Elements of a Successful Cybersecurity Program

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Create Opportunities

Disclaimers

The information contained herein is general in nature and is not intended, and should not be construed, as legal, accounting, or tax advice or opinion provided by CliftonLarsonAllen LLP to the user. The user also is cautioned that this material may not be applicable to, or suitable for, the user's specific circumstances or needs, and may require consideration of non-tax and other tax factors if any action is to be contemplated. The user should contact his or her CliftonLarsonAllen LLP or other tax professional prior to taking any action based upon this information. CliftonLarsonAllen LLP assumes no obligation to inform the user of any changes in tax laws or other factors that could affect the information contained herein.

Housekeeping

- If you are experiencing technical difficulties, please dial: **800-422-3623**.
- **Q&A session will be held at the end of the presentation.**
  - Your questions can be submitted via the **Questions Function at any time during the presentation.**
- The **PowerPoint presentation**, as well as the **webinar recording**, will be sent to you within the next 10 business days.
- For future webinar invitations, subscribe at CLAconnect.com/subscribe.
- Please complete our online survey.

CPE Requirements

- Answer the polling questions
- Remain logged in for at least 50 minutes
- If you are participating in a group, complete the CPE sign-in sheet and return within two business days
  - Contact webmaster@CLAconnect.com
- Allow four weeks for receipt of your certificate; it will be sent to you via email from certificates@CLAconnect.com.

** This webinar, once recorded, has not been developed into a self study course. Therefore, watching the recording will not qualify for CPE credit.*

Learning Objectives

At the end of this session, you will be able to:

- Recognize new and emerging cyber threats through review of case studies from actual breaches
- Describe strategies to mitigate the risks of ransomware and other cyber attacks
- Define key controls to mitigate cybersecurity risks and comply with GLBA requirements.

C:\whoami

- Randy Romes
  - “Professional Student”
  - Science Teacher/Self Taught Computer Guy
  - IT Consultant - Project Manager – IT Staff/Help Desk – Hacker
  - Principal in Charge of Cybersecurity Practice
  - Assistant Scout Master (Boy Scouts)
- Kadian Douglas
  - Manager
  - More than eleven years of experience in the industry
  - Provides information security services for higher education, governmental entities, and financial institutions
  - Experience in risk assessments, IT general controls review, GLBA assessments and internal auditing outsourcing for financial and operational audits

Cyber Security Services

- Cyber security assessment and consulting offered as specialized service for over 20 years
- Penetration Testing and Vulnerability Assessment
  - Black Box, Red Team, and Collaborative Assessments
- IT/Cyber security risk assessments
- IT audit and compliance
  - GLBA/FFIEC, HIPPA/HITRUST, PCI-DSS, NIST, NERC/CIP, CJIS, etc…
- Incident response and forensics
- Security awareness training
- Independent security consulting
  - Internal audit support

Sun Tzu:
“Know your enemy and know yourself and you can fight a hundred battles without disaster.”

The Current State of Cybercrime

Cyber Fraud Themes – “Know Thy Enemy”

- Hackers have “monetized” their activity
  - More sophisticated hacking - more “hands-on” effort
  - Cybercrime as an industry
- Phishing is a root cause behind the majority of cyber fraud and hacking attacks
- Black market economy to support cyber fraud
  - Business models and specialization

- Most common cyber fraud scenarios we see affecting our clients
  - Theft of PII and PFI
    - ◊ W2/Payroll/Benefit info
  - Theft of credit card information
  - Theft of Credentials and Account take overs
  - Ransomware and Interference w/ Operations

Firewalls Are Hard to Break People on the Other Hand…

Social Engineering Improves the Hackers Odds

What Makes Social Engineering Successful?

"Amateurs hack systems, professionals hack people."

Bruce Schneier

- Social Engineering relies on the following:
- The appearance of "authority"
- People want to avoid inconvenience
- Timing, timing, timing…

Pre-text Phone Calls (Phishing by phone)

- “Hi, this is Randy from Comcast Business users support. I am working with Dave, and I need your help…”
  - Name dropping → Establish a rapport
  - Ask for help
  - Inject some techno-babble

- “I need you to visit the Microsoft Update site to download and install a security patch. Do you have 3 minutes to help me out?”

- Schemes result in losses from fraudulent ACH transactions….

