The Association of Accountants and Financial Professionals in Business

Delmarva Dispatch
Winter 2022

A Publication of the Delmarva IMA Chapter

A New Year's Resolution!

Have you been thinking about what New Year's resolutions you will make for 2023? One option to consider is to begin studying for the Certified Management Accountant (CMA) exam. The CMA is the fastest growing accounting certification and provides many benefits. Among those called out by our current CMA's are:

1. Sharpening time management skills in balancing a full-time job, with family, church, and life in general with the time it takes to study and do the work.

2. The benefit of learning new skills and being exposed to the study options available. Makes one "think outside of the box" and consider new and different possibilities.

3. Adding another tool, skill, accomplishment that will assist in the future – aiding in things like promotion, increases, and recognition.

4. Basically, a much better understanding of cost accounting as well as project analysis to ensure that we are receiving the expected benefits from the implementation of the projects.

5. Knowledge is power, and CMA is a powerful and comprehensive tool to gain that competency.

If you are interested in finding out more about the CMA program contact Jim Kaylor at jim.kaylor@perdue.com or (443) 235-8731.

In this issue:

Your IMA Chapter Board

Awards, Recognition, and Plain Great Stuff!

IMA Chapter Awards

We will keep you posted on future awards.

New CMA Licenses

Let's get those New Year's Resolution's going, shall we!

Recent Educational Achievements

Mr. William N. Perry earned his CSCA designation in May 2022.

Please submit any completions that may have been missed.

Thank you for your participation in our IMA Chapter!!

If you would like to share any "Plain Great Stuff" in the next Dispatch, please email cjensencma@gmail.com.

President's Message

Jesse Reid, CPA, MBA
Delmarva Chapter President

Happy Fall everyone and welcome to the Delmarva Chapter of the Institute of Management Accountants. I am excited and honored to serve as your Chapter President for another year. We have a great Board of Directors that have committed to providing you with quality continuing professional education and a rewarding networking environment. Your Delmarva board has been hard at work planning for this upcoming chapter year and will continue to schedule monthly speakers and keep you informed of any upcoming chapter events. Please go to Events & Education/Chapter Events for details. If you would like to find out more about our chapter or about becoming a member, we encourage you to contact us by clicking here to get to our website.

Who are we and what do we do?

The Delmarva Chapter of the IMA is a non-profit organization committed to providing educational, networking, and leadership opportunities to accounting professionals on the Delmarva Peninsula. We welcome accounting professionals from industry, public accounting, and academic fields.

The mission of our chapter is to promote accounting knowledge, provide educational opportunities, and serve the community through:

- Chapter meetings that include speakers on relevant accounting, tax, and business topics.
- Providing low cost continuing education programs for members and non-members.
- Supporting nearby IMA student chapters by providing speakers and inviting student members and faculty advisors to Delmarva Chapter functions.
- Partnering with other organizations to sponsor educational programs.
- Soliciting ideas from other chapters and the National Organization on effective programs.
- Using chapter funds when available to support scholarships and educational activities.
- Promotion of the Certified Management Accounting program.
- Providing volunteer accounting and tax expertise in the community to individuals and small businesses.
- Providing professional networking opportunities for members.

Jesse Reid, CPA, MBA
Delmarva Chapter President

Delmarva Chapter IMA Event

"CPE Event Recap: Finance Leader as an Organizational Influencer"

Submitted by Kate Reinert, IMA Member Since 2006

On Thursday, July 28th, the Delmarva Chapter of the IMA hosted its first in-person event in over 2 years!

The CPE event featured chapter board member Jim Kaylor as the presenter who spoke about the "Finance Leader as an Organizational Influencer". Eight chapter members took advantage of the free event and earned 2 hours of CPE.

The interactive course helped attendees "broaden their impact across the organization by becoming influencers". The term influencer has earned more recognition in recent years as referring to people on social media who have built a reputation for their knowledge in a certain area, whether that is business, fashion, parenting or one of thousands of topics. Within an organization, though, having an influence means being a trustworthy source on a particular topic and leads to shaping the decisions and mind-sets of others. The course highlighted four ways to gain influence: trailblazing new opportunities, developing tools to spread expertise, using teamwork to learn from others as well as teach others and helping decision makers understand complex content.

Jim did a great job involving attendees in the discussion through case studies and conversation. Always a dynamic speaker, we appreciate his willingness to provide this valuable training to our members!

UPCOMING EVENTS

Dispatch Submissions

If you have a submission for the Spring Delmarva Dispatch, please submit it by **02/15/2023** to cjensencma@gmail.com

Connect with Us

Delmarva Chapter

DIGITAL PAYMENTS ARE HERE TO STAY

BY SEAN STEIN SMITH, DBA, CMA, CPA, CGMA, CFE
December 1, 2020

Management accountants must stay ahead of the current and fast-changing trends in blockchain and cryptocurrencies.

It may seem like blockchain and cryptocurrencies have run out of steam and that every high-impact application has already been discussed; that couldn't be further from the truth. The rise of central bank digital currencies (CBDCs) is happening faster than many practitioners expected, and its implications spread far beyond just accounting.

