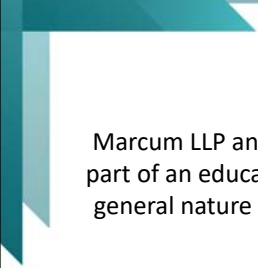


INFORMATION
SECURITY
GOVERNANCE
DURING TIMES OF PANDEMIC

May 7, 2020

MARCUM
TECHNOLOGY



Marcum LLP and Marcum Technology have 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

3
0520032N

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

4

0520032N

Our Speakers: Peter Campbell

Senior Strategic Consultant, Marcum Technology



- 30+ years in IT leadership roles at law firms and nonprofits
- Peter's focus has been on transforming unaligned technology systems into integrated, usable platforms
- Brought a mid-sized commercial law firm from eleven disparate systems to an integrated, SQL-Server based platform with MS Outlook serving as a portal
- Developed award-winning retail reporting and management software for a large thrift enterprise
- Moved a Federal funding agency into a unified, cloud-based platform for information management built on Salesforce, Box, and Tableau
- Peter specializes in technology/security consulting and outsourced CIO services for Marcum Technology clients.
- Specialties include CRM, Finance/ERP, Knowledge Management, Cloud migrations, IT staffing strategy and mentoring, technology assessments, and strategic planning

MARCUM
TECHNOLOGY

5

0520032N

Agenda

- **The New Normal:** Assessing the Situation
- **Addressing Immediate Concerns:** Safety While Social Distancing
- **Security Awareness:** The First Defense
- **Security 101:** Basic Precautions
- **Security Policies:** Organizational Governance
- **Compliance and Frameworks:** Meeting Regulatory Requirements
- **Compliance By Culture:** Fostering a Security-Minded Workforce

MARCUM
TECHNOLOGY

6

0520032N

The New Normal

Assessing the Situation

MARCUM
TECHNOLOGY

The New Normal

- The sudden migration to a largely virtual workforce has created new security challenges while barely alleviating any of the existing concerns
- Companies with largely established remote workforces and/or heavy cloud/SaaS infrastructure had an easier time with this than companies with traditional server and desktop environments.
- Traditional remote access options like Citrix or Microsoft Remote Desktop don't scale quickly when usage skyrockets, and are subject to serious security concerns.

Pandemic-Related Threats

As with any major event, scammers have quickly capitalized on the pandemic in powerful ways



Are We In It For The Long Haul?

“Hope for the best, be prepared for the worse.”
 – Maya Angelou

- Best case? Summer, 2020.
- Worst case? Late summer/early fall, 2021.
 - Safe conditions without a vaccine require ample testing, contact tracing, PPE, and hospital capacity
 - Testing and mitigation efforts must ramp up considerably
 - It could take 18 months to certify a vaccine.
- We assumes that businesses will not require employees that can work remotely to work on-site until it is safe to do so.

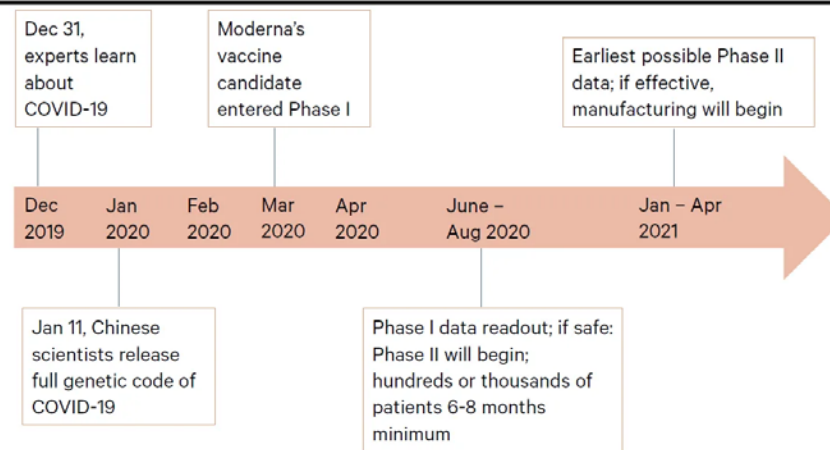


10

0520032N

Best Case Scenario For a Vaccine

Exhibit 11: Dr. Fauci's projection of COVID-19 vaccine development timeline



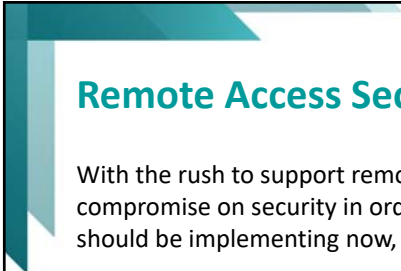
Source: VOA website, Berenberg Capital Markets