Email Phishing Is a Root Cause Underlying Most Breaches

Two Minutes of Inconvenience

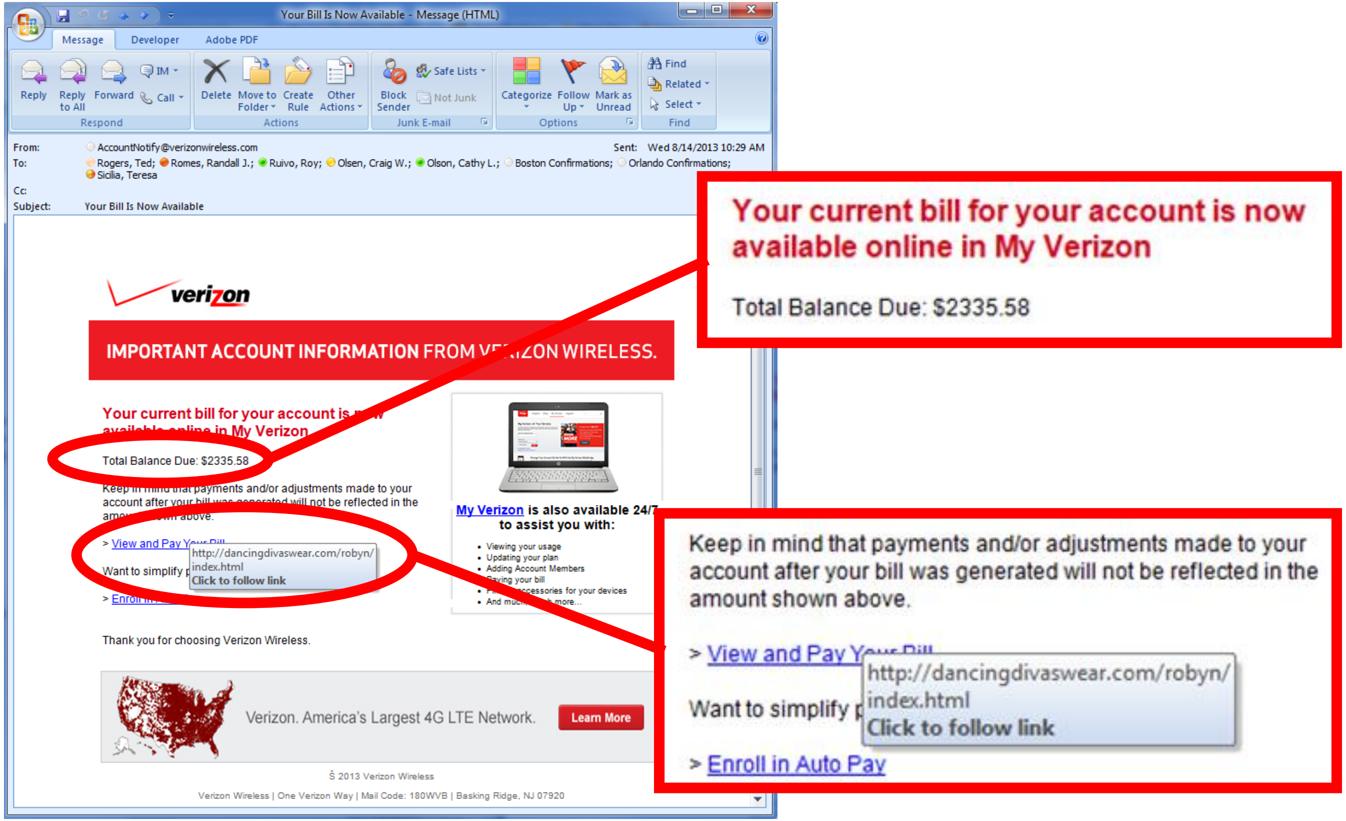
Email Phishing Objectives

- Goals:
  - Convince target to do something
  - Gain access to:
    - ◊ Business email accounts (“BEC” or “Business Email Compromise”)
    - ◊ Financial accounts (payroll, AR/AP, e-Treasury management, etc.)
    - ◊ Network resources and confidential/sensitive information
    - ◊ Personal email accounts, cloud accounts, social media accounts

- Malware infection via:
  - Links to malicious website containing drive-by malware
  - Email attachments
    - ◊ ZIP, RAR, HTA, JAR, etc.…
    - ◊ Office documents with MACROS and/or PowerShell script

“The identity I stole was a fake!
Boy, you just can’t trust people these days!”

Phishing?



From: AccountNotify@verizonwireless.com

Sent: Wed 8/14/2013 10:29 AM

To: Rogers, Ted; Romes, Randall J.; Ruivo, Roy; Olsen, Craig W.; Olson, Cathy L.; Boston Confirmations; Orlando Confirmations; Sicilia, Teresa

Cc:

Subject: Your Bill Is Now Available

verizon

IMPORTANT ACCOUNT INFORMATION FROM VERIZON WIRELESS.

Your current bill for your account is now available online in My Verizon

Total Balance Due: $2335.58

Keep in mind that payments and/or adjustments made to your account after your bill was generated will not be reflected in the amount shown above.

> View and Pay Your Bill

http://dancingdivaswear.com/robyn/index.html
Click to follow link

Want to simplify p

> Enroll in Auto Pay

Thank you for choosing Verizon Wireless.

My Verizon is also available 24/7 to assist you with:

- Viewing your usage
- Updating your plan
- Adding Account Members
- Paying your bill
- Purchasing accessories for your devices
- And much, much more...

Verizon. America's Largest 4G LTE Network. Learn More

Š 2013 Verizon Wireless

Verizon Wireless | One Verizon Way | Mail Code: 180WVB | Basking Ridge, NJ 07920

Your current bill for your account is now available online in My Verizon

Total Balance Due: $2335.58

Keep in mind that payments and/or adjustments made to your account after your bill was generated will not be reflected in the amount shown above.

> View and Pay Your Bill

http://dancingdivaswear.com/robyn/index.html
Click to follow link

Want to simplify p

> Enroll in Auto Pay

Payment Fraud

Impersonation and Persuasion

Payment Fraud – Account Take Overs

- Most organizations and individuals perform payments electronically
  - Wire transfers & ACH payments
  - Online banking
- Corporate Account Take Over (CATO)
  - Compromise accounts/credentials that can move money
- Persuasion Attacks
  - Convince others to send money

