Ways COVID-19 is Reshaping Cybersecurity, Privacy and Fraud Risk for Nonprofits

CPAs & ADVISORS

Ricardo Trujillo,
CPA, CITP, CISA
Partner

Melissa Musser,
CPA, CITP, CISA
Principal

Gelman, Rosenberg & Freedman CPAs is now GRF CPAs & Advisors

Please note our new address:

4550 Montgomery Avenue, Suite 800N, Bethesda, MD 20814

grf CPAs & ADVISORS

Housekeeping

CPE Credit/Technical Support

- **Important:** Three (3) CPE words will be provided during the presentation. Please write them down – **we will not provide them again via GoToWebinar or email (no exceptions)**.
- Please complete the electronic survey that will appear automatically at the **end of the webinar**.
- Attendees seeking CPE for this presentation must complete the survey and **enter all three CPE words**. You cannot claim CPE unless we receive a completed evaluation with the correct words.
- This presentation will be recorded and made available to download at www.grfcpa.com/webinars.
- Technical questions about the survey can be addressed to Nathan McElveen at nmcelveen@grfcpa.com.

Housekeeping

Additional Information

Learning Objective To provide attendees with an overview of the cybersecurity & fraud landscape and best practices for protecting their organizations from threats	**Instructional Delivery Methods** Group Internet-based
Recommended CPE 1.0 CPE Credit	**Recommended Fields of Study** Information Technology
Prerequisites None required	**Advance Preparation** None
Program Level Basic	**Course Registration Requirements** None
Refund Policy No fee is required to participate in this session.	**Cancellation Policy** In the event that the presentation is cancelled or rescheduled, participants will be contacted immediately with details.
Complaint Resolution Policy GRF CPAs & Advisors is committed to our participants' 100% satisfaction and will make every reasonable effort to resolve complaints as quickly as possible. Please contact *kdavis@grfcpa.com* with any concerns.	
Disclaimer This webinar is not intended as, and should not be taken as, financial, tax, accounting, legal, consulting or any other type of advice. Readers and users of this webinar information are advised not to act upon this information without seeking the service of a professional accountant.	

Presenters

Meet the Instructors

Melissa Musser,

CPA, CITP, CISA

Principal

Ricardo Trujillo,

CPA, CITP, CISA

Partner

grf CPAs & ADVISORS

Presenters

Meet the Instructors

Ricardo Trujillo,

CPA, CITP, CISA

Partner | *rtujillo@grfcpa.com*

Mr. Trujillo has worked in auditing and accounting since 2000. He has proven expertise in assurance and advisory services, and his nonprofit experience spans across a variety of organizations, including foundations, trade and membership associations, charitable institutions and US-based non-governmental organizations.

Mr. Trujillo leads the firm's information technology initiative and helps for-profit and nonprofit organizations bridge the gap between business and technology by carefully analyzing IT infrastructures. He presents to the nonprofit community on cybersecurity and enterprise risk management topics.

Melissa Musser,

CPA, CITP, CISA

Principal | *mmusser@grfcpa.com*

Mrs. Musser is a principal at GRF with over 15 years of professional experience. She and her team deliver comprehensive risk-based assessments to help organizations respond to strategic, financial, compliance, operational and IT risks. Her expertise includes establishing, maintaining and optimizing internal controls, compliance, Enterprise Risk Management (ERM), and cybersecurity programs. Mrs. Musser is the proud recipient of the 2018 AICPA Information Management and Technology Assurance (IMTA) Standing Ovation award.

Agenda

The Importance of Cybersecurity in Preventing Fraud

- Evolution of information technology in business
- Cybersecurity and preventing fraud
- Cyber Risk Landscape
- Increased rate of risk
- Digital transformation risk
- Fraud
    - Recent events
    - Phishing
    - Ransomware
- How to protect your organization
    - CISO and CIO
    - Implement strategy and controls
    - Third party due diligence
    - Useful technologies
- Summary

grf CPAs & ADVISORS

The Importance of Cybersecurity in Preventing Fraud

Anatomy of an IoT Attack by Cisco

grf CPAs & ADVISORS

Cyber Risk Landscape

Climbing Rate of Risk

Cyber Risk Landscape

Digital Transformation Risk

- More organizations are embracing modern technology than ever before
- Each year more goes from physical to digital

Digital Transformation - the integration of digital technology into all areas of an organization changing how they operate and deliver value.

