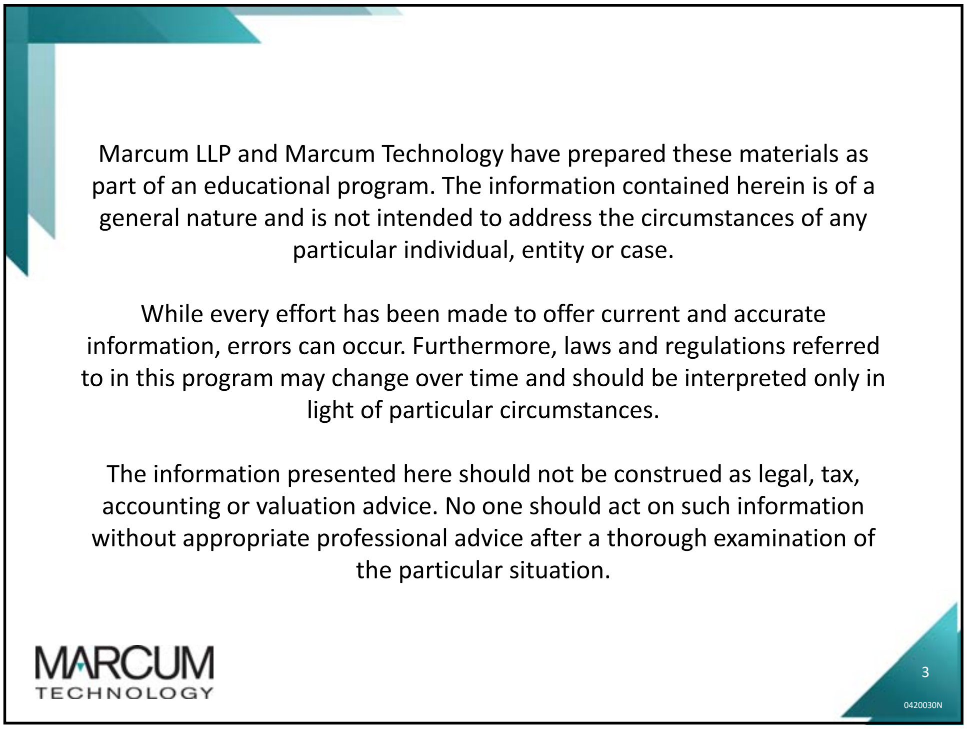
IMPROVING CYBERSECURITY BY INFLUENCING GOOD USER BEHAVIOR

April 30, 2020

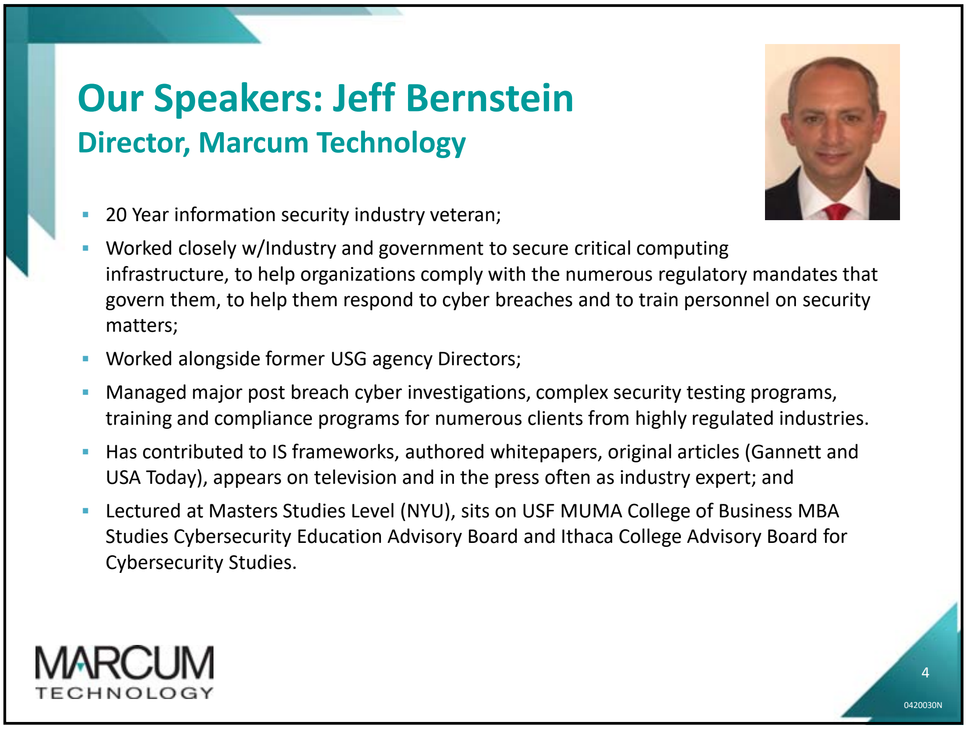
Global Learning Systems
MARCUM TECHNOLOGY



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.



