WISEGATE ANSWERS

REPORT SERIES

What does Information Security have in common with Eastern Air Lines Flight 401?

REPORT SERIES

EXECUTIVE OVERVIEW

What does Information Security have in common with Eastern Air Lines Flight 401? It's an odd question, with an important—and potentially tragic—answer. Information Security, with its sundry standards and glut of gizmos, has been on a nearly imperceptible descent for years. In this seven-part think piece, Wisegate member and security expert Martin Zinaich looks at the problems endemic to business and information security, how we got into this mess, and suggests ways to get out of this predicament.

Part I: In the Beginning

What does Information Security have in common with Eastern Air Lines Flight 401? It's an odd question, with an important—and potentially tragic—answer.

On December 29, 1972, Eastern Air Lines Flight 401 crashed into the Florida Everglades, causing 101 fatalities. The crash occurred because the entire flight crew became preoccupied with a burnt-out nose gear indicator light. Meanwhile, they failed to notice the autopilot had been inadvertently switched from Altitude Hold to Control Wheel Steering mode. In this mode, once the pilot releases pressure on the yoke the autopilot maintains the pitch attitude selected by the pilot until the pilot moves the yoke again. The investigators believe the mode was accidentally switched and then an ever-so-slight forward pressure was applied to the stick, causing the aircraft to enter a slow descent.

As a result, the aircraft gradually lost altitude and eventually crashed while the flight crew was distracted with the indicator problem.

What is the parallel with Information Security? Information Security, with its sundry standards and glut of gizmos, has been on a nearly imperceptible descent for years…while those involved and those that should be concerned are focused on the indicator light.

I have been in this industry for many years; I cut my teeth installing networks. At the time I was the young techno punk thinking that my technology was so very "kewl." I still remember the day an "old-timer" mainframe person asked me how I did *turnover*. I had never heard the word applied to computers, so I pointed to the floppy disk drive on the server I was installing and said, "you pull that out, turn it over and you get twice the space," with my young kid smirk. I guess *I* am now the old-timer network person…but I do better understand that question.

In the early days of personal computers and the DOS operating system, you did not need a password. Indeed, you could not even add one if you *wanted* to. The first Windows operating system started by typing WIN, pressing [Enter] and that was all one needed.

Then people stumbled onto the thought that a password would be innovative, so that was added—even before Windows NT (New/Next Technology)—in the humble Windows 95. This was hardly any kind of security at all; like so many security ideas that are afterthoughts, you could simply boot to DOS and delete all the PWL files and then log in as a new user.

IBM's LAN Manager added an LM hash algorithm that used a method of hashing passwords so weak, it could be cracked in *seconds*. Now—for the truly technical readers out there—I do realize there were other operating systems at the time that *did* support some decent security, but like with many things—what caught on like fire was the "easy" one.

The slow descent of the Information Security aircraft began with the personal computer. It was rare to hear about someone "cracking" into a mainframe, and even less common to hear about a mainframe virus spreading.

There is a reason for that.

Mainframes were built with a business mindset; they cost so much they were treated like a large piece of the business. Therefore, that question about turnover—which is a process of moving application code from a test environment to a production environment—included segregation of duties. The design afforded the developer to develop code, but have it submitted by an operator. Operators could not *write* code, they could only take code written from a developer and move it into production: an enforced segregation of duty built directly into the system.

And it didn't stop there. To connect to the mainframe, you had to first be connected to a *controller*, which like its name implies, controlled access to the main system for both performance and security. If you needed to connect from a remote location there were dial-

back systems. Your phone number had to be listed and it was matched to your login ID. You would call into the system, enter your login and—yes—a password; the system would hang up and call you back at the number listed in your account.

Mainframes were usually put in secure locations with restricted access; backups were standard operating procedure, along with off-siting that media. Job logs of backups and applications were monitored daily and if the mainframe connected to another system, it was all very well defined and secured.

Obviously, none of this was very agile.

Furthermore, it was expensive and not at all user-friendly. That is partly because the technology had not evolved to present day standards, but those business thought processes were all baked-in and provided a great deal of assurance.

The Personal Computer changed all of that structure by putting the computing power closer to the end-user. Soon payroll could be running on Bob's PC over in the corner and no one batted an eye, not even the CIO—who was under pressure to get more of these thingamajigs in the hands of users.

