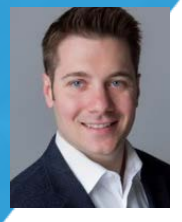
MARCUM
ACCOUNTANTS ▲ ADVISORS

ALERAGROUP

Webinar Series 3
August 19, 2020

Cyber Liability
&
Protecting Business From Cybersecurity Threats In The Wake Of Covid-19

Today’s Speakers



Zachary Slade

Alera Group
zachary.slade@aleragroup.com
224-257-5011

Jeff Bernstein

Director – Cybersecurity & Data Privacy
Marcum LLP
Jeffrey.bernstein@marcumtechnology.com
732-640-3690

Cyber Liability

Cyber Liability, Background & Current State

- Emerging Coverage
- Non-Standardized
- Less Common than other lines (>50% businesses do not purchase)
- Can be purchased several ways, most commonly:
    - Standalone
    - Combined with Professional Liability (E&O)
    - Combined with General Liability Package Policy (BOP)
- Increased Exposure due to COVID, more to come here.

Civil Rights Acts & Employment Related Protections

- EEOC – Equal Employment Opportunity Commission
- Civil Rights Act 1964 (Title VII) and Civil Rights Act 1991
- Equal Pay Act of 1963
- ADA (Americans With Disabilities Act) of 1990
- ADEA (Age Discrimination in Employment Act) of 1967
- FMLA (Family & Medical Leave Act)

Key Coverage Parts

- First Party Coverage:
  - Replacement/Repair Costs to network & cost to recreate data
  - Loss of Business Income
  - Forensic costs to determine cause/extent of breach
  - Notification to breached parties (required by law in all states) & Credit monitoring
  - Cyber Extortion demands

- Third Party Coverage:
  - Liability to third parties for unauthorized disclosure/release of sensitive information
  - Liability to third parties for transmission of virus/malicious code to others
  - Liability for unauthorized access/use of your system to harm others

--Complicated by Endorsements & Exclusions --

Common Cyber Claims (Mid-Market)

- Ransomware
- Social Engineering/Employee Error
- Data Breach
- Business Interruption
- Physical Data Theft

Warning: Increased Exposure due to COVID-19

- Attacks have increased dramatically, primarily due to increase in endpoints from employees working remote and various COVID-Related Cyber Crime/Social Engineering attacks.

- Key Coverage Areas, Endorsements, and Exclusions:
  - Unencrypted Mobile Device
  - Social Engineering/Cyber-Crime
  - Employee Owned Device
  - Ransomware

Cyber Liability: Best Practices

- Broad, well-written, Cyber Coverage with a top carrier
- Pre-Claim Assistance: What is the action plan if I am attacked?
- Cybersecurity/MSP Expertise Needed! Pre & Post Breach Concept

MARCUM
ACCOUNTANTS ▲ ADVISORS

Protecting Business From Cybersecurity Threats In The Wake Of Covid-19

Agenda

- Introduction;
- Current Business Climate;
- Why Cybersecurity is Important;
- Current Cyber-Attack Exploits;
- Security Risk Management Programs;
- Third Party Threats and Governance;
- Best Practices; and
- Discussion, Questions and Answers.

COVID-19 Has Changed the Way We Do Business

Health Crisis Had Driven a Drastic Shift in Operations

- Organizations have virtualized and deployed remote access;
- Few travel or live meetings;
- Three of four of us working from home;
- Coronavirus has affected businesses of all sizes within all business sectors and in every geography;
- New collaboration and other technologies are being implemented to optimize productivity;
- Ease of use and access for the telecommuter is critical;
- Ease of use and access almost always comes at the expense of security;
- Home networks often lack the security controls enjoyed by corporate networks;
- Most policies were not designed for our current COVID environment;
- Hackers are out in larger force and more determined than ever;
- Exploits are highly effective in our current environment. Everyone is on edge and also awaiting stimulus assistance; and
- Alerts issued by almost every major law enforcement, government, business and industry agency.

Why is Cybersecurity and Data Privacy So Important?

- Two Primary drivers:
  - Protect systems, networks, data and information; and
  - Comply with the various legal and regulatory mandates faced by business and connected organizations.
- What is at stake? Data security compromises result in very costly and difficult situations to recover from and could lead to:
  - Identity theft of clients and/or personnel;
  - Theft, lock-out, loss and/or leakage of private data, sensitive information and files;
  - Loss of competitive advantage;
  - Fraud and/or sabotage;
  - Theft of funds, data or intellectual property;
  - Disruption to the business;
  - Non-compliance with laws and regulations;
  - Damage to brand and reputation; and
  - Total collapse of the business.

Organizations from all sectors, sizes and geographies are at risk from cyber-threats and attacks. Have a response plan and a response capability. Cyber liability insurance is a must!