Persuasion Attacks

CEO asks the accountant…

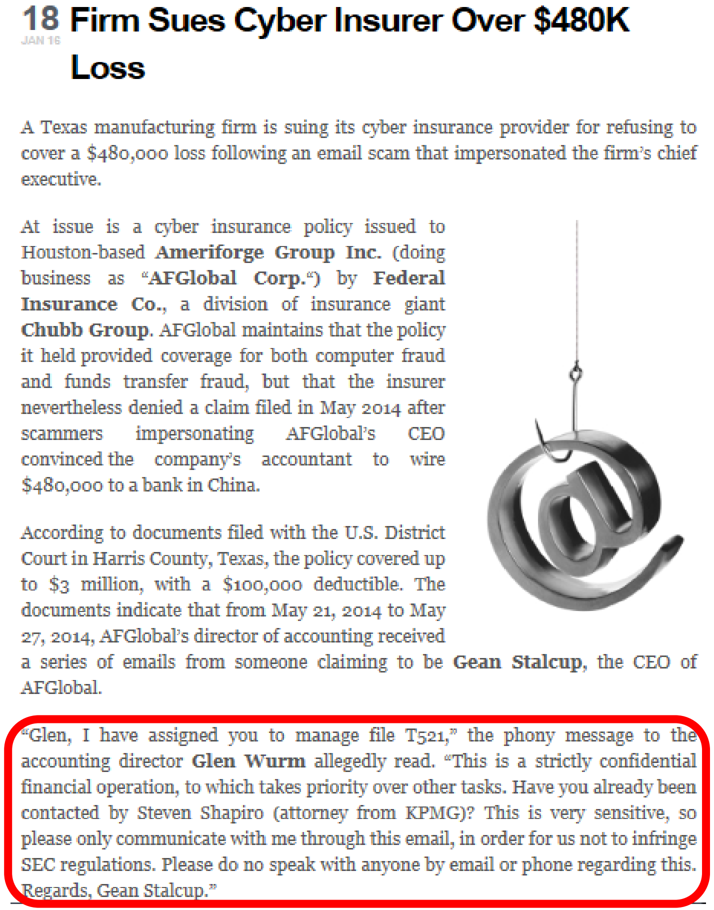
Common mistakes

1. Use of private email
2. “Don’t tell anyone”

KrebsonSecurity

In-depth security news and investigation

- https://krebsonsecurity.com/tag/bec/



18 JAN 16 **Firm Sues Cyber Insurer Over $480K Loss**

A Texas manufacturing firm is suing its cyber insurance provider for refusing to cover a $480,000 loss following an email scam that impersonated the firm’s chief executive.

At issue is a cyber insurance policy issued to Houston-based **Ameriforge Group Inc.** (doing business as “**AFGlobal Corp.**“) by **Federal Insurance Co.**, a division of insurance giant **Chubb Group**. AFGlobal maintains that the policy it held provided coverage for both computer fraud and funds transfer fraud, but that the insurer nevertheless denied a claim filed in May 2014 after scammers impersonating AFGlobal’s CEO convinced the company’s accountant to wire $480,000 to a bank in China.

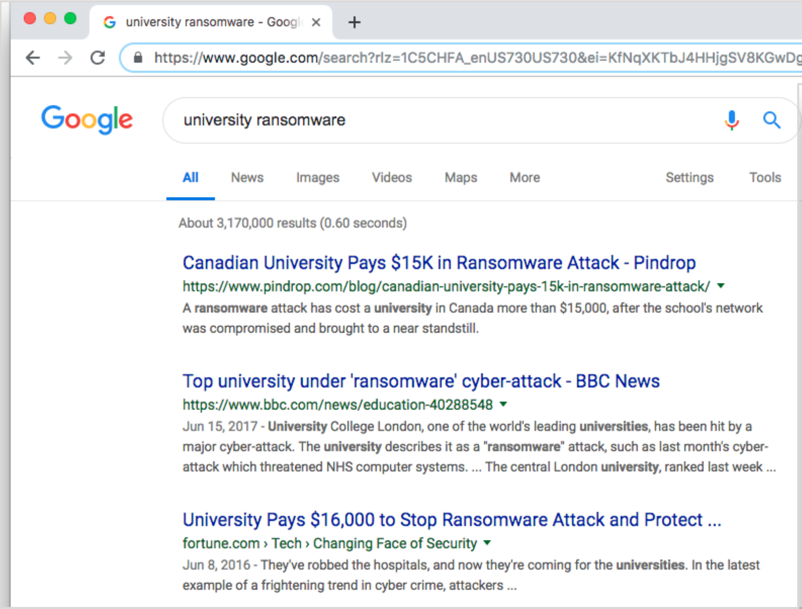
According to documents filed with the U.S. District Court in Harris County, Texas, the policy covered up to $3 million, with a $100,000 deductible. The documents indicate that from May 21, 2014 to May 27, 2014, AFGlobal’s director of accounting received a series of emails from someone claiming to be **Gean Stalcup**, the CEO of AFGlobal.

“Glen, I have assigned you to manage file T521,” the phony message to the accounting director **Glen Wurm** allegedly read. “This is a strictly confidential financial operation, to which takes priority over other tasks. Have you already been contacted by Steven Shapiro (attorney from KPMG)? This is very sensitive, so please only communicate with me through this email, in order for us not to infringe SEC regulations. Please do no speak with anyone by email or phone regarding this. Regards, Gean Stalcup.”

Ransomware

Would you like your pictures back?

Ransomware



university ransomware - Googl
https://www.google.com/search?rlz=1C5CHFA_enUS730US730&ei=KfNqXKTbJ4HHjgSV8KGwDg&q=univer
Google
All
News
Images
Videos
Maps
More
Settings
Tools

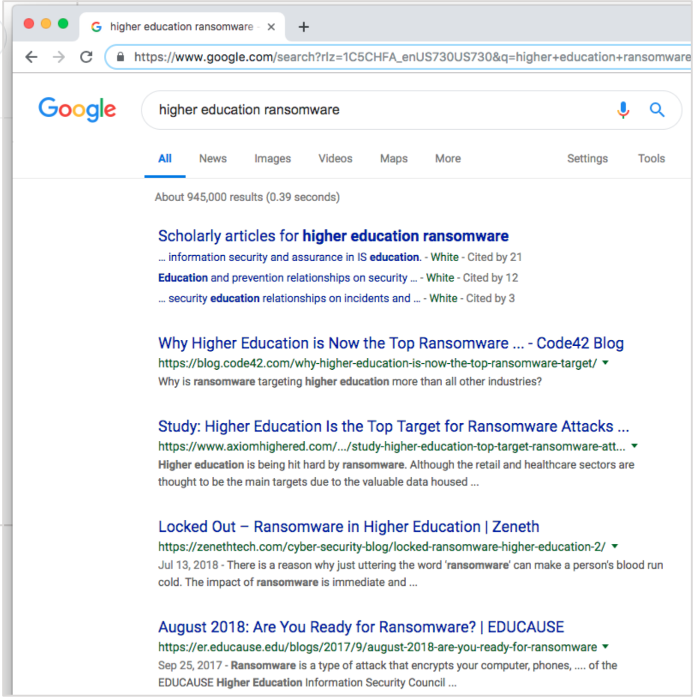
university ransomware

About 3,170,000 results (0.60 seconds)

