IDENTIFYING CYBER THREATS CREATED BY REMOTE ACCESS

April 23, 2020

MARCUM TECHNOLOGY

Agenda

- Introduction
- How COVID-19 has Changed Business
- Adversaries and their Motivation
- Changing Threat Landscape
- Mitigation Strategies
- Recent Compromises
- Advice for End Users
- Questions, Answers and Contact Information

MARCUM TECHNOLOGY

2

0420026N

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

3

0420026N

Jaike Hornreich

- 12 Year information technology / data privacy industry veteran.
- Founded Marcum Technology Cybersecurity Consulting Team.
- Responsible for 100s of complex Security Reviews, Penetration Tests, and Compliance (SOC 1 / 2, HITRUST, etc.) annually throughout career for organizations of all size and scope;
- Extensive experience in privacy, compliance, and related risk areas with understanding of business considerations, limitations, and other factors to design comprehensive solutions for unique compliance, regulatory, and security requirements;
- Security, Audit, and Compliance certifications :
  - Certified Information Systems Auditor (CISA);
  - GIAC Web Application Penetration Test (GWAPT);
  - GIAC Penetration Test (GPEN);
  - Core Impact Certified Professional (CICP); and
  - HITRUST Certified Practitioner (CCSFP).

MARCUM TECHNOLOGY

4

0420026N

Remote Workforce Risk – Here To Stay

MARCUM TECHNOLOGY

COVID-19 Has Changed Business Forever

- Organizations racing to virtualize and deploy remote access solutions;
- Exacerbating the transition to secure video conferencing and reduced physical interaction;
- Organizational risk factors now include home networks, personal devices, and friends and family of employees.
- Businesses in every size, sector and geography are affected;
- Unknown cloud solutions being implemented without knowledge, review, or approval of IT Management; and
- Losing direct in-house control over corporate secrets and other confidential data.

➢ **It has become harder than ever to secure the business and equally challenging to remain compliant with legal and regulatory demands.**

MARCUM TECHNOLOGY

6

0420026N

Attack Vectors of the Remote User

- The pervasiveness of mobile computing, wireless networking, hosted cloud services and the internet of things also creates advantages for hackers, as they only need to find one vulnerable point to successfully perpetrate their attacks;
- With the move to a remote workforce we often trade security for ease of use and access;
- "Attack surface" has increased exponentially making us a fairly easy and accessible target. This refers to all of the end points where unauthorized users and attackers can enter, extract or corrupt data;
- Main attack vectors include:
  - The remote user;
  - The remote users system;
  - The configuration of the system which includes everything on it as well as the security controls enabled to protect those components; and
  - Physical elements.

MARCUM TECHNOLOGY

7

0420026N

Dynamic Adversaries and Motives

- **Disgruntled family members, children, spouses, and friends**
  - Reputational harm to key personnel.
- **Cyber-criminals, competitors, foreign nations, and hacktivists**
  - Stock price manipulation.
  - Theft of trade secrets, financial data, or otherwise confidential information.
  - Theft of PII, PHI of individual users for use in other attacks.
  - Supply chain infiltration, installation of malware or other remote access tools.
  - Access cardholder data.
  - Targeted attacks on individual system users.
- **Script kiddies and bots**
  - Because they can; low effort due to security lapses; easy wins.

MARCUM TECHNOLOGY

8

0420026N

The Changing Risk and Threat Landscape

MARCUM TECHNOLOGY

Third Party Vendor Risk

Increased reliance on 3rd parties for data security and privacy needs.

- **Know Your Vendors** – Vendor risk management becomes a higher priority, not a checkbox.
- **Know your Data** – Need to know the type of data transmitted or processed and to whom.
- **Know your Risk** – Data and vendor risk classifications should be revisited.
- **Mitigate the Risk** – Implement a layered approach to new data identification (manual processes, automated tools, etc.).

➢ This applies to all in-house or controlled data, whether that be internal employee, customer, user data, or all of the above.

MARCUM TECHNOLOGY

10

0420026N

Third Party Vendor Risk

New tools and easy access are great, but at what risk?