1. Third Parties
2. Operational Resilience
3. Internet of Things

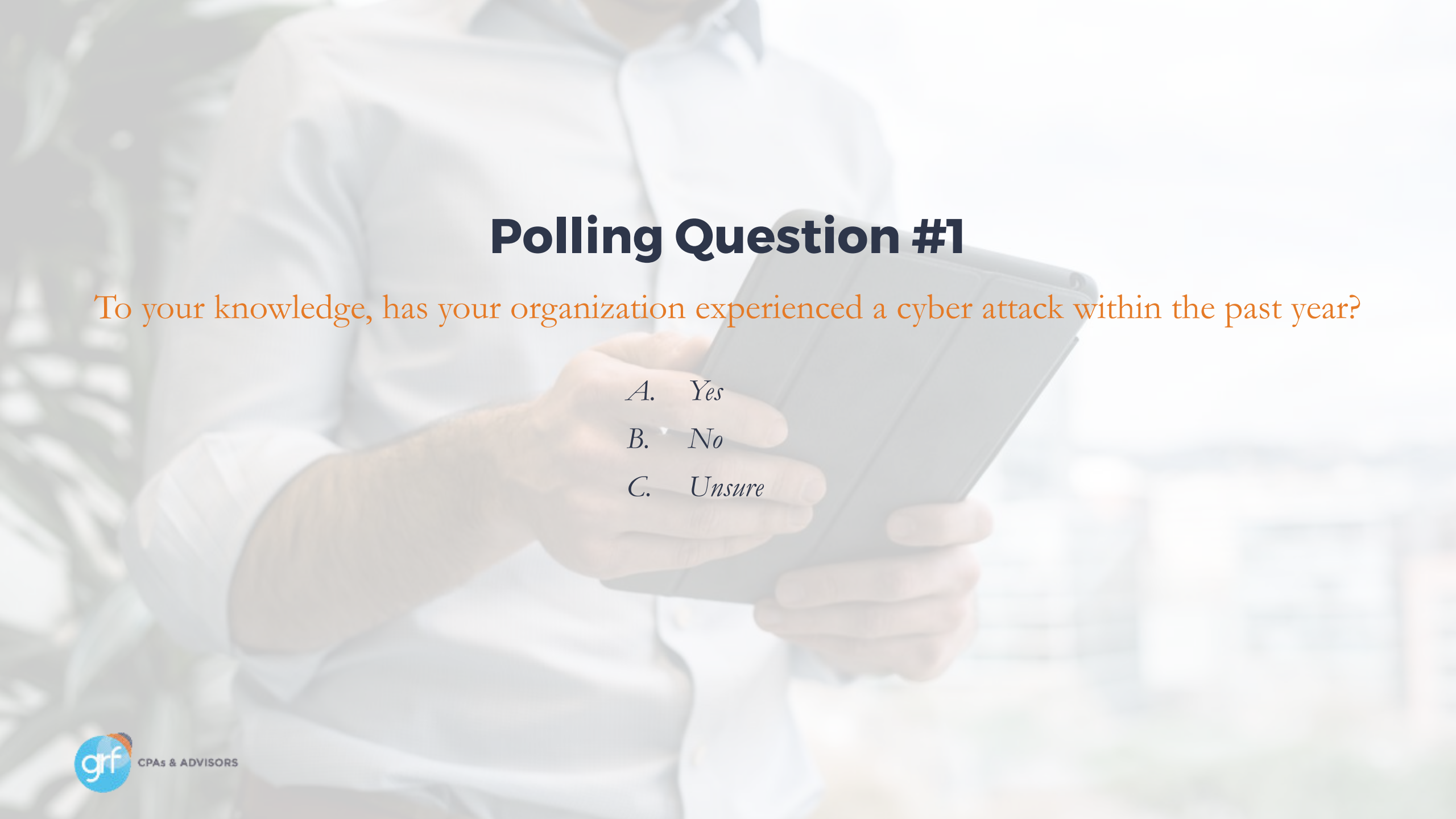
How to protect your organization

Who owns Information Security?

- **Ideal #1:** Chief Information Security Officer (CISO) or the like
- **Ideal #2:** Info Sec Committee
- **CFO**
    - In smaller organizations CFO's often find themselves acting as the Chief Information Security Officers. Or at least participating on privacy or information security committees. Why? - CFO understand internal controls and data flows to third party providers such as cloud accounting software, payroll, payables, membership or donor databases, marketing, travel providers etc.
- **CEO, COO, Executive Director** - Other possible internal "owners"
- **vCISO (Virtual Chief Information Security Officer)** - Advisory solution gaining in popularity and need for small to midsized organizations – Note "responsibility" is never fully outsourced!

Cybersecurity and preventing fraud

- As IT evolves, so do the schemes used by hackers
- Prevent unauthorized access to your network
- Monitoring and evaluation
- Protect sensitive data (PII, financial, IP, etc.)
- Consequences of a breach can be catastrophic (loss of money, loss of data, reputational damage, etc.)



Polling Question #1

To your knowledge, has your organization experienced a cyber attack within the past year?