Comments at the end of 2020 by the chair of the Federal Reserve System highlight that while a CBDC project isn't under way at this specific time, there are several quantifiable ways in which blockchain can improve the current payment infrastructure.

CBDC is a cryptocurrency that's issued and governed by a central bank or central government. While CBDCs and existing fiat currencies will coexist at the beginning, the pivot toward digital payment options is a structural one rather than a passing fad. Unlike with traditional cryptocurrencies such as bitcoin,

CBDC development will be accompanied by regulation, which can facilitate and accelerate adoption. Simply put, CBDCs are a potential game-changing iteration of blockchain and cryptoasset technology, and they're arriving quickly.

Two distinct trends need to be acknowledged regarding the continued development of CBDCs. First, this is a much broader conversation than simply discussing e-money. Every major economic power in the world is investing resources and dedicating personnel to the development of this blockchain application. Second, no major economic power in the world has dismissed the potential for CBDCs. See Figure 1 for CBDC status in select places around the world.

Figure 1: CBDC Development

Country/Union	Currency	CBDC Update
China	yuan	Digital yuan already being tested in certain Chinese cities and in partnership with the ride-hailing company, DiDi.
U.S.	U.S. dollar	The Federal Reserve is researching the viability of the digital dollar, both at the national level and at regional Feds (Boston, Mass.).
European Union	euro	Digital euro project under way by the European Central Bank.
Japan	yen	Bank of Japan announced it'll begin proof-of-concept testing in 2021.
United Kingdom	pound	Bank of England has joined an international roundtable to discuss development and implementation of a CBDC.
Australia	Aus. dollar	Playing a wait-and-see approach pertaining to other efforts under way at other central banks.
Canada	Can. dollar	Bank of Canada is hiring an entire internal team to assist with developing an original CBDC.

As we approach the end of 2020, China seems to be in a clear leadership position, with market testing of the digital yuan already taking place in several major cities. That early success aside, the true indicator of a successful CBDC will be one that's used both in its country of origin as well as internationally. Developing markets within Africa—with Kenya having received significant coverage for its efforts—or small nations such as the Bahamas have leapfrogged the United States and Western Europe in terms of digital or blockchain-enabled payments. These developments show just how dramatically accounting, payments, and reporting can change over time.

THE PAPERLESS REVOLUTION

Transaction speed, immediate settlement, paperless flows, and straight-through processing are obvious benefits of a digital currency and payment system. Payment digitization and automation will continue to reduce the dependence on

humans to perform manual and repetitive operational tasks. While manual tasks are being eliminated, digitization is creating a rich array of complex data that requires unique skills to mine, model, and analyze—sometimes in real time. With the digital world expanding around us, the need for advanced data analytical skills is a huge opportunity for finance professionals.

Treasury and payments departments are ahead of the game in terms of implementation, but they still have opportunities to generate additional cost savings. Digital payments, whether they're connected to blockchain and cryptocurrencies or not, have transformed almost every form of treasury functionality. Letters of credit, wire transfers, automated clearing house payments, bond issuances, and the accounting that goes along with these are quantitative examples of benefits that have already been actualized. With digital payments and other forms of automation, the push for a continuous close and reporting process will only increase. Outstanding balances connected to accounts receivable and accounts payable, and the need for confirmations and verifications, will also shrink.

THE BLOCKCHAIN CONNECTION

Blockchain and cryptocurrencies have generated nearly endless headlines since 2017. That said, for practitioners to be able to offer comprehensive and realistic advice to colleagues and supervisors, it's important that the type of blockchain technology being discussed is understood by all parties involved. Without diving into overly technical details of specifications (for more, see bit.ly/387HdNV), there are several core considerations that need to be assessed and incorporated into a blockchain digital payments network.

The most important consideration is the set of controls around the payment channels, from both a cybersecurity and financial reporting point of view. Assuming that the type of blockchain being considered is a permissioned blockchain—a type of blockchain that allows the organizing companies to customize the blockchain to fit the need of the enterprise—establishing controls over access and data rights is critical. Following initial implementation, there should always be an assessment of how the blockchain itself will interoperate, i.e., communicate with other technology platforms that are already in place at the entity. Nearly all of the hacks and breaches that have occurred around the digital and crypto payment space have occurred at these connection points rather than at the specific blockchain or digital payment platform.

The underlying reality of the situation is that, no matter what specific payment technology tool or infrastructure is being used—blockchain or not—digital

transactions are here. Whether they take the form of applications developed by incumbent financial institutions or cryptocurrencies, the accounting profession will need to keep pace. The role of accounting and finance will obviously evolve and change as a result of this increased digitization—but that doesn't mean it will become less important, especially as various iterations of blockchains become increasingly integrated into payment infrastructure practices. Whatever the future holds, CBDC will be game-changing.

GET SMART ABOUT CYBERSECURITY ATTACKS

BY KRISTINE BRANDS, CMA
December 1, 2019

The time to act on cybersecurity prevention and response planning is right now.