All of a sudden, making a change didn't take an act of congress, it took the end-user fiddling around until the "thingamajig" did what was needed… or even close was good enough if one could just do it on his/her own. Was Bob's PC being backed up? Were changes controlled? Was there any security (other than typing in WIN)? No, but who needed all of that overly complicated stuff anyway? Everything was working fine, and it was a lot more agile.

Around that same time a buzzword began being thrown around about the PC and these changes: *paradigm shift*. And to be sure it was, and it did indeed put computing power closer to the user. I was "paradigm shifting" networks like a madman, hooking up PC's to Token-Ring, creating shares, and even adding passwords (on occasion).

However, the other paradigm shift was *away* from security and standard business practices. All eyes were fixated on the nose gear indicator light, while the secure standard business practices began their gentle negative glideslope.

Part II: A Glimmer of Hope

All was not lost, as in stepped the International Information Systems Security Certification Consortium (ISC)[2] in 1988. *"The Consortium" was formed among several professional*

organizations to create a global information security certification process for professionals and address the need for standardized curriculum for the burgeoning profession.

The goal was noble and the need certain, however the execution might be considered less than particularly effective. In 1992 ISC² released the Common Book of Knowledge (CBK). The CBK established a common framework of information security terms and principles, which allowed information security professionals worldwide to discuss, debate, and resolve matters pertaining to the profession with a common understanding. The CBK exposes Information Security (InfoSec) professionals to a very broad landscape of InfoSec coverage and is an excellent resource. However of the some thousand pages of content in the CBK I used for study, only two were devoted to Information Security Governance. In essence, we were still fixated on the nose-gear light, instead of business indicators.

Auditors—people InfoSec professionals know all too well—actually took a lead role in developing what is known as the Generally Accepted Accounting Principles (GAAP), a standard framework of guidelines for financial accounting. The need is almost too obvious for definition, but if GAAP did not exist, companies would not be able to provide accurate and consistent financial information to investors, creditors and stakeholders of a company. Surely Information Security has a standard framework of Generally Accepted Information Security Principles — a GAISP if you will. And of course, there is one. Or rather, there *was* one. The Information Systems Security Association (ISSA) had a GAISP. GAISP was the successor to the GASSP, the Generally Accepted System Security Principles. The original GASSP project was formed in mid-1992 in response to Recommendation #1 of the report "Computers at Risk" (CAR), published by the United States of America's National Research Council in December of 1990. The GAISP even had its own domain (www.gaisp.org). Both the framework and domain are now dead.

As near as I can tell, GAISP was dropped between 2004 and 2007. I quote from the last version (emphasis added):

> *Recognizing the hierarchic nature of principles, GAISP will be organized in three levels: The Pervasive Principles which* ***target governance*** *and describe the conceptual goals of information security; the Broad Functional Principles which* ***target management*** *and describe specific building blocks (what to do) that comprise the Pervasive Principles; and the Detailed Principles, which* ***target the information security professional*** *and include specific "how to" guidance for implementation of optimal information security practices.*

InfoSec Governance, directing InfoSec Management, directing InfoSec Professionals' actions: the right target focus areas, and the right order of focus. It is as if someone lifted

their head enough to recognize that the landing gear light might not be the only problem. Unfortunately, something happened and all eyes were refocused back on the light, which in this case *is* the "target information security professionals" and the descending glide slope became "target governance" and "target management."

What We Need Here is a Good Framework

Mr. Michael Dell, founder of Dell Computers, was right when he said, "You don't have to be a genius or a visionary or even a college graduate to be successful. You just need a framework and a dream." Notice he didn't say you need a cornucopia of frameworks, just *a* framework.

Frameworks are not perfect; they are living standards that get adjusted through growth and learning. Nevertheless, having what I like to call a "littering of frameworks" is not helpful. Some may see this as a great thing, because the professional can pick what fits best. In some ways that is true, but Information Security should not be treated like a doughnut shop.

Why do I say this?

