ACUA
WEBINARS

Ransomware: What’s next?

Presented by Kathy Cruz
Director, Cyber Government, KPMG

—

January 23, 2020

ACUA

ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

Did you know that Connect ACUA allows you to post new messages directly from your email without logging in to the Connect ACUA website?

For more details, check out the Quick Tip post on

Connect.ACUA.org

Your Higher Education Auditing Connection

ACUA Kick Starters

Use a Kick Starter to launch your next audit!

- Developed by ACUA members with subject matter expertise
- Focused on higher education specific topics

https://acua.org/Audit-Tools/ACUA-Kick-Starters

ACUA

ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

Advancing Auditing in Higher Education

Do you have a great idea for an ACUA Kick Starter? Contact Heather Lopez at hlopez@wsu.edu.

ACUA WEBINARS

New Kick Starters Available!

Payment Card Industry Data Security Standards (PCI DSS)

and

Faculty Workload

Download today in the members-only section

ACUA
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS
Advancing Auditing in Higher Education

ACUA WEBINARS

ACUA

ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

Advancing Auditing in Higher Education

Stay Updated

- The College and University Auditor is ACUA's official journal. Current and past issues are posted on the ACUA website.
- News relevant to Higher Ed internal audit is posted on the front page. Articles are also archived for your reference under the Resources/ACUA News.

Get Educated

- Take advantage of the several FREE webinars held throughout the year.
- Attend one of our upcoming conferences:

Audit Interactive
April 5 – 8, 2020
Nashville, TN

AuditCon
September 13 – 17, 2020
San Antonio, TX

- Contact ACUA Faculty for training needs.

Get Involved

- The latest Volunteer openings are posted on the front page of the website.
- Visit the listing of Committee Chairs to learn about the various areas where you might participate.
- Nominate one of your colleagues for an ACUA annual award.
- Submit a conference proposal.
- Present a webinar.
- Become a Mentor
- Write an article for the C&U Auditor.
- Write a Kick Starter.

Connect with us

www.ACUA.org

Connect with Colleagues

- Subscribe to one or more Forums on the Connect ACUA to obtain feedback and share your insights on topics of concern to higher education internal auditors.
- Search the Membership Directory to connect with your peers.
- Share, Like, Tweet & Connect on social media.

Solve Problems

- Discounts and special offers from ACUA's Strategic Partners
- Kick Starters
- Risk Dictionary
- Mentorship Program
- NCAA Guides
- Resource Library
- Internal Audit Awareness Tools
- Governmental Affairs Updates
- Survey Results
- Career Center......and much more.

ACUA WEBINARS

WEBINAR MODERATOR

ACUA
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS
Advancing Auditing in Higher Education

- Don’t forget to connect with us on social media!

ACUA SOCIAL NETWORKING

ACUA Distance Learning Director
Lisa Gendusa
Internal Auditor
Texas State University System

Overview

- Ransomware is predicted to rise 500% over the next two years.
- Educational institutions are attractive targets estimated to receive 3x the rate of ransomware infections than Healthcare and 10x the rate of the Financial sector.
- Today’s webinar will explore what ransomware is, common ways it is introduced into an environment, incident readiness and response and ways that information security programs can build resilience.

Polling Question #1

What do you believe is the top IT risk facing your organization in 2020?

A. Aging IT systems create a higher risk for ransomware
B. Lack of trained information security resources
C. Lack of information security awareness
D. Do not know or other

Polling Question #1 results

What do you believe is the top IT risk facing your organization in 2020?

A. **Aging IT systems that create a higher risk for ransomware or a data breach**

B. **Lack of trained information security resources**

C. **Lack of information security awareness among staff, students and contractors**

D. **Do not know or other**

Aging systems that are no longer vendor supported and therefore unpatched, lack of trained resources and insufficient security awareness throughout the organization are the perfect storm for ransomware.