Hackers had a field day breaking into computer systems during the spring and summer of 2019. In May 2019, the City of Baltimore suffered a phishing ransomware attack, paralyzing the city's IT services. Another ransomware attack shut down 23 state agencies across Texas during the same period. Don't think it can't happen to you.

Management accountants are on the front line of data governance to "ensure the availability, utility, integrity, and security of data" according to the IMA® (Institute of Management Accountants) enhanced Management Accounting Competency Framework. Let's examine safeguards your organization can take to defend against the growing risk of cybersecurity attacks.

THE CYBERATTACH PLAYBOOK

According to Verizon's *2019 Data Breach Investigations Report* (DBIR; vz.to/34fXxam), an annual report analyzing cybersecurity breaches, small businesses were the victims of 43% of cyberattacks out of 2,013 confirmed data breaches analyzed. Sixty-nine percent were perpetrated externally, 34% internally, and 23% by foreign nation-states, and 71% were financially motivated. A scary finding is that in 56% of the cases, discovering the attack took months. The most common type of attack was caused by hackers (52%) followed by social engineering (33%) and malware (28%). It's time to get your finger on the pulse of the risks, exposures, and trends in the cyberattack playbook.

Forecasting the cost of a cybersecurity attack should be enough to get your attention to shore up your organization's cybersecurity defenses. The Baltimore ransomware attackers demanded $80,000—the city refused to pay. The final recovery cost was estimated at $18 million. According to Target's 2015 Form 10-K, 40 million customers' credit and debit card data was stolen during a malware attack in late 2013, costing the company about $252 million in pretax earnings. Insurance coverage and tax deductions reduced the cost to about $105 million.

The first line of defense is to raise awareness throughout your organization about the risk of cyberattacks and what employees can do to avert the risk. Mandating employee cybersecurity training—at least annually—is imperative. Texas passed legislation requiring cybersecurity training for most state employees by June 2019, five months before the state's cyberattacks. Robert Herjavec of *Shark Tank* fame and owner of a cybersecurity company says, "People, process—then technology—will address the greatest challenges we all face in cybersecurity."

CONTINGENCY PLAN AND CYBERSECURITY POLICY

Thirty years ago, backup and recovery measures from a computer crash involved restoring data from a backup and marching on smartly. Downtime was limited to the time needed to restore the backup. Times have changed. Hackers can take control of your IT system and freeze it, denying all access, causing your business to come to a grinding halt. A small, private university in Denver, Colo., was the victim of a cyberattack in August 2019 at the beginning of the fall semester. Its entire IT infrastructure—website, phones, email, and computer system—was down for more than two weeks. Communication initially occurred

through its Twitter account until a temporary website was built. The start of classes was delayed until the system was restored. Though no leader wants to see their organization fall victim to a cyberattack, it's important to be prepared.

Basic Cybersecurity Terms

Actor: Cyberattack perpetrator.

Breach: An incident when a third-party obtains unauthorized access to an organization's data.

Ransomware: An attack that demands a monetary ransom to return system access.

Social Engineering: A technique to manipulate a computer user to disclose confidential information to access a computer system, such as a password.

Phishing: Using fake emails or social media to trick a user into divulging personal information to gain access to a computer system.

Malware: Software intended to access and damage a computer, software, server, or network.

Because of the risk of losing your IT infrastructure, it's imperative to have a disaster recovery plan to respond to the attack and restore your system and a business continuity management plan to continue to operate your business while you recover from an attack. The longer you're out of action, the more expensive it will be in terms of lost revenue and reputational damage. You must develop a formal cybersecurity policy that includes how to deploy it. Even if the first version of the plan only says to disconnect the servers to halt the spread of the damage and call a forensic cybersecurity firm to investigate, that's a step in the right direction. The more comprehensive the policy, the better. Just like your system of accounting internal controls, the policies must be tested for effectiveness. If you don't know how to proceed, engage a cybersecurity consulting firm to develop, test, and audit your plan.

CYBERSECURITY INSURANCE: CAVEAT EMPTOR

The cost of recovering from a cybersecurity attack can be expensive, as noted in the Target example. One strategy for mitigating the risk of the cost of the attack is to purchase cybersecurity insurance. Allied Market Research forecasts that cybersecurity insurance will grow to $14 billion by 2022 primarily driven by the U.S. market. Insurance policies include premium cost, deductibles, and coverage exclusions limiting coverage.

But be careful: Make sure you understand the policy and the application process. Many insurance policies require completing a questionnaire asking questions about your business' current cybersecurity policy. If you don't have one, that's your answer—you don't have one. Beware of coverage exclusions. Foreign nation-state-sponsored cyberattacks, one of the biggest risks identified in Verizon's DBIR, may be excluded. Also, social engineering attacks may not be covered since they indicate lax cybersecurity policies and could have been prevented by a cybersecurity policy and employee training.

Management accountants understand the adverse effect of risk on their companies and should be active participants in safeguarding their company's data by participating in the development of internal controls and policies to prevent attacks. Cyberattacks are in the risk red zone and are on the rise. Don't leave your company exposed. Acting tomorrow to defend against a cyberattack might be too late. It can happen to you today.