- **Single Sign-on Solutions**
  - Integration or other end-user misconfiguration, permitting unintended elevated access to users.
  - A bug in one of these solutions could (worst case) provide access all connected environments for a single user or even all users.
- **Insurance, HR, and other Personal Data Intensive Platforms**
  - Inappropriate ability to access PHI.
    - Social security numbers
    - Medical data or results
  - Inappropriate ability to access Financial Data
    - Payroll or bonus information
    - Company financial records (internal or external)
- **Remote Access**
  - Unauthenticated administrative access provided to an attacker
  - Misconfiguration exposing critical network components

MARCUM TECHNOLOGY

11

0420026N

Third Party Vendor Risk

New tools and easy access are great, but at what risk?

- **Secure Video Conferencing**
  - Eavesdropping, insecure software, unknown system changes with many new platforms.
- **Cloud File Storage / Collaboration Tools**
  - Inappropriate access to data.
  - Data sprawl, unable to monitor or manage, or maintain compliance with data privacy requirements.
- **Subservice Organizations**
  - Do your data processing vendors also prioritize the assessment of their vendors?

➢ Security is only as safe as the weakest link in the chain and is becoming more opaque.

MARCUM TECHNOLOGY

12

0420026N

Network and Device Security

- **Laptops, Workstations, Personal Devices**
  - New solutions are required to prevent unintentional exposure.
  - Remote workforce creates complexities to maintaining security patching.
  - Access permissions defined for users by device such as firm laptop vs personal phone.
  - New physical security risks to consider when a remote workforce is a factor.
  - Helpdesk / device repair or maintenance.
  - Local device configuration changes to reduce insecure local network threats.
- **Firewall / Router Changes**
  - Insecure implementation of remote access solution / quick fixes.
- **Hybrid / Cloud Environments**
  - New technology requires appropriate staff, training and experience to implement securely.

MARCUM TECHNOLOGY

13

0420026N

Legacy Applications and Backend Services

Legacy ERP and other EOL business systems are security risks.

- **Require Outdated and Insecure Operating Systems**
  - A critical system running on Windows 2000 can expose an organization to undue risk.
- **Vulnerable to Exploits**
  - Unpatched, end of life, or otherwise outdated software contain vulnerabilities.
- **Require Excessive Permissions to Function**
- **Backbone of an Organization?**
  - Patchwork of service and legacy employee accounts running key business processes.

➢ When introducing remote access / workers, these risks are further compounded.

MARCUM TECHNOLOGY

14

0420026N

Data Backup, Retention, and Disposal

- **Local / On-Site Processing Interruptions**
  - Can key personnel work remote? What data is needed to do their job? Would providing access to that data remotely be a security risk?
- **Third Party Service Failure**
  - There is no room for forgiveness when critical data is lost due to poor planning.
  - A properly outlined, defined, and tested incident response and data restoration testing might though.
- **Physical / Hybrid / Cloud**
  - Inconsistent processing requirements across multiple environments without a defined policy.
  - Sprawl with lack of tight controls could lead to key data loss or inability to meet regulations.
- **Compliance**
  - GDPR, CCPA, and other privacy frameworks define strict data handling requirements that extend to all locations information resides.

MARCUM TECHNOLOGY

15

0420026N

End-User Risk

End-users habitually fail to practice good digital hygiene and fall victim to phishing and other social engineering exploits

- Network Access Permissions Don't Discriminate
  - Everyone with access to business resources can be a security risk to the business, from the CEO to intern.
- Increased Distractions
  - Spearphishing is amazingly easy to fall victim to when most vigilant.
  - Now, with family at home, staying mentally aware is even more critical, with attacks up exponentially related to COVID.
  - The vast majority of security breaches begin with human error – opening a malicious attachment, website, phished credentials.
- Insecure Home Networks
  - Other devices with malware, weak credentials, increased man-in-the-middle attack risk.

MARCUM TECHNOLOGY

16

0420026N

Other Considerations

Balancing privacy and security rights of employees, their personal lives, and asset costs.