Our Speakers: Jeff Bernstein

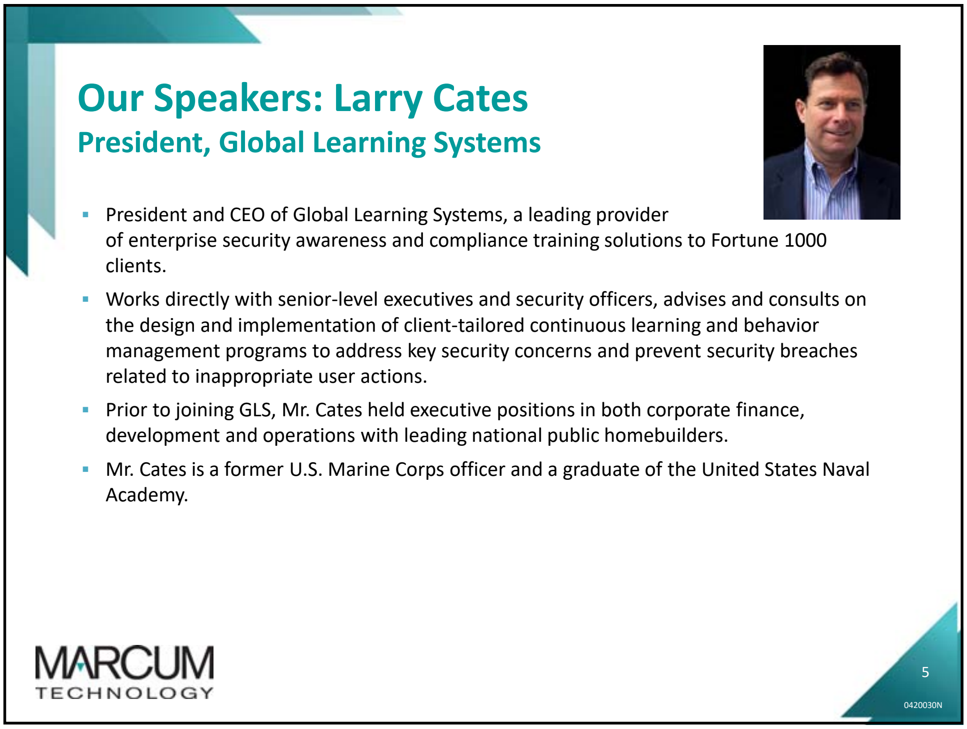
Director, Marcum Technology

- 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

0420030N



Our Speakers: Larry Cates

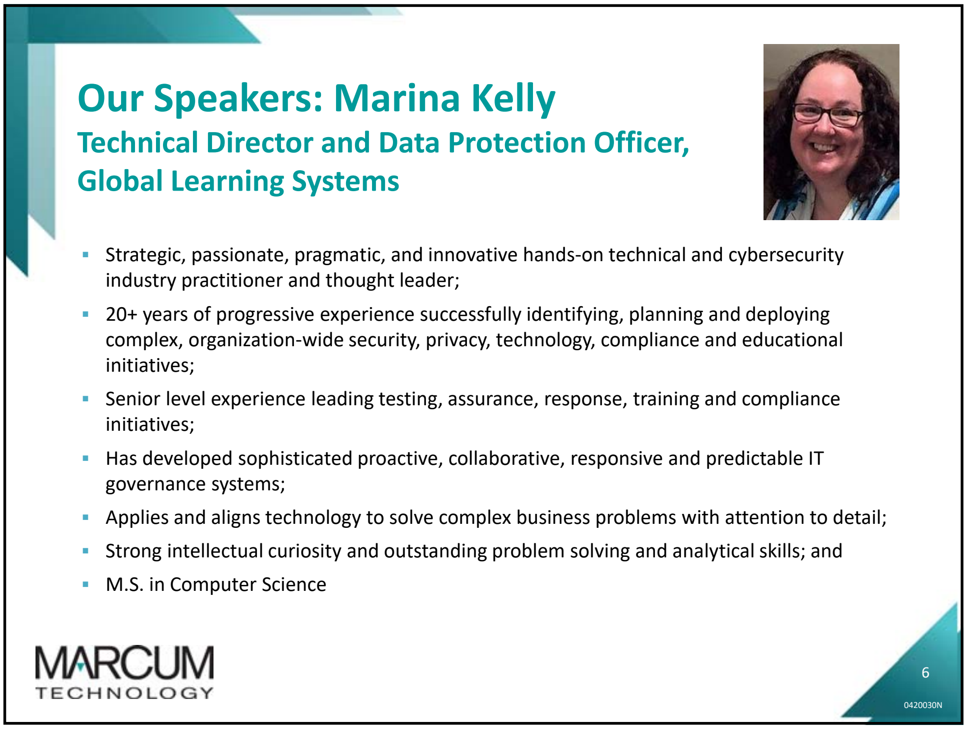
President, Global Learning Systems

- President and CEO of Global Learning Systems, a leading provider of enterprise security awareness and compliance training solutions to Fortune 1000 clients.
- Works directly with senior-level executives and security officers, advises and consults on the design and implementation of client-tailored continuous learning and behavior management programs to address key security concerns and prevent security breaches related to inappropriate user actions.
- Prior to joining GLS, Mr. Cates held executive positions in both corporate finance, development and operations with leading national public homebuilders.
- Mr. Cates is a former U.S. Marine Corps officer and a graduate of the United States Naval Academy.

MARCUM TECHNOLOGY

5

0420030N



Our Speakers: Marina Kelly

Technical Director and Data Protection Officer, Global Learning Systems

- Strategic, passionate, pragmatic, and innovative hands-on technical and cybersecurity industry practitioner and thought leader;
- 20+ years of progressive experience successfully identifying, planning and deploying complex, organization-wide security, privacy, technology, compliance and educational initiatives;
- Senior level experience leading testing, assurance, response, training and compliance initiatives;
- Has developed sophisticated proactive, collaborative, responsive and predictable IT governance systems;
- Applies and aligns technology to solve complex business problems with attention to detail;
- Strong intellectual curiosity and outstanding problem solving and analytical skills; and
- M.S. in Computer Science

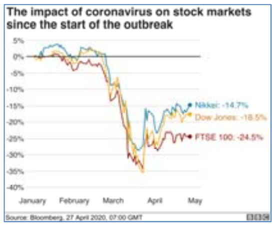
Agenda

- COVID-19 has changed the way business is done
- The cybersecurity stakes are higher
- New cyber exploits are emerging
- Security program basics: people, process, technology
- Focus: people
- Where do we go from here?

Changing the Way Business is Done

MARCUM TECHNOLOGY

COVID-19 Has Changed the Way We Do Business



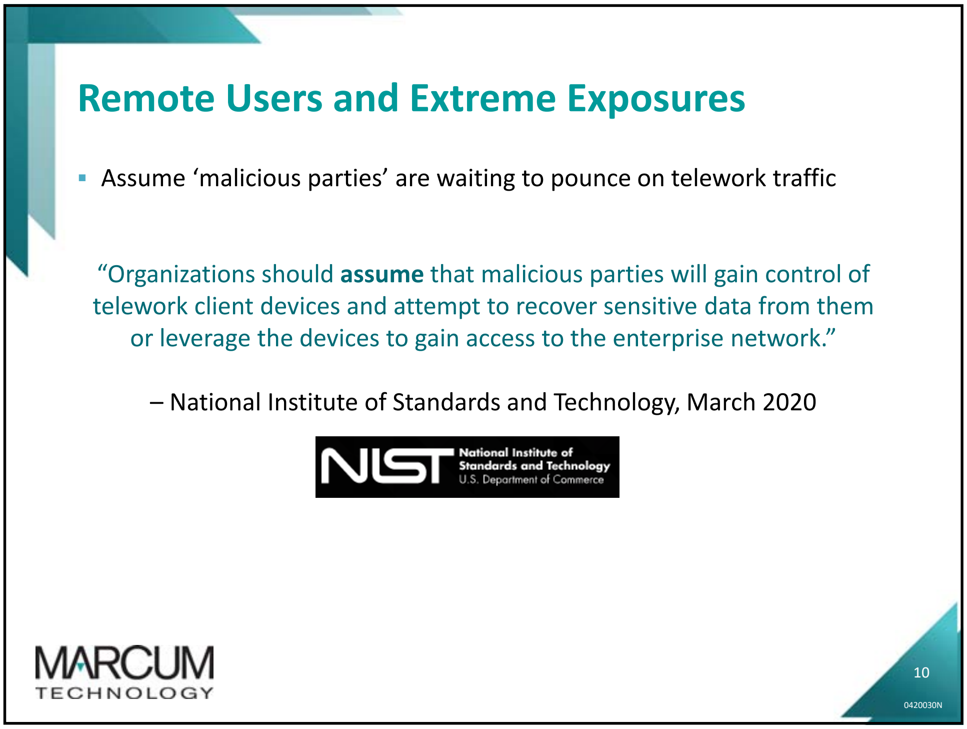
The impact of coronavirus on stock markets since the start of the outbreak

Source: Bloomberg, 27 April 2020, 07:00 GMT

Health Crisis Causing Drastic Shift in Operations

- Private, public, and not for profit companies have virtualized;
- No more travel or live meetings;
- Majority of US citizens remain under Stay at Home orders;
- 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; and
- Hackers are out in larger force and more determined than ever. Insider threats are much higher due to massive changes in a limited period of time. Exploits are highly effective in our current environment.

