PROTECTING BUSINESS FROM CYBERSECURITY THREATS

IN THE WAKE OF COVID-19

April 16, 2020

EPIC Insurance Brokers & Consultants

MARCUM TECHNOLOGY

PROTECTING BUSINESS FROM CYBERSECURITY THREATS IN THE WAKE OF COVID-19

If you have a question during today's broadcast…

1. Type your question in the chat box (technology related questions such as sound) or
2. Ask your question in the Q&A box (CONTENT related questions)

An instructor will either respond in the chat or Q&A, or verbally during the presentation.

IMPORTANT CPE NOTICE

Periodically during today's seminar there will be slides with CPE words. Write these words down. You will receive an email from Marcum University with a link to the webinar recording and the CPE Survey within the next 24 hours.

MARCUM TECHNOLOGY

PROTECTING BUSINESS FROM CYBERSECURITY THREATS

IN THE WAKE OF COVID-19

Marcum LLP has 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.

TECHNOLOGY

Agenda

- Introduction
- How COVID-19 has Changed the Way We Do Business
- Top Concerns for Business Prior to COVID-19 and Currently
- Why Is Security Important and What's at Stake?
- Security Risk Management and the Three Pillars
- Considerations for the Organization
- Advice for End Users
- Easy Fixes
- Cyber Insurance Discussion
- Questions, Answers and Contact Information

MARCUM TECHNOLOGY

Jeff Bernstein

- 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

Adam Glick

- Principal, EPIC Insurance Brokers and Consultants
- Member of EPIC's National Cyber and Management Liability Practice Teams
- Leader of EPIC NYC Media and Advertising Practice
- 20 years of Risk Management and Human Capital experience
  - Financial Services
  - Legal
  - Media and Ad Agency
  - Private Equity Portfolio Company Roll-Ups
  - Employee Benefit Plan Design
- B.S. in Organization and Behavior & Human Resources – Miami University
- Masters from Fordham University

MARCUM TECHNOLOGY

COVID-19 -
Changing the Way We Do Business


CyberSecurity MAGAZINE

TOPICS NEWSLETTER JOB MARKET JOURNALS COVID-19 OFFERS ABOUT

Q1 2020 KnowBe4 Finds Coronavirus-Related Phishing Email Attacks Up 600%

April 9, 2020 Editors Desk

KnowBe4 releases Q1 2020 top-clicked phishing report

TAMPA BAY, Fla., April 9, 2020 /PRNewswire/ — KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, revealed the results of its Q1 2020 top-clicked phishing report.

The results found that phishing email attacks related to COVID-19 were up 600% in Q1 2020. Covering the entire first quarter, simulated phishing tests with an urgent message to check passwords immediately was most popular at 45%. Following this was a coronavirus-related message as the second most popular at 10%. Social media messages are another area of concern when it comes to phishing. Within the same report, KnowBe4's top-clicked social media email subjects reveal new login alerts, password resets and someone may have accessed your account messages are coming onto the radar.

Health Crisis Causing Drastic Shift in Operations

- Organizations racing to virtualize and deploy remote access;
- No more travel or live meetings;
- Three of four US citizens now home (non-essential);
- Businesses in every size, sector and geography are affected;
- Ease of use and access for the telecommuter is critical;
- New collaboration and other technologies are being implemented to optimize productivity;

MARCUM TECHNOLOGY

Top Concerns of Business Q4 2019

Cybersecurity Rose to Top Business Concern Prior to Coronavirus Outbreak

- Allianz Global Business Risks Report for Q4 2019 - cyber security incidents ranked as the most important business risk globally;
- Surveyed 2,718 client respondents from 102 countries/territories included participants from business, brokers and trade organizations, consultants, underwriters, senior managers and claims experts from corporate insurance segments. Surveys taken during Q4 2019 and included large, mid and small-sized enterprises;
- Survey definitions of "cyber-risk" included but were not limited to cybercrime, IT failure/outage, data breaches, ransomware, penalties levied to do non-compliance with legal and regulatory mandates, post breach fines and others.
- Cyber incidents displaced business interruption, changes in regulation and legislation, natural catastrophes, market developments, climate change, fire/explosion, loss of reputation or brand value and the development of new technologies;
- Only 7 years ago "cyber-risk" ranked only 15th in the same survey; and
- Surveys were performed prior to Covid-19.

MARCUM TECHNOLOGY

Top Concerns of Business

MARCUM - HOFSTRA
CEO SURVEY

The Marcum LLP-Hofstra University CEO Survey is a periodic gauge of middle-market CEOs' outlook on the current business environment and their priorities and concerns for the next 12 months.