Ransomware vs Data Breach

- Although data is held for ransom, ransomware is not the same as a data breach.
- A data breach is a security incident in which sensitive or confidential data is copied and stolen from an organization.
- However, as ransomware and malware becomes more sophisticated, it can do both.

Cryptography + Malware = Ransomware

- Ransomware is a type of malicious software (malware) designed to block access to a computer, network, files, etc. until a sum of money (ransom) is paid.
  - Ransomware attacks account for nearly 24% of incidents were malware was used.
- Ransomware typically encrypts files, making them inaccessible until the ransom is paid for the decryption key.
  - However, non-encryption SamSam ransomware used Remote Desktop Protocol (RDP) brute-force attack to guess weak passwords until one was broken. Estimates are the developers of SamSam have made $6M in ransom and caused over $30M in damages.
- Bad actors generally request payment in cryptocurrencies, such as Bitcoin, as it is untraceable.

Payment of ransomware doesn’t always guarantee unlocking of network or files. Remember, these are criminals.

Why Ransomware?

- Ransomware is generally a crime of opportunity. Where sensitive data can be monetized, ransomware will follow.
- It does not rely on data theft in order to be lucrative and is the shortest distance between investment and revenue, however, ransomware is evolving to both disabling systems and stealing data.
- Bad actors offer “Ransomware as a Service (RaaS) which allows less sophisticated attackers to outsource negotiations and payment facilitation.
- Ransomware can be the distraction before the real attack.

Ransomware Trends

- Ransomware has morphed from spray-and-pray phishing to highly targeted and extremely damaging network-wide infections that can cause weeks of downtime.
- Evidence increasingly shows that attacks could also be sophisticated agents of a foreign entity or government.
- The United States publically attributed the WannaCry ransomware attack in 2017 to North Korea. WannaCry afflicted over 200,000 computers worldwide with estimated global costs of $8B.
- Attackers are using automation to find vulnerabilities and exploit them.
- Organizations that under-spend, under-prioritize and under resource information security programs are most vulnerable.

Ransomware Stats

- A new organization will fall victim to ransomware every 14 seconds in 2019, and every 11 seconds in 2021 (Source: Cyber Security Ventures)
- 1.5 million new phishing sites are created every month (Source: webroot.com)
- In 2019 ransomware from phishing emails increased 109 percent over 2017 (source: Phishme)
- The average cost of data breaches will reach into the hundreds of millions of dollars by 2020 (Source: Juniper Research)
- Cybercriminals will target Software as a Service (SaaS) and cloud computing businesses, which store and secure private data (Source: Massachusetts Institute of Technology)

Ransomware and Education

- Universities that partner with private companies, run policy institutes or research are more likely to be targets for both ransomware and cyber-espionage.
  - In March 2018, the US Department of Justice charged nine Iranians over a cyber-theft campaign stealing more than 31 terabytes of documents and data from American universities and companies.
- Education is known to have a limited budget for IT staff and infrastructure, making them targets.
- Colleges and universities are the most complex and vulnerable with each academic department having specific networking requirements including research labs and connected equipment. The more decentralized, the greater the risk.

Ransomware and Education

- 382 incidents *reported* at education organizations in 2019 with 99 confirmed data disclosures.
  - Denial of Service (DoS) attacks account for half of all incidents (226) (and of the industries analysed, the most are in education). Other notables:
    - Cyber-Espionage – 6 incidents
    - Privilege Misuse – 19 incidents
    - Web applications – 30 incidents
    - *Miscellaneous* Errors – 37 incidents
- For sanctioned phishing exercises, education had a 4.93% click rate, highest in the industries analysed.

Source: Verizon 2019 Data Breach Investigations Report

Education Ransomware Incidents

- 2019: Crowder College of Neosho, Missouri reported a damaging ransomware virus that shut down the college’s email, website and computers. No data was breached or stolen, however, the virus had been dormant in the college’s system since 2018.
  - $1.6M demanded but not paid.
  - Months to full restoration, using paper forms and schedules.