A. Yes

B. No

C. Unsure

CPAs & ADVISORS

Indications of a Hacker

Accounting anomalies?

Companies investigating hacks put too much emphasis on technology and too little on business analysis. Organizations should look closely into accounting anomalies as they could be indicators of a breach.

What we forget to do is to focus on the business transactions

- FBI concluded that Chinese hackers had penetrated a U.S. chemical company network using a phishing email and gained control of servers.
- Hackers were **intercepting inbound orders**, as well as **outbound e-mails** with price quotes and other terms.
- Tampered with the **ordering system for raw materials**, causing production delays, and made off with valuable research related to a line of environmental products.
- The likely beneficiary of all the malicious activity emerged, when a Chinese firm made a low-ball offer for the U.S. company after its performance began faltering as a result of the hack.

Take away: Look closely at each financial statement line item for anomalies and ask for professional help to investigate if something seems to be amiss.

Cybersecurity and Fraud

Jewish Federation of Greater Washington reports $7.5 million hack – Washington Post – September 2, 2020

"Members of the federation first discovered the hack Aug. 4, when its information-technology contractor detected suspicious activity in an employee's email account. They said authorities believe the hackers first gained access to its system in early summer."

https://www.fico.com/blogs/social-engineering-and-push-payment-fraud-who-should-pay

Cybersecurity and Fraud

Continued

Blackbaud Faces Class Action Lawsuit After Data Breach - The Nonprofit Times – August 27, 2020

"The suit stems from a data breach which happened on Feb. 7 and was not discovered by the company until May 14. Users were not notified until July, as reported exclusively by The NonProfit Times."

The incident was in the form of a ransomware attack in which hackers downloaded information and attempted to wrest control of Blackbaud's systems and data hosting operations."

Cybersecurity and Fraud

Continued

Phishing

- Use of email, phone, or text message to lure individuals into provide sensitive information
- Employees receive an average of approximately 4 phishing emails in a 5-day work week
- Nearly 1/3 of all breaches in 2019/2020 involve phishing
- An organization's biggest risk is its employees

https://blog.malwarebytes.com/101/2018/09/6-sure-signs-someone-is-phishing-you-besides-email/

Cybersecurity and Fraud

Continued

Ransomware

- Malware designed to deny access to a system or obtain sensitive data for the purpose of holding for ransom
- Typically spread through phishing emails or when visiting an infected website
- Increased over 97% in the past 2 years

https://www.newsweek.com/ransomware-attacks-rise-250-2017-us-wannacry-614034

Why Privacy is a Critical Concern

Definitions

What's the Difference?

Trust and Value

Reputation Risk

- Notifying donors, employees, students, government agencies
- Erosion of trust impacting recruitment, donations, and grants
- Personal value vs. legal requirement
    - Privacy is considered to be a right by many, similar to the US view of the "right of free speech"
    - High profile reputation risk – permeates all of society
    - Business imperative – branding opportunities

Cost of a breach or noncompliance

- Litigation, fines and penalties
- Distraction from mission

grf CPAs & ADVISORS

Is Your Organization Taking Privacy Seriously?

Questions to Ask

- Do you have a privacy policy?
- Are employees, donors, members and other stakeholders educated regarding your privacy policy?
- What personal information about donors, members, employees and other stakeholders does your organization collect and retain?
- What personal information does your organization really need and use in carrying out its functions, for example, in fundraising, marketing, and public relations activities? Is it disposed of after its intended use?
- What personal information is obtained from or disclosed to affiliates or third parties?
- What is the impact of United States privacy laws and regulations and/or international privacy requirements on your institution?
- How well does your policy address the privacy of personal information?

Assess (continued)

Example Formats of Private Data

Electronic documents

Paper documents

Information systems/databases

Storage media (e.g., disks, memory cards, etc.)

Information transmitted verbally

Email

Negative Media Attention

Pentagon Staff Hit by Major Data Breach

30,000 civilian and military personnel PII Compromised

"The department is continuing to gather additional information about the incident, which involves the potential compromise of personally identifiable information (PII) of DoD personnel maintained by a single commercial vendor that provided travel management services to the department," the statement noted. "This vendor was performing a small percentage of the overall travel management services of DoD."

https://www.infosecurity-magazine.com/news/pentagon-staff-hit-by-major-data/

Third Party Risk Management

Third Party Risk Management (TPRM)

- The process of analyzing and mitigating risks to your organization by parties OTHER than your own organization.
- Due Diligence is the process by which the vendor is reviewed to determine its suitability for a given task.
    - Due diligence is an ongoing activity, including review, monitoring, and management communication over the entire vendor lifecycle!

Why Implement TPRM?

