VOLUME 2 ISSUE 3 · QUARTER 3 JULY—SEPT 2019

WELCOMING SHANNON BLUETT TO THE UNISHKA FAMILY

UNISHKA is pleased to welcome our newest staff member, **Shannon Bluett**. Shannon has been hired as a Finance Specialist providing payroll, accounting and finance support. Shannon is an Accounting major at the University of Alaska and plans to complete her Certified Public Accounting (CPA) exams in conjunction with her university degree. Shannon previously worked as the Operations Manager for Gross-Alaska, Inc. and continues to provide administrative support to Merdes Law Offices. Shannon lives in Juneau with her dog Leo.

DUNNING-KRUGER EFFECT

From 1951 through 1990, Mr. Wizard appeared on television screens across America teaching children about basic science. These classics are still available on YouTube. In one episode, Mr. Wizard described how writing with lemon juice made words invisible until they were subjected to a heated iron.

Affirming Alexander Pope's observation that "a little learning is a dangerous thing," is the now infamous case McArthur Wheeler of Pittsburgh, PA. USA.

On the morning of April 19, 1995, Mr. Wheeler was filled with confidence. Perhaps too much confidence, but as Charles Darwin noted, "ignorance more frequently begets confidence than does knowledge."

Using his Mr. Wizard knowledge, Wheeler reasoned that if lemon juice made words disappear, if he rubbed his face in lemon juice, he would be invisible to everyone, including security cameras. Consequently, Wheeler bathed his face and exposed skin in lemon juice and boldly robbed two banks in broad daylight without using a disguise. Security cameras caught him in the act and within an hour he was arrested. When investigators explained how they had used surveillance cameras to catch him, Mr. Wheeler incredulously muttered, "but I wore the juice!"

Wheeler went to jail but David Dunning, a Cornell psychology professor saw in Wheeler's tragic tale something universal. Building on Darwin's observation, that "ignorance more frequently begets confidence," Dunning and a graduate student, Justin Kruger, embarked on a series of experiments testing this premise. They tested undergraduate psychology students then asked the students to estimate how well they did relative to others (on a percentile basis). Students who scored near the bottom estimated that their skills were superior to two-thirds of the other students. Those who scored in the middle, had a more accurate perception of their abilities; but the group that scored highest actually *underestimated* their performance relative to others. This provided the first evidence of what had been an intellectual observation for many years, and has come to be known as the Dunning-Kruger Effect.

Bertrand Russell's 1933 essay entitled "The Triumph of Stupidity" lamented the rise of the Nazi movement in Germany. In that essay Russell wrote:

> ***"The fundamental cause of the trouble is that in the modern world the stupid are cocksure while the intelligent are full of doubt."***

NEWS BRIEFS

- The **Veterans Administration** as renewed UNISHKA's designation as Service-Disabled Veteran Owned Small Business through October 2022. The validation appears at: https://www.vip.vetbiz.va.gov

- **The Center for Digital Resilience** and **Digital Impact Labs** completed a Website Security Audit for UNISHKA. While some vulnerabilities were discovered in the audit, UNISHKA has already contracted with an outside company to strengthen the website and decrease vulnerabilities.

- In conjunction with **Blue Cross and Blue Shield of Alaska**, UNISHKA launched its company wellness plan. Its first activity was to offer employees who received a flu shot on or before Halloween, a $25 gift certificate at Kroger/Fred Meyer grocery stores.

- **UN Women** and the **UN Global Compact** approved UNISHKA's "Statement of Support for the Women's Empowerment Principles" confirming UNISHKA's commitment to make a difference for women in the workplace, marketplace and community For a global list of signatories, visit their website at: https://www.empowerwomen.org/en/weps/companies

- UNISHKA joins the **UN Water Mandate** to address global water challenges through corporate water stewardship. For a global list of signatories, visit their website at: https://ceowatermandate.org/about/endorsing-companies/

- The **Alaska Department of Labor and Workforce Development** has concluded its unemployment insurance tax audit for UNISHKA for 2018. As a result, UNISHKA received an additional tax credit for the year which can be applied to future payments.