- 2019: Monroe College (New York City) reported a cyberattack had disabled many of their technology systems and platforms.
  - $2M in Bitcoin demanded, College did not comment on payment.
  - College resorted to paper until systems restored.

The Cost of Ransomware

- Estimates are that ransomware costs will reach $20B globally by 2021 vs $5B in 2017.
- Costs per incident vary by industry and type. The cost of a single ransomware incident can cost an entity more than $713,000 on average. (Source: CNBC/Tech Transformers)
- Costs include:
  - Business disruption. Critical systems, including email, could be unavailable for weeks.
  - Redirection of staff from other critical tasks and projects to help with recovery efforts.
  - Some hardware and/or systems may not be fully recovered and need replacement.
  - Loss of revenue.
  - Damage to reputation.
  - Loss of public trust.

Polling Question #2

Has your organization made an advanced decision to pay or not pay ransomware if demanded for data and/or system access?

A. Yes

B. No

C. Don’t know

Paying the Ransom

- A plan to protect the organization against ransomware should be a critical component of a broad, holistic cyber strategy that is aligned with your organization’s business and governance objectives.
- Determining how to respond to ransomware in the context of a larger cybersecurity program will help address specific threats, defend against an attack and if necessary, recover from one.
- Organizational leaders must consider in what circumstances they would pay, or not pay, a ransom and then establish processes for decision making.
- Policy guided by legal and business factors to formulate a response will significantly reduce the stress and allow for a more informed response.

How Does Ransomware Get into an Environment?

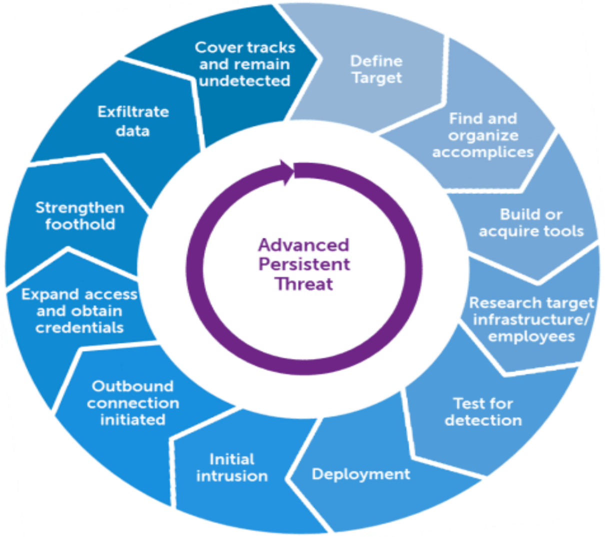
- Email is increasingly being weaponized to steal user credentials and deliver ransomware.
  - December 2019 U.S. Coast Guard reported that Ryuk ransomware had struck a facility affecting industrial control systems and cameras. It took 30 hours for everything to be restored. The ransomware gained a foothold after an employee opened a phishing email and clicked on the link.
- Office documents and Windows applications are the most common vehicles to gain initial access.
- Attacks on mobile devices are increasing due to limited screen size making it more difficult to scrutinize emails and URLs.
- After initial infection, the ransomware attempts to spread to shared storage and other accessible systems.

How Systems are Compromised with Ransomware

- Insufficient Identity and Access Management (IAM) allows the attacker to steal credentials and navigate the system and gain elevated permissions and access.
- An unauthorized (and undetected) Access Point is attached to the network to gain access to the network, systems and databases as if they were legitimate employees.
- Using stolen credentials the attacker logs in to a legitimate user’s account and uses that account to infect systems.
- Malware routinely embeds command-and-control (C2) ability enabling attackers to control and encrypt systems and data.
- Attackers compromise hardware that has out-dated patching and installs malicious firmware that will execute code outside of the operating system and main system firm or BIOS.

Encryption-to-Ransom Timeline

- From click to infection can be as little as 5 seconds. This is the primary technique for criminals who want to do the smallest amount of work : payoff. As soon as the malware is installed, data is encrypted and ransom demanded.
- More patient criminals looking for maximum damage and reward are Advanced Persistent Threats (APT).