- Reduce likelihood of:
  - data breach costs
  - operational failures
  - vendor bankruptcy
  - reputation damage

Pinpointing Third Party Risks

- Assess your current environment
- Develop a 3rd party framework based on your organizations context
- Develop a risk stratification guidelines to highlight risks by vendor
- Implement and conduct vendor assessments
- Establish a reporting process

Example Stratification

Vendor stratification - Example

- Tier 1 – Critical vendors (10%) – PII + critical systems
- Tier 2 – Major vendors (40%) – PII OR critical systems
- Tier 3 – Vendors (50%) – commodities/low risk purchases

Design

Third Party Due Diligence

Risk Assessment (Documentation, Categories of Risk,

Financial projections & review

Insurance Review

Legal Review

Vendor Audits and/or SOC reports

Background check

Legal Review of Contracts

At a minimum, third party contracts should address the following:

- Scope of arrangement, services offered and activities authorized;
- Responsibilities of all parties;
- Service level agreements addressing performance standards and measures;
- Performance reports and frequency of reporting;
- Penalties for lack of performance;

Legal Review of Contracts

- Ownership, control, maintenance and access to financial and operating records;
- Audit rights and requirements (including responsibility for payment);
- Data security and confidentiality (including testing and audit);
- Business resumption or contingency planning;
- Insurance;
- Compliance with regulatory requirements
- Dispute resolution, Default, termination and escape clauses.

Older Contracts Create the Following Risks

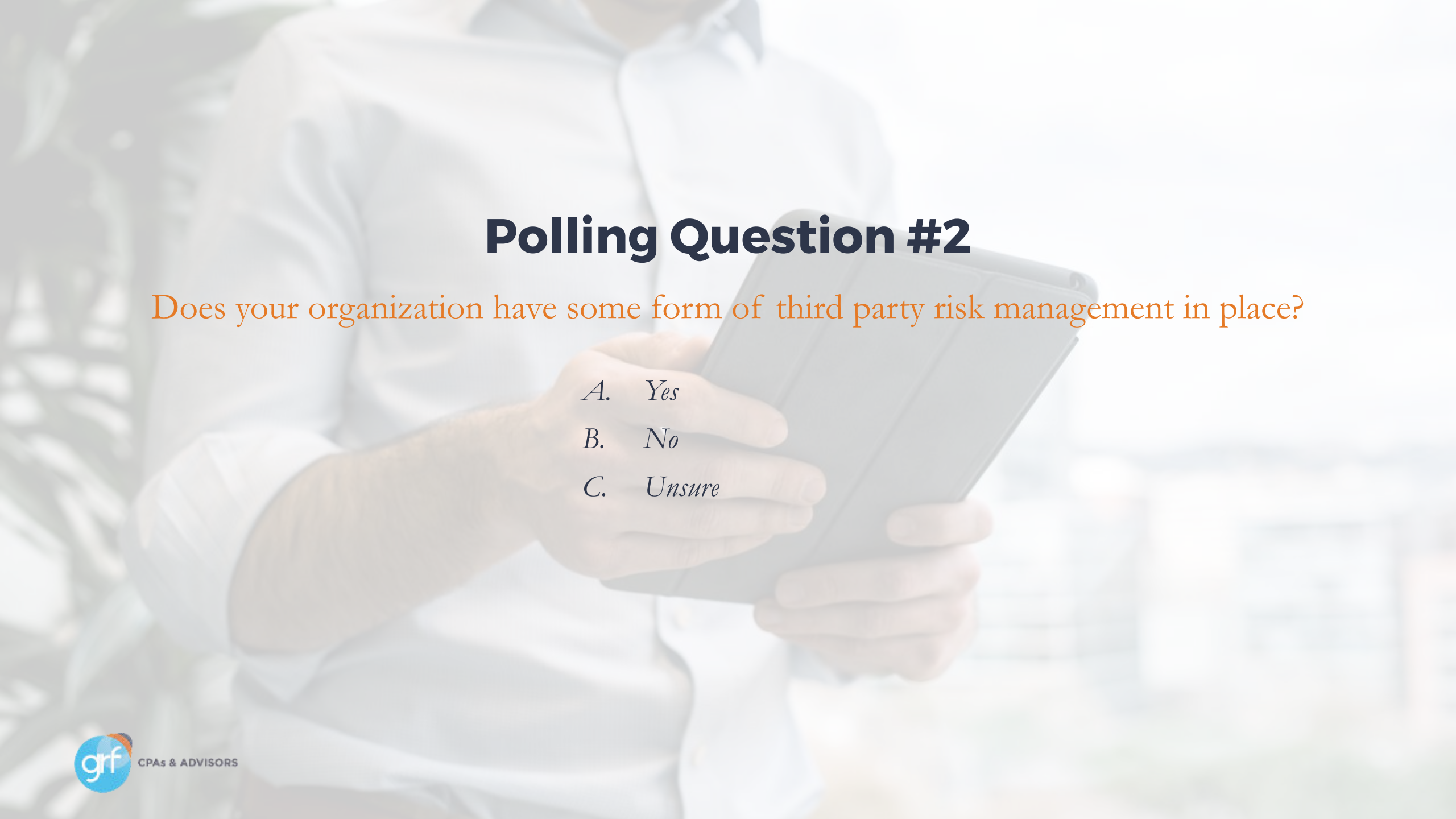
- the requirements for cyber technology become a ceiling and not a floor; that is the technology requirements prohibit the vendor from using modern technology
- there are no requirements, and little incentive, for the provider to adopt new technology that meets current threats;
- the requirements for privacy protection may be outdated and insufficient for compliance with current laws or soon to be adopted laws;
- cyber insurance is available, but provider's services fail to meet the threshold requirements established by insurance companies for the company to obtain and maintain coverage;
- database breaches may be covered but not ransomware and other new threats; and
- the IT contracts may not meet the governing regulatory requirements for companies in regulatory environments.

