THIRD PARTY VENDOR RISK…

DURING COVID19 AND BEYOND

May 21, 2020

Chiesa Shahinian & Giantomasi PC

MARCUM TECHNOLOGY

If You Have a Question During Today's Broadcast…

Ask your question in the Q&A box.

To activate the Q&A box, move your mouse to the bottom of the screen and click the black circle with three dots. Then, select "Q&A" from the menu.

IMPORTANT CPE NOTICE

Periodically during today's seminar a **polling question** will appear in the panel on the right side of the screen. Respond to each polling question in order to log your participation for CPE purposes.

Marcum LLP and Marcum Technology and Chiesa Shahinian & Giantomasi PC have together prepared these materials as part of an educational program. The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual, entity or case.

While every effort has been made to offer current and accurate information, errors can occur. Furthermore, laws and regulations referred to in this program may change over time and should be interpreted only in light of particular circumstances.

The information presented here should not be construed as legal, tax, accounting or valuation advice. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

MARCUM TECHNOLOGY

CSG Chiesa Shahinian & Giantomasi PC

Our Speakers: Jeff Bernstein

Director, Marcum Technology

- 20 Year information security industry veteran;
- Worked closely w/Industry and government to secure critical computing infrastructure, to help organizations comply with the numerous regulatory mandates that govern them, to help them respond to cyber breaches and to train personnel on security matters;
- Worked alongside former USG agency Directors;
- Managed major post breach cyber investigations, complex security testing programs, training and compliance programs for numerous clients from highly regulated industries.
- Has contributed to IS frameworks, authored whitepapers, original articles (Gannett and USA Today), appears on television and in the press often as industry expert; and
- Lectured at Masters Studies Level (NYU), sits on USF MUMA College of Business MBA Studies Cybersecurity Education Advisory Board and Ithaca College Advisory Board for Cybersecurity Studies.

MARCUM TECHNOLOGY

CSG Chiesa Shahinian & Giantomasi PC

Our Speakers: Michelle A. Schaap

Member, Privacy & Data Security and Corporate & Securities Groups, Chiesa Shahinian & Giantomasi PC

Michelle regularly advises on cybersecurity preparedness, counsels when data security incidents arise and trains companies on best practices for security procedures addressing both their business operations and their customers' concerns. Michelle assesses risk management practices and security incident preparedness in developing proactive security incident response and recovery plans. Additionally, she works with clients in contract review, drafting and negotiation in critical areas of privacy and security.

Michelle counsels clients on incident and breach response – often serving as quarterback to the incident response team, working closely with her client's senior executives, forensics, law enforcement and other critical members of the team.

She is a Certified Information Privacy Professional, awarded from the International Association of Privacy Professionals, with a concentration on U.S. private-sector law (CIPP/US).

MARCUM TECHNOLOGY

CSG Chiesa Shahinian & Giantomasi PC

Agenda

- COVID-19 and the current climate
- Third Party Partner and Vendor Risk
- Newly emerging cyber exploits
- Data Breaches, Detection and Notification
- Mitigation through Governance
- Where to Begin

MARCUM TECHNOLOGY

CSG Chiesa Shahinian & Giantomasi PC

Changing the Way Business is Done

CSG
Chiesa Shahinian
& Giantomasi PC

MARCUM
TECHNOLOGY

COVID-19 Changing Business

Global Pandemic Driving Shift in Operations

- Companies, organizations and institutions have gone virtual;
- Little to no travel or live meetings;
- Majority of US citizens remain under Stay at Home orders;
- New collaboration and other technologies 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;
- Hackers are out in larger force and more determined than ever;
- Insider threats are also higher due to massive changes in procedure; and
- Attach exploits are highly effective in our current environment.

➢ **Governing the protection of our networks, data, applications, systems, people and property must also include effective oversight of our trusted business partners and vendors. We are only as secure as our weakest partner that has access to our data.**

MARCUM TECHNOLOGY

Remote Users and Extreme Exposures

Increased Global Attack Activity

- Law enforcement, government, business, academic and military authorities have all published advisories relating to the increase in cyber attacks
- A well-known security education provider says that phishing attacks alone are up by 700%
- Assume ‘malicious parties’ are waiting to pounce on telework traffic

> “Organizations should **assume** that malicious parties will gain control of telework client devices and attempt to recover sensitive data from them or leverage the devices to gain access to the enterprise network.”

– National Institute of Standards and Technology, March 2020

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.

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.

Third-Party Governance and Mitigating the Risk

CSG
Chiesa Shahinian & Giantomasi PC

MARCUM
TECHNOLOGY

Timing is Everything

How Long to Detect

- According to the June 2019 Ponemon Institute Study, the average time to detect a breach is 197 days (more than 6 months!)
- In the case of dental and vision insurer Dominion National, the answer is nearly nine years! That's 63 dog years, if you are keeping count….or 3,000 days from [intrusion] to discovery!

https://www.secureworldexpo.com/industry-news/9-years-incident-to-breach-discovery-time

How Long to Recover

- In 2019, the average "life cycle" of a data breach was reported to be more than nine months.
- This reflects an increase by 5% against the same figure in 2018

Ponemon Institute 2019 "Cost of a Data Breach"

But then consider:

- The small business that does not survive and shutters its doors within a year following a breach
- The mega-breaches which have a litigation life seemingly of its own
- In 2019, nearly 30% of the consumers surveyed reported they would not return to a small business that suffered a [data] breach.

https://www.techrepublic.com/article/how-data-breaches-are-hurting-small-businesses/

MARCUM TECHNOLOGY

CSG Chiesa Shahinian & Giantomasi PC

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!

Your work force is (probably) working remotely… So is your vendor workforce

- Is their workforce properly trained?

- Are vendors' personnel using personal devices to access and process your data?

➢ Even if you undertook a risk assessment of any given vendor, it probably did not address remote operations.

MARCUM TECHNOLOGY

CSG Chiesa Shahinian & Giantomasi PC

“The risk of negligent employees and contractors causing a data breach or ransomware is getting worse.”

60% of respondents in companies that had a data breach say the **root cause of the data breach was a negligent employee or contractor.**

61% of respondents say **negligent employees put their company at risk for a ransomware attack.**

- Couple these facts with a remotely-working vendor, and by definition, you have a disaster waiting to happen.

MARCUM TECHNOLOGY

https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf

Consider what you are outsourcing and the risks different functions and data create

- Is the data to be shared with the vendor consumer data?
  - Is the data PII? PHI?
- Are you purchasing lists for marketing purposes from a third party?
  - Did the vendor secure any required consents?
- Is the third party designing a new website for you?
  - What type of cookies are being build into that site?
- Is the data being shared intellectual property?
- Is the data being shared YOUR data?
  - Are you using the vendor as a "subprocessor"?
- Where will the vendor be "processing" your data?
- When you part ways with the vendor, how will you get your data back?
- Are you subject to CCPA, HIPAA, NYS DFS Regulations, GDPR…

MARCUM TECHNOLOGY

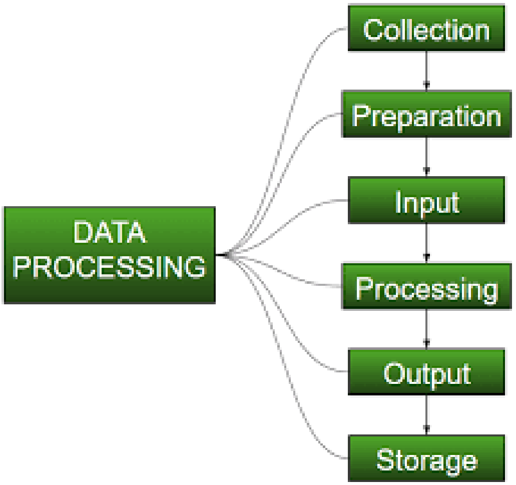
CSG Chiesa Shahinian & Giantomasi PC

What is a Vendor “Doing” with Your Data?

“Processing” is an all encompassing word (at least legally). Under Article 4 of GDPR, Processing includes:

Any “operation” or set of operations on personal data

- Collection
- Recording
- Sorting
- Structuring
- Altering
- Retrieving
- Transmitting
- Storage
- “Processing” (traditional sense)
- Retention
- Destruction



From the moment you begin to “process” PII or PHI until you securely anonymize that data or properly destroy that data, whether as a data “controller” or “processor” ***you (probably) have a duty to take “reasonable” measures to secure that data***

Vet and Monitor Your Vendors

- As with a risk assessment, and training, this is NOT just a “best practice” but is also mandated by many proactive legislative and regulatory frameworks
- Prioritize your assessments – which vendors are most critical to YOUR continued operations?

Third Party Processors = Third Party Risk

Vet new AND existing vendors

- Ask how they are securing and managing their remote work forces
- Ask what they have done to secure their videoconferencing
- Assess their practices… and ask for confirmation

Due Diligence Cannot Be a “One and Done”

- What framework(s) did your vendor use to set up its own systems?
- What laws and regulations do you need your vendor to meet?
- Has your vendor experienced prior data breaches? Fines for non-compliance?
- If your vendor has a data breach, what are you requiring of the vendor contractually?
  - By law, vendors must notify their customers of a breach. But as we all know, not all do…

MARCUM TECHNOLOGY

CSG Chiesa Shahinian & Giantomasi PC

Risk Shifting – Cloud Providers

Concerns:

- Relinquishment of control
- Access to your data
- Reliability

What you need to know:

- Dedicated or Public
  - Where located?
  - Right to audit
  - Physical Security

➢ Ask for Certifications (specific to services)

Video Conferencing – What are Vendors Doing?

FBI has reported an increasing number of cases involving the hijacking of Zoom videoconferences (called "Zoom-bombing").

- In the middle of a classroom lesson, a business meeting or a friendly online visit, malicious actors are posting pornographic images, messages of hate and threatening language.

- Zoom has and continues to release patches and updates
  - do not hit "remind me later!"
  - Verify the patch and then distribute to your remote workforce

Whether you are onboarding a vendor, or renewing a contract…

Ask how they are managing their remote staff:

- How are they managing access credentials?
- How are they managing personal devices and/or company issued devices?
- How are they controlling use of removable media?
- Are personnel printing documents on personal devices?
- Are personnel using public Wi-Fi?
- How is least rights being managed?
- When the vendors moved to a remote environment, were personnel trained on the risks created by this alternate environment?
- How are systems and software being patched and updated?
- Are home devices encrypted?

➢ "Assuming" you have a vendor questionnaire already, did YOU dust it off and add to it remote working considerations?

A Word about Insurance….

- Does your cyber insurance include third party vendor business interruption related claims?

- Does your vendor's cyber insurance cover its work force working remotely?

- Consider whether policy limits should be revisited with you and your vendors working remotely

MARCUM TECHNOLOGY

CSG Chiesa Shahinian & Giantomasi PC

Notice Requirements

- If your contract requires your vendor to provide to you notice of a data breach, is YOUR point of contact up to date now that you are working remotely?

- If you incident response team includes third party vendors, are those vendors' points of contact up-to-date?

- Timing of notice….
  - Statutory
  - Regulatory
  - Contractual

➢ And remember, if you are using subprocessors, what is your obligation for notice upward?

Has Your Vendor Assessed ITS Vendors?

All of your considerations for your remote staff should be concerns when you look at your vendors…

- And your vendors should be (contractually required to) ask the same questions of their vendors…

Other Contractual Considerations…

- Data retention and destruction policies
- Representations and warranties
- Indemnities
- Return of data
- Confidentiality obligations
- Definition of "applicable laws"
- Insurance requirements
- Terms that may have applied to your vendor in its office may not take into consider your vendor (and its vendors) working outside the office

Force Majeure and Impossibility of Performance

- Are your vendors still performing?
    - If not, why not?
    - And what can you do about it?

Chiesa Shahinian & Giantomasi Solutions

- Incident response planning
- Identifying statutory and contractual obligations for data security and privacy considerations
- Policy and procedures review – regulatory and contractual
- Breach coach
- Contract review and negotiation
- Training
- Website privacy policies and terms of use
  - Preparation, review and assessment
- Advising employers regarding COVID19 data
  - The do's and don'ts

MARCUM TECHNOLOGY

CSG Chiesa Shahinian & Giantomasi PC

Marcum Technology Solutions

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

MARCUM TECHNOLOGY

CSG Chiesa Shahinian & Giantomasi PC

Questions?

Jeffrey Bernstein
Director, Marcum Technology
jeffrey.bernstein@marcumtechnology.com

Michelle A. Schaap
Member, Chiesa Shahinian & Giantomasi PC
mschaap@csglaw.com

MARCUM TECHNOLOGY

CSG Chiesa Shahinian & Giantomasi PC