Addressing Immediate Concerns

Safety While Social Distancing

MARCUM
TECHNOLOGY



Remote Access Security

With the rush to support remote work, some companies have had to compromise on security in order to continue operations. Things that you should be implementing now, if they aren't in place, include:

- Multi-Factor Authentication (MFA)
- A policy regarding which systems are authorized to connect via VPN and security requirements for connecting systems
- A Remote Desktop/Citrix server architecture that keeps the servers behind the firewall and requires MFA

MARCUM
TECHNOLOGY

13
0520032N

Home Offices

Security Awareness Training

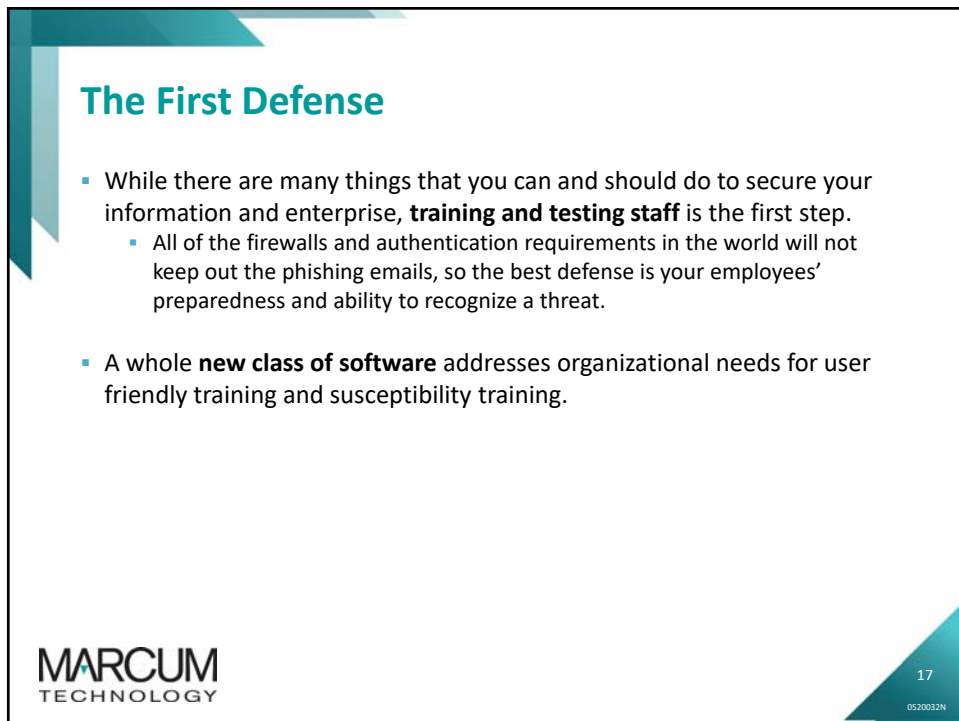
- Susceptibility to phishing might be higher on systems that are used for personal computing as well as work
- The Covid-19 themed attacks are playing on real anxiety and pose a serious threat

Standards for the safety of remote work environments

- Remote workers need uncluttered and safe work environments, with equipment up to reasonable standards. Companies are still liable for workplace injuries, even when the workplace is home.

Information Security

- Clear policies on handling of sensitive information and use of remote access software
 - Are documents being saved to local drives or personal cloud services on home computers?
- Protected communications
 - Is Zoom safe? Probably, as long as you are following the recommended procedures on securing invites, limiting access to waiting rooms, etc.
- Malware protection
 - Does your anti-malware solution deploy updates via the cloud? Are you confident that the systems being used at home are sufficiently protected?



Key Threats

Threat	Description
Phishing	Spam emails or texts designed to catch as trick people as possible into a link. These can appear to be authentic emails from a vendor or financial institution.
Spear Phishing	Targeted emails designed to trick the recipient. These might claim to be from your boss or your IT department. They sometimes have a recognizable email signature and other attributes that make them appear authentic.

- For both phishing and spear-phishing, users need to be suspicious about clicking any unverified links, and know how to recognize verified/unverified links and senders.

Key Threats

Threat	Description
Social Engineering	Phone calls, surveys, Facebook memes that are designed to get information that can be used to compromise an account.
Spoofing	Impersonating a known contact (used often in spear-phishing). Elaborate schemes can involve registering a domain name slightly misspelled and using what looks like a valid email for a known contact (e.g. bgates@miicrosoft.com) in order to supply "updated ACH information."