- How far is too far?
  - Is there a right to assess external (and even internal) networks of employees?
  - Is social engineering testing and monitoring of employee social media accounts permissible?
- Is a secure device issuance and management program needed?
- How robust are endpoint protection systems? Do they cover all endpoints?

MARCUM TECHNOLOGY

17

0420026N

Mitigation Strategies

MARCUM TECHNOLOGY

Verify Your Security

- External and Internal Network Penetration Testing
  - Many emergency or rushed changes can lead to mistakes and accidental exposures.
- Network Segmentation Testing
  - Verify Firewall ACLs are set inline with the Network Diagram
  - Can legacy software risk be reduced
- Red-Team Exercises
- Penetration Testing of Applications
  - In-house and Vendor Developed
- Domain, Server, and Workstation Policy Review
- Remote Access and Network Configuration Reviews
- Device Hardening and Baseline Configuration Review
- Wireless Network Surveys
- Mobile Device Security Assessments

MARCUM TECHNOLOGY

19

0420026N

Stay Vigilant

- **Execute Advanced Social Engineering Exercises**
  - Spearphishing
  - Vishing
  - Customized attacks utilizing publicly known company information to lower guard.
  - Forged or otherwise malicious sites
  - Leveraging stolen credentials to verify endpoint security
- **Data Monitoring Solutions**
  - Know when employee or company data, passwords, etc. are potentially leaked through a breach.

MARCUM TECHNOLOGY

20

0420026N

Review Policies and Procedures

- Policy Management
- Risk Management
- Data Management
- Systems Access / Roles
- Data Confidentiality
- Auditing
- Application Development Policy
- Configuration Management
- Breach / Incident Response and Reporting
- Disaster Recovery
- Disposable Media
- IDS
- Vulnerability Scanning / Penetration Testing
- Data Integrity
- Data Retention
- Employees
- 3rd Party Vendor / Contractor Management

MARCUM TECHNOLOGY

21

0420026N

Inventory New Risks

Execute a top-to-bottom review of newly identified risks through security assessments performed, security incidents, and internal meetings to perform an updated risk assessment.

			Adversarial Threat Source Characteristics														
	Threat Event	Threat Type (Adversarial/Non-Adversarial)	Capability	Intent	Targeting	Non-Adversarial Range of Effects	Relevance	Likelihood Of Threat Initiation or Occurence	Vulnerabilities	Severity of Vulnerability	Predisposing Conditions	Pervasiveness of Predisposing Conditions	Likelihood Initiated Threat Succeeds	Overall Likelihood	Level of Impact	Risk
NEFARIOUS ACTIVITY/ ABUSE	Spyware or deceptive adware	Adversarial												Pending		Pendi
	Viruses	Adversarial												Pending		Pendi
	Rogue security software/ Rogueware/ Scareware	Adversarial												Pending		Pendi
	Exploits/Exploit Kits	Adversarial												Pending		Pendi
	Social Engineering	Adversarial												Pending		Pendi
	Phishing attacks	Adversarial												Pending		Pendi
	Spear phishing attacks	Adversarial												Pending		Pendi
	Abuse of Information Leakage	Adversarial												Pending		Pendi
	Leakage affecting mobile privacy and mobile applications	Adversarial												Pending		Pendi
	Leakage affecting web privacy and web applications	Adversarial												Pending		Pendi
	Leakage affecting network traffic	Adversarial												Pending		Pendi
	Leakage affecting cloud computing	Adversarial												Pending		Pendi
	Generation and use of rogue certificates	Adversarial												Pending		Pendi
	Loss of (integrity of) sensitive information	Adversarial												Pending		Pendi
	Man in the middle/ Session hijacking	Adversarial												Pending		Pendi
	Social Engineering / signed malware (e.g. install fake trust OS updates – signed malware)	Adversarial												Pending		Pendi
	Fake SSL certificates	Adversarial												Pending		Pendi
	Manipulation of hardware and software	Adversarial												Pending		Pendi
	Anonymous proxies	Adversarial												Pending		Pendi
	Abuse of computing power of cloud to launch attacks (cybercrime as a service)	Adversarial												Pending		Pendi
	Abