July 21, 2020

VSCPA
Virginia Society of CPAs
Tidewater Chapter

PART TWO – NOT FOR PROFIT CONFERENCE

UBIT and 990 Update

NFP Governance

NFP A&A Update

Cyber Security

PPP Q&A


BROWNEDWARDS
certified public accountants

Formed in 1967 through the merger of two firms with histories dating back to the 1920s, we are a full-service regional public accounting firm. Our firm has grown to 11 offices with a staff of more than 350, and is recognized as one of the top 100 firms in the nations.

Our professional staff is noted by our clients for their accessibility and hands-on style, as well as the depth of knowledge and capabilities. Brown Edwards believes that in a professional relationship, ***people make the difference***.

Your Success is Our Focus

BROWNEDWARDS
certified public accountants

Let's Talk About Accounting!

BROWNEDWARDS
certified public accountants

***Warning: these accountants are trained jumping professionals, do not try this at home.**

Agenda

- 990 / UBIT Update
- Not-for-Profit Governance
- A&A Update
- Cyber Security
- PPP Q&A

BROWNEDWARDS
certified public accountants

990 / UBIT Update

Kristen Jones, CPA - Manager

KJones@BEcpas.com 757-316-3227

Kristen has over fourteen years of experience in public accounting. During this time, she has gained both audit and tax experience in a variety of industries, specializing in nonprofit organizations.

Kristen has managed the audit and tax engagements for a number of nonprofit entities, including regional foundations and nationally recognized museums. She has been an active member of the Hampton Roads region nonprofit and governmental group and led the industry education segment for this group for a number of years. Her nonprofit experience includes organizations subject to governmental auditing standards as well as extensive Form 990 preparations for exempt organizations.

Kristen's internal leadership roles with local nonprofit organizations offer an enhanced perspective and understanding of the risks and relevant issues to her clients. In addition, she has assisted in developing and teaching numerous workshops and continuing education courses.

Minor Changes to 2019 Form 990

- Due to the repeal of the “parking tax”, references to UBTI regarding IRC Section 512(a)(7) have been removed from the instructions

- Due to new guidance under ASC 958-205, updated language throughout from "temporarily restricted" and "permanently restricted" funds to "donor" and "board designated" funds.

Minor Changes to 2019 Form 990

- Definition of interested person clarified and is stated as “the creator or founder, a substantial contributor, a family member of an interested person, and a 35% controlled entity of any interested person(s)”

BROWNEDWARDS
certified public accountants

Minor Changes to 2019 Form 990

Instructions include additional guidance for order of reporting compensation:

"List the persons required to be included in Part VII, Section A, in order from highest to lowest compensation based on the sum of columns (D), (E), and (F) for each person…

Minor Changes to 2019 Form 990

"…When the amount of total compensation is the same, list the person in the following order:

Individual trustees or directors

Institutional trustees

Officers

Key employees

Highest compensated employees

Former such persons"

Polling Question #1

UBIT Update

- Tax on Nonprofit Transportation Benefits Repealed

- Tax on Separate Trade or Business

“Parking Tax”

In December 2019, the “Parking Tax” provision was repealed

“Parking Tax”

- On January 22, 2020, the IRS issued “How to Claim a Refund of Unrelated Business Income Tax on Form 990-T”

Tax on Separate Trade or Business

- Previously, UBTI was gross income of all unrelated trades or businesses less the allowed deductions from all unrelated trades or businesses

Tax on Separate Trade or Business

- Now, the loss from one trade or business (including any NOLs) may not offset the income from a separate trade or business
- UBTI reported separately on Schedule M

BROWNEDWARDS
certified public accountants

Tax on Separate Trade or Business

- Notice 2018-67, permitted taxpayers to identify separate trades or businesses by using the six-digit NAICS code

- Proposed regulations note broader classification using the two-digit NAICS code

Tax on Separate Trade or Business

- After separating, you must determine how to allocate expenses that may apply to more than one activity to each silo

- Until further guidance is issued, any reasonable allocation method may be used

There's some hope…

- Nonprofit Relief Act (H.R. 3323), currently in committee, would repeal the silo requirement
- AICPA has issued recommendations for a de-minimis exception for NFP organizations reporting < $100,000 gross UBI

Not-for-Profit Governance

Leslie Roberts, CPA – Relationship and Audit Engagement Partner

LRoberts@BEcpas.com 757-316-3220

Leslie is a Partner in our Newport News office. She has more than 30 years of accounting experience, most of which is in public accounting. She has supervised and performed audits and consulting services in various industries including various non-profits including foundations, higher education, religious organizations, state and local governmental entities, governmental authorities, boards and commissions, regional and municipal airports, government contracting and healthcare and construction contractors. She also served as Controller for a regional non-profit hospital and nursing home and has provided consulting services for healthcare clients (both long-term and acute-care facilities).

A large part of Leslie's practice involves auditing not-for-profit and institutions of higher education. As such, Leslie has extensive experience and has received advanced training in these industries. Her responsibilities include engagement management, client correspondence, presentations, practice development, work-paper review, and staff supervision, scheduling and consulting.

Leslie graduated from University of North Carolina at Chapel Hill with a Bachelor of Science in Business Administration. She is actively committed to serving the community through current or past memberships on various community committees or boards including:

- Carolina Alumni Association
- Peninsula Women's Network

Leslie is a member of the Virginia Society of Certified Public Accountants, the American Institute of Certified Public Accountants, and the Governmental Audit Quality Center. She has also previously been named a "Super CPA" in the Non-Profit and Governmental area of practice by *Virginia Business* magazine.

Steven S. Kast
President & CEO
United Way of the Virginia Peninsula

Steven S. Kast is the President and Chief Executive Officer of United Way of the Virginia Peninsula. The United Way of the Virginia Peninsula is a 501-c-3 that has served the Peninsula community for over 75 years. The organization brings people together from all over the community-government, business, faith groups, other non-profits and citizens to identify and tackle our most serious problems. To accomplish this, the United Way builds partnerships with other funders, municipalities, and community organizations.

