Human, Part Machine, Cyborgs Are Becoming a Reality", *Newsweek,* July 2014

George Dvorsky, "The 12 cognitive biases that prevent you from being rational", *io9*, September 2013

Experian, *2015 Second Annual Data Breach Industry Forecast* October 2015

Sydney Finkelstein, "Why Smart People Make Bad Decisions", *Harvard Business Review*, February 2009

FireEye Threat Intelligence Reports

Herbert William Heinrich, *Industrial Accident Prevention: A Scientific Approach*, McGraw-Hill, 1931

F. Heylighen, "Occam's Razor", *Principa Cybernetica*, September 1995

Identity Theft Resource Center, *2015 Data Breaches*, January 2016

Ari Kaplan Advisors, *Defending Data: Turning Cybersecurity Inside Out With Corporate Leadership Perspectives on Reshaping Our Information Protection Practices*, December 2015

Hans Moravec, *ROBOT: Mere Machine to Transcendent Mind,* Oxford University Press, October 1998

Frank Pennachio, "Going beyond the Limits: A 10-Year Study Conducted by DuPont Found That 96 Percent of Accidents at the Company Were the Result of Unsafe Actions by Employees Going beyond Their Limits, Rather Than Unsafe Conditions", *Occupational Hazards*, September 2008

Ponemon Institute, *2015 Cost of Data Breach Study,* May 2015

Verizon *2015 Data Breach Investigations Report*, July 2015

World Health Organization, *Report of the Ebola Interim Assessment Panel*, July 2015

i Identity Theft Resource Center, *2015 Data Breaches*, January 2016

ii Ibid.

iii Ponemon Institute, *2015 Cost of Data Breach Study*, May 2015

iv F. Heylighen, "Occam's Razor", *Principa Cybernetica*, September 1995

v Michael Carroll, "Part Human, Part Machine, Cyborgs Are Becoming a Reality", *Newsweek*, July 2014

vi Ari Kaplan Advisors, *Defending Data: Turning Cybersecurity Inside Out With Corporate Leadership Perspectives on Reshaping Our Information Protection Practices*, December 2015

vii Experian, *2015 Second Annual Data Breach Industry Forecast*, October 2015

viii BakerHostetler, *Data Security Incident Response Report 2015*, May 2015

ix Frank Pennachio, "Going beyond the Limits: A 10-Year Study Conducted by DuPont Found That 96 Percent of Accidents at the Company Were the Result of Unsafe Actions by Employees Going beyond Their Limits, Rather Than Unsafe Conditions", *Occupational Hazards*, September 2008

ABOUT THE AUTHOR

Christopher E. Pogue

Chris Pogue is the Senior Vice President of Nuix's Cyber Threat Analysis security consulting team, and a member of the US Secret Service Electronic Crimes Task Force.

Pogue is responsible for the company's security services organization; he oversees critical investigations and contracts, and key markets throughout the United States. His team focuses on incident response, breach preparedness, penetration testing and malware reverse engineering.

Over his career, Pogue has led multiple professional security services organizations and corporate security initiatives to investigate thousands of security breaches worldwide. His extensive experience is drawn from careers as a cybercrimes investigator, ethical hacker, military officer, and law enforcement and military instructor.

In 2010, Pogue was named a SANS Thought Leader.

Pogue served in the United States Army as a Signal Corps Warrant Officer and Field Artillery Sergeant. He distinguished himself as an Honor Graduate from a variety of Army Academies and Schools and received multiple awards and commendations for excellence.

To find out more about Nuix's approach to addressing cybersecurity threats visit:

nuix.com/security-intelligence

ABOUT NUIX

Nuix protects, informs, and empowers society in the knowledge age. Leading organizations around the world turn to Nuix when they need fast, accurate answers for investigation, cybersecurity incident response, insider threats, litigation, regulation, privacy, risk management, and other essential challenges.

North America
USA: +1 877 470 6849
» Email: sales@nuix.com

EMEA
UK: +44 203 786 3160
» Web: nuix.com

APAC
Australia: +61 2 9280 0699
» Twitter: @nuix

CY1604US1