Advanced Persistent Threat
Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Cover tracks and remain undetected

Poll Question #3

Does your institution have a playbook ready and tested as part of your business continuity plan if attacked by ransomware?

A. Yes

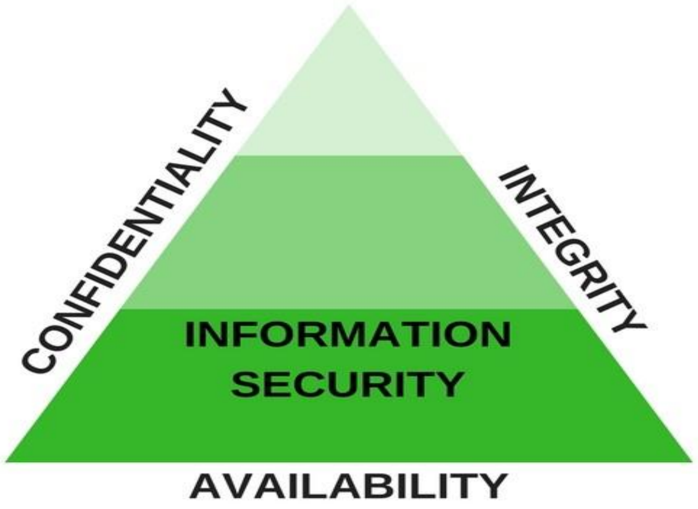
B. No

C. Don’t know

PLANS ARE NOTHING; PLANNING IS EVERYTHING.

DWIGHT D. EISENHOWER

The CIA Triad



- **Confidentiality**: Protecting information from unauthorized access.
- **Integrity:** Ensuring the authenticity of information – that information is not altered, and the source is genuine.
- **Availability:** Information is accessible to authorized users.

Business Continuity

- A business continuity plan is your organization's ability to ensure operations and core business functions are not severely impacted by a disaster or *incidents* that disables your critical systems for a sustained period of time.
- Business continuity plans continue to be the most effective way to lessen the impact of ransomware.
- The CIA Triad should be the foundation of your information security business continuity plan.
- Incident readiness and response for malware, ransomware and other types of information security events should be considered essential components of every business continuity plan. Have a clear plan to address attacks, including when internal capabilities are overwhelmed.

Plan your dive, dive your plan!

- Cybersecurity incident readiness and response plans are not static.
  - Make forensics part of the plan to ensure you understand infection vector, file execution, malware analysis, lateral movement and indicators of compromise.
- Annual cybersecurity crises exercises are highly recommended.
- Quarterly table-top exercise should be mandatory and result in updates and revisions to the plan.
- Regular rehearsals of cyber incidents is important.
- Back-up data regularly.

About Back-ups….