As of April 15, 2016, Steve Kast ended his remarkable 32-year career with Boys & Girls Clubs of the Virginia Peninsula, Steve helped the organization grow from a single Club serving 250 boys to the premier youth development organization in the community, serving over 9,000 boys and girls ages 6-18 at 25 Club sites. The footprint on the Peninsula is large, spanning the cities of Newport News, Hampton and Williamsburg, and the counties of York, Gloucester and Mathews, and on the Southside in Norfolk, Virginia Beach, Chesapeake, Portsmouth, Suffolk, Franklin and Eastern Shore. Steve was the fourth Executive Director in the 70-year history of Boys & Girls Clubs of the Virginia Peninsula. Steve was a designated field consultant for Boys & Girls Clubs of America and in that capacity traveled to assist Boys & Girls Club organizations across the country. He was also the founding President and served as President of the Virginia Alliance of Boys & Girls Clubs where he led the effort to raise private and public dollars for Clubs across the state. In 2015, due to a management agreement, he became the President & CEO of Boys & Girls Clubs of Southeast Virginia.

Steve was honored in 2003 as a distinguished member of the Academy of Boys & Girls Club Professionals. In 2005, Steve received the "Sykes Award for Professional Excellence" at the Southeast Boys & Girls Club Leadership Conference and was awarded National Boys & Girls Clubs Contribution to the Profession Award in 2012. Steve has also been honored as the recipient of the National Cable Association "National Leaders in Learning Award". He was the recipient of the Humanitarian Award by the Virginia Center for Inclusive Communities and also received the "Local Hero Award" by Bank of America. Steve is a graduate of the Boys & Girls Club Leadership University School of Executive Leadership through the University of Michigan Ross Business School and is a graduate of the Thomas Garth Executive Leadership Program.

Steve is a native of Giles County, Virginia, and has lived on the Peninsula for 35 years. He is married to Alyson with three stepchildren Julia, Mason, and Libby (CNU Class of '23). He graduated with honors in 1987 from Christopher Newport University and serves as a member of the Christopher Newport Education Foundation, Alumni Society Board of Directors and the Virginia Complete Count Commission. He was inducted into the Christopher Newport University Athletic Hall of Fame in 2010 and was honored as a Top 50 Distinguished Alumni. In 2015, he was elected to Christopher Newport University's Board of Visitors. Steve is leading Community Captains, which will enable economically disadvantaged Newport News Public School students to attend CNU.

Associations or Boards

Christopher Newport University Alumni Board –Senior Designated Board of Visitors' Representative
Christopher Newport University's Board of Visitors
Christopher Newport University Education Foundation
Virginia Complete Count Commission
Graduate CIVIC Leadership Institute
Peninsula School for Autism Board Member
Peninsula Chamber of Commerce Board Member

Leslie Roberts, CPA
Partner
Brown Edwards

Steve Kast
President & CEO
United Way of the Virginia Peninsula

BROWNEDWARDS
certified public accountants

Polling Question #2

Polling Question #3

Not-for-Profit A&A Update

Katie Ward, CPA - Engagement Audit Manager

KWard@BEcpas.com 757-316-3209

Katie has been with the firm's assurance department since September 2012. Her focus is on not-for-profit organizations and governmental entities as well as manufacturers and construction contractors. Katie has performed audits, reviews, and agreed upon procedures in various industries including not-for-profit organizations, foundations, boards, and commissions. She is well-versed in audit and accounting procedures generally and for the specific industries she serves.

Katie's not-for-profit experience includes organizations with large investment portfolios. Her not-for-profit clients include charitable organizations and foundations, nationally recognized museums and a health care organization. Katie's responsibilities include engagement planning, fieldwork supervision, client correspondence, and work-paper review.

She graduated with a Master's of Science in Accounting from Liberty University and a Bachelor of Arts in Business from Virginia Wesleyan College. She is a member of the American Institute of Certified Public Accountants the Virginia Society of Certified Public Accountants and the Virginia Government Finance Officers' Association. Katie currently serves on the Children's Hospital of the King's Daughters Special Needs Task Force.

Revenue Recognition Guidance for NFPs:

- ASC Topic 606: Revenue from Contracts with Customers *(ASU 2014-09)*
  - Reciprocal
- ASC 958-605: Not-For-Profit Entities – Revenue Recognition – Contributions*
  - Non-reciprocal

*Red text represents the title after implementation of ASU 2014-09

Initial assessment for revenue recognition:

1. Is it a reciprocal transaction or not?
   - Yes = ASC 606, 5 step process (stop)
   - No = ASC 958-605, contribution guidance (ASU 2018-08) (go to #2)
2. Is there a barrier AND right of return/release?
   - Yes = Conditional contribution (stop until condition met)
   - No = Unconditional contribution, recognize revenue in appropriate net asset class (go to #3)
3. Are restrictions present?
   - Yes = Net assets with donor restrictions
   - No = Net assets without donor restrictions

Reciprocal or Non-Reciprocal? Example 1

- The local government provided funding to NFP C to perform a research study on the benefits of a longer school year.
- The agreement requires NFP C to plan the study, perform the research, and summarize the findings and submit the research to the local government.
- The local government retains all rights to the study.

Reciprocal or Non-Reciprocal? Example 2

- University D applied for and was awarded a grant from the federal government.
- University D must follow the Uniform Guidance.
- University D is required to incur qualifying expenses to be entitled to the assets. Any unspent money during the grant period is forfeited, and University D is required to return any advanced funding that does not have related qualifying expenses.
- University D also is required to submit a summary of research findings, but University D retains the rights to the findings and has permission to publish the findings.

Polling Question #4

Topic 606: 5 Step Process

- Revenue stream examples:
  - Membership dues
  - Tuition & housing
  - Products & services
  - Sponsorships
  - Exchange grants
- Will impact disclosures for all NFPs with reciprocal transactions regardless of whether or not there is an impact on accounting.

Topic 606: 5 Step Process

- Overview of 5-step process:
  1. Identify the contract(s) with the customer
  2. Identify the performance obligations (PO)
  3. Determine the transaction price
  4. Allocate the transaction price
  5. Recognize revenue when (or as) a PO is satisfied

Topic 606: 5 Step Process

- Core Principle:
  - Old Standard –
    - Recognize revenue when it is earned & realizable.
  - New Standard –
    - Recognize revenue to depict the transfer of promised goods or services to customers in an amount that reflects the consideration to which the entity expects to be entitled in exchange for those goods or services.

Example - Membership Dues

- Step 1:
  - Existence of contract (anticipate membership contracts would easily meet the 5 criteria under step 1)
- Step 2:
  - Distinct POs: On-demand services, member discounts, journal subscriptions, software/IP access.