Canadian University Pays $15K in Ransomware Attack - Pindrop
https://www.pindrop.com/blog/canadian-university-pays-15k-in-ransomware-attack/ ▾
A **ransomware** attack has cost a **university** in Canada more than $15,000, after the school's network was compromised and brought to a near standstill.

Top university under 'ransomware' cyber-attack - BBC News
https://www.bbc.com/news/education-40288548 ▾
Jun 15, 2017 - **University** College London, one of the world's leading **universities**, has been hit by a major cyber-attack. The **university** describes it as a "**ransomware**" attack, such as last month's cyber-attack which threatened NHS computer systems. ... The central London **university**, ranked last week ...

University Pays $16,000 to Stop Ransomware Attack and Protect ...
fortune.com › Tech › Changing Face of Security ▾
Jun 8, 2016 - They've robbed the hospitals, and now they're coming for the **universities**. In the latest example of a frightening trend in cyber crime, attackers ...



higher education ransomware
https://www.google.com/search?rlz=1C5CHFA_enUS730US730&q=higher+education+ransomware
Google
All
News
Images
Videos
Maps
More
Settings
Tools

higher education ransomware

About 945,000 results (0.39 seconds)

Scholarly articles for **higher education ransomware**
... information security and assurance in IS **education**. - White - Cited by 21
Education and prevention relationships on security ... - White - Cited by 12
... security **education** relationships on incidents and ... - White - Cited by 3

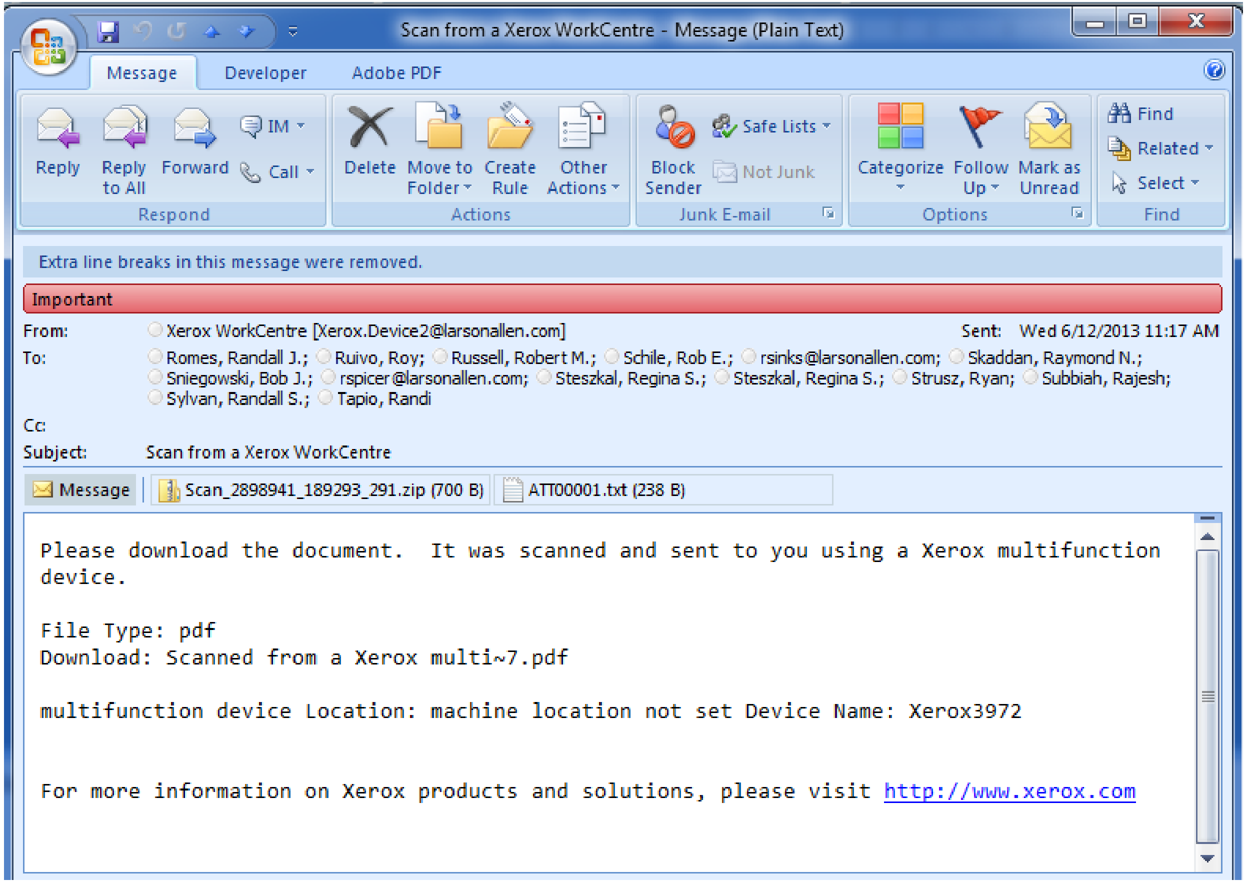
Why Higher Education is Now the Top Ransomware ... - Code42 Blog
https://blog.code42.com/why-higher-education-is-now-the-top-ransomware-target/ ▾
Why is **ransomware** targeting **higher education** more than all other industries?