MARCUM TECHNOLOGY



Remote Users and Extreme Exposures

- 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

NIST National Institute of Standards and Technology U.S. Department of Commerce

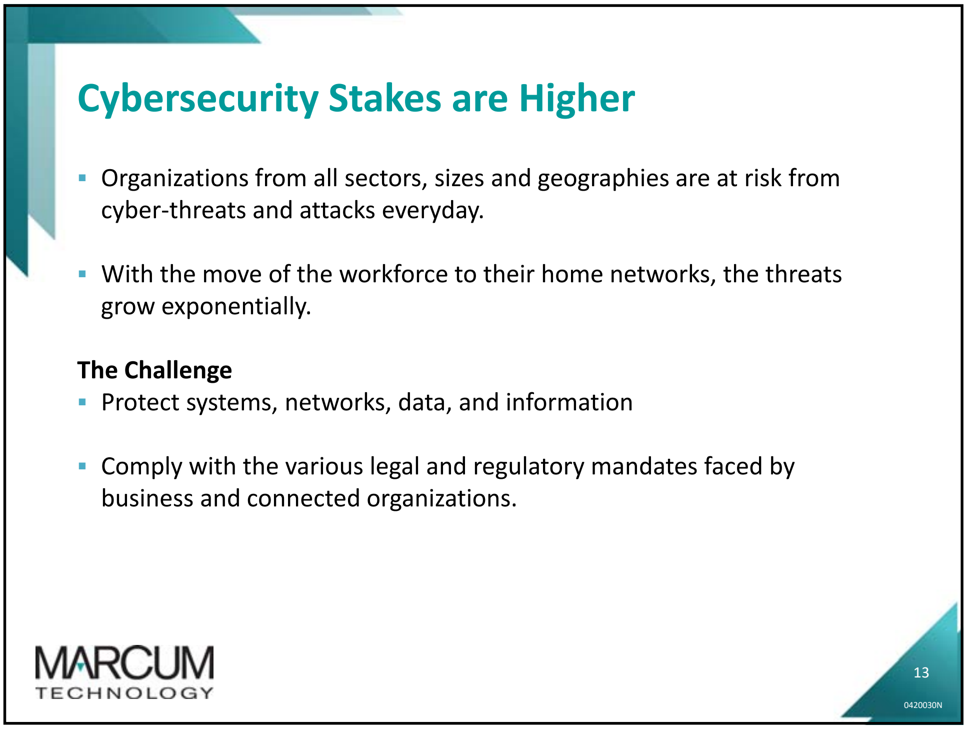
MARCUM TECHNOLOGY

10

0420030N

Cybersecurity Stakes

MARCUM TECHNOLOGY



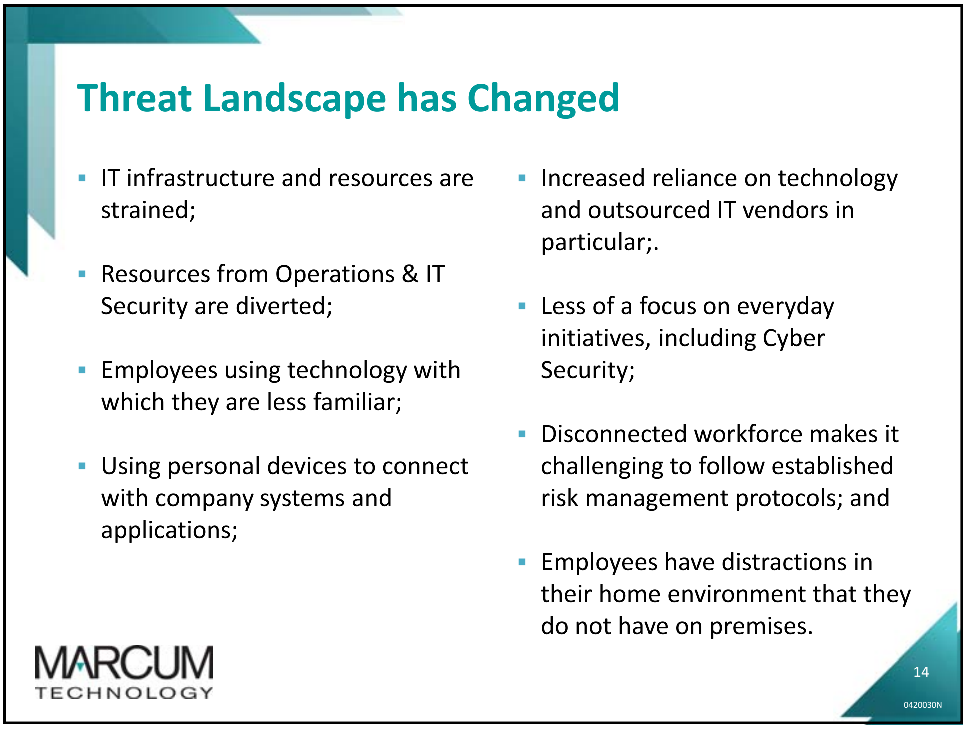
Cybersecurity Stakes are Higher

- Organizations from all sectors, sizes and geographies are at risk from cyber-threats and attacks everyday.
- With the move of the workforce to their home networks, the threats grow exponentially.

The Challenge

- Protect systems, networks, data, and information
- Comply with the various legal and regulatory mandates faced by business and connected organizations.

MARCUM TECHNOLOGY



Threat Landscape has Changed

- IT infrastructure and resources are strained;
- Resources from Operations & IT Security are diverted;
- Employees using technology with which they are less familiar;
- Using personal devices to connect with company systems and applications;
- Increased reliance on technology and outsourced IT vendors in particular;.
- Less of a focus on everyday initiatives, including Cyber Security;
- Disconnected workforce makes it challenging to follow established risk management protocols; and
- Employees have distractions in their home environment that they do not have on premises.

MARCUM TECHNOLOGY

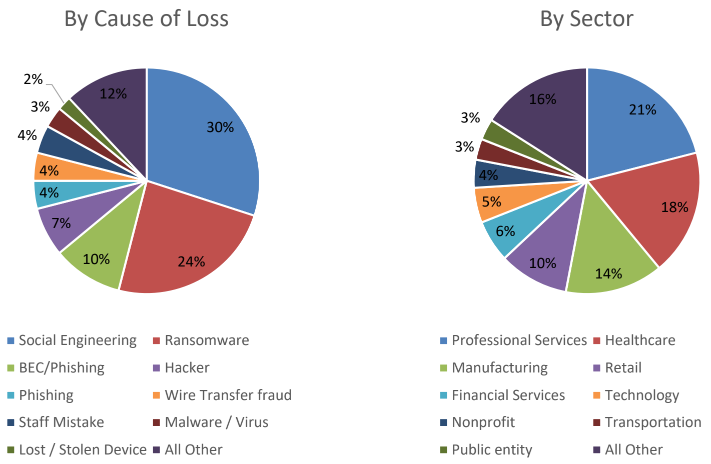
What Do We Have to Lose?

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, loss, leakage or perversion 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.