Example - Membership Dues

- Step 3:
  - Total contract transaction price, including:
    - Fixed amounts (dues)
    - Variable amounts (incentives, discounts)
    - Consideration payable (scholarships, vouchers)

Example - Membership Dues

- Step 4:
  - Allocate transaction price (only applicable if 2+ POs)
    - Membership dues $ 250
    - Member Services $(215) (FMV)
    - Quarterly Journal $ (35) (FMV = $8.75ea)
    - Contribution $ 0
- Step 5:
  - Recognize revenue at a point in time (journals)
  - Recognize revenue overtime (member services)

Other NFP Examples:

- Exchange grants -
  - Would only include those grants where grantor receives commensurate value in exchange for the good/service provided.
  - POs would vary based on the nature of grant
- Event sponsorships -
  - If sponsor receives tangible benefits (commensurate value) than you'd need to bifurcate contribution & exchange components.

Other NFP Examples:

- Products & services (gift shops, book stores, food, etc.) -
  - Difference in accounting treatment not likely
  - Will still require increased disclosures
- Tuition & housing -
  - Need to consider withdrawal refunds, scholarships, fees, etc. when recognizing revenue.
  - Determine whether financial aid & scholarships apply to tuition, housing or both
  - Summer semesters may create nuances for June 30th FYEs.

Polling Question #5

Gifts-in-Kind

Fair Value – Gifts-in-Kind

- Fair value is “the price that would be received to sell an asset or paid to transfer a liability in an orderly transaction between market participants at the measurement date” (FASB ASC Glossary).
- Certain GIK may not have a readily determinable marketplace, but typically, they have a base utility that is marketable to someone.
- NFPs should consider that base utility when determining market values for GIK

FASB Proposed Amendment

Presentation and Disclosures by Not-for-Profit Entities for Contributed Nonfinancial Assets

- Intent is to increase transparency around gifts-in-kind
- Proposal provides new presentation and disclosure requirements for gifts-in-kind but does not change the current requirements for recognition and fair value measurement

FASB Proposed Amendment

Presentation and Disclosures by Not-for-Profit Entities for Contribute Nonfinancial Assets

- Separate line item for gifts-in-kind of nonfinancial assets on financial statement
- Disclosures to include:
  - The types of gifts-in-kind received
  - Any donor restrictions
  - Valuation techniques used to calculate FMV

CYBERSECURITY:
Low-Cost Solutions and Best Practices

NFP Webinar
July 21, 2020
Tyler Gall, CPA, CISA, CFE,

Tyler Gall, CPA, CISA, CFE
Senior Associate

Tyler works in IT assurance for the various clients we serve. Tyler has performed various IT audits and assessments related to IT controls across various industries. Tyler has over 7 years of experience as an auditor. Before joining Brown Edwards in April of 2019, Tyler primarily focused on financial and performance audits of large government entities. Tyler led audits for an Inspector General office to assist in the preventing and detecting of fraud, waste, and abuse. Also, Tyler has assisted on various consulting engagements focusing on the development of indirect cost rates and data reliability.

PROFESSIONAL AFFILIATIONS

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

EDUCATION

B.S., ACCOUNTING AND FINANCE, RADFORD UNIVERSITY

EXPERTISE AND EXPERIENCE

- Performed IT Assessments, IT audits, and IT risk assessments
- Performed various audits over internal control compliance with standards
- Functioned as the lead auditor for financial audits and performance audits of various entities and programs

Learning Objectives

- Cybersecurity organizational risk considerations
- Cyber statistics
- When cybersecurity efforts really matter
- Common threats
- Low-cost solutions and best practices

BROWNEDWARDS
certified public accountants

Cybersecurity Organizational Risk Consideration

- Virtually no such thing as absolute Cybersecurity
- One size does not fit all
  - Organizational culture considerations (current and preferred)
  - Regulatory, legal, and industry considerations
  - Resource limitations
  - Diverse user risk profiles within same organization
  - In commercial businesses, the term *commercially reasonable cybersecurity* is used to help determine levels. What does your organization call this level and is it discussed in this manner?
- Starting the process
  - Is there agreement in the organization on what the organizational culture will allow to be restricted?
  - Have current regulatory, legal and industry considerations been agreed to and mapped out in considering the framework to be used?
  - If user risk profiles are diverse, can different security be applied to these different segments differently?
  - With resource limitations, all organizations are “buying” at least some level of risk
  - The acceptable levels of risk and resource limitations should be balanced.

Statistics

- 43% of all cyber attacks are aimed at small businesses*
- 91% of attacks launch with a phishing email*
- 85% of all attachments emailed daily are harmful for intended recipients*
- 95% of data breaches have cause attributed to human error*