If you are in Information Security you have many choices, not only in how you will be defeated (and you will be—either by hackers, bad code, or management), but in the framework you elect to follow (if you actually pick a framework). Some of my favorites are ISO/IEC 27002:2005, COBIT, COSO, Common Criteria, ITIL, FISMA, ISF, ISM, NIST SP800's, PCIDSS, SABSA, to name a few. You can imagine my joy when DHS teamed up with NIST to release yet another, the *Cyber Security Framework.* It stems from a couple of executive orders, which created the *Critical Infrastructure Cyber Community (C3) Voluntary Program*. There is a word in that title that should stick out to you as spelling impending doom. If you do not know which word, you should probably keep reading. If you do know the word, keep reading anyway for the cathartic pleasure.

There is no framework I have read—from ISO27002 to Cobit to the Cyber Security Framework—for which I do not appreciate the amount of work invested or the completeness of vision. If you have never worked on a committee to develop one of these, you may find it hard to appreciate what a painful journey it can be, with a lot of emotional drain thrown in for good measure. However, as painful as putting a framework together can be, it pales in comparison with trying to implement one.

We are now getting very close to being able to take our eyes off the non-functioning landing gear light and take full appreciation of our glide path. Does anyone think we just do not have enough frameworks? Does anyone think the frameworks we have are pitifully unequal to the task? Maybe we need more certifications. I could list all of those but it would add

another 200 pages. Maybe we just do not have enough schools offering Cyber Security curricula. Could it be the "compliancy based" versus "risk based" security paradigm?

Part III: Back to the Future

I apologize for this, but I have to jump back to the beginning again. You see, the Internet was designed during the cold war, and a prime driver was the ability to sustain communication in the event of a nuclear attack. Back then, communication was usually point-to-point. DARPA and many smart people gave us "packet-switched networks". It meant that a piece of data could flow through different paths and reassemble on the receiving side. This meant if communication hubs were taken out of service between you and where you were trying to communicate, due to, say, a nuclear bomb being dropped, your packets could now travel a different route and your Twitter post about the latte you purchased this morning would stick. However, it was not designed to be a public network and security was not invited to the party.

The lesson here is age-old; bolting on security after the fact is always more costly, time-consuming and less effective than baking it in from the start. The first email servers on the Internet were open relay by design, known as store and forward. That meant anyone could send email through your email server to someone else. After all, the idea was sustained communications so if my email server went down, why not use one of the other available email servers?

Unfortunately, as with many well-intentioned plans, it fails to account for bad people. Soon spam became a well-known term to define something other than the delicious food of previous association. Domain Name Services (which translates the web sites we type into IP addresses) is not secure. It has suffered from numerous attacks. The weakness of this core protocol has been known for a very long time and a secure DNS (DNSSEC) was proposed in 2005 via RFC 4033. You can go to http://www.dnssec-deployment.org/ to see how *that* has been going.

In general, the US Root DNS servers were operational in 2010. DNSSEC does not in any way totally fix DNS, as in recent months there has been a rash of DNS Amplification Denial of Services attacks. DNS is just one small area of vulnerability; the list of protocol weaknesses and associated attack vectors is legion.

In short, what we have put in place are insecure computing devices connected together using insecure protocols over a fabric connected to support some of our most critical dependencies and let anyone in the world—good or bad—have access to it.

I remember watching a video with one of the engineers that worked on the initial Internet design and protocols. He stated that, “If you would have told us that we would be putting critical infrastructure on a public network, we would have just laughed – that will never happen.” There was a completely different mindset back in those days. Business standards existed beyond the “want of the moment.” Thought was given to business risk, mostly driven top-down. Today, one could argue business risk is driven bottom-up and in the Information Security world, I would posit that 80-90% of InfoSec programs are driven in exactly that same direction.

Part IV: Pay Now or Pay Later

I have a saying: “In business, agility will trump information security...until such time that the lack of information security decimates agility”. The first part of my saying is just a law of staying in business, but the second part does not have to be true.

So why *is* it true so often?

On April 20, 2011, Sony acknowledged on the official PlayStation Blog that it was "aware certain functions of the PlayStation Network" were down. At the time, Sony announced that it might take one or two days to put things back in order. In reality, Sony had been hacked and their popular PlayStation Network was offline for some 24 days. When the smoke cleared, the personally identifiable information (PII) of over 77 *million* customers had been compromised, making it one of the largest data breaches to date.

