Welcome to Manage Risk to Your Organization with Effective Data Security

Presented by: Gelman, Rosenberg & Freedman CPAs

The program will start promptly at 11:00 AM ET

Please note: Use the "Q&A" function to speak with the administrator if you experience any technical issues while logging into WebEx. For the best audio quality, please call-in by phone vs. connecting via your computer.

Call: +1-415-655-0002 | Access code/event number: 623 603 000

Housekeeping

General Information/Technical Questions

We strongly recommend that you connect by phone instead of your computer for the best audio quality. Call 415-655-0002. The event number is 623 603 000 and the password is DataRisk.

Please use the "Q&A" function for any technical questions, or you may contact WebEx with the event information above at 866-229-3239.

This presentation will be recorded and made available to download at www.grfcpa.com/webinars/.

Housekeeping

CPE Credit

- Important: Three (3) CPE words will be provided during the presentation. Please write them down – we will not provide them again via WebEx or email (no exceptions).
- Please complete the electronic survey that will appear automatically at the end of the webinar. Turn off your pop-up blocker (leaving it on could block the survey).
- 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.
- Technical questions about the survey can be addressed to Dominic Acosta at dacota@grfcpa.com.

Housekeeping

Webinar Objectives

Learning Objective *To better understand data security and risk management*	**Instructional Delivery Methods** *Group Internet-based*
Recommended CPE *1.0 CPE Credit*	**Recommended Fields of Study** *Audit*
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 *Gelman, Rosenberg & Freedman CPAs is committed to our seminar 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.*	

Manage Risk to Your Organization with Effective Data Security

August 15, 2018

GELMAN, ROSENBERG & FREEDMAN
CERTIFIED PUBLIC ACCOUNTANTS

Presenters

Ricardo Trujillo, CPA, CITP, CISA
Nonprofit Audit Partner

Mac Lillard, CPA, CISA, CITP, CFE
Senior Auditor

Moderator

Laura Malcom, CPA
Nonprofit Audit Manager

Our Team

Meet Your Instructors

Ricardo Trujillo, CPA, CITP, CISA

Nonprofit Audit Partner

Mac Lillard, CPA, CISA, CITP, CFE

Senior Auditor

Anatomy of an IoT Attack

https://www.youtube.com/watch?v=GvLnb4YQHho

FBI - 2017 Internet Crime Report

https://pdf.ic3.gov/2017_IC3Report.pdf

Agenda

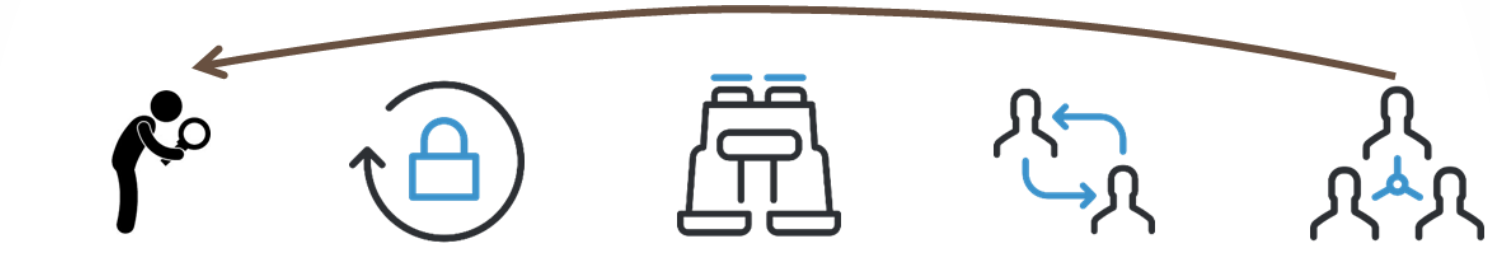
- Implementing security controls
- Technology assets inventories
- Cyber insurance
- Risk from 3rd party providers
- Security awareness training
- Payment Card Industry Data Security Standard– PCI DSS
- General Data Protection Regulation - GDPR

Implementing Security 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

Implementing Security Controls



Identify

- Training and awareness
- Methodology and practices for incident discovery
- Reporting steps defined for any type of incident
- Forensic team is available

Protect

- Incident response team members - roles and responsibilities clearly defined
- Detection mechanisms tested and operational
- Communication Plan by incident category
- Triage steps for any threat leading to execution

Detect

- Entry points from detection or start of incident
- Determine threat vectors and typical incidents
- Detect mechanisms / discover intrusion

Respond

- Reporting needs when a potential threat is detected
  - Trouble ticket(s)
  - Affected infrastructure(s)
  - Necessary data and contact points
  - Incident categories
- Eradication procedures
- Containment procedures
- Recovery Steps

Recover

- Plans to restore any lost capabilities or services
- Lessons learned
- Plan review and revision

Technology Asset Inventories

Managing and monitoring your IT assets

- Hardware, software, platforms, applications, databases, etc.
- Create risk schema
  - Critical systems
  - Effect of failure
- Monitoring and oversight
  - Patching
  - Updates
  - Performance evaluation

http://datasystemsincny.com/it.html

Technology Asset Inventories

(continued)

- Policies and procedures
  - Periodic review of listing
  - Logging crashes/failures
  - Disposition plan
- Keep hardware up-to-date
  - Process for upgrading
  - Budget for IT projects

http://datasystemsincny.com/it.html

Poll Question #1

Does your organization have a technology asset inventory?