Identify High-Risk Cyber Activities

- Housing confidential data in a cloud-based system
- Housing or outsourcing confidential data offshore
- Outsourcing sensitive activities and/or a number of critical operations
- Using web-based services to conduct business transactions with customers
- Permitting access of confidential data to third-party providers

Privacy and Data Breach

- Include language in contract that vendor will comply with data/privacy laws, rules, and regulations
- Reporting obligations and remedies in event of security breach
- Have a plan for how a security breach will be handled
- Is there built in redundancy from multiple locations
- Do they provide alternative methods of access?
- Consider cyber liability insurance



Polling Question #2

Does your organization have some form of third party risk management in place?

A. Yes

B. No

C. Unsure

grf CPAs & ADVISORS

Service Level Agreements (SLA)

The Service Level Agreement contains the contractually relevant data for an outsourced Service:

- Contact persons
- Contract duration
- Service description
- Procedures for requesting service
- Responsibilities
- Quality assurance and Service Level Reporting

Service Level Agreement (SLA) Considerations

- How are service levels and availability measured, monitored & reported?
- How are SLA issues resolved?
- Incident reporting systems, access and usage reports
- Notifications of scheduled downtime

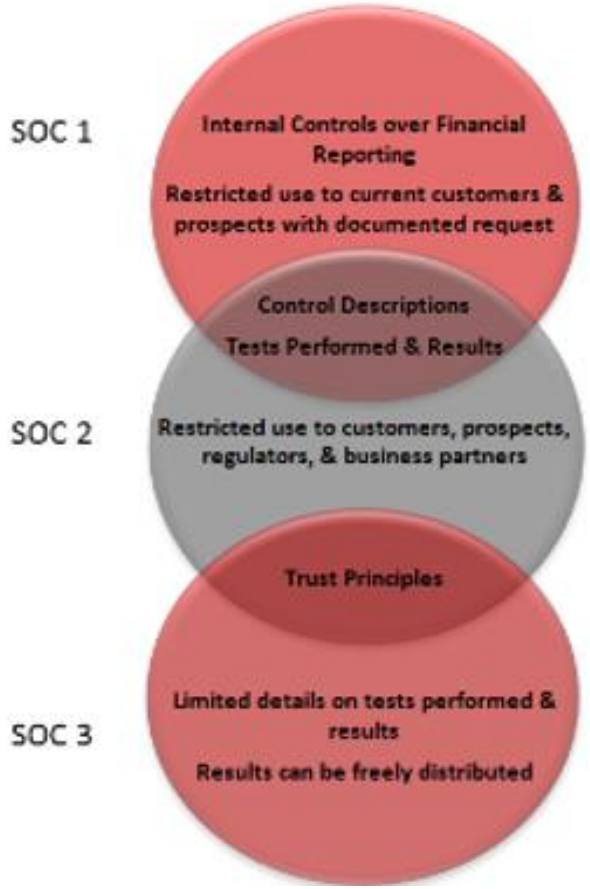
Procurement Process

- Competition is good. Don't decide on a vendor too early in the process.
- Best price does not equal best vendor, focus on meeting your requirements

Audits

- Request Audit your own TPRM process (internal audit)
- Request audits of Vendors (i.e. SOC Audits)

Not just a one time deal…must audit again, and again!