MARCUM TECHNOLOGY

What Losses Happen and To Whom

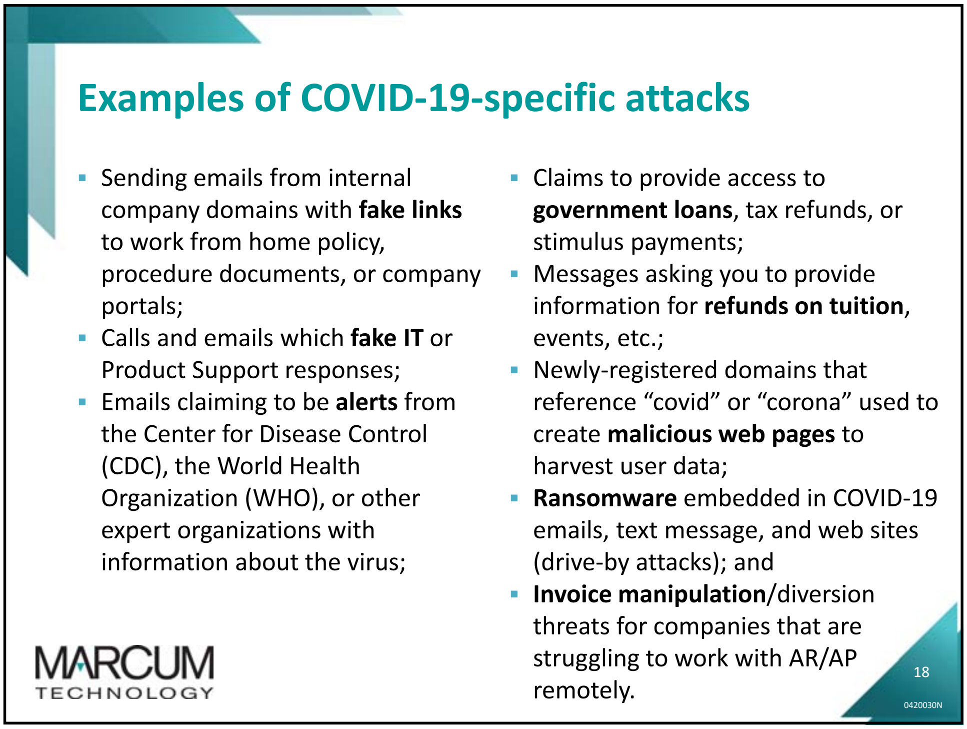


MARCUM TECHNOLOGY

Source: 2019 NetDiligence Cyber Claims Study – Companies up to $2b revenues

Cyber Exploits

MARCUM TECHNOLOGY



Examples of COVID-19-specific attacks

- Sending emails 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 TECHNOLOGY

How To Identify a Data Breach?

The greatest security challenge of this “new normal” is identifying a data breach.

- Most organizations are “hardened” for internal users of infrastructure, not external
- New attack surfaces have opened
  - Home networks/devices
  - Increased use of mobile devices
  - Bring Your Own Device (BYOD)
  - Home Smart/IoT Devices
- Increased legitimate network accesses can hide illegitimate ones
- Increased “noise” in data logs
- How do you enforce critical processes related to sensitive data (e.g., HR, payments)?

MARCUM TECHNOLOGY

Any Single Gap in Security Can Create a Catastrophe

Capital One - Third-party security exposures gained significant attention during July of this year when Capital One announced that “an outside individual gained unauthorized access and obtained certain types of personal information” about Capital One customers and credit applicants;

- The financial services giant says that the “unauthorized individual” was able to exploit a "configuration vulnerability" to steal sensitive records held in an Amazon Web Services (AWS) database;
- The breach exposed 106 million US and Canadian citizens.

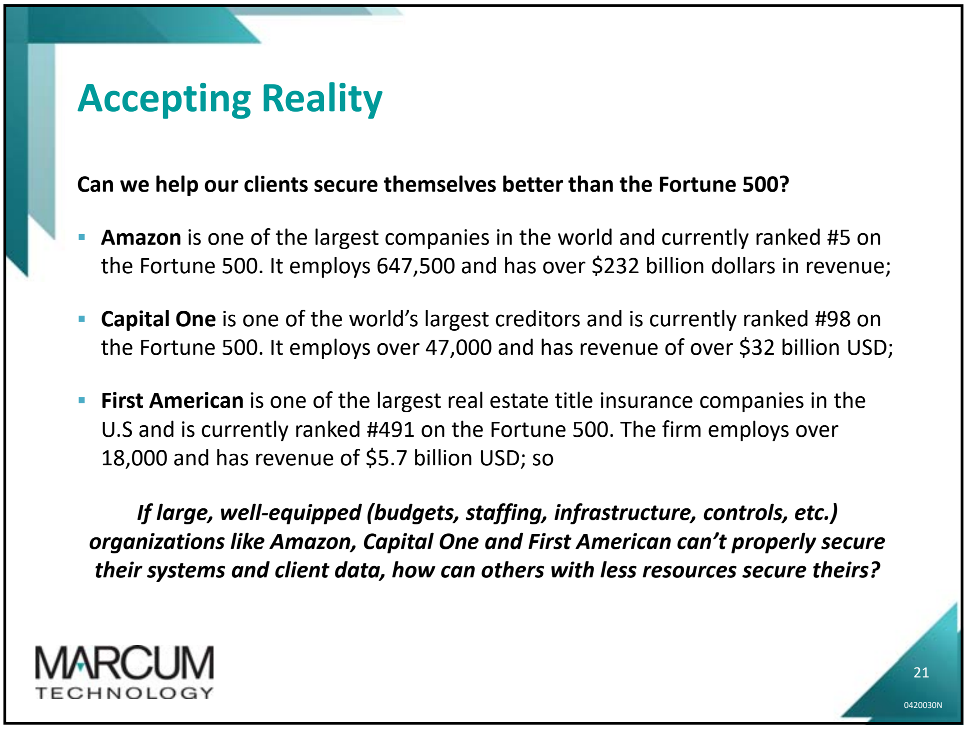
First American Financial - Fortune 500 real estate title insurance company exposed approximately 885 million sensitive records.

- 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.

MARCUM TECHNOLOGY



Accepting Reality

Can we help our clients secure themselves better than the Fortune 500?

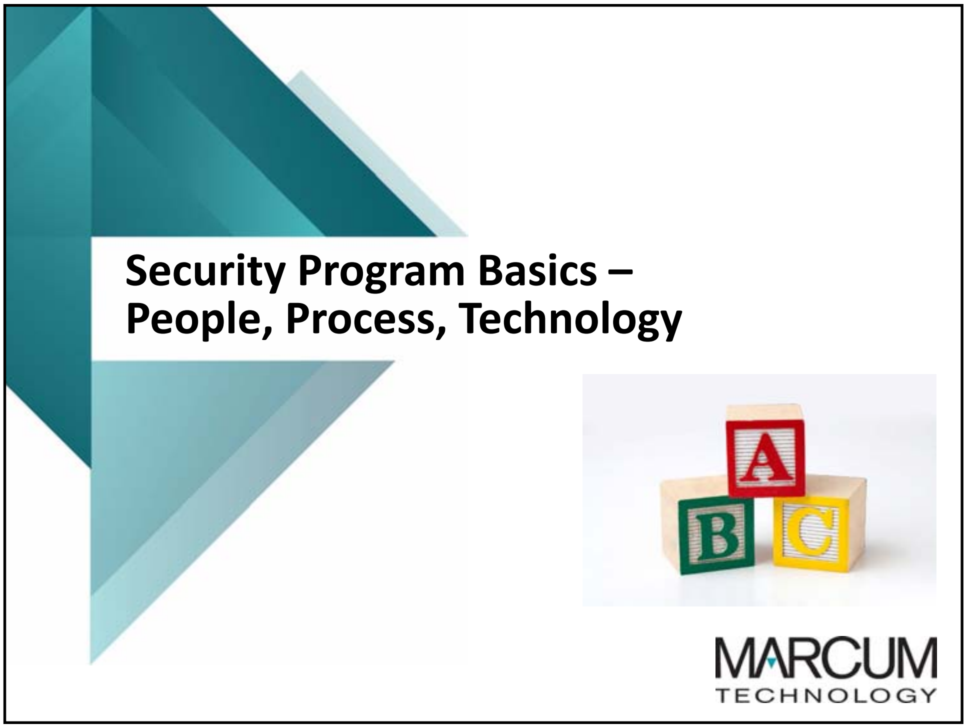
- **Amazon** is one of the largest companies in the world and currently ranked #5 on the Fortune 500. It employs 647,500 and has over $232 billion dollars in revenue;
- **Capital One** is one of the world's largest creditors and is currently ranked #98 on the Fortune 500. It employs over 47,000 and has revenue of over $32 billion USD;
- **First American** is one of the largest real estate title insurance companies in the U.S and is currently ranked #491 on the Fortune 500. The firm employs over 18,000 and has revenue of $5.7 billion USD; so

If large, well-equipped (budgets, staffing, infrastructure, controls, etc.) organizations like Amazon, Capital One and First American can't properly secure their systems and client data, how can others with less resources secure theirs?