It was a costly event for Sony in many ways.

An important item is often omitted from the Sony breach event. Sony made their public announcement about the breach in April 2011, but they made another big announcement in May of that same year. In May of 2011 Sony announced it was creating a post of Chief Information Security Officer (CISO). We know at the time of the breach it had at least 77 Million customers on the PlayStation Network, we know it was taking credit card information, and we know it was making lots of money. Yet, in spite of all this, *it did not have a CISO position*.

One can assume Sony has its share of highly educated and highly trained MBA’s. Yet, evidently, none thought it strange—with 77 million customers, an online network and credit card information—that they did not have a CISO position. That is not hard to believe because it happened and because Information Security, as I noted earlier, is a business discipline that is usually pushed from the bottom up.

Lest you think I am just picking on Sony, in March of 2011 it was not a game developer but an Information Security company, RSA, that suffered a breach. In June of 2011, you guessed it: RSA appointed their first Chief Security Officer (CSO). In June of 2012 LinkedIn reported 6.5 million accounts were compromised. In that same month, it was reported that LinkedIn had neither a Chief Information Officer nor a Chief Information Security Officer.

Breaches are now almost a monthly—if not weekly—occurrence. Some are big, some are small, some cost reputation and some cost millions of dollars. One could write volumes covering all the security breaches we have seen in this industry, and even more volumes on the details. I picked the three incidents above to underscore a point. While government, universities, legislatures, certification industries and magazines all sound the "Cybergeddon" alarm, business education and business leaders still think this is only a technology issue.

The Light is Burned Out

The Information Security professional is asked to be a business enabler, participate in all new projects (if he/she is lucky), understand code weaknesses, monitor everything involving information access and movement, put in place the proper protections be it software or hardware related, find all corporate technology assets and their vulnerabilities, interface with other companies in a secure manner, provide secure anywhere/anytime access to everything, defend against attacks from around the globe, classify data and systems, review all logs, practice incident response, create policies that are friendly to the organization yet provide the best protections to business risk, train others, get certified, stay on top of all new vulnerabilities, stay current with secure coding practices, stay current with penetration testing, stay current with technology changes and sell the Information Security Program. That's a lot.

One thing is certain: if you cannot do that last item, you are doomed. That is truly a problem with the Information Security profession. With a breach-a-day environment and with a heavy business reliance on technology, why is Information Security still a paradigm that has to be "sold"?

Information Security has to be sold because the light is burned out. For all the expansion in the InfoSec profession, everyone is still looking at the burned out landing gear light (the technology alone). Let's be honest: there is a good deal of money to be made selling the technical aspects of Information Security, but by focusing on only one small area, we eliminate the responsibility of the flight crew to the overall duty of keeping the airplane flying properly and safely.

The current model for most businesses is that Information Security is pushed up from a corner of the IT Department. Combine that prototypical design with the insecure infrastructure that relies on it for protection and you can very easily see why Information Security has problems!

Part V: Wake the Flight Crew

The National Association of Corporate Directors (NACD), Director's Handbook Series, Cyber-Risk Oversight (2014) noted that in the past 20 years, the nature of corporate asset value has changed significantly, shifting away from the physical and toward the virtual. One recent study found that 80% of the total value of the Fortune 500 now consists of intellectual property and other intangibles. The report also states that along with the rapidly expanding "digitization" of corporate assets, there has been a corresponding digitization of corporate risk. NACD found some estimates predicting that between $9 and $21 trillion of global economic value creation could be at risk if companies and governments are unable to successfully combat cyber threats.

Businesses now face advanced attacks, by ultra-sophisticated teams that look to exploit any advantage against a company. Add to that risk the immense amount of interconnection among corporate systems, and it is no longer adequate that organizations secure only "their" network. Vendors, suppliers, partners, customers, or any entity connected with the company electronically can become a potential point of vulnerability. NACD also noted in their Cyber-Risk Oversight report a pivotal statement that is usually absent from Information Security training and business education, "Similar to other critical risks, cybersecurity cannot be considered in a vacuum. Members of management and the board must strike the appropriate balance between protecting the security of the organization and mitigating downside losses, while continuing to ensure profitability and growth in a competitive environment." This subtle statement is at the core of the need to professionalize the Information Security industry. Corporate management and board of directors, for the most part, do consider cyber security risks in a vacuum and do not equate it to other critical business risks.