A) Yes
B) No
C) I don't know

Cyber Insurance

Risk Mitigation

- What protection do you have through your 3rd party providers?
- What kind of data does your organization store?
- Cost vs. Benefit of cyber insurance

https://www.travelers.com/cyber-insurance/how-does-cyber-insurance-work

Risk from 3rd Party Providers

Are your vendors secure?

- Critical vendors
  - Risk-rated
  - Risk-managed
- Vendor Management program
  - Risk assessment
  - Due diligence
  - Contract structuring
  - Oversight

https://www.lexisnexis.com/en-us/products/lexis-diligence/ctr/9-steps-to-effective-third-party-due-diligence.page

Risk from 3rd Party Providers

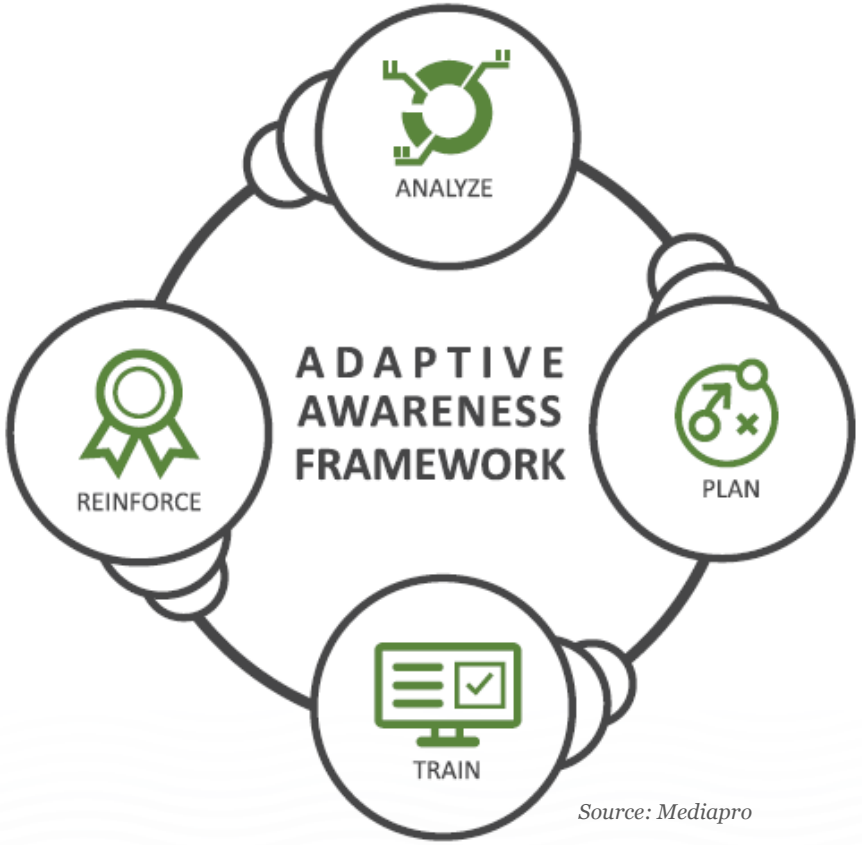
(continued)

- Procurement procedures
  - Bid solicitation
  - Evaluation of competency
  - Lowest cost provider

- Business continuity and contingency plans
  - Identify critical vendors and outsourced services
  - Effect of breach/crash
  - Minimum allowable downtime

http://www.supplychain247.com/article/2015_top_50_global_domestic_third_party_logistics_providers