- **Health care benefits** under UNISHKA's Blue Cross and Blue Shield Plan have been expanded to cover eligible family members effective with the plan renewal in November.

- The **Anti-Corruption Training Center** (ACT Center) in Manila and UNISHKA have entered into a strategic Memorandum of Understanding to collaborate on training and anti-corruption initiatives in the Pacific and beyond. This initiative will include both training as well as project implementation.

US Median Individual Earnings by Gender

Full-Time, Year-Round Workers	2017 Median Individual Earnings (2018 Dollars)	2018 Median Individual Earnings (2018 Dollars)
Men	$53,459	$55,291
Women	$43,658	$45,097

Source: United States Census Bureau, *Current Population Survey, 2018 and 2019 Annual Social and Economic Supplements.*

Note: The differences between all of the values above are statistically significant at the confidence level used by the Census Bureau.

DO PROPOSAL REVIEWS HAVE YOU FEELING BLUE?

Proposal development is a strange world filled with its own acronyms, euphemisms and lexicon. For those whose only function is to contribute technical information (a subject matter expert), the proposal schedule can have you seeing red. For example, you might be invited to participate with the Blue Team and the Red Team, but the White Team doesn't need you and the Green Team doesn't want you. So, what does it all mean?

Blue Team Review

Most companies have a proposal template to develop the initial framework for a proposal. The Blue draft is simply an outline. The mission of the Blue Team is to ensure that the best qualified person is assigned to write each section of the proposal and to identify knowledge gaps. The emphasis is on content, not style, grammar, spelling, etc.

Pink Team Review

Once the writers have completed their sections, and the parts assembled, the emphasis shifts to the story and fact checking the story. Is the story correct? Is the information current and relevant? Does the story speak to the RFP (request for proposal)? Are the sections consistent? Again, the emphasis is on content, but consistency should also be established in spelling etc. (*e.g.* center or centre).

Red Team Review

The function of the Red Team is to have a complete technical proposal. The proposal should speak with one voice; tell a consistent and compelling story; and demonstrate value for money. Most importantly, at Red Review the proposal should speak to compliance and clarity. Is the proposal responsive to the RFP?

Green Team Review

The Green Team is the budget. After the activities of the proposal are clear in Red Review, the Green Team goes to work to ensure that all pricing information required in the RFP is presented in the prescribed format. A critical aspect of the Green review is that it must reflect the technical solution identified in the proposal. The worst situation is proposing a solution that cannot be accomplished at the proposed price.

Gold Team Review

The Gold Review document is pre-submission quality. It should be complete in all sections, all information, all graphics, and fully compliant. It is formatted and looks exactly like it will for submission. The Gold Team Review is usually done by 2-3 senior executives or managers who are in the authority chain for the units providing services under the RFP. The Gold Team reviewers focus is on high level win themes and discriminators and select aspects of the technical proposal that are considered key to winning the award. Critically, the Gold Review must ensure that the proposal is priced to win.

White Team Review

The White Review, often called White Glove, review is a page by page mostly visual review of the document to catch any obvious errors in printing. The review will check those select items identified at Gold Review for correction. Focus is primarily on compliance items.

Summary

The color-coded review process can be confusing. Also, unless you have been through the entire process, the type and quality of information needed at each step of the review may not be fully appreciated.

The good news is that this process is methodical and takes you from reading the proposal to developing a high quality, winning document if followed correctly.

Professional proposal writers, like **Kris Humbert** at UNISHKA, are certified by the Association of Proposal Management Professionals (APMP) which requires biannual recertification (see https://www.apmp.org).