Study: Higher Education Is the Top Target for Ransomware Attacks ...
https://www.axiomhighered.com/.../study-higher-education-top-target-ransomware-att... ▾
Higher education is being hit hard by **ransomware**. Although the retail and healthcare sectors are thought to be the main targets due to the valuable data housed ...

Locked Out – Ransomware in Higher Education | Zeneth
https://zenethtech.com/cyber-security-blog/locked-ransomware-higher-education-2/ ▾
Jul 13, 2018 - There is a reason why just uttering the word '**ransomware**' can make a person's blood run cold. The impact of **ransomware** is immediate and ...

August 2018: Are You Ready for Ransomware? | EDUCAUSE
https://er.educause.edu/blogs/2017/9/august-2018-are-you-ready-for-ransomware ▾
Sep 25, 2017 - **Ransomware** is a type of attack that encrypts your computer, phones, ... of the EDUCAUSE **Higher Education** Information Security Council ...

Ransomware



Extra line breaks in this message were removed.

Important

From: Xerox WorkCentre [Xerox.Device2@larsonallen.com]

Sent: Wed 6/12/2013 11:17 AM

To: Romes, Randall J.; Ruivo, Roy; Russell, Robert M.; Schile, Rob E.; rsinks@larsonallen.com; Skaddan, Raymond N.; Sniegowski, Bob J.; rspicer@larsonallen.com; Steszkal, Regina S.; Steszkal, Regina S.; Strusz, Ryan; Subbiah, Rajesh; Sylvan, Randall S.; Tapio, Randi

Cc:

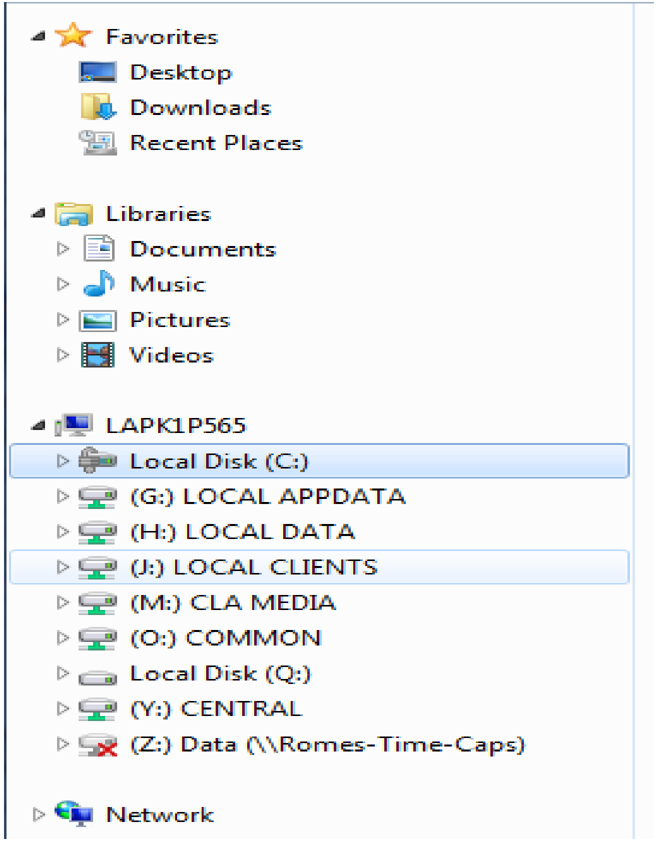
Subject: Scan from a Xerox WorkCentre

Scan_2898941_189293_291.zip (700 B) ATT00001.txt (238 B)

```
Please download the document.  It was scanned and sent to you using a Xerox multifunction
device.

File Type: pdf
Download: Scanned from a Xerox multi~7.pdf

multifunction device Location: machine location not set Device Name: Xerox3972


For more information on Xerox products and solutions, please visit http://www.xerox.com
```

Ransomware

- Malware encrypts everything it can interact with


Favorites
Desktop
Downloads
Recent Places

Libraries
Documents
Music
Pictures
Videos

LAPK1P565
Local Disk (C:)
(G:) LOCAL APPDATA
(H:) LOCAL DATA
(J:) LOCAL CLIENTS
(M:) CLA MEDIA
(O:) COMMON
Local Disk (Q:)
(Y:) CENTRAL
(Z:) Data (\\Romes-Time-Caps)

Network

Ransomware Defensive Strategies

1. Filtering capabilities

2. Users that are aware and savvy

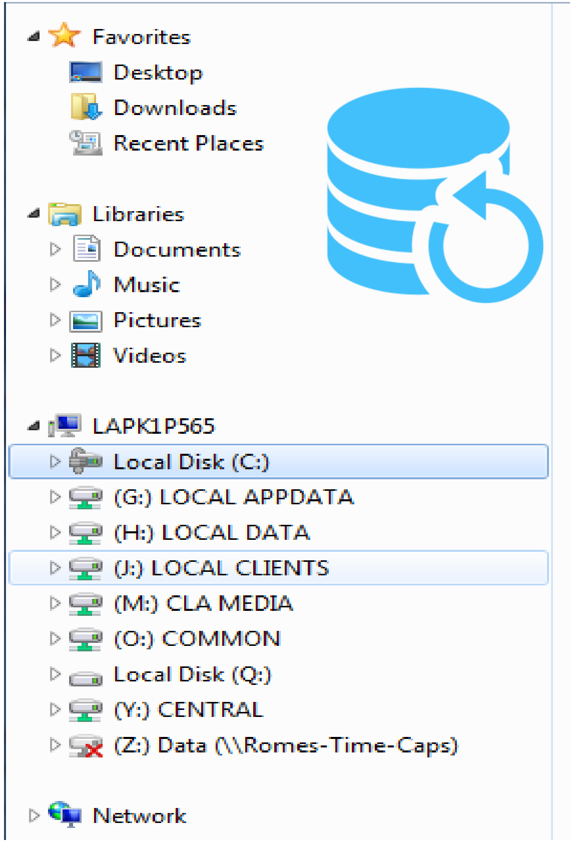
3. Minimized User Access Rights

4. Current operation systems and up to date/patched software

Ransomware
Defensive Strategies

- Working backup and restore capabilities

- Secure the backup process
  - Backups should be done with a service account.
  - Storage location of back ups should be very restrictive – read only access even for most administrators.
  - Identify which users could encrypt backups if they were to become infected.
  - You could also restrict the backup network access temporally similar to a bank vault.