Developing a Third-Party Framework

In general, best practices for any risk management framework include:

•An inventory all third-party vendors your organization has a relationship with (you may need to see who you are paying to find out who they are!);

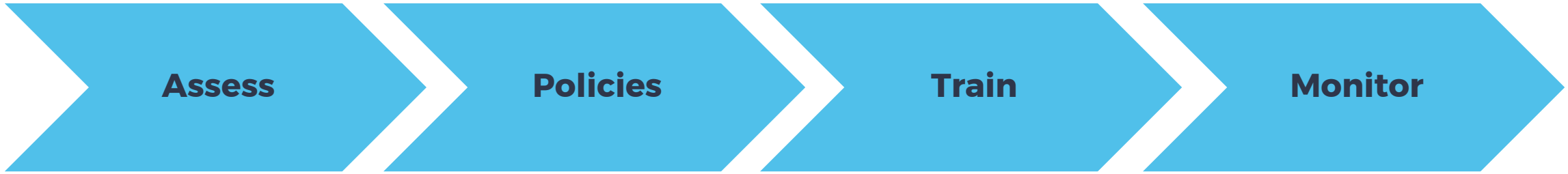
•An assessment of possible cybersecurity risk exposure from all third-parties;

•A system to assess vendors and set a minimum acceptable standards based on the risk assessment guides (as applicable to the specific tiered vendor); and

•Development of contingency plans for when a third-party is deemed below quality or a data breach occurs.

Next Steps - IT Strategy

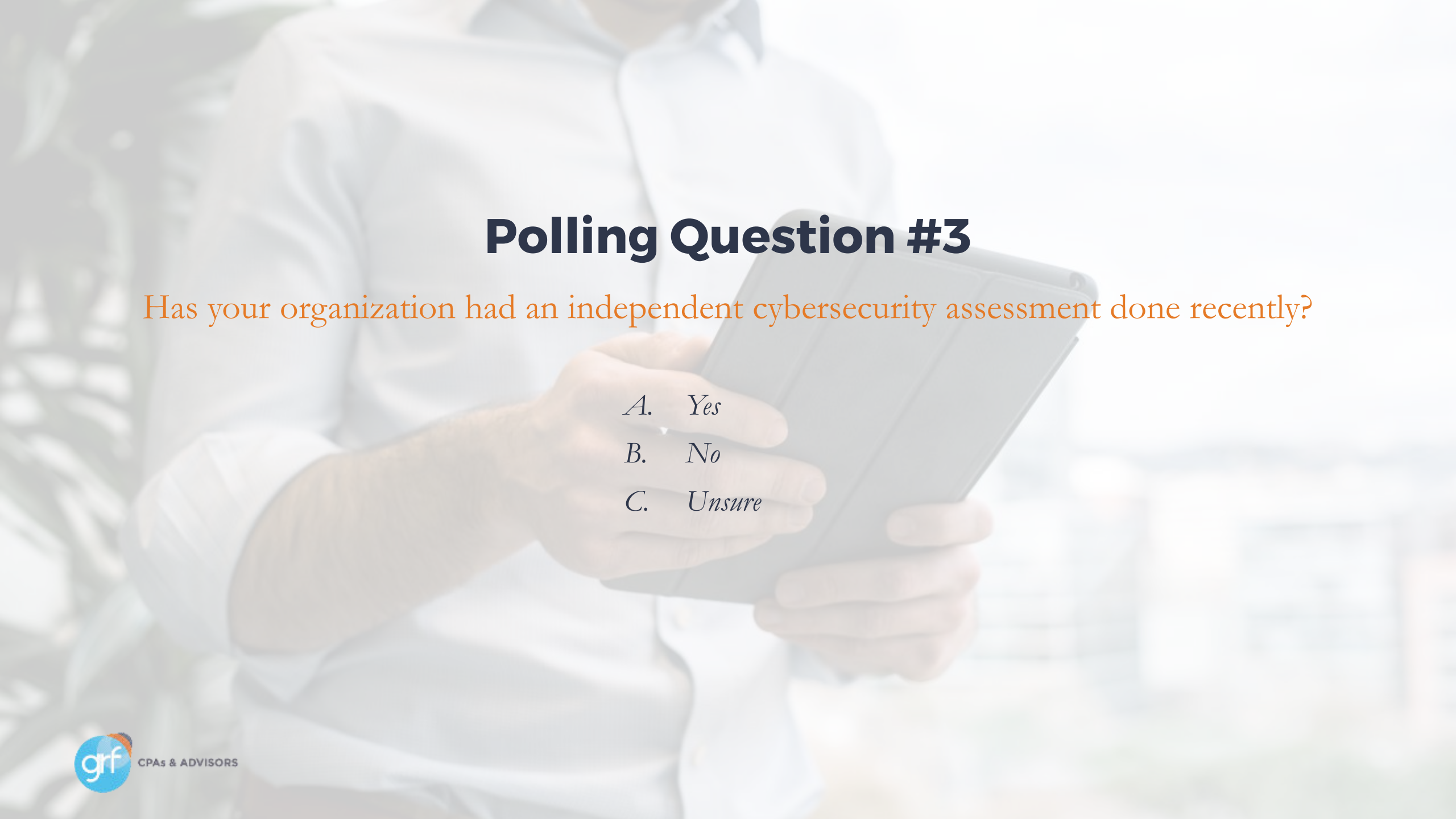
IT Strategy



IT Strategy

Proper Controls

- Implement proper controls – need to understand threats
    - Patch applications
    - Consistency in the application of controls
    - Automate where possible
    - Physical security
    - Software security
    - Manage vendor risks
    - CISecurity.org – a non-profit that provides great tools for control implementation



Polling Question #3

Has your organization had an independent cybersecurity assessment done recently?