DELETING SIRI VOICE RECORDINGS FROM IPHONE APPLE SERVERS

If you've ever sat down to read the Apple IOS Security Guide, you'll note that on page 69, Apple makes the following disclosure:

> *User voice recordings are saved for a six-month period so that the recognition system can utilize them to better understand the user's voice. After six months, another copy is saved, without its identifier, for use by Apple in improving and developing Siri for up to two years. A small subset of recordings, transcripts, and associated data without identifiers may continue to be used by Apple for ongoing improvement and quality assurance of Siri beyond two years. Additionally, some recordings that reference music, sports teams and players, and businesses or points of interest are similarly saved for purposes of improving Siri.*

Apparently, what we place on Siri stays on Apple's servers, potentially forever. So, if you want your Siri Voice Recordings deleted, it is your responsibility. Here's how to delete your recorded voice remarks on an iPhone—but you'll need to repeat similar processes on every Apple device you own.

- ◆ Go to "Settings" > "Siri & Search"
- ◆ Turn off all the ways there are to activate Siri. There are two: "Listen for 'Hey Siri'" and "Press Side Button for Siri." When you turn off the last way to activate Siri, that effectively turns Siri off. You'll get a warning that there is one more step you need to take to delete your data from Apple's servers.
- ◆ Go to "Settings" > "General" > "Keyboard." Scroll down to where you see "Enable Dictation." When you tick that to off, you'll get a warning that if you ever want to use it again, you'll have to go through some re-uploading. Not to worry, that part is simple. (Source: https://www.theverge.com/2019/8/2/20734681/apple-siri-privacy-settings-how-to-delete-voice-servers)

Disabling and deleting your Siri history is equally as cumbersome, but for those for whom security is important, How-to-Geek offers a good tutorial at: https://www.howtogeek.com/446308/how-to-disable-and-delete-your-siri-history-on-iphone-ipad/.

BUSINESS EMAIL COMPROMISE (BEC)

BEC is an exploit in which an attacker obtains access to a business email account and imitates the owner's identity, in order to defraud the company, its employees, customers or partners. Often, an attacker will create an account with an email address almost identical to one on the corporate network, relying on the assumed trust between the victim and their email account. BEC is sometimes described as a "man-in-the-email attack". Carried out by transnational criminal organizations that employ lawyers, linguists, hackers, and social engineers, BEC can take a variety of forms. In most cases, scammers will focus their efforts on the employees with access to company finances, and attempt to trick them into performing wire transfers to bank accounts thought to be trusted, when in reality the money ends up in accounts owned by the criminals.

BEC Techniques

- ◆ **Spoofing email accounts and websites:** Slight variations on legitimate addresses (john.kelly@abccompany.com vs. john.kelley@abccompany.com) fool victims into thinking fake accounts are authentic.
- ◆ **Spear-phishing:** Bogus emails believed to be from a trusted sender prompt victims to reveal confidential information to the BEC perpetrators.
- ◆ **Malware:** Used to infiltrate networks in order to gain access to internal data and systems, especially to view legitimate email regarding the finances of the company. That information is then used to avoid raising the suspicions of an any financial officer when a falsified wire transfer is submitted. Malware also lets criminals gain access to their victim's sensitive data.

Specific Types of BEC

Often, messages sent by perpetrators will follow a number of archetypes. As defined by the FBI, there are 5 major types of BEC scams:

- ◆ **False Invoice Scheme:** Companies with foreign suppliers are often targeted with this tactic, wherein attackers pretend to be the suppliers requesting fund transfers for payments to an account owned by fraudsters.

- **CEO Fraud:** Attackers pose as the company CEO or any executive and send an email to employees in finance, requesting them to transfer money to the account they control.
- **Account Compromise:** An executive or employee's email account is hacked and used to request invoice payments to vendors listed in their email contacts. Payments are then sent to fraudulent bank accounts.
- **Attorney Impersonation:** An attacker will impersonate a lawyer or other representative from the law firm responsible for sensitive matters. These types of attack often occur through email or phone, during the end of the business day where the victims are low level employees without the knowledge or authority to question the validity of the communication.
- **Data Theft:** HR and bookkeeping employees will be targeted in order to obtain personal or otherwise sensitive information about the employees or executives. This data can be very helpful for future attacks.