MARCUM TECHNOLOGY

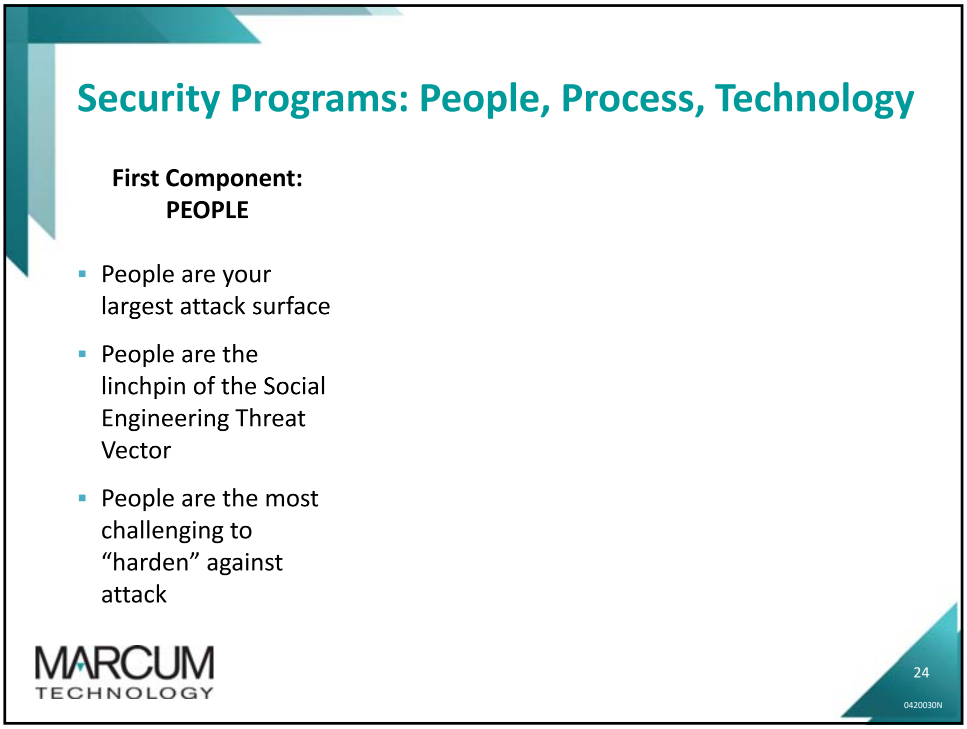
21

0420030N



Security Program Basics – People, Process, Technology

MARCUM TECHNOLOGY



Security Programs: People, Process, Technology

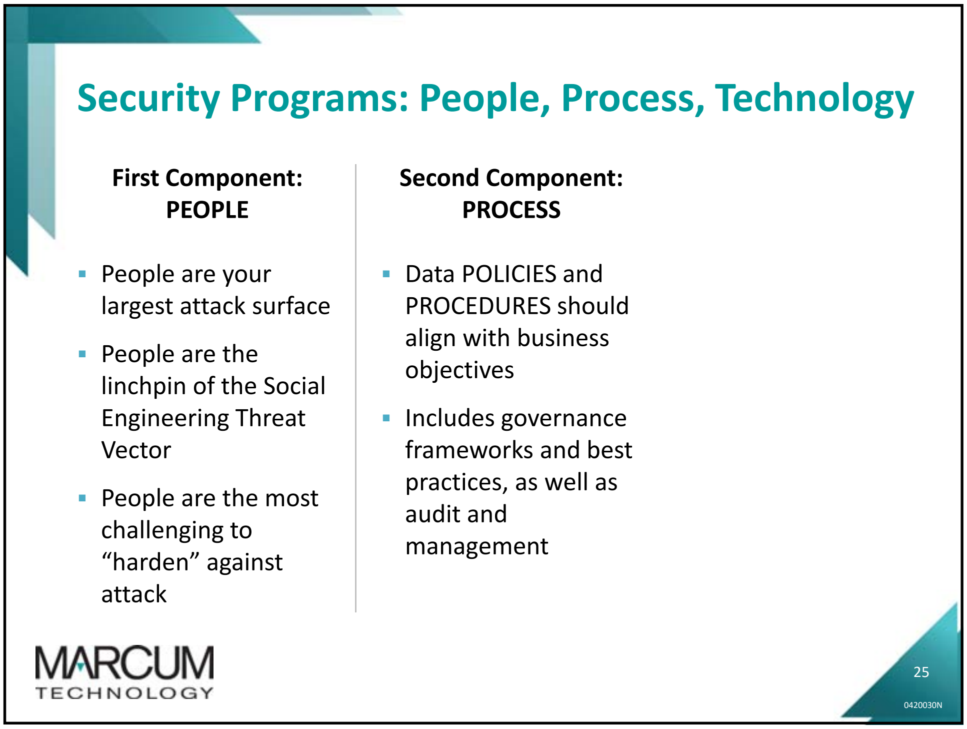
First Component:
PEOPLE

- People are your largest attack surface
- People are the linchpin of the Social Engineering Threat Vector
- People are the most challenging to "harden" against attack

MARCUM
TECHNOLOGY

24

0420030N



Security Programs: People, Process, Technology

First Component:
PEOPLE

- People are your largest attack surface
- People are the linchpin of the Social Engineering Threat Vector
- People are the most challenging to "harden" against attack