A. Yes

B. No

C. Unsure

grf CPAs & ADVISORS

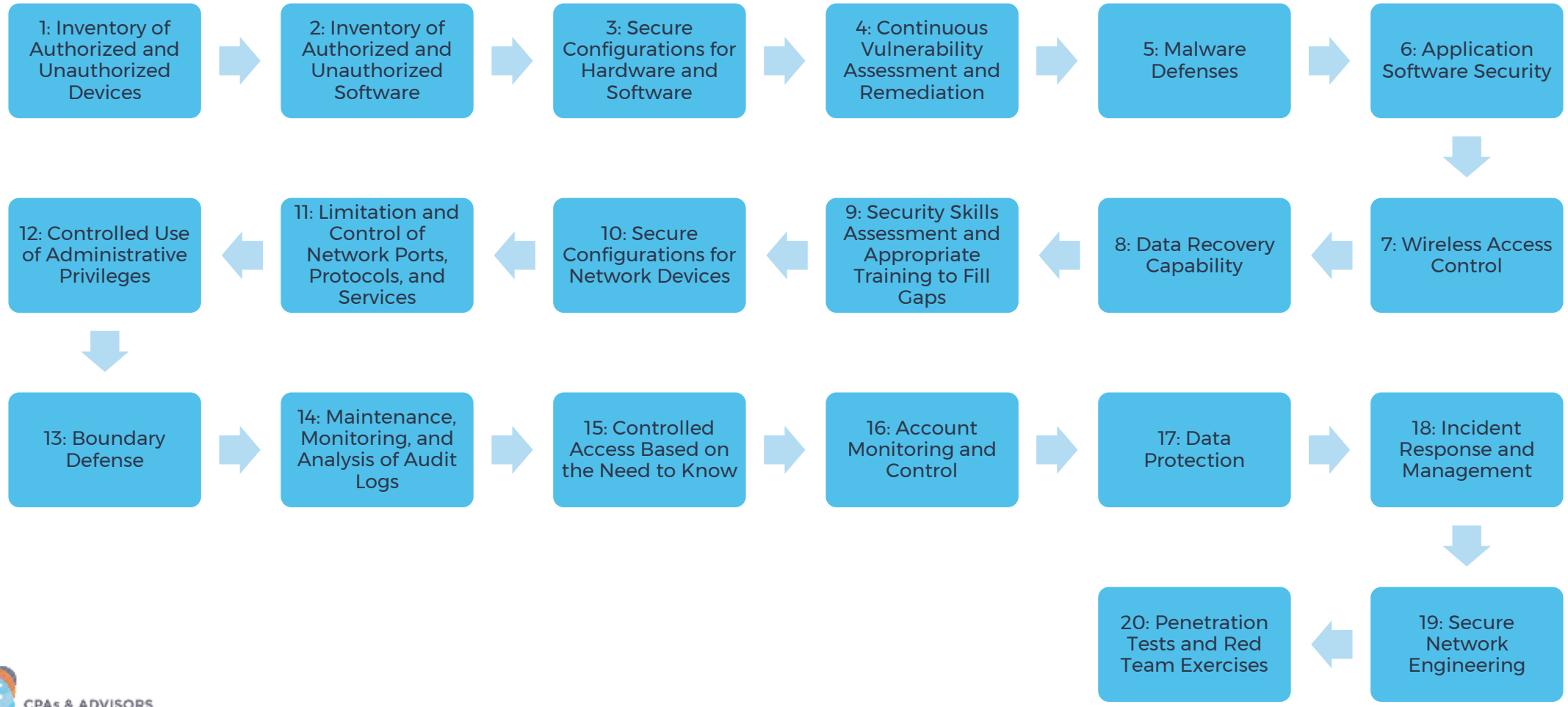
IT Strategy

Useful Technologies

- Useful technologies
  - Cyber Scorecard
  - Firewall
  - IDS/IPS
  - Anti-virus and malware software
  - Multifactor Authentication
  - Spam filter
  - User security training/phishing campaigns
  - Content Filter
  - DNS Filtering
  - Encryption
  - Backups following 3-2-1 rule
  - Remote management
  - Password policy enforcement
  - AI and Machine Learning (i.e. MindBridge)
  - Positive Pay and ACH-block
  - B2B Integration