* - according to Cyber Defense Magazine

** - according to EdTechmagazine.com K-12 – October 2019 – The Cybersecurity Threats that keep K-12 CIOs up at night

BROWNEDWARDS
certified public accountants

Statistics*

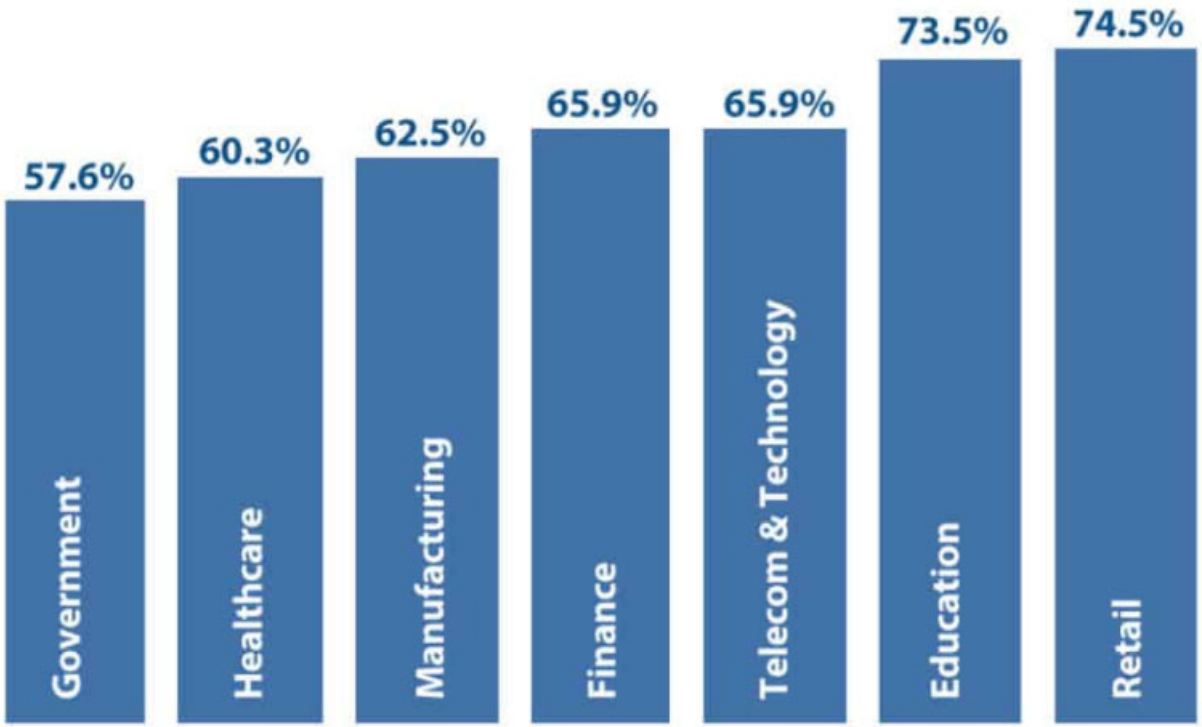


Figure 4: Percentage indicating compromise is "more likely to occur than not" in the next 12 months.

* Imperva 2019 Cyberthreat Defense Report issued in March 2019

BROWNEDWARDS
certified public accountants

Polling Question #6

When Cybersecurity Really Matters

Does your organization:

- Have a small IT staff, with significant outsourcing/online portal use?
- Have aging infrastructure?
- Conduct e-commerce on a website?
- Store and transfer “personally identifiable information,” about anyone (including sending data to the cloud)?
- Collect information on preferences and habits of customers/external users?
- Provide users with devices that aren’t just used onsite?
- Allow users to install “rogue” applications that aren’t specifically installed by the organization
- Have a clear plan as to what it should really be doing for cybersecurity?
- Understand that for almost all organizations, the question isn’t *if* there will be a breach, but *when* will there be a breach?
- Have a Cybersecurity insurance policy?

Common Threats

- Data can reside in many places and is difficult to manage.
  - Aging infrastructure may make systems less secure, especially on systems that are no longer supported by the maker.
- Organizations are highly dependent on technology
  - As technology, security, and global internet connectivity continue to grow in complexity and scope, there is no way to avoid cybersecurity risk.
- Organizations increasingly outsourcing key functions and transitioning data to third parties or cloud vendors.
  - Outsourcing does not equate to no risk. You are accepting the risk level of the organization you do business with, assuming it properly manages its operations to its desired risk level and performing monitoring on the service.

Common Threats

Common cyber threats that face organizations include:

1. **An inside attacker.** A malicious or disgruntled employee can change, delete or destroy data, damage systems, and steal or sell sensitive information.
2. **An outside attacker.** These attackers can hack into systems, develop social engineering attacks, and perform email hacking or extortion.
3. **A virus or malware.** An organization can become infected or infiltrated by a virus or malware that can originate with a phishing email or infected file.

Common Threats

4. **An employee accident** where an employee causes a breach through an innocent error.
5. **Non-malicious system or coding errors** implemented by IT personnel through inadvertent creation of vulnerabilities in software or applications.
6. **When it comes to trusted third-parties,** such as cloud providers or other vendors that control your organization's data or systems, can suffer a breach that exposes critical information.

Low-Cost, High-Priority Solutions

Entity Level

1. **Assess your risk.**
   - Perform risk assessments - can be conducted within the organization or by an outside specialist.
   - Risk assessments help identify vulnerabilities related to sensitive data.
   - Assessments should be updated at least annually or whenever a significant change occurs.

Low-Cost, High-Priority Solutions

Entity Level

2. Upgrade computers and software.

- Older operating systems, computers, and networks are more susceptible to data breaches.

3. Train and inform employees.

- Don't assume that employees understand terms like spear-phishing and how to recognize malicious links in emails and website pop-ups.
- Get professional training on how to protect against viruses, malware, spyware and other items.
- Develop strict policies on what employees can download and install on computers.

Low-Cost, High-Priority Solutions

Entity Level

4. Invest in reputable technology.

- Are company newsletters sent through Outlook or is a customer database kept in an Excel Spreadsheet on a desktop? Consider using an email provider like Constant Contact or MailChimp to send email blasts. Explore purchasing a CRM system to keep information on customers.
- Cloud-based products allow companies to outsource a big part of their security needs to leaders in the market.

Low-Cost, High-Priority Solutions

Entity Level

However, there are important data security risks to consider when storing data in the cloud.

- If you don't take the time to understand your data, then you are setting yourself up for failure in a public cloud environment. Securing data has to begin with data classification.

  Some data classification steps to follow are to:
  - Identify the data that will be processed or stored in the cloud.
  - Classify the information in regards to sensitivity. This would include identifying regulatory requirements for the data.
  - Define the rules by which particular data classes must be stored, transmitted, archived, transported and destroyed. Many data handling requirements result from contractual or regulatory requirements.

Low-Cost, High-Priority Solutions

Entity Level

- If there are restrictions on the physical location of data, you'll need to find a provider that can handle them. Amazon Web Services uses regions, and many of the other cloud providers offer similar structures.

- Also use one of these methods to meet your data protection requirements:

  - **File system access control lists:** This means using the access control mechanisms inherent in the cloud offering to ensure appropriate restrictions on the data. Access control lists should be used in all cases, but it would not protect from malicious acts by staff within your organization.
  - **Using encryption with a mixture of public and private key solutions** would most likely be used to protect against malicious staff.
  - **In addition, using transport level encryption** whenever sensitive information is being passed or transmitted.

Low-Cost, High-Priority Solutions

Entity Level

5. Use a reputable online payment processor.

Many donors want to give online. But donors will not give online if the payment process is complicated or not secure. A majority of entities such as nonprofits use PayPal, but you should give donors at least one other option. You might consider third-party services specially designed for your type of organization, such as Network for Good or Razoo for nonprofits.

Also, be aware of how fraudsters can use your donation pages to process fake donations using stolen credit card numbers.