Security Awareness Software

- Most packages offer an initial, overall training and shorter refreshers.
- Trainings are designed to be entertaining and easy to follow, while informational.
- Network directory and Learning Management System integrations make them easy to incorporate into your environment.
- Full statistics by user on course completion and phishing test results allows management to act on results by scheduling more training for those more susceptible and/or tying results to performance evaluations.

MARCUM
TECHNOLOGY

20

0520032N

Security 101

Basic Precautions

MARCUM
TECHNOLOGY

The Uneveled Playing Field

The old days:

- Data was stored on servers behind locked doors and we each had no more than a handful of passwords

The current situation:

- Organizational data lives everywhere
 - Data access points can't be locked down
 - We each have 100 passwords and they can all be breached or cracked
 - Hacking is easy, if you know where to find the tools.
- Security is now more about ensuring that data access is authorized than locking down data (although both apply).

Passwords

NIST Special Publication 800-63B, Digital Identity Guidelines recommendations

Password Length	Allow at least 64 characters in length to support the use of passphrases. Encourage users to make memorized secrets as lengthy as they want, using any characters they like (including spaces), thus aiding memorization.
Complexity	Do not impose other composition rules (e.g. mixtures of different character types) on memorized secrets.
Longevity	Do not require that memorized secrets be changed arbitrarily (e.g., periodically) unless there is a user request or evidence of authenticator compromise. (See Section 5.1.1 for additional information).*

* Make sure that your auditors approve of these changes

Single Sign-On and Password Managers

- **Basic Password Management tools** store all passwords in a secure “vault” and fill them in for you on your computers and devices, so that you just have to memorize one password to open the vault that holds the rest of them.
- A better solution, that generally makes life easier for users, is **Single Sign-On (SSO) software**, which similarly lets one password suffice for all applications. The best SSO software also interacts with popular applications so that users can be set up in apps at the same time that they’re set up on the SSO system (provisioning).

Multi-Factor Authentication

- Multi-Factor Authentication (MFA) provides a second layer of verification, showing that you are not only who you say you are, but you have your phone, or access to your email as well. This immediately protects you from a hacker in Romania who either cracked your account or got your password from a data breach.
- Any password (or pass-phrase) can be cracked, but MFA is over 99% effective* at stopping the kinds of breaches that occur when a password is compromised.

* Per recent Google and Microsoft studies

Encryption, Firewalls, Advanced Threat Detection, Dark Web Monitoring

Laptop Encryption	Ensures that a lost or stolen laptop, once opened, will not give someone access to the system.
Firewalls	While they are no longer sufficient to protect all data, firewalls still protect the systems that remain in your server room.
Advanced Threat Detection	Goes beyond firewalls and spam filters to analyze and alert you about potential breaches.
Dark Web Monitoring	Alerts you when a company email is breached. However, this is a new software market and product quality varies. Shop carefully. Similarly, personal services like HaveIBeenPwned and Firefox Monitor do breach alerting.



Security Policies

Organizational Governance



Making Policies Matter

- Written policies are often published and neglected. In the current environment, a policy should not only be drafted, but also trained on and incorporated into business practices and employee performance expectations.
- Ideally, adherence to the policy is baked into organizational culture. Staff understand and respect the need to protect organizational assets and customer data, and they model the behavior.

Basic Security / Mobile Devices

Basic Security Policy / Acceptable Use Policy (AUP)

- Outlines the base expectations for confidentiality, information handling, passwords, security awareness, etc.
- An AUP might go further, and include guidelines on representing the company in common communications and on social media.

Mobile Device Policy

- Sets expectations and rules for both personal and company-owned laptops, smartphones, and tablets.
- Outlines procedures should they be lost or stolen.
- Specifies where company data should be saved.
- Reserves right for company to wipe data.
- Sets a maintenance schedule, if warranted.

Incident/Breach Response

Incident Response Plan

- Prepares the organization in the case of a sensitive data breach.
- Establishes a core and ad hoc response team, which should include highly-placed executive and IT staff
- Mandates the schedule for response, factoring in legal deadlines and compliance requirements (e.g. GDPR)
- Outlines the scope of the response
- Defines the investigation requirements and plan
- Describes the remediation options (e.g. supplying free credit monitoring to constituents who are breached)

Telecommuting / Business Continuity

Telecommuting Policy

- Establishes allowable telecommute schedules
- Outlines what equipment and services the company will and will not provide
- Dictates minimum technical standards required
- Assures workspace safety.