The Boy Scouts Motto:

“Be Prepared”

Strategies and Action Items

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Strategies

- Our information security program should have the following objectives:
    - Users who are aware and savvy
    - Systems that are hardened and resistant to malware and attacks
    - Resilience Capabilities: Monitoring, Incident Response, Testing, and Validation

Strategies to Mitigate and Manage Cybersecurity Risks and Comply with GLBA Requirements

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

GLBA Requirement - Safeguards Rule

- Safeguards Rule –
  - Section 314.4 of the Rule noted the following:
    - ◊ Designating an individual to coordinate your information security program (ISP)
    - ◊ Identify internal and external risk to users' information security, information confidentiality and, integrity
    - ◊ Design and implement information to control the risks identified during the risk assessment and regularly test the controls
    - ◊ Oversee service providers
    - ◊ Evaluate and update ISP based on testing and monitoring procedures

Safeguards Rule

1) Information Security Program

- Governance oversight
- Third-party service provider and vendor risk management
- Tools in place to identify vulnerabilities and threats
- Cyber risk management
- Defense-in-depth strategy
- Incident response

Safeguards Rule

2) Risk Assessments

- The institution should identify reasonable foreseeable internal and external risks to the institution (NIST SP 800-30)
- Risk assessments are performed to identify vulnerabilities or gaps
- Risk assessments at a minimum should include the following:
  - ◊ Employee training and management
  - ◊ Information systems, including network and software design, information processing, storage, transmission, and disposal; and
  - ◊ Detection, and prevention of and response to attacks, intrusions, or other systems failures

Safeguards Rule

3) Aligning safeguards with risk identified

- Identify controls to prevent or mitigate the risks identified
- Monitor and regularly test controls
  - ◊ Evaluate the effectiveness of the safeguards’ key controls, systems and procedures. Examples include:
    - Password management
    - Response to social engineering; such as email phishing
    - Backup testing
    - Penetration testing to test the security infrastructure

Safeguards Rule

4) Oversee service providers by:

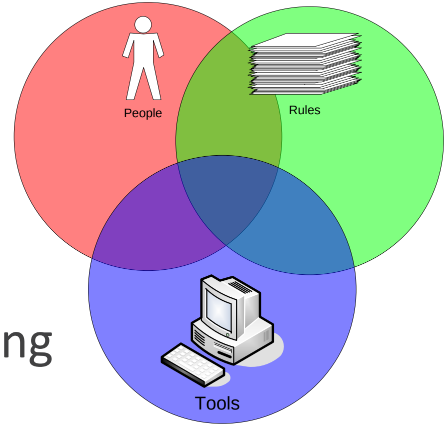
- Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue
- Requiring the service providers, by contract, to implement and maintain such safeguards

5) Monitor and update the information security program

- Change based on results from evaluating the effectiveness of the safeguards' key controls, systems and procedures
- Update based on any changes in operations or any other known circumstances

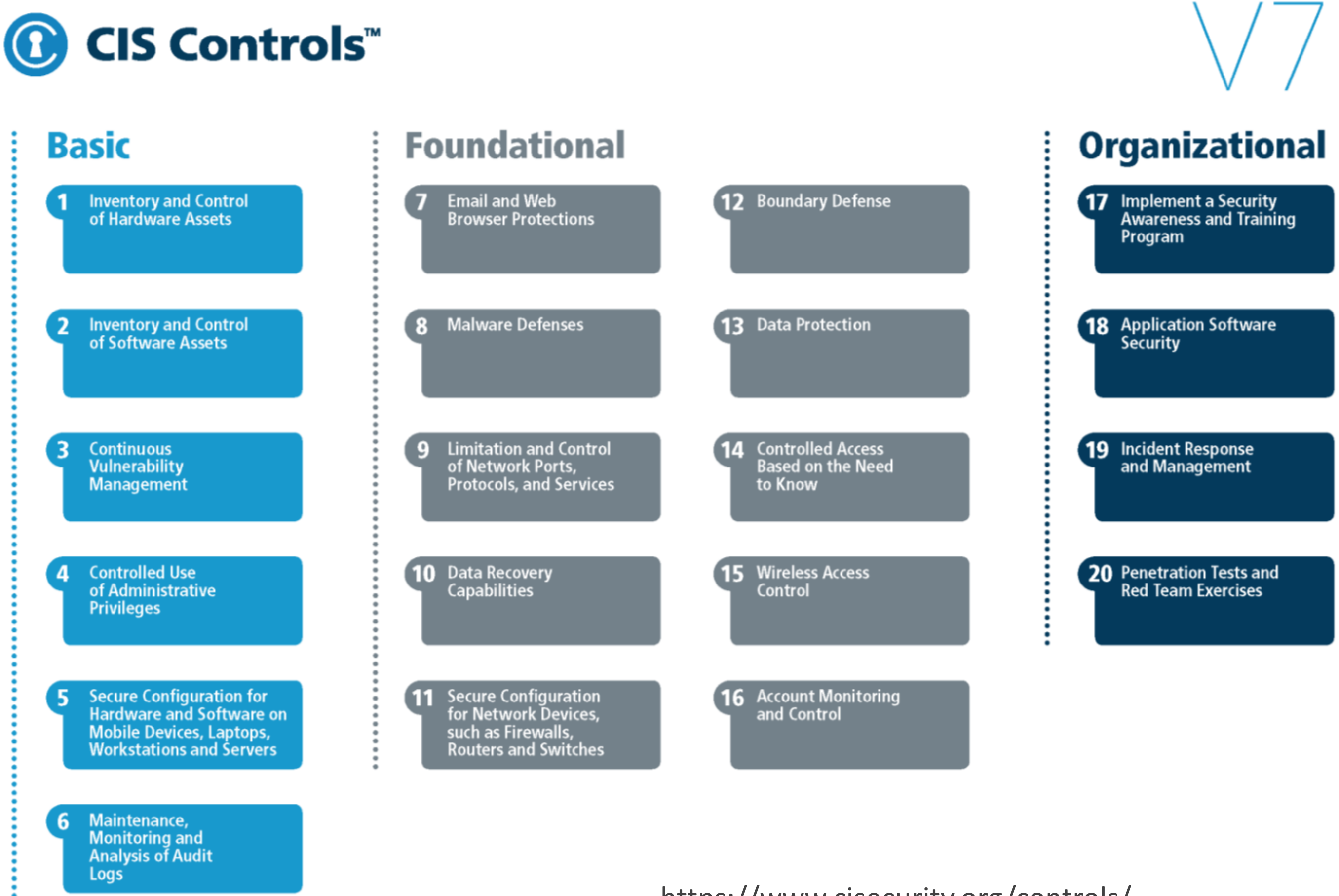
How Do I Comply?