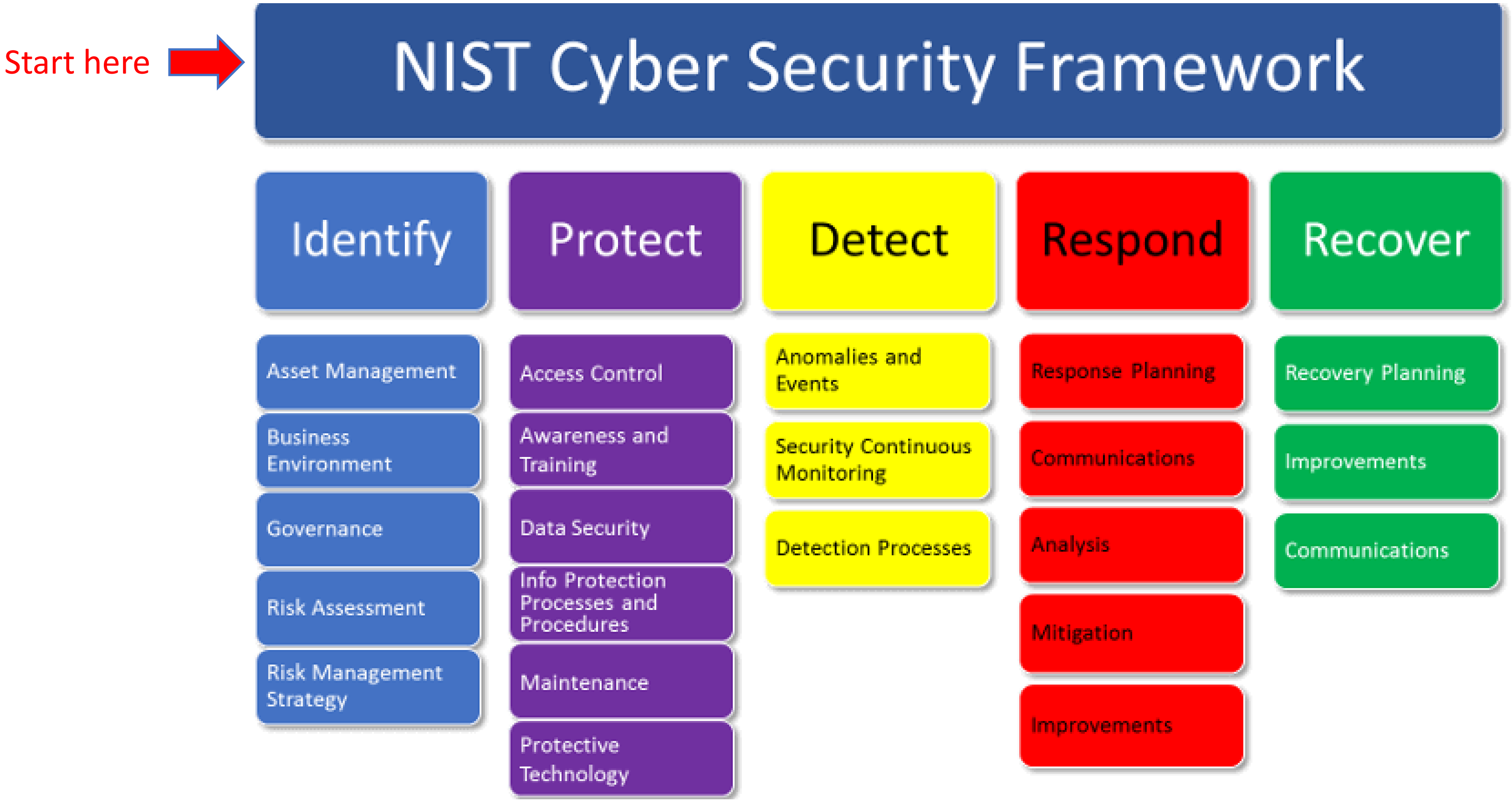
- Back-ups are critical in ransomware recovery and response. It may be the best way, or the only way, to recover your critical data.
- Verify integrity of back-up and test restoration process on a regular basis as part of business continuity.
- Secure your backups!
    - Ensure back-ups are not connected permanently to computers and networks they are backing-up. Store back-ups in the cloud or off-line.
    - Some ransomware have the ability to lock cloud-based backups when systems continuously back-up in real-time (persistent synchronization) so have an alternate plan for this data.

Polling Question #4

Is cyber crime a driving factor in your audit planning?