Strategies to keep your charity and your donors safe include:

Low-Cost, High-Priority Solutions

Entity Level

- Making sure donors have access to the card they are using. Most credit card thieves do not have the physical credit card. More often than not, they know very little about the cardholder or their card. For this reason, your organization can usually weed out fraudulent donations by making it harder to use card numbers illegally. You can do this through:
  - **CVV2 verification.** This is A card's short code found on the back of a credit card (usually 3 or 4 digits). You'll want to require that online donors input this number when entering their card information. By doing this you will likely eliminate fraudsters who do not have access to the code.
  - **Address verification.** Verifies a donor's billing address with the address his or her bank has on file. This can be completed in seconds, and if the thief does not know the correct address, he will not be able to proceed.

Low-Cost, High-Priority Solutions

Entity Level

- **Verify the cardholder's identity** before completing a transaction.
- A few steps you can take to verify a donor's identity include:
  - **A BIN and IP address verification.** Included in every card number is information identifying the cardholder's bank, called the Bank ID Number or BIN. When processing a donation, have your system compare the donors' regional IP address against their BIN. If they are making their donation from a different country than their regional IP address, this could be a red flag.
  - **Use 2-factor authentication.** Before completing a donation, the user will have to confirm their identity via SMS or another communication platform.

Low-Cost, High-Priority Solutions

Entity Level

- **Make your donation form more sophisticated.**
  Many nonprofits shy away from using sophisticated donation forms online because they do not want to make it harder than they have to for donors to complete a donation. However, the more simplistic your donation form, the more likely it will be exploited by scammers. You can make your donation form more secure by using these two strategies:

  - **Require a minimum donation amount** before completing a transaction to prevent refund fraud tactics. This might seem counter-intuitive, but most donors usually give more than $15 when they donate.
  - **Use encryption and tokenization.** With encryption and tokenization, donors' payment information is turned into a code that only your payment processor can read. If thieves hack your data, they will not be able to extract a donor's information.

Low-Cost, High-Priority Solutions

Entity Level

6. Institute a cybersecurity breach response plan.

Should a cyber attack occur, having a plan ready to go will ensure that all appropriate members are able to react instantly, work together faster, and be strategic. When dealing with an attack, it is important to note that timing is critical. The more time that passes the more hackers can cover their tracks or steal more data from your systems.

Low-Cost, High-Priority Solutions

Entity Level

To ensure your plan is effective, it should include at least these four elements.

- *It's Tested Consistently*

  Unless the plan has been tested, you really have no idea if it is effective. Routinely testing an incident response plan gives your organization the practice it needs to identify weak spots and make improvements.

- *It's Detailed but Flexible*

  Flexibility is crucial to being able to apply the plan to different kinds of attacks and incidents. Flexibility and variety in a plan also ensures it can be updated regularly — so it can evolve as cyberattacks change over time.

Low-Cost, High-Priority Solutions

Entity Level

- *It's Clear About Communication*

  Clear communication plans are essential for incident response. Many incident response plans are too informal and assume communication across a network that may have been compromised.

- *It's Inclusive When It Comes to Stakeholders*

  A concise list of stakeholders and how each should be involved in incident response is imperative. Also think through who your external partners will be that are going to help in a time of crisis.

  An incident response plan should also include the intention to get your legal department involved as early on in the process as possible. Your legal department can often advise if it's necessary to involve law enforcement or other external partners. This action may also provide protection to the organization via attorney-client privilege.

Low-Cost, High-Priority Solutions

Individual Level

At the individual level you can do some of the following things:

1. **Focus on your passwords.**

Do not have the same password for every social network and website you access! Change it slightly and make sure to keep that information in a secure location. Consider using a password manager to store your logins to systems.

What makes a great password? Mix up the types of characters you use (numbers, letters, symbols) and don't use words you can find in the dictionary.

Low-Cost, High-Priority Solutions

Individual Level

2. Nonprofit organizations are the stewards of information for their donors and need to ensure that only individuals with the right authorization can access the information required, and nothing more. You, as an individual, are part of this stewardship responsibility.

As an authorized user, you are responsible for contributing to the security of computer systems. A secure information system maintains the principles of confidentiality, integrity, availability, authentication, and non-repudiation. You must abide by these principles in your daily work routine to protect information and information systems.

Low-Cost, High-Priority Solutions

Individual Level

When storing sensitive information, including PII, you can help **prevent *breaches*** by following these security tips:

- **Store** data on the **network** in accordance with your organization's data classification policies
- Keep in mind, **some systems** are strictly **non-sensitive—never** transmit, store, or process **sensitive data** on a non-sensitive system (i.e., unsecured fax machine, unencrypted thumb drive)
- **Label** paperwork containing personally identifiable information (PII) **appropriately** and ensure it is **not left lying around**
- **Use secure bins** to **dispose** of paperwork containing PII
- **Keep** only what you need

If you suspect a breach, notify the appropriate individuals in accordance with your organization's incident response plan.

Low-Cost, High-Priority Solutions

Individual Level

3. Social Engineering best practices (social engineering includes activities such as *phishing*, *spear phishing*, *vishing, and smishing*):

- If you receive a suspicious call: document the situation and attempt to verify the caller identity; if caller ID is available, write down the caller's number; take detailed notes of your conversation
- Don't share personal information
- Don't give out computer system or network information
- Listen to your gut – When something feels off, it probably is. You should be generally reluctant to download attachments and click links.
- Scrutinize the address an email says it came from and the text of any URLs it contains. If the source is legitimate, the text may still seem out of character for that sender. In this case, reach out to the person outside of email to confirm.

Low-Cost, High-Priority Solutions

Individual Level

- Protect your facility by:
  - Always using your own badge to enter secure operational areas
  - Never granting access for someone else using your badge
  - Challenge people who do not display badges or passes
  - Report any suspicious activity that you see in accordance with the incident response plan

- Avoid discussing sensitive operations outside work premises, whether you are talking face to face or on the phone

- Be discreet when retrieving messages from smart phones or other media

Low-Cost, High-Priority Solutions

Individual Level

4. If your system begins to act unusual, maybe running more slowly, or exhibits an increase in CPU utilization, you need to consider that you might have a virus on your system. This should be reported immediately in accordance with your incident response plan or procedures. Methods to prevent viruses are:

- Removing software you don't use
- Keeping internet activity relevant (IT can use webcontent filtering to help reduce irrelevant activity)
- Logging out at the end of the day
- Updating your operating system, browsers, and plugins as soon as updates are available
- Only accessing SSL protected websites **(how can you tell if a website is SSL protected?)** – Look for the padlock symbol in the upper left corner of the web browser

Low-Cost, High-Priority Solutions

Individual Level

5. When it comes to social media

Be aware of what you post online. Even information you might consider inconsequential, such as a spouse's name, employer, or birthday, could be used by someone to steal your identity or gather information for other purposes.