Steps To Take Going Forward



- Review and update the information security program specifically with regards to GLBA
- Complete a formal risk assessment or update your existing assessment
- Test and assess people, processes and systems to validate controls are mitigating risks as expected
- Update and deliver information security training to address risks noted in the GLBA information and provide best practices in securing data
- Review third party contracts for gaps

Standards Based Operations



CIS Controls™ V7

Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols, and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

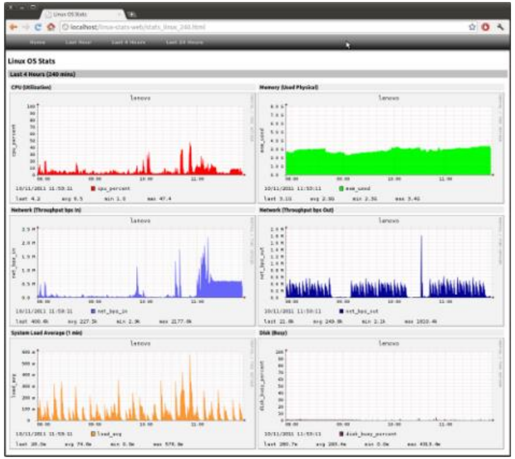
https://www.cisecurity.org/controls/

Disciplined Change and Exception Management

- Disciplined change management
- Disciplined vulnerability and patch management
  - Consistent Exception Control & Documentation
  - Should include risk evaluation , risk mitigation strategies, and acceptance of risk
  - Expiration and re-analysis of risk acceptance

System and Vulnerability Management and Monitoring

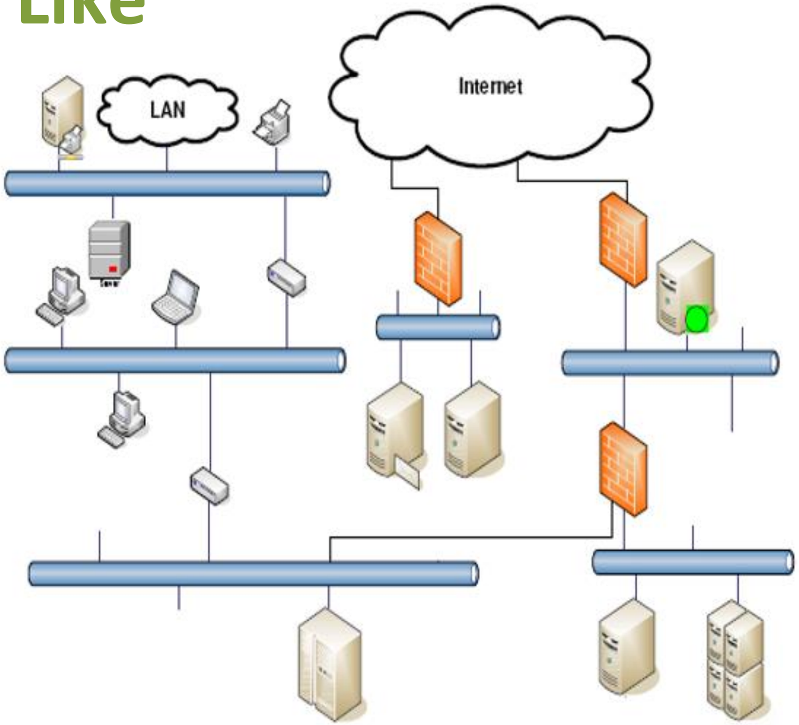
- Monitoring (built in)
  - Key system configurations
  - System and application logs
  - Accounts
  - Critical data systems/files
  - Data activity and flow
- Scanning (independent)
  - Patch Tuesday and vulnerability scanning
  - Rogue devices