MARCUM ACCOUNTANTS ADVISORS

ALERAGROUP

Current Exploits

- Phish from internal company domains with **fake links** to work from home policy, procedure documents, or company portals;
- Calls and emails which **fake IT** or Product Support responses;
- Emails claiming to be **alerts** from the Center for Disease Control (CDC), the World Health Organization (WHO), or other expert organizations with information about the virus;
- Claims to provide access to **government loans**, tax refunds, or stimulus payments;
- Messages asking you to provide information for **refunds on tuition**, events, etc.;
- Newly-registered domains that reference “covid” or “corona” used to create **malicious web pages** to harvest user data;
- **Ransomware** embedded in COVID-19 emails, text message, and web sites (drive-by attacks); and
- **Invoice manipulation**/diversion threats for companies that are struggling to work with AR/AP remotely.

MARCUM ACCOUNTANTS ADVISORS

ALERAGROUP

Security Risk Management:
Achieving Success - Confidentiality, Integrity and Availability

- People
  - Most security compromises begin with human error;
  - Educate and train all staff and focus on the importance of good digital hygiene; and
  - Socialize policies and test personnel to gauge retention and compliance.

- Process
  - Design and implement POLICIES and PROCEDURES - guide on remote connectivity and telecommuting, acceptable usage, data retention and destruction, encryption; bring your own device (BYOD) and secure mobile computing.
  - Business Continuity and Disaster Recovery, Incident Response and Data Forensics; and
  - Ask all employees to read and accept the policy and include as part of the onboarding process.

- Technology
  - Adopt/leverage latest technologies - message and conferencing solutions, collaboration tools; cloud and archiving solutions, spam and content filtering, malware and anti-virus, security monitoring; and
  - Configure systems properly, validate security posture of everything internally but also via third party advisor.

There are now too many factors, attack vectors and entry points. Only a single mistake can wreak havoc.

MARCUM ACCOUNTANTS ▲ ADVISORS

ALERAGROUP

Now Add To That Equation A Third Party….

In March 2019, the Ponemon Institute reported that a staggering

63% of breaches

were linked to a third party!

MARCUM ACCOUNTANTS ADVISORS

ALERAGROUP

Why Do We Need Vendor Governance?

Example: Mortgage Broker, Lending Business or Bank Lender

- Data collected during the underwriting of a mortgage loan:

  - Names;
  - Date of Birth;
  - Social Security Numbers;
  - Financial Records;
  - Tax Returns;
  - Pay Stubs;
  - Spouse and Family Information;
  - Personal References;
  - Bank Statements;
  - Credit Reports;
  - Employer Information; and
  - Bank.

What does the Lender do with this information?

- They share it with Third Parties including the title company, insurer, appraiser, underwriter, law firm, application service provider, cloud services and hosting providers, marketing partners, etc.

- **The data collected during a typical loan transaction is only as secure as the weakest of any of these third party partners.**

Any Single Gap in Security Can Create a Catastrophe

Facebook App Data Exposure - World's largest Social Media Network exposed 540 Million Records

- Two third party-developed Facebook app datasets were exposed to the public. One database originated from a Mexican based media company and weighed in at 146 gigabytes with more than 540 million records detailing comments, likes, reactions, account names, Facebook IDs and more.
- The other third party app, "At the Pool," was exposed to the public internet via an Amazon S3 bucket, say the researchers. This database backup contained columns for user information such as username IDs, friends, likes, music, movies, books, photos, events, groups, check-ins, interests, passwords and more.
- Misconfiguration by Third Party partner leads to massive leak.

First American Financial - Fortune 500 real estate title insurance company exposed approximately 885 million sensitive records.

- The leak was caused by an application security flaw in its website.
- The hundreds of millions of digitized documents that were exposed related to mortgage deals dated as far back as 2003 and included Social Security numbers, bank account numbers and statements, tax and mortgage records, wire transaction receipts, and driver's license images.
- Prior to discovery of the flaw, all of the sensitive data had been openly accessible without the need for user/password authentication of any kind and could be reached by anyone with an Internet connection and web browser.

885 Million Records?

This is more than double the current U.S. population!
A simple application security vulnerability assessment could have identified the deficiency and allowed the firm to properly secure its data.

Best Practices for the Organization

Adopt technologies that will enable the workforce to maintain productivity but secure them properly:

- VPN, encryption, MFA, antivirus, firewall, security monitoring.

Develop new or enhance existing security policies:

- Information security policy;
- Incident response plan;
- Business Continuity and Disaster Recovery;
- Vendor governance; and
- Socialize the policies among staff.

Incident response plan

A written plan with multiple distinct steps to assist information-technology professionals recognize and respond to cyberattacks, data breaches or other incidents involving digital technology. These plans may be tested annually, and specific employees may be trained and assigned to respond to incidents on a 24/7 basis.

Perform vulnerability assessments and penetration testing studies to identify gaps in security controls

- Networks, application, systems; and
- Staff - perform social engineering studies on personnel to test retention of policy socialization as well as resilience to Internet-born attacks.