Ensure you monitor privacy settings carefully as these can change from time-to-time.

Refrain from discussing any work-related matters on such sites.

Low-Cost, High-Priority Solutions

Individual Level

6. Wire transfers.

- verbally confirm that a request to initiate a wire is from an authorized person. DO NOT confirm these requests through email.
- anytime you receive new wire instructions or a change to existing wire instructions verbally verify with the wire recipient
- If you receive a request for a payment that is out of the ordinary payment arrangement, confirm by phone with the vendor.
- Double check email addresses – a common trick is to slightly modify email addresses.
  john.smith@abc.com may be change to jon.smith@abc.com

Low-Cost, High-Priority Solutions

Individual Level

- rather than reply to an email, forward the email to the address that you have on file.

- be on alert for fraud anytime the wire transfer instructions include tight deadlines or pressure you to act quickly.

Low-Cost, High-Priority Solutions

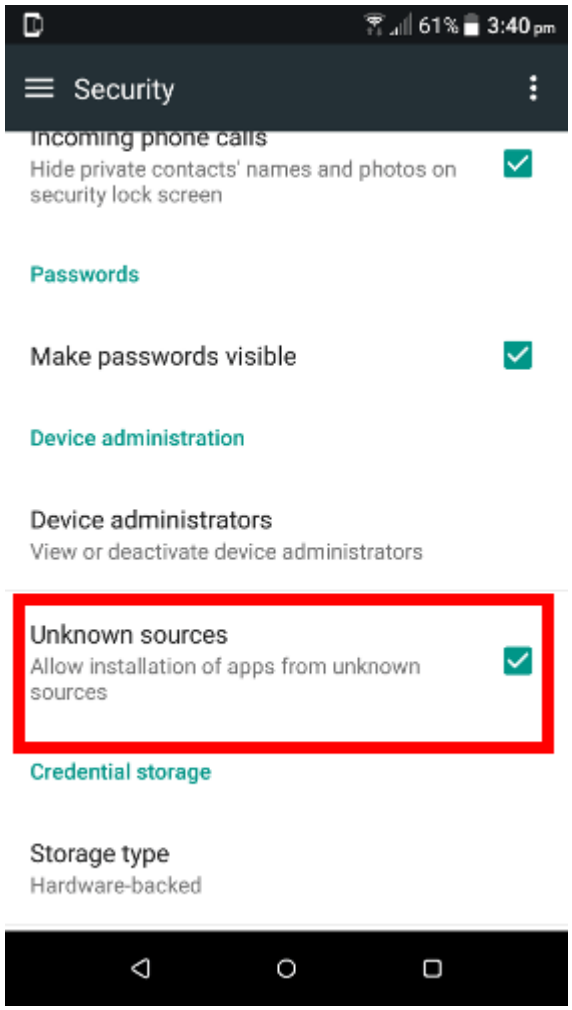
Individual Level

7. When it comes to Mobile computing.

- Always maintain physical control of mobile devices
- Disable wireless functionality when you are not using it
- As much as possible, have separate devices and email accounts for personal and business use. This is especially important if other people, such as children, use personal devices. Do not conduct any sensitive business activities (like online business banking) on a personal computer or device, and do not engage in activities such as web surfing, gaming, or downloading videos on business devices. Do not send sensitive business information to personal email addresses.
- Lastly - Do not leave devices unattended.

Mobile Phone Security

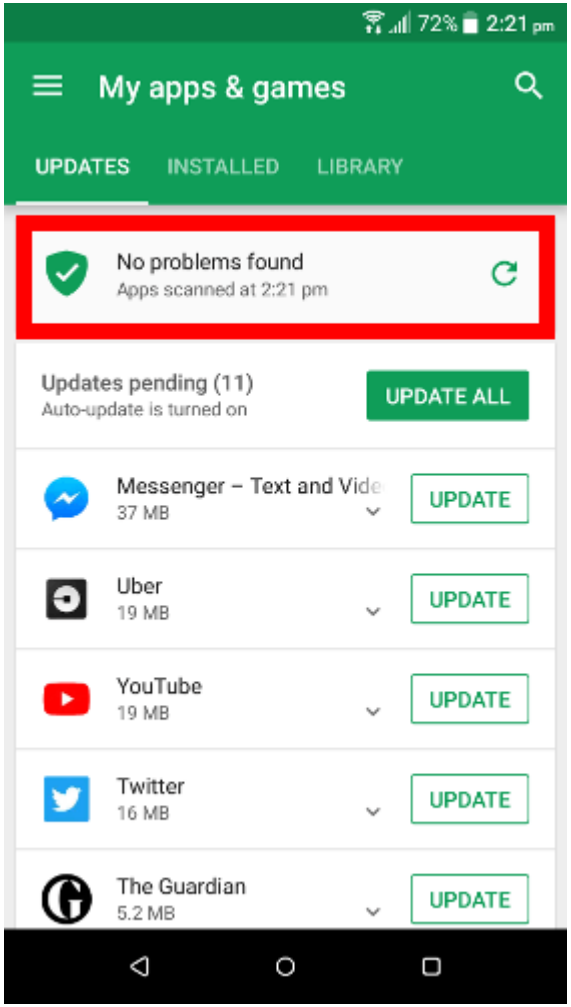
- Android
  - Android has built its reputation on its relative openness compared to iOS.
  - You can download apps from anywhere and you can root your device.
  - If you're downloading from unknown sites or rooting your devices, you should consider an antivirus app.
  - If always downloading apps from the Google Play and following good security practices, then you might be ok without one.