Best Practice Benchmarking

SANS 20 Critical Security Controls

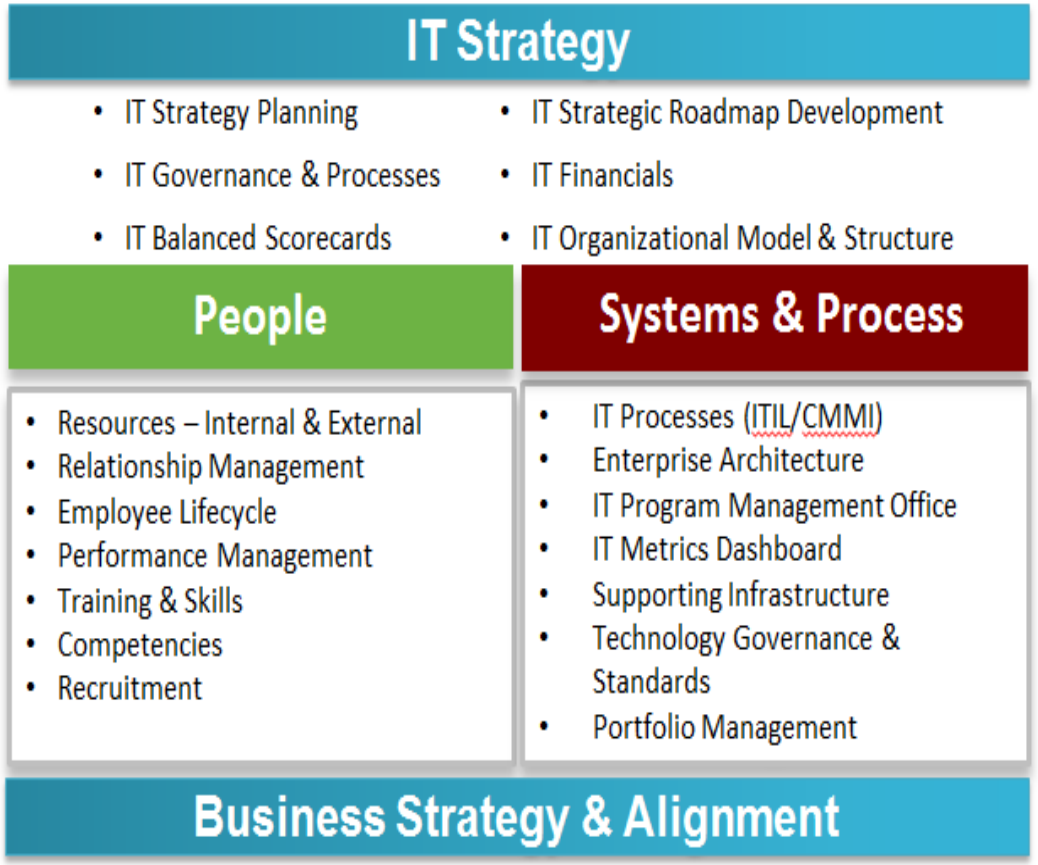


grf CPAs & ADVISORS

IT Strategy

Summary: What to do to best protect your organization

- Organization
  - Roles & Responsibilities
  - Know your data
- Monitor and Enforce
  - Encourage Communication
  - Log, document, review
  - Manage Employee Error
- Policies and Procedures
  - Info. Sec., privacy, retention Business continuity, etc.
  - Disseminate throughout org.
- Processes
  - Determine Systems tied to Data
  - Technologies
  - Collaboration
  - Training



http://www.jwaffinityit.com/our-services/it-strategy-planning-consulting

Questions?

Contact Us

CPAs & ADVISORS

Maryland | DC | New York

877-437-4771 | www.grfcpa.com

Melissa Musser,
CPA, CITP, CISA

mmusser@grfcpa.com
301-951-9090

Ricardo Trujillo,
CPA, CITP, CISA

rtrujillo@grfcpa.com
301-951-9090

Disclaimer

This webinar is not intended as, and should not be taken as, financial, tax, accounting, legal, consulting or any other type of advice. While we use reasonable efforts to furnish accurate and up-to-date information, we do not warrant that any information contained in or made available in this webinar is accurate, complete, reliable, current or error-free. We assume no liability or responsibility for any errors or omissions in the content of this webinar.

The use of the information provided in this webinar does not establish any contractual or other form of client engagement between GRF CPAs & Advisors and the reader or user. Any U.S. federal tax advice contained in this webinar is not intended to be used for the purpose of avoiding penalties under U.S. federal tax law. Readers and users of this webinar information are advised not to act upon this information without seeking the service of a professional accountant.