Have a plan to respond

- Develop an incident response plan which will guide all activity following a security incident or event;
- Develop an internal capability to respond of partner with a provider like Marcum to assist; and
- Educate end users on the Importance of Security in and out of the workplace. We are only as secure as our weakest single employee therefore security is the responsibility of everyone.

➢ **Cyber liability Insurance is a must!**

Considerations for the End User (1 of 3)

- Be skeptical of **any communication relating to COVID-19** and the economic stimulus package
  - The Federal Trade Commission (FTC), the Securities and Exchange Commission (SEC), the Better Business Bureau (BBB) and the World Health Organization (WHO) have all issued warnings in recent weeks about an increase in criminal scams with exploits that leverage the Coronavirus public health scare and the economic stimulus package;
- Be equally skeptical of **all other emails**, SMS, IM and text messages.
  - Examine sender and domain sources carefully. Review and verify all links (URLs) and attachments for legitimacy prior to clicking/opening them - social engineering remains the dominant exploit of choice for cybercriminals and attackers;
- Use **strong, unique passwords** for each site and application utilized and update passwords frequently
  - Complex passwords greatly strengthen end-user security and will alleviate critical security exposures caused by credential theft;
- Enable and utilize **Multi-Factor Authentication (MFA**) whenever an option.
  - MFA makes credential theft harder. Stealing user name/password combinations are the go-to method utilized by hackers in a majority of attacks;
- Utilize **anti-virus software** and set it to update automatically;
- **Encrypt everything** - encryption places stored and transmitted data into unreadable state.
  - Even if a hacker steals your data, they won't be able to use anything encrypted because they don't have the encryption key to access it;
- Set computers, systems and devices to **lockout and logout** during idle time
  - Automatic log outs on idle systems will prevent unauthorized access to email, data, websites, personal files, software, applications and the like;

Considerations for the End User (2 of 3)

- Keep **software updated** - the vast majority of all successful cyber-attacks leverage only a small number of security vulnerabilities.
  - Updating web browsers and other software will harden your devices against these widely leveraged flaws as well as others;
- Avoid using **public computing systems** and Wi-Fi connections
  - Use only SSID protected wireless networks and preferably utilizing a VPN connection;
- Make purchases on trusted **secure websites** only
  - Secure site URLs begin with HTTPS (not HTTP) and display a padlock icon;
- Download and use mobile apps from **reputable sources** (Apple, Amazon, etc.) only.
  - If you are unsure, about the authenticity of an app, research it prior to downloading.
  - Also - delete unused apps;
- Never use an **unknown USB device** - USB connections are a common entry point for malware and infection.
  - Any device connected to a USB drive can be infected with malware, a remote access Trojan and other malicious tools that can mimic legitimate files like WORD, EXCEL, PDF or music files;
- Harden your device settings on **fixed and mobile systems** and devices
  - Configure devices to avoid shared connections from other users, lock down application permissions and unnecessary access to personal information;
- Always use a **credit card** when purchasing online.
  - Purchases from dishonest or fraudulent websites can be more easily disputed through credit card companies. Purchases made with debit cards are harder to dispute and can expose your bank accounts;

Considerations for the End User (3 of 3)

- Always **hide usernames, password and pins.**
  - Keep account credentials safe by keeping user names and passwords secretive;
- If you do make a mistake and fall victim to cyber-exploitation, it is imperative to **seek help immediately**.
  - A good place to start is by seeking immediate assistance from your organizations IT Team, partners like us or your local police. The FTC and the FBI also have resources online if you've fallen victim to cybercrime;
- Good **personal hygiene** is our best protection against infection from the Coronavirus.
  - Wash your hands with soap and warm water, cover your nose and mouth when you sneeze or cough. Avoid touching your mouth and eyes…
  - The basic concept of improving general hygiene is also worthy of immediate adoption by all of us in the **digital** world and is now more important than ever.

Easy Fixes and Best Practice

- **Enable Security Controls – ZOOM is a good example**

- Out of the box the solution leaves end-users somewhat exposed;
- Simple click to enable many important controls;
- ZOOM's website has simple to use direction for security, https://zoom.us/security;
- Available Controls Include:
  - Secure a meeting with end-to-end encryption;
  - Create Waiting Rooms for attendees;
  - Require host to be present before meeting starts;
  - Expel a participant or all participants;
  - Lock a meeting;
  - Screen share watermarks;
  - Audio signatures;
  - Enable/disable a participant or all participants to record;
  - Temporary pause screen-sharing when a new window is opened;
  - Password protect a meeting; and
  - Only allow individuals with a given e-mail domain to join.

Our Solutions

MARCUM TECHNOLOGY

- Training and Education
- Response
- Assurance
- Compliance
- Security Technology Solutions; and
- Managed Services

Alera Group and Marcum

CORONAVIRUS RESOURCE CENTER

Stay up-to-date on how the coronavirus (COVID-19) will impact your business.

aleragroup.com/coronavirus
marcumllp.com/coronavirus

Questions and Answers

MARCUM
ACCOUNTANTS ▲ ADVISORS

ALERAGROUP