Security Awareness Training



Source: Mediapro

Poll Question #2

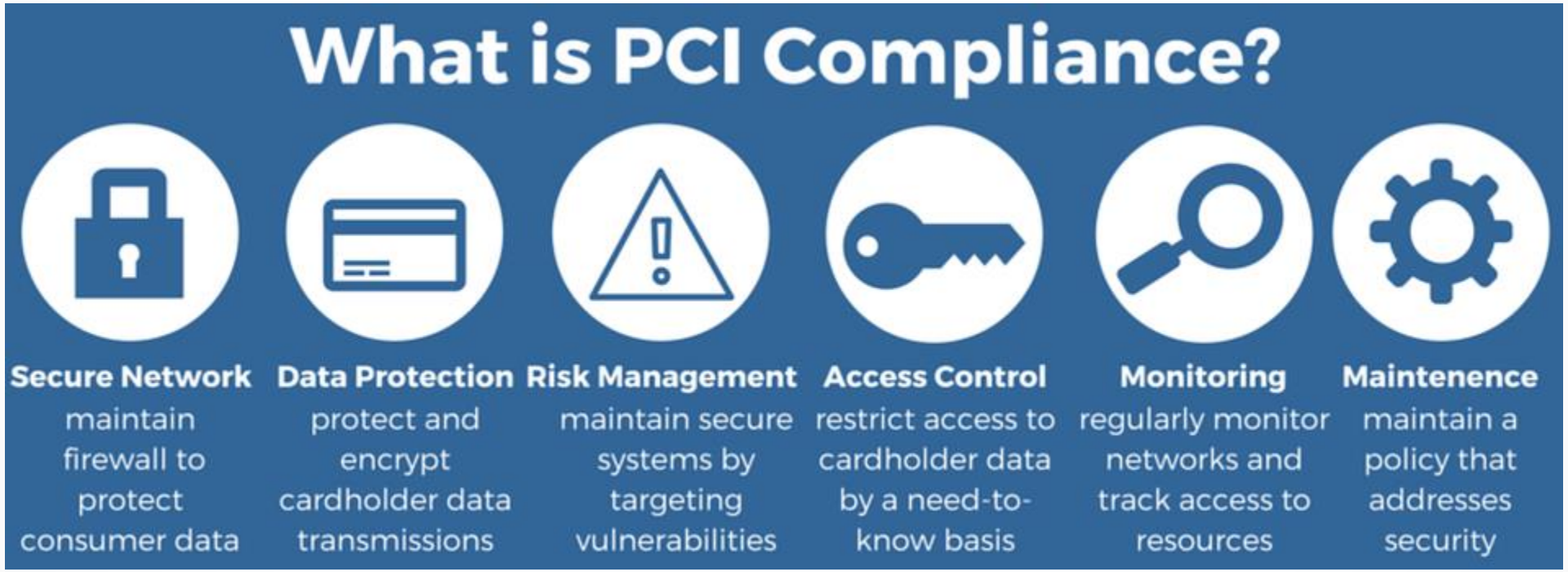
Does your organization have a formal security awareness training program in place?

A) Yes
B) No
C) I don't know

Payment Card Industry Data Security Standard – PCI DSS

- What is PCI?
- To whom does PCI DSS apply?
- Different levels based on number of credit card transactions – Levels 1 - 4
- What are the penalties for non-compliance?
- 6 goals
- 12 requirements

Payment Card Industry Data Security Standard – PCI DSS



Poll Question #3

Has your organization gone through an IT risk assessment?

A) Yes
B) No
C) I don't know

General Data Protection Regulation

What to know

- Became effective May 25, 2018
- Sets guidelines for the collection and processing of personally identifiable information for *individuals within the European Union*
- Emphasis on data storage/management
- Notification requirement

https://www.endpointprotector.com/blog/top-5-ways-dlp-can-help-with-gdpr-compliance/

General Data Protection Regulation

(continued)

- Does this apply to your organization?
  - Overseas operations
  - Donors
- Revenue-based fines
  - Up to 20M Euros of 4 percent of annual revenue
- Cost vs benefit
  - How relevant is GDPR to you?

https://www.cyberdb.co/will-u-s-adopt-similar-gdpr-privacy-concerns/

Questions?

We'd like to hear from you!

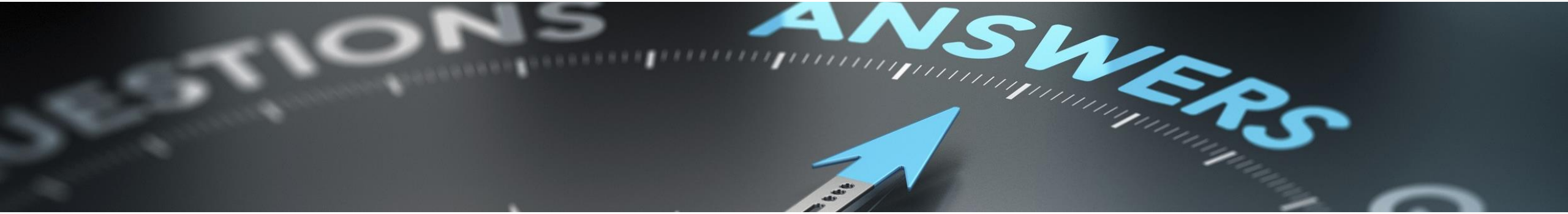
Join us again

September 13, 2018, 11:00am – 12:00pm

Topic 606 - Revenue from Contracts with Customers (webinar)

Registration will be opening shortly at www.grfcpa.com/resources/events

Get In Touch



GELMAN, ROSENBERG & FREEDMAN
CERTIFIED PUBLIC ACCOUNTANTS

4550 Montgomery Avenue, Suite 650N

Bethesda, MD 20814

(301) 951-9090

www.grfcpa.com

twitter.com/grfcpas

facebook.com/grfcpas

instagram.com/grfcpas/

linkedin.com/company/gelman-rosenberg-&-freedman-cpas

Ricardo Trujillo, CPA, CITP, CISA

rtrujillo@grfcpa.com

(301) 951-9090

Mackenzie Lillard, CPA, CISA, CITP, CFE

mlillard@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 Gelman, Rosenberg & Freedman P.C. 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.