UNISHKA Defends Against BEC with Barracuda

There are many ways to defend against Business Email Compromise. Common techniques that are employed include:

- **Intrusion Detection System Rules:** these flag emails with extensions that are similar to company email. For example, legitimate email of xyx_business.com would flag fraudulent email of xyz-business.com.
- **Email Rules:** these flag email communications where the "reply" e-mail address is different from the "from" email address shown.
- **Color Coding:** virtual correspondence so e-mails from employee/internal accounts are one color and e-mails from non-employee/external accounts are another.
- **Payment Verification:** ensures security by requiring additional two-factor authentication.
- **Confirmation Requests:** for fund transfers with something like phone verification as a part of a two-factor authentication scheme. Also, confirmations may require that company directory numbers are used, as opposed to numbers provided in an email.
- **Careful Scrutiny:** of all e-mail requests for transfer of funds to determine if the requests are out of the ordinary.

TIDBITS

- Director of the ***Centre for the Study of Global Christianity***, Todd M. Johnson, PhD, said "there is a lack of research on fraud within the church," but that is something he has been trying to change. In one of Johnson's studies, *Status of Global Mission 2013,* there is a line item for "Ecclesiastical Crime" or corruption which is projected to be $37 billion per year worldwide, or nearly 6% of the total $594 billion given to churches. If you include synagogues, mosques and temples, this number would probably be significantly higher.
- According to the **World Bank**, corruption costs at least $2,000,000,000,000 (that's $2 trillion dollars per year.)
- Finally, members of the military, government and higher education are eligible for free online access to **The Washington Post**. If you have a valid .mil, .gov or .edu email address, you can activate your digital subscription at https://subscribe.washingtonpost.com/specialoffer/#/gov-mil.

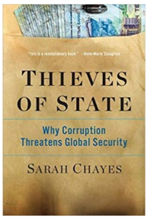
BEC Attacks up 476% in 2018

Since 2013, when the FBI began tracking an emerging financial cyber threat called business e-mail compromise (BEC), organized crime groups have targeted large and small companies and organizations in every U.S. state and more than 100 countries around the world—from non-profits and well-known corporations to churches and school systems. Losses are in the billions of dollars and climbing.

Source: https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

What We're Reading

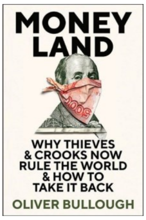
In a recent conversation over dinner in an friend's home in Kabul, I learned that his apartment had cost him a bit more than $50K – he said that after some 18 years in senior positions in the government, that it was all he could afford. He went on to say that a number of junior colleagues owned much bigger homes, some even had property in Turkey and elsewhere. He knew their salaries, and knew that corruption had made them wealthy. While the administrative corruption that permeates Afghanistan seems nonviolent, according to Sarah Chayes in her book *Thieves of State*, it is exactly this type of corruption that threatens global security.



Chayes begins her story in Kandahar, where local colleagues were so angry with police corruption they said they would not warn them against insurgent bombs. Systematically, Chayes describes corruption as a type of pyramid scheme, where front-line employees who buy their positions, extract extra fees from citizens seeking services – in part to recover what they paid for their job, and also to funnel money upward through a chain of patronage relationships until the most senior levels are receiving huge sums from below. She goes on to describe the relationship between corruption and insurgencies in places like Nigeria and other kleptocracies where the poor seem to have little recourse but to take up arms against their leaders – some join movements such as the Al Qaeda and ISIS in their search for purification and others just take to the streets.

While *Thieves of State* links corruption to global instability, Oliver Bullough's *Moneyland* describes an intricate global system that enables the crooks and kleptocrats who are engaged in large-scale corruption, to conceal their ill-gotten gains. This system uses banks and other financial entities to transfer billions stolen mainly from poorly-governed states into an almost completely impenetrable web of interlocking, anonymous shell companies that are hosted in places like Jersey and the Cayman Islands, and also by some of the world's most respected financial institutions. Some of these are in financial centres such as London, and others are in trusts set up in U.S. states such as Nevada, Montana, and others.