Business Continuity Plan

- Establishes communication protocols and channels in case of a crisis
- Procedures for establishing connectivity to company systems and data
- Expectations should the company lose or lose access to facilities for an extended period.



An Aggregated Approach to Compliance

- We all have technical compliance requirements: PCI, Sarbanes-Oxley (SOX), HIPAA, and GDPR, to name a few common ones.
- There are also a number of security frameworks that you can adopt and comply with, such as NIST 800-171 (R2) (Federal guidance for non-Government entities), ISO 27001, and FISMA (Federal Agency standards).
- While it's important to regularly recertify your compliance with the individual regulations, 90% of what they require is covered by any one of these frameworks. (GDPR might be an exception here.)
- Accordingly, if you are required to comply with multiple regulations, then enacting a common framework and tracking the variances can be more efficient than fully recertifying each individual regulation's requirement list.

MARCUM
TECHNOLOGY

33
0520032N

Common Controls

Common to PCI, HIPAA, SOX, and others are:

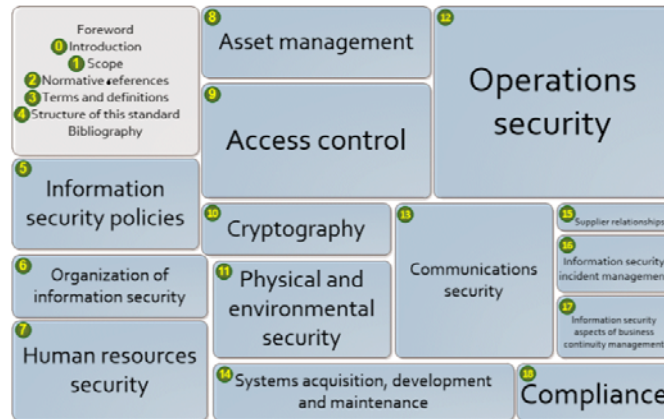
- The need to control access to sensitive data
 - The need to monitor data access
 - Identify and report on data breaches
 - Encrypt data (both in storage and transmission)
 - Conduct regular security audits
 - Establish and maintain a security policy
- All of these requirements are covered by the popular security frameworks.

NIST and ISO 27001

NIST Publication 800-171 and the ISO 27001 security framework cover similar territory:

NIST 800-53 r4 CONTROL FAMILIES	
Access Control	Identification and Authentication
System and Communications Protection	Incident Response
Program management	Awareness and Training
Maintenance	Contingency Planning
Audit and Accountability	Media Protection
Configuration Management	Physical and Environmental Protection
System and Information Integrity	Risk Assessment

ISO 27001 Topics



Framework/Regulation Variances

- Each regulatory set has it's focus, PCI on credit card data, HIPAA health, SOX finance. Frameworks address data security for all sensitive data.
- Full NIST or ISO 27001 compliance covers almost every PCI requirement.
- HIPAA adds risk assessments and creation of a risk management policy with defined sanctions for health information mishandling.
- SOX adds specific reporting to SOX auditors and the requirement that they can personally test the security.
- GDPR varies most, as many of the privacy requirements involve data collected over the web and the relationship with web visitors, which goes beyond the scope of standard frameworks. But the key back office requirements – data access, encryption, policies – all apply.



Fostering a Security-Minded Workforce

Securely configuring the applications and servers, implementing the policies, and limiting the access rights are all critical actions, but key to being secure is maintaining an organizational understanding and respect for data security.

- Assess security awareness as part of the employee interview process
- Build security compliance into job descriptions and performance expectations
- Include security training in employee onboarding
- Put all of the training in context, so that staff not only understand that they should act securely, but understand why it's important to do so.

MARCUM
TECHNOLOGY

39
0520032N

Our Solutions

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



MARCUM
TECHNOLOGY

40

0520032N

Questions?

Jeffrey Bernstein

Director, Marcum Technology
jeffrey.bernstein@marcumtechnology.com

Peter Campbell

Sr. Strategic Consultant, Marcum Technology
peter.campbell@marcumtechnology.com

NEXT in Marcum Technology Webinar Series:

- May 14 at 1 pm EDT:** Leveraging Digital Forensics for Better Human Resources Outcomes
- May 21 at 1 pm EDT:** Third Party Vendor Risk During the Pandemic

www.marcumllp.com/coronavirus

MARCUM
TECHNOLOGY

41

0520032N