BROWNEDWARDS
certified public accountants

Mobile Phone Security

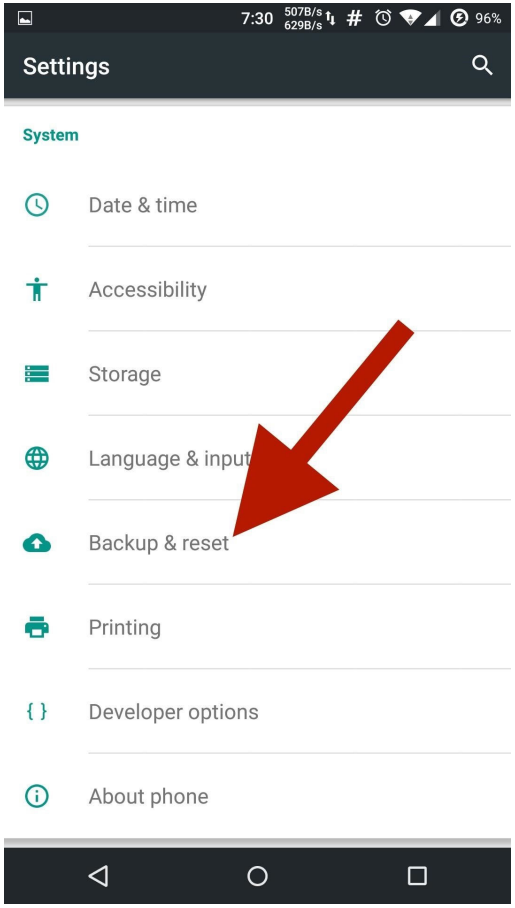
- Android
  - Google provides a tool called Play Protect to scan your device for malicious apps and purges them.
  - Go to Play Store app, select “My apps & games”, then under “updates” tap the “refresh” icon near the top of the screen to scan.

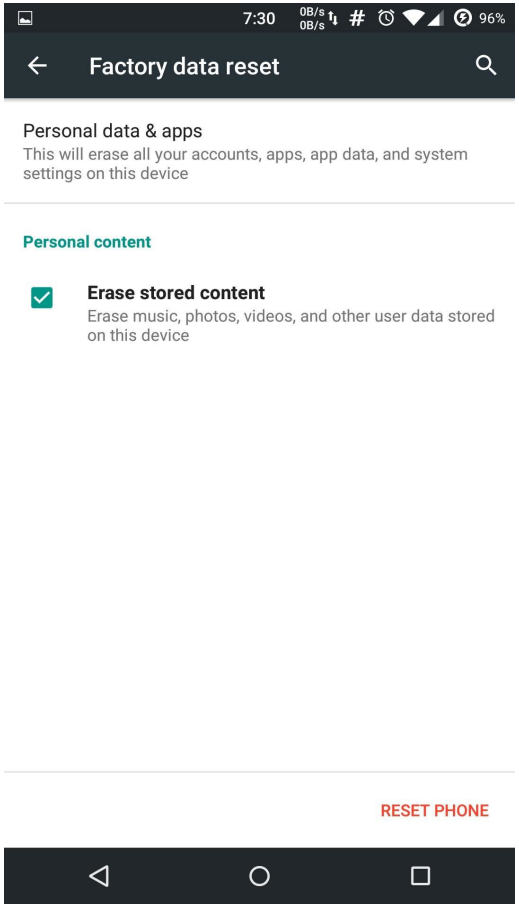


BROWNEDWARDS
certified public accountants

Mobile Phone Security

- Android
  - If, after following all of this advice, your device still gets a virus, a factory reset should solve the problem. However, you can lose data and settings if you use this method.





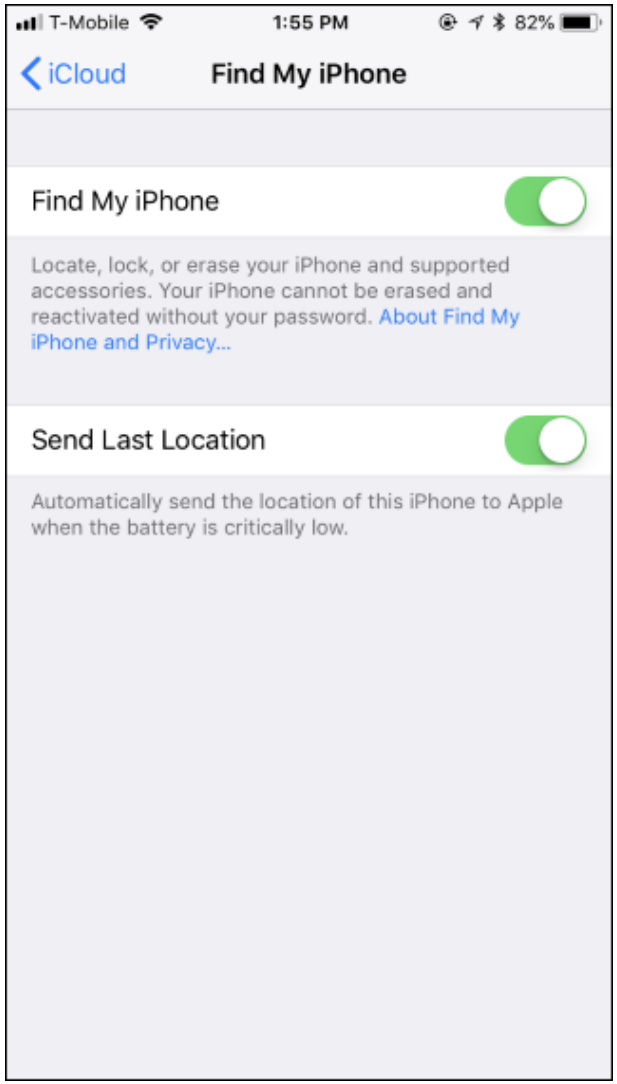
BROWNEDWARDS
certified public accountants