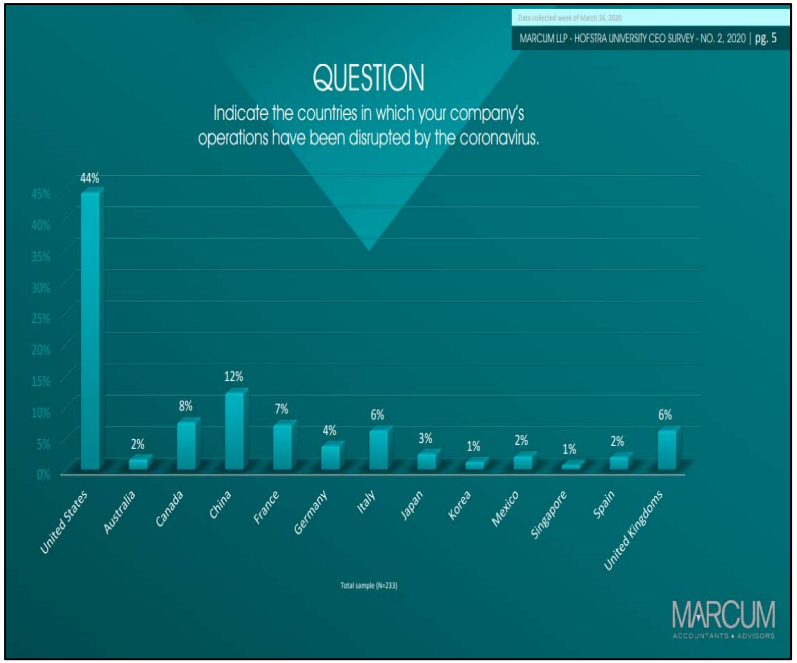
In the Wake of the Coronavirus Outbreak and the Move to a Remote Workforce - Technology Remains a Concern

- Marcum-Hofstra CEO Survey of Disruptions to Coronavirus Q1 2020 found more than half of companies had been disrupted after the beginning of only the first four statewide stay-at-home orders

QUESTION

Indicate whether you are still operating in the countries where your company's operations have been disrupted by the coronavirus.

Country	Operating as normal	Operating at reduced capacity	Not currently operating
United States (230)	19.2%	73.1%	7.7%
Australia (4)	25.0%	50.0%	25.0%
Canada (18)	5.6%	72.2%	22.2%
China (29)	0.0%	55.2%	44.8%
France (17)	11.8%	82.4%	5.9%
Germany (9)	19.2%	73.1%	7.7%
Italy (15)	0.0%	20.0%	80.0%
Japan (6)	0.0%	83.3%	16.7%
Korea (3)	0.0%	66.7%	33.3%
Mexico (5)	20.0%	80.0%	0.0%
Singapore (2)	0.0%	100.0%	0.0%
Spain (5)	20.0%	0.0%	80.0%
United Kingdom (15)	6.7%	80.0%	13.3%



MARCUM
TECHNOLOGY

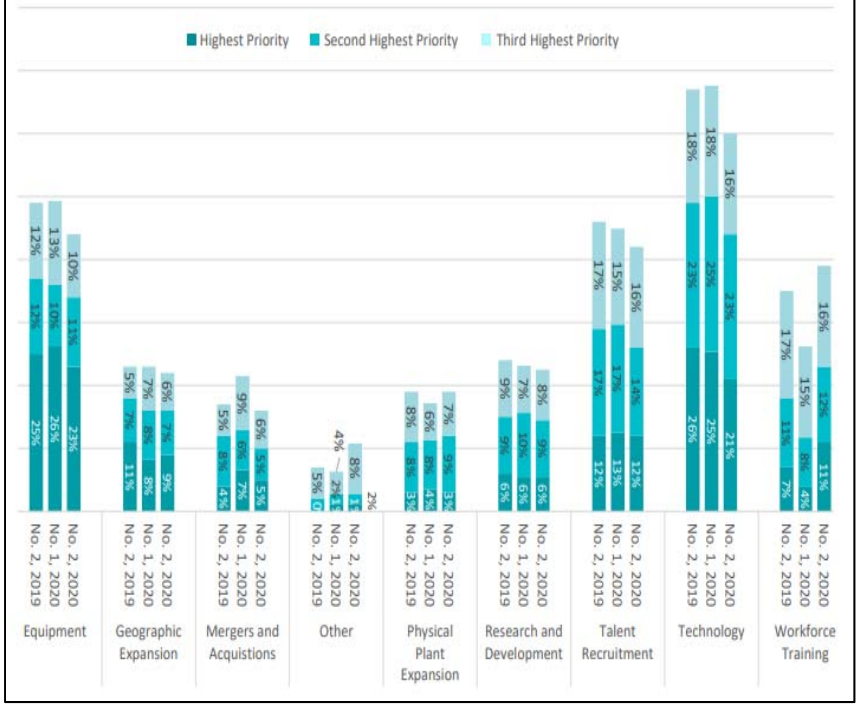
Top Concerns of Business Q4 2019

MARCUM - HOFSTRA
CEO SURVEY

The Marcum LLP-Hofstra University CEO Survey is a periodic gauge of middle-market CEOs' outlook on the current business environment and their priorities and concerns for the next 12 months.

Technology also Remains Top Priority

QUESTION:
In which ways do you plan to invest in your company?



QUESTION:
What are the most important influences for your business planning in the next 12 months?

MARCUM
TECHNOLOGY

Top Concerns of Business Q4 2019

MARCUM - HOFSTRA CEO SURVEY

The Marcum LLP-Hofstra University CEO Survey is a periodic gauge of middle-market CEOs' outlook on the current business environment and their priorities and concerns for the next 12 months.

Survey Participants

DEMOGRAPHICS

Which of the following best describes your company's industry?

Construction/Engineering/Mining	21	8.2%
Energy/Utility	10	3.9%
Financial Services	29	11.3%
Government and Non-profit	11	4.3%
Health Care (Providers and Payers)	14	5.5%
Manufacturing (Consumer Goods)	10	3.9%
Manufacturing (Industrial Goods)	31	12.1%
Personal/Consumer Services	7	2.7%
Professional Services	38	14.8%
Real Estate	10	3.9%
Restaurants/Catering/Hospitality	8	3.1%
Retailing	18	7.0%
Technology Services	22	8.6%
Transportation	11	4.3%
Wholesale/Distribution	6	2.3%
Other *	10	3.9%
Total	**256**	**100.0%**

*Other: Agriculture (2); Aircraft repair (1); Arts/Entertainment (2); Sports/Recreation (2); Vending machine services (1); Unspecified (2)

What best describes your title?

Owner	67	26.2%
CEO	52	20.3%
Divisional President	47	18.4%
Managing Partner	40	15.6%
President	42	16.4%
Founder	4	1.6%
Chairman	4	1.6%
Total	**256**	**100.0%**

What is the total number of permanent employees in your company?

Less than 50	61	23.8%
50 to 99	26	10.2%
100 to 499	43	16.8%
500 to 999	42	16.4%
1,000 to 2,499	34	13.3%
2,500 to 4,999	25	9.8%
5,000 or more	23	9.0%
Not sure/Decline to say	2	0.8%
Total	**256**	**100.0%**

In which revenue size range was your company last year?

Less than $5 million	59	23.0%
$5 million to $9.9 million	28	10.9%
$10 million to $24.9 million	22	8.6%
$25 million to $49.9 million	25	9.8%
$50 million to $99.9 million	23	9.0%
$100 million to $249.9 million	22	8.6%
$250 million to $499.9 million	17	6.6%
$500 million to $999.9 million	26	10.2%
$1 Billion or more	29	11.3%
Not sure/Decline to say	5	2.0%
Total	**256**	**100.0%**

MARCUM ACCOUNTANTS ▲ ADVISORS

MARCUM TECHNOLOGY

CPE WORD – Write this down and submit in the course evaluation for CPE credit

RED

MARCUM TECHNOLOGY

Current World Health Crisis

Why is Cybersecurity More Important than Ever?

- The COVID-19 crisis has triggered “Shelter in Place” orders that have forced businesses to migrate workers to remote home based operations;
- Remote connectivity is all about “ease of use and access” but ease of access almost always comes at the cost of security;
- Two Primary drivers of concern for IT security:
  - Protect systems, networks, applications, data, information, productivity, brand, people and property; and
  - Comply with the various legal and regulatory mandates faced by business and connected organizations.

MARCUM TECHNOLOGY

Current World Health Crisis

What's At Stake?

Data security compromises result in very costly and difficult situations:

- Identity theft of clients and/or personnel;
- Loss and/or leakage of private data and sensitive information;
- Loss of competitive advantage;
- Fraud and/or sabotage;
- Theft of funds, data or intellectual property;
- Disruption to the business and productivity;
- Non-compliance with laws and regulations;
- Damage to brand and reputation; and
- Total collapse of the business.