Know Your Network
Know What “Normal” Looks Like

- Infrastructure
- Servers & Applications
- Data Flows
- Archiving vs. Reviewing

- System inventory
- Application inventory
- Data inventory



Action Items

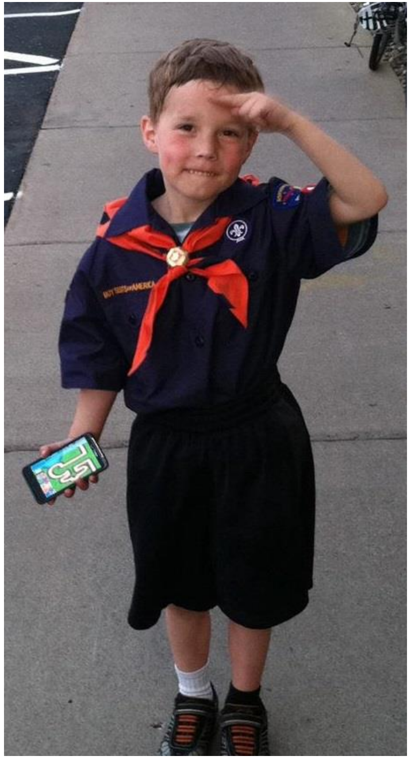
- TEST systems, processes, and people - Validate that your expectations are being met for IT operations, cybersecurity, and protection of data
  - Penetration Testing
    - ◊ Collaborative/Informed/White Box
    - ◊ Uninformed/Black Box
  - Social Engineering Testing
  - True Breach Simulation
    - ◊ Red Team/Blue Team

➢PRACTICE

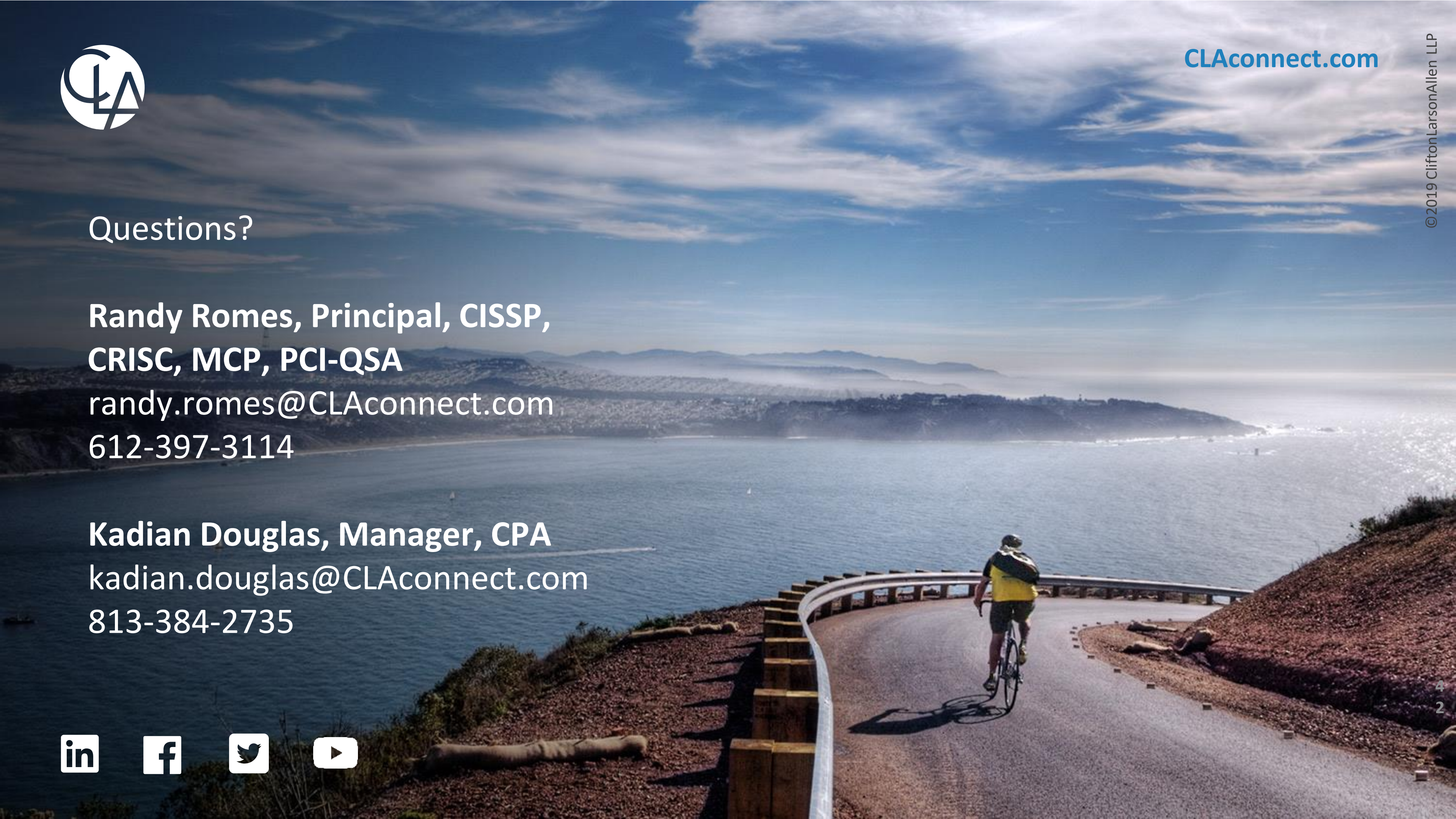
Action Items

- Test backup systems
  - Periodically test backup systems to ensure you can recover from ransomware
  - Have IT perform a full, bare-metal system restore (operating system, applications, and data
  - Have IT document how long it takes to recover various files or systems

➢ PRACTICE



Questions?



CLAconnect.com

Questions?

Randy Romes, Principal, CISSP, CRISC, MCP, PCI-QSA
randy.romes@CLAconnect.com
612-397-3114

Kadian Douglas, Manager, CPA
kadian.douglas@CLAconnect.com
813-384-2735