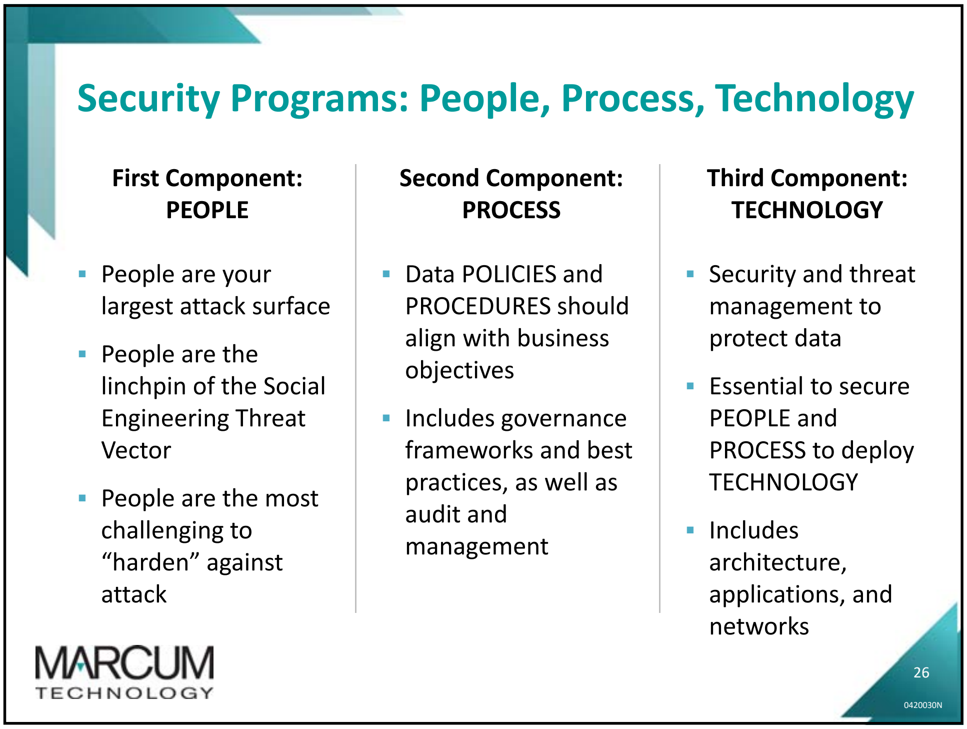
Second Component:
PROCESS

- Data POLICIES and PROCEDURES should align with business objectives
- Includes governance frameworks and best practices, as well as audit and management

MARCUM
TECHNOLOGY

25

0420030N



Security Programs: People, Process, Technology

First Component: PEOPLE

- People are your largest attack surface
- People are the linchpin of the Social Engineering Threat Vector
- People are the most challenging to "harden" against attack

Second Component: PROCESS

- Data POLICIES and PROCEDURES should align with business objectives
- Includes governance frameworks and best practices, as well as audit and management

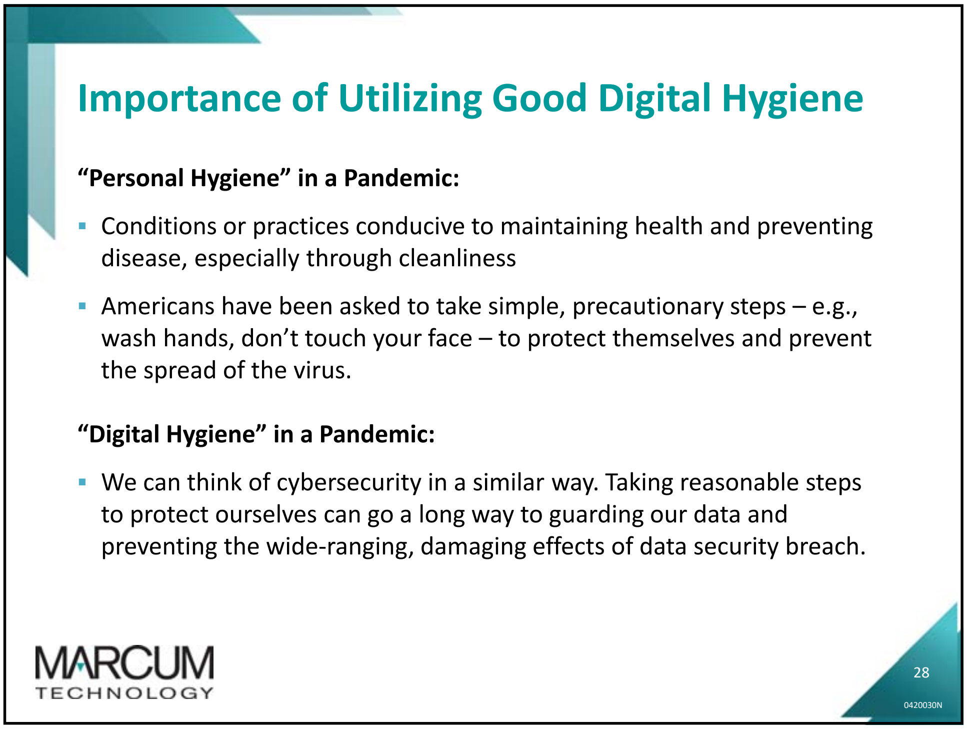
Third Component: TECHNOLOGY

- Security and threat management to protect data
- Essential to secure PEOPLE and PROCESS to deploy TECHNOLOGY
- Includes architecture, applications, and networks

26

0420030N

Focus: People



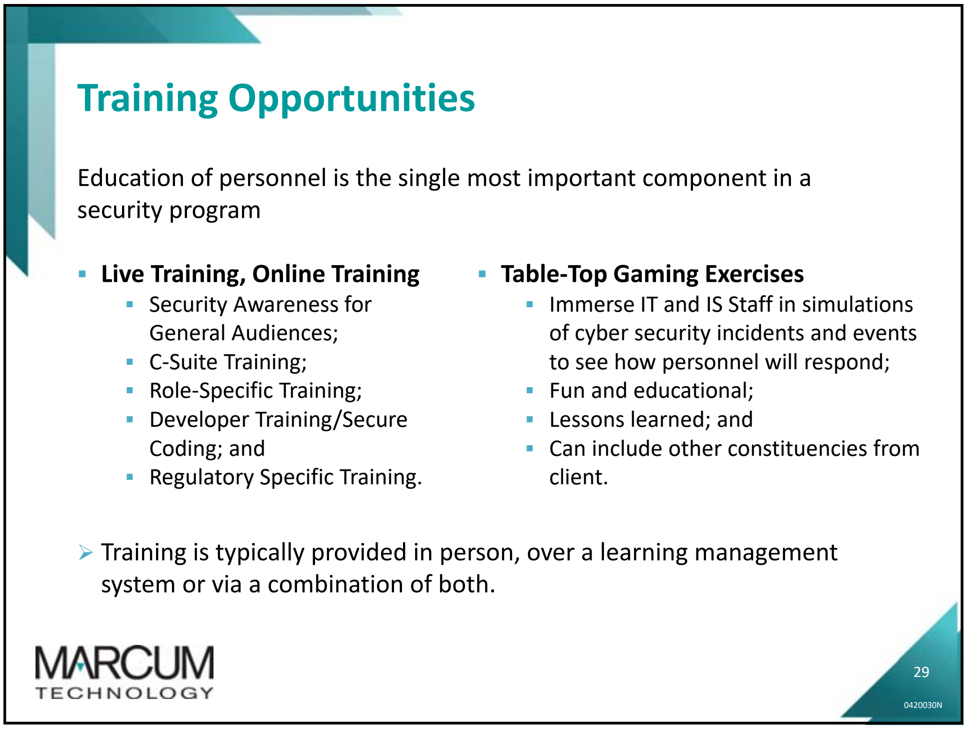
Importance of Utilizing Good Digital Hygiene

“Personal Hygiene” in a Pandemic:

- Conditions or practices conducive to maintaining health and preventing disease, especially through cleanliness
- Americans have been asked to take simple, precautionary steps – e.g., wash hands, don’t touch your face – to protect themselves and prevent the spread of the virus.

“Digital Hygiene” in a Pandemic:

- We can think of cybersecurity in a similar way. Taking reasonable steps to protect ourselves can go a long way to guarding our data and preventing the wide-ranging, damaging effects of data security breach.