The Wisegate 2013 IT Security Benchmark Report showed that 62% of those Information Security Officers surveyed report to a Chief Information Officer (CIO). The same report shows that only 5% report to a Chief Risk Officer and only 3% report to the Chief Executive Officer. How likely is it that Information Security, as a subcomponent of IT, can influence the business at the board level? Referencing the National Association of Corporate Directors Cyber-Risk Oversight report again, it recommends five key areas for corporate directors with regard to Information Security.

1. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
2. Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.
3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.
4. Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.
5. Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

Clearly, NACD senses these business risk implications of Information Security are not inculcated into business hierarchies. A professional organization working with business leaders and business educators is undoubtedly needed to make progress. This organization should be of one mind and one voice, not a disparate set of frameworks, certification bodies and vendor solutions as it is today. The current ad-hoc approach keeps this critical business function in an isolated state from the business proper.

Businesses do not know what they do not know and practitioners are unlikely to break into the C-Level to elevate this part of the business. Currently the way this usually happens in business is subsequent to a major incident, rarely prior.

Part VI: Taking Control of the Stick

One cold—but rarely addressed—reality of Information Security is the "institutional attack vector." Practitioners are battling against attackers from around the globe, from private individuals to state sponsored teams. They also battle against the basic insecure foundation of Internet protocols and personal computer operating systems. Add to that list poor programming techniques and the ever-dissolving edge of what they have to protect. However, there is another battle just as difficult and just as removed from their sphere of authority: the very business they are endeavoring to protect.

Information Security practitioners often face the challenge of battling the business. These battles take the form of coping with simple policies to facing complex issues like BYOD and compliancy. It's rare for the business and the security office to be partners, because the security office is not observed at the board level.

Likewise, the security office is often not thinking at the board level, but happily isolated in the technology. In such cases the Information Security Office is not business *enabling* but business *adverse*, further isolating its participation and influence.

The question becomes, how would professionalizing this field help drive solutions?

A recently released report, "Professionalizing the Nation's Cybersecurity Workforce? Criteria for Decisionmaking," by the National Research Council (2013), concluded that cybersecurity is still too new to professionalize standards for its practitioners. The National Research Council's arguments against professionalizing fall into three categories. In the first category, the council's claim is that the knowledge, skills, and abilities required of the cybersecurity workforce are so dynamic that one cannot effectively establish a baseline for professionalization. Next, they claim that the knowledge and competencies required by the cybersecurity workforce are too broad and diverse to enable professionalization. Lastly, they state that at a time where demand for cybersecurity workers far exceeds supply, professionalization would create additional barriers to entry.

The questions, if observed with a historical context, might find parallel associations in other nascent times when disruptive technologies emerged. The American Medical Association (AMA) was founded in 1847 to address one of the very same issues: a lack of professionalization in the medical field. During the early nineteenth century, the major concern was a medical profession increasingly overrun with self-taught practitioners, only some of who knew what they were doing. Risk to the public was simply too great to bear, and a movement began to minimize "self-taught practitioners" and professionalize the industry.

The AMA accelerated the professionalization of medicine and the establishment of minimum standards in medical training, education and apprenticeship requirements to gain entry to the profession. The same could and should be done in the Information Security field with a similar cybersecurity national body and professional associations.

The Department of Homeland Security released a recent paper entitled, "The Path towards Cybersecurity Professionalization: Insights from Other Occupations" (2014). The paper makes a comparison of the similarities between the professions of Aviation and Cybersecurity. The aviation industry has a number of categories of pilot that include student, sport, recreational, private, commercial and airline transport. All levels require different training and licensing.

In contrast, the National Research Council in its report, "Professionalizing the Nation's Cybersecurity Workforce? Criteria for Decision-making" (2013) stated that cybersecurity is

still too new a field in which to introduce professionalization standards for its practitioners. Yet a similar break down of "pilots" for cybersecurity has already occurred from the National Initiative for Cybersecurity Careers and Studies (NICCS) with the National Cybersecurity Workforce Framework 2.0 (NCWF). The framework assembles similar types of cybersecurity work into seven broad areas of practice—securely provision, operate/maintain, protect/defend, investigate, collect/operate, analyze and oversight/development.