Moneyland links the origins of this corruption-enabling system to flaws in the initial establishment of the Bretton Woods institutions after WWII – the IMF and others were set up to bring order to a global economic framework. Unfortunately, the kleptocrats and their enablers have found ways to subvert the system for their own illicit advantage. If the founders had listened to John Maynard Keynes' attempts to have them establish a global currency, the system likely would have worked as intended. Unfortunately, they did not listen, and the consequences include the theft of billions of public funds that could otherwise be applied to education, health care and other beneficial purposes, and an increase in global insecurity from transnational insurgencies and protests by disillusioned masses in one country after another.


MONEY LAND
WHY THIEVES & CROOKS NOW RULE THE WORLD & HOW TO TAKE IT BACK
OLIVER BULLOUGH

Chayes' analysis is compelling but incomplete – she does not give due credit to the reformers in the many poorly-governed states who are attempting, often at considerable personal cost, to apply the rule of law and stem the hemorrhage of public funds from their poverty-stricken societies into *Moneyland*. My Afghan dinner host mentioned at the beginning of this review is one of these reformers. He said he has endured years of escalating nasty personal attacks, and now feels his family is in danger – he is looking for a safe place to raise his children and pursue his dream of higher education so he can be an increasingly effective agent in the global anti-corruption crusade. He has his work cut out for himself: *Thieves of State* and *Moneyland* are well-written and useful, but they describe only part of the global corruption system – there is more, much more, to be done to stop the crooks, kleptocrats and enablers they describe.

Bullough, O. (2019). *Moneyland: The Inside Story of the Crooks and Kleptocrats Who Rule the World.* New York: St. Martin's Press.

Chayes, S. (2015). *Thieves of State: Why Corruption Threatens Global Security.* New York: Norton & Co.

About the Author: *Dr. Andy Tamas is a Senior Governance and Organizational Development Advisor for UNISHKA.*

SOCIAL MEDIA

https://www.facebook.com/Unishka-Research-Service

https://twitter.com/UNISHKAResearch

https://www.linkedin.com/company/unishka-research-service-inc/

UPCOMING HOLIDAYS AND OTHER ACKNOWLEDGMENT DAYS

October:
Cyber Security Awareness Month

- October 2: International Day of Non-Violence
- October 5: World Teachers' Day
- October 10: World Mental Health Day
- October 17: International Eradication of Poverty Day
- October 18: Alaska Day
- October 24: United Nations Day

November:
American Indian Heritage Month

- Nov. 2: International Day to End Impunity for Crimes Against Journalists
- Nov. 11: Remembrance Day
- Nov. 13: World Kindness Day
- Nov. 16: International Day for Tolerance
- Nov. 21: Thanksgiving
- Nov. 25: International Elimination of Violence Against Women

December:
Self-Care Awareness Month

- Dec. 2: International Day for Abolition of Slavery
- Dec. 5: International Volunteers Day
- Dec. 9: International Anti-Corruption Day
- Dec. 10: Human Rights Day
- Dec. 20: International Human Solidarity Day
- Dec. 25: Christmas

TARGETING GENDER EQUALITY

The United Nations announced a new global initiative to increase women's representation and leadership in business. To be rolled out early in 2020, the initiative—**Target Gender Equality**—will support companies participating in the UN Global Compact to set and meet ambitious, time-bound corporate targets for women's representation and leadership across the business and at all levels. Through the initiative, companies will deepen their implementation of the ***Women's Empowerment Principles*** and strengthen their contributions towards Goal 5 of the 2030 Agenda for Sustainable Development, which calls for women's full and effective participation and equal opportunities for leadership at all levels of decision-making. UNISHKA has been a signatory of the UN Global Compact since April 2018. For more information on the Target Gender Equality program, please see: https://www.unglobalcompact.org/take-action/target-gender-equality.