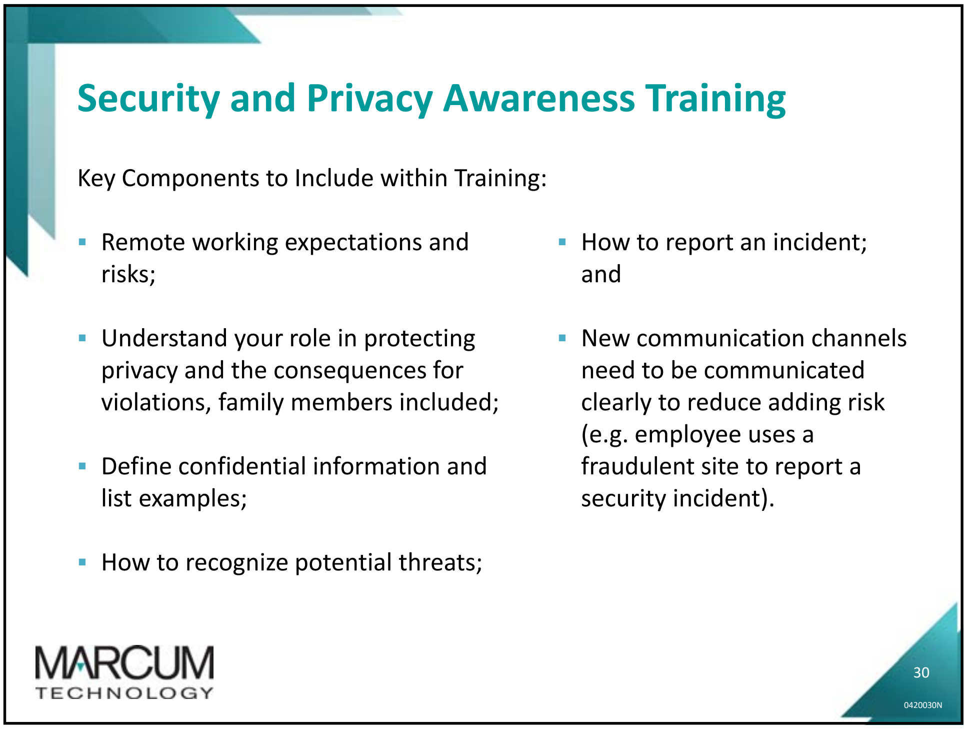


Training Opportunities

Education of personnel is the single most important component in a security program

- **Live Training, Online Training**
  - Security Awareness for General Audiences;
  - C-Suite Training;
  - Role-Specific Training;
  - Developer Training/Secure Coding; and
  - Regulatory Specific Training.
- **Table-Top Gaming Exercises**
  - Immerse IT and IS Staff in simulations of cyber security incidents and events to see how personnel will respond;
  - Fun and educational;
  - Lessons learned; and
  - Can include other constituencies from client.

➢ Training is typically provided in person, over a learning management system or via a combination of both.

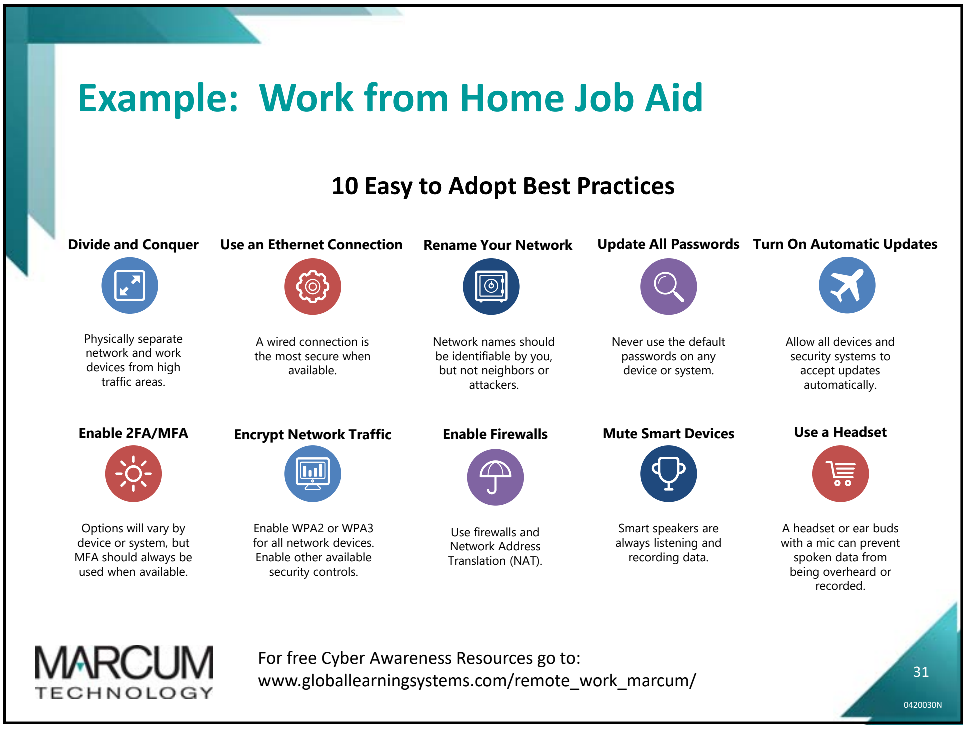


Security and Privacy Awareness Training

Key Components to Include within Training:

- Remote working expectations and risks;
- Understand your role in protecting privacy and the consequences for violations, family members included;
- Define confidential information and list examples;
- How to recognize potential threats;
- How to report an incident; and
- New communication channels need to be communicated clearly to reduce adding risk (e.g. employee uses a fraudulent site to report a security incident).

MARCUM TECHNOLOGY



Example: Work from Home Job Aid

10 Easy to Adopt Best Practices

Divide and Conquer

Physically separate network and work devices from high traffic areas.

Use an Ethernet Connection

A wired connection is the most secure when available.

Rename Your Network

Network names should be identifiable by you, but not neighbors or attackers.

Update All Passwords

Never use the default passwords on any device or system.

Turn On Automatic Updates

Allow all devices and security systems to accept updates automatically.

Enable 2FA/MFA

Options will vary by device or system, but MFA should always be used when available.

Encrypt Network Traffic

Enable WPA2 or WPA3 for all network devices. Enable other available security controls.

Enable Firewalls

Use firewalls and Network Address Translation (NAT).

Mute Smart Devices

Smart speakers are always listening and recording data.

Use a Headset

A headset or ear buds with a mic can prevent spoken data from being overheard or recorded.

MARCUM TECHNOLOGY

For free Cyber Awareness Resources go to:
www.globallearningsystems.com/remote_work_marcum/