Francesca Spidalieri and Sean Kern, in an excellent paper titled, "Professionalizing Cybersecurity: A path to universal standards and status" from the Pell Center (2014), noted that the American Board of Medical Specialties has 24 general certificates and 125 subspecialty certificates. In terms of depth and breadth, Information Security does not appear to be any more complex than other professionalized occupations.

The National Research Council report against professionalizing went on to state that the knowledge, skills, and abilities required of the cybersecurity workforce are so dynamic that one cannot effectively establish a baseline for professionalization. A counterargument seems clear: in such dynamic times, an expectation of coalescing direction and business alignment from such chaos is highly unlikely.

Francesca Spidalieri and Sean Kern's paper provides guidance to help professionalize the cybersecurity workforce following the traditional model of professionalization as represented by the medical profession and suggests a number of broad steps.

1. Create a nationally recognized, regulatory body to serve as a clearinghouse for the cyber-security profession, similar to the AMA in the medical field.
2. Establish member professional associations for each specialty.
3. With these in place, develop a common body of knowledge (CBK) for each specialty. These bodies will then establish and maintain rigorous standards of training and education along with establishing certification/licensing requirements.
4. To complete the training and certification an establishment of apprenticeships and residency requirements in each specialty will be developed.
5. Finally, establish a standard code of ethics.

Part VII: Refocus on the Glide Path

Often missing from the professionalization of Information Security debate is that of business intersection. The best-trained and certified professional will be of little use if injected into a working environment that is unconscious to need or risk. Where would the medical profession be today if it had not professionalized? What about the airline industry?

Providing businesses with trained professionals (not only in the technical aspects but also in the business aspects), combined with certification on a national or global level delivers to the business some basic assurance. A professional organizing body creating paths for the field and bringing together the brightest to help forge general directions and coverage across business verticals becomes a natural process benefiting practitioner and business alike.

However, the largest benefit comes from elevating the field into the business arena, where businesses are aware of, better understand the role of, and are able to fit Information Security into the proper level of business process. No longer would Information Security be just an IT problem, but what it actually is: a business problem. When businesses undertake Information Security like any other business risk, businesses enhance their level of security; this enhancement flows down to the products and services they deliver. When the current ad-hoc approach is exchanged with a holistic approach, it benefits the business, the industry, the consumer and the nation.
The rapid growth of technology since the birth of computers has revolutionized the world and the way both individuals and corporations leverage the Internet and computing devices. However, the rate of change has created new paradigms in business models at the same time complexity and risk acceptance has increased homogeneously.

Reliance on this multifarious cyber universe has likewise intensified and is projected to be increasingly ubiquitous as the “Internet of Things” looms on the near horizon. Yet the foundations baked into the very fabric of this creation were never designed to be secure. A central basic maxim of Information Security is that security after the fact is more costly, less effective and has a longer time to value. The current state of Information Security has borne out this truth in its very own industry.

Information Security is playing catch up at the same time it is trying to define a core in a multitude of security frameworks. As a relatively new industry, Information Security is facing challenges not unlike other new industries but it is not self-realizing its own deficiencies. Like the entry-level Information Security professional, that dives too deep into extraneous threat vectors but is unable to connect real business risk to the business, so goes the Information Security profession as a whole.

The Information Security profession must connect real business risk with the business in such a way that places the business in a position to lead Information Security. *Professionalizing* this industry may just be the only hope of making that switch and thus solidifying a permanent positive impact.

Report Author

Martin Zinaich is the Information Security Officer for the City of Tampa's Technology and Innovation department. He has written articles published in Popular Communications and Network World and holds a BS in Information Technology, a BS in Business Administration, an Associate of Science in Electronics Technology, Is a Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified In Risk And Information Systems Control (CRISC), Certified Secure Software Lifecycle Professional (CSSLP), Certified Ethical Hacker (C\|EH), Certified Novell Engineer (CNE), Microsoft Certified Professional (MCP) And A Toastmasters Competent Communicator (CC).

PHONE 512.763.0555

EMAIL info@wisegateit.com

www.wisegateit.com