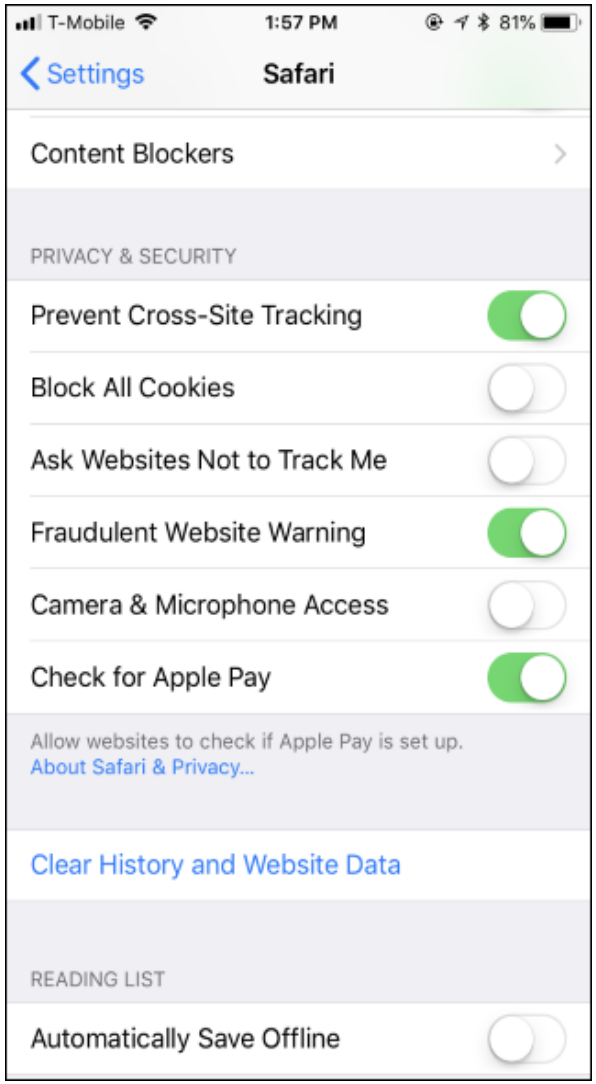
Mobile Phone Security

- iPhone
  - Any apps you install on your iPhone run in a sandbox that limits what they can do.
  - Any “security” apps you install are forced to run in the same sandbox as all other apps.
  - These “security” apps can’t see a list of apps you’ve installed and can’t scan anything on your device for malware.

Mobile Phone Security

- How your iPhone already protects you





BROWNEDWARDS
certified public accountants

Mobile Phone Security

- iPhone
  - Additionally, your iPhone device can only install apps from Apple's App Store. If malware is found in an app later, Apple can remove it from the Store and have your iPhone immediately delete the app.
  - "Find My iPhone" functionality lets you remotely locate, lock, or erase a lost or stolen iPhone.
  - "Fraudulent website warning" will present you with a warning if you end up on a malicious website.
  - DON'T JAILBREAK YOUR IPHONE!! This allows your device to run outside of the normal security sandbox. It also lets you install apps from outside the App Store.

Example -Catawba Valley Medical Center & Atrium Health

- Catawba Valley Medical Center (Individual Hack)
  - Hack originated by an employee mistakenly opening an email that turned out to be a phising scam. This led to three employee emails being hacked.
  - Potential to impact 20,000 patients – included names, birthdates, social security numbers.

- Atrium Health (Hack of a third party provider)
  - Their billing provider (AccuDoc) was hacked potentially affected more than 2.5 million patients where patient data could be viewed. This was due to a Database hack.
  - Potentially compromised all those accounts for a week.
  - Included data of guarantors and patients, names, addresses, dates of birth, insurance policy details, medical record numbers, account balances, and dates of service. Approximately ¼ of the total also had social security numbers.

Polling Question #7

Takeaways

- Discussion - Takeaways
  - Entity Level – Goals, risk assess, mitigate issues based on assessed risk, have a cybersecurity response plan, encourage employee communication about anything “unusual” as relates to their systems/communications.
  - Entity Level – organizations may consider other reports such as 2019 data breach information across industries, and other resources such at www.idtheftcenter.org –ITRC non -profit to broaden education and awareness
  - Entity Level – Discuss with those in your organization, peers, and other resources to ensure that actions that can be taken align with goals, and what risks are to be accepted.

Takeaways

- Discussion - Takeaways
  - Entity Level – with smaller IT staff sizes, determine what the most vital areas are to be covered with that staff, including monitoring outsourced items, and work downward until out of staff time/resources.
  - Individual Level - Training, training, training!!
    - As an example of some basic training to start - “Cybersecurity Resources for Nonprofits” is a website from the Federal Trade Commission where they provide cybersecurity quizzes. The quizzes cover cybersecurity basics, ransomware, and vendor security. Ask your employees to take the quizzes to see how much (or how little) members of your staff know; this can create a first step in a training program.
    - Don’t just depend on any software/hardware/security setup to protect you from unusual items that come up.
    - Listen to your gut.
    - Scrutinize the email addresses of unknown senders, or requests that appear unusual.
  - Use technology tools such as Mimecast to filter email messages.

Clarence Rhudy, CPA, CISA, CITP
crhudy@becpas.com
Tyler Gall, CPA, CFE, CISA Candidate
tgall@becpas.com
540 345-0936

BROWNEDWARDS
certified public accountants

PPP Q&A

Jessica Hewitt, CPA – Tax Senior Manager

JHewitt@BEcpas.com 757-316-3235

Jessica joined the firm in 2011 and has worked in a variety of areas. She has experience with partnership, corporate, and fiduciary tax issues. She is well versed in multi-state income taxation and serves on the firm's multi-state tax team. The Dealership, Real Estate and Construction industries are her niche focus.

She graduated with a Master's of Science in Accounting from Liberty University and a Bachelor of Science in Business Administration - Accounting Concentration from Christopher Newport University. She is a member of the American Institute of Certified Public Accountants, the Virginia Society of Certified Public Accountants and treasurer of Windsor Castle Park Foundation.

Patrick Pittman, CPA

PPittman@BEcpas.com 540-345-0936

Patrick is a Tax Services Manager in the Roanoke office with extensive experience providing management and tax consultations, business and tax planning, and tax compliance services.

Patrick holds a Bachelor of Science in Accounting from Virginia Tech and a Master of Science in Accounting, from James Madison University. He is a member of the Virginia Society of Certified Public Accountants and the American Institute of Certified Public Accountants. Patrick frequently speaks at lectures and conferences on a wide array of topics.

Patrick's area of expertise include:

- C corporation income tax accounting and planning
- S corporation, partnership, and LLC taxation
- Compensation and benefit reporting
- Nonprofit tax-exemption compliance
- Multi-state tax compliance
- Individual income tax planning, including high net worth individuals
- International tax compliance, including 5965, FDII, and GILTI

Patrick serves the community by serving as Treasurer of a nonprofit childcare center and youth soccer club. In addition, he has served on various boards for community organizations.

Jessica Hewitt, CPA
Senior Manager
Brown Edwards

Patrick Pittman, CPA
Senior Manager
Brown Edwards

BROWNEDWARDS
certified public accountants

Polling Question #8

VSCPA
Virginia Society of CPAs
Tidewater Chapter

THANK YOU TO BROWN EDWARDS AND TO OUR SPEAKERS

Kristen Jones, CPA
Leslie Robert, CPA and Steve Kast, UWVP
Katie Ward,CPA
Tyler Gall, CPA
Jessica Hewitt, CPA and Patrick Pittman, CPA