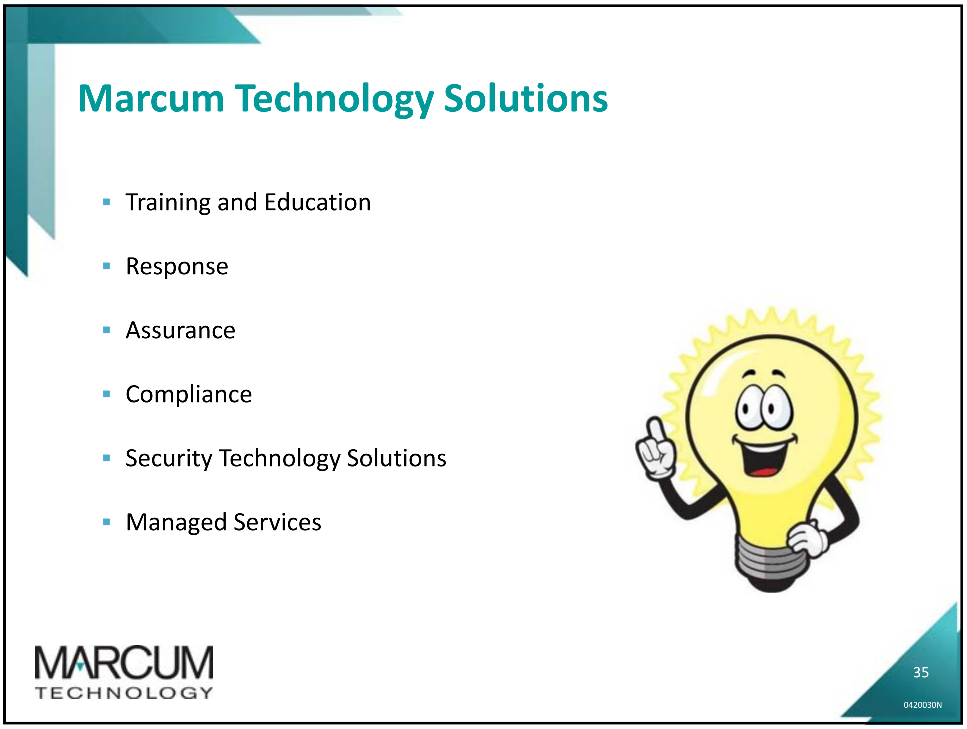
Where Do We Go From Here?

MARCUM
TECHNOLOGY

Where Do We Go From Here?

- In the future, businesses will be begin the process of rebuilding from this crisis
- The COVID-19 pandemic not only created new cybersecurity vulnerabilities, it also exposed existing ones
- The “new normal” of telework is here to stay
- Your people must become security champions
- Policies, processes, and procedures need to be in a constant cycle of update as new threats emerge
- Technology challenges will continue to evolve
- Trusted partners are essential

MARCUM
TECHNOLOGY



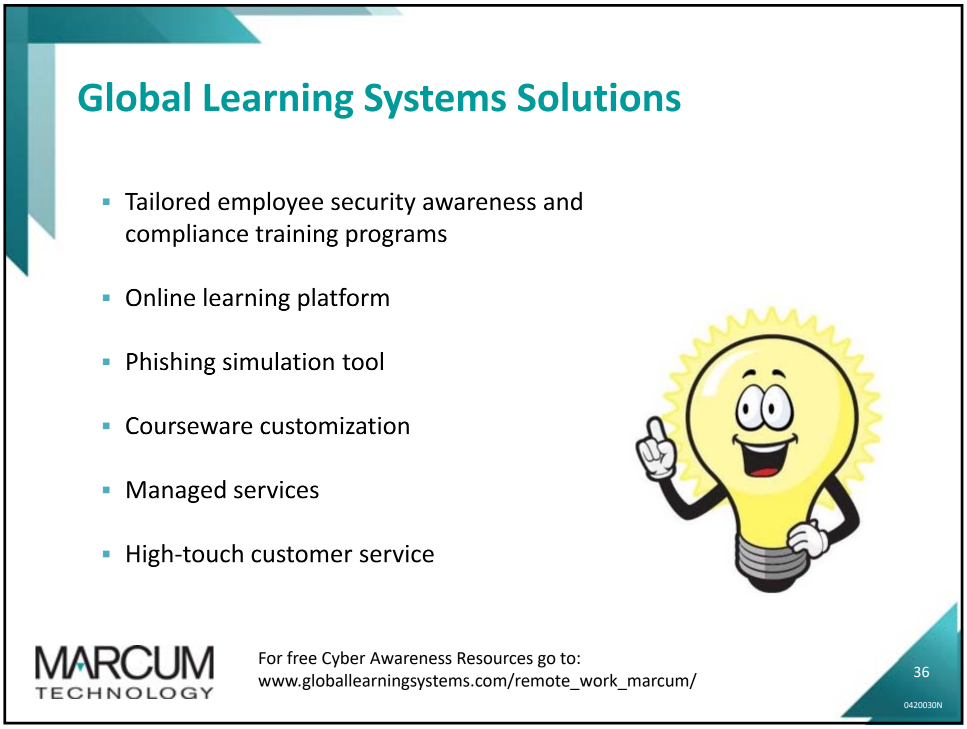
Marcum Technology Solutions

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

MARCUM TECHNOLOGY

35

0420030N



Global Learning Systems Solutions

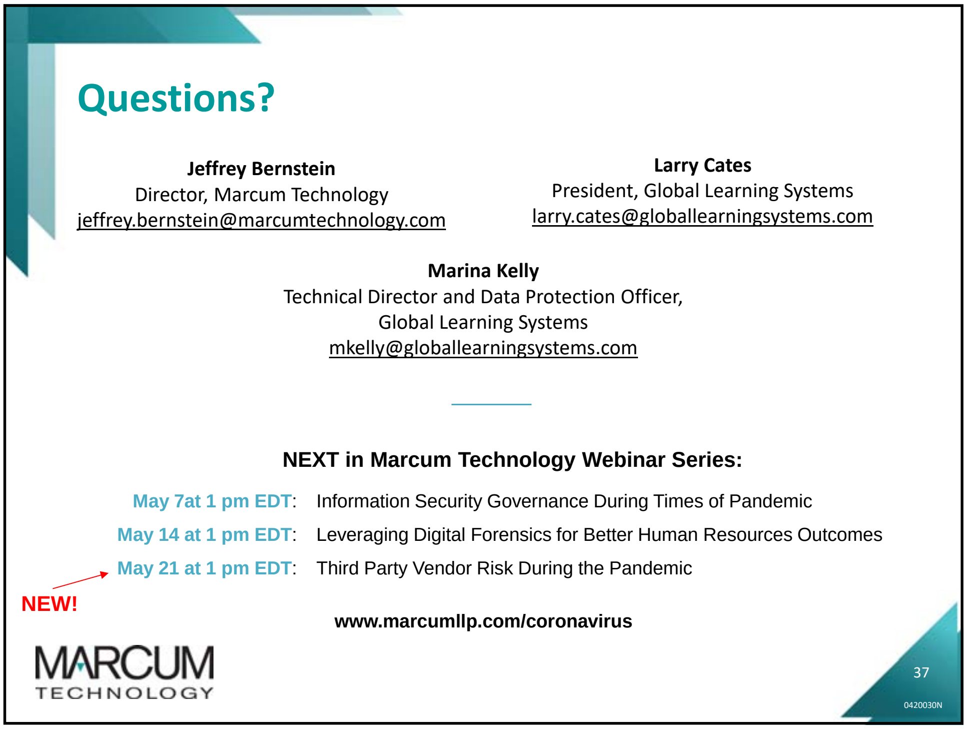
- Tailored employee security awareness and compliance training programs
- Online learning platform
- Phishing simulation tool
- Courseware customization
- Managed services
- High-touch customer service

MARCUM TECHNOLOGY

For free Cyber Awareness Resources go to:
www.globallearningsystems.com/remote_work_marcum/

36

0420030N



Questions?

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

Larry Cates
President, Global Learning Systems
larry.cates@globallearningsystems.com

Marina Kelly
Technical Director and Data Protection Officer,
Global Learning Systems
mkelly@globallearningsystems.com

NEXT in Marcum Technology Webinar Series:

May 7at 1 pm EDT:	Information Security Governance During Times of Pandemic
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

NEW!

www.marcumllp.com/coronavirus

MARCUM
TECHNOLOGY

37

0420030N