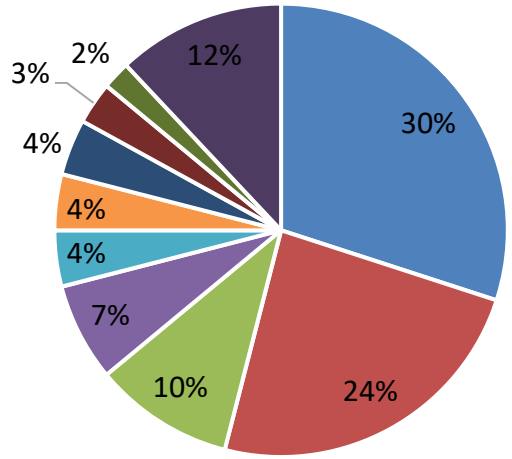
Organizations from all sectors, sizes and geographies are at risk from cyber threats and attacks.

With the move of the workforce to their home networks, the threat has grown exponentially.

MARCUM TECHNOLOGY

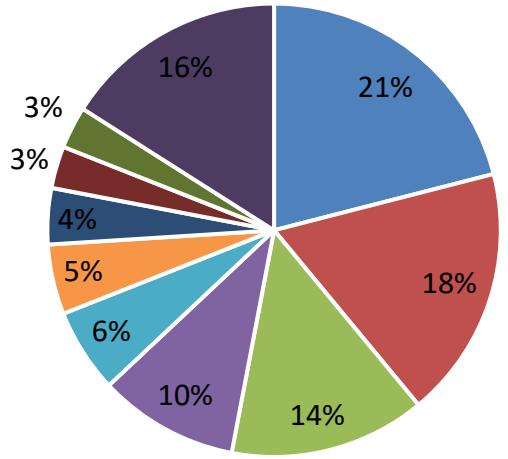
What Losses Happen and To Whom

By Cause of Loss



- Social Engineering
- Ransomware
- BEC/Phishing
- Hacker
- Phishing
- Wire Transfer fraud
- Staff Mistake
- Malware / Virus
- Lost / Stolen Device
- All Other

By Sector



- Professional Services
- Healthcare
- Manufacturing
- Retail
- Financial Services
- Technology
- Nonprofit
- Transportation
- Public entity
- All Other

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

MARCUM TECHNOLOGY

Security Risk Management

Three Pillars - Confidentiality, Integrity and Availability

- People
  - 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
    - Formal guides 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;

- Technology
  - Adopt and leverage the latest cutting-edge technologies - message and conferencing solutions, collaboration tools; cloud and archiving solutions, spam and content filtering, malware and anti-virus, Security monitoring (IDS, IPS, SIEM), performance, availability and resiliency, security devices; 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.
Even a single mistake can wreak havoc.

MARCUM TECHNOLOGY

Best Practices for the Organization

Adopt technologies that will enable the workforce to be productive but secure

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

Develop new or enhance existing security policies:

- Publish IT policies governing protection of network systems and data, including policies on secure telecommuting, acceptable usage, BYOD, data retention and destruction;
- Incident response plan;
- Business Continuity and Disaster Recovery Plans (BCP/DRP);
- Vendor governance (we are only as secure as our weakest partner that has access to our data);

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

- Networks, applications, systems; and
- Staff - perform social engineering / phishing exercises studies on personnel to both test and develop 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 or partner with a provider like Marcum to assist;
- 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.

MARCUM TECHNOLOGY

Cyber Insurance is a must!

Advice for End Users

- **Be skeptical** of any communication relating to COVID-19 and the economic stimulus package - The FTC, SEC and others have issued warnings about an increase in criminal scams that exploit the current crisis;
- **Social engineering** remains the exploit of choice for cybercriminals - be equally skeptical of all other emails, SMS, IM and text messages by examining sender and domain sources carefully. Review and verify all links (URLs) and attachments for legitimacy prior to clicking/opening them;
- Enable and utilize **Multi-Factor Authentication (MFA)** whenever it is 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;
- **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;

MARCUM TECHNOLOGY

Advice for End Users

- **Encrypt everything** - encryption places stored and transmitted data into an 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;
- 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;
- **Avoid using public computing systems and Wi-Fi connections**, use only SSID protected wireless networks and preferably utilizing a VPN connection;
- Download and use mobile apps from **reputable sources only** (Apple, Amazon, etc). If you are unsure, about the authenticity of an app, research it prior to downloading. Also - delete unused apps;

MARCUM TECHNOLOGY

Advice for End Users

- **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 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 organization's IT Team, partners like us and/or your local police. The FTC and the FBI also have resources online if you've fallen victim to cybercrime;

MARCUM TECHNOLOGY