A. Yes
B. No
C. Don’t know

National Institute of Standards and Technology



Start here

NIST Cyber Security Framework

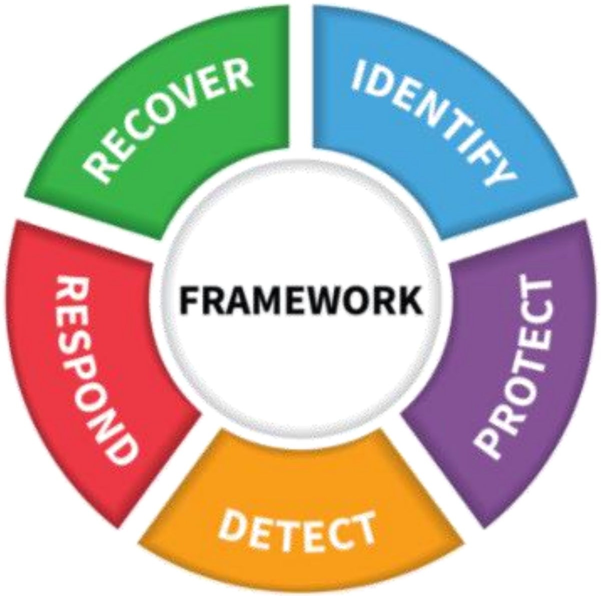
Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

NIST SP 800-53

Key Framework Attributes

Principles of Current and Future Versions of the Framework

- Common and accessible language
- Adaptable to many technologies, lifecycle phases, sectors and uses
- Risk-based
- Based on international standards
- Living document
- Guided by many perspectives – private sector, academia, public sector



Offense vs Defense

- IT and Information Security budget and resources are always insufficient. Work with what you have and build a case for more.
- Plan and prioritize information security resources against organizations goals and objectives, risk profile and risk appetite.
- Complete an internal information security risk assessment annually and an independent risk assessment bi-annually. Include technical risks and policy reviews. Assessment is the first step in effective cybersecurity.
- Auditors can be your best friend. Audit findings help prioritize critical areas, identify risks and can strengthen justification for additional resources.

Auditors as Anti-ransomware Champions

- Audits of information security should include these key areas that are targets of ransomware.
- Are there processes for updating and maintaining an accurate asset inventory which includes software and firmware patch levels?
- Is there a process for testing and applying hardware and firmware patches in a timely manner.
- Is there a continuous monitoring policy, procedures and practice. Malware and ransomware doesn’t work M-F, 9-5.
- Is there an end-point protection policy and robust protection beyond anti-virus.
- Are incoming and outgoing emails scanned to detect threats and filter executable files from reaching end users.

Auditors as Anti-ransomware Champions

- Are Software Restriction Policies (SRP) or other controls in place to prevent programs from executing from common ransomware locations such as temporary folders supporting internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- What is the application whitelisting program and policy?
- How are privilege accounts managed? Is there a policy?
- Is least privilege a policy with processes that are implemented and used? Are access controls, including file, directory and network share permissions only for those who need it, read-only for specific files with limited write access?
- Are passwords robust, changed frequently and never shared.
- How many users have admin rights?

Develop a Security-Minded Culture

- The #1 way that ransomware will enter your organization is through the action of a human: clicking a link, opening an attachment, not complying with least privilege protocols, misuse of admin privileges.
- Information security is everyone’s job, not just IT, the auditors or the information security staff.
- Security awareness training must be continuous, not an annual compliance exercise.
- Evaluate user readiness: Consider approved phishing campaigns throughout the year to build awareness and to reinforce, “look before you click”. Make reducing the click rate and organization-wide objective.

Final thoughts

- Shift from compliance to risk-based audits (if you haven’t already).
- Auditors can be valued partners in the prevention of malware and ransomware. Join forces.
- Know in advance what you will do if hit with ransomware or a significant security incident.
- Spend where it makes sense. Smart technology spending is essential to defending data assets.
- Don’t forget third party risk. Cloud vendors and other technology supported by vendors can also pose a risk. Consider vendor risk assessments as well.

Disclaimer

- The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.
- © 2019 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity.
All rights reserved.
- The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Upcoming ACUA Events

March 12, 2020

Webinar on using the ACUA Kick Starter:
Investigations – Misappropriation of Assets

April 4 – 8, 2020

Audit Interactive in Nashville, TN – Registration is now open. Visit the ACUA website for details.

ACUA
WEBINARS

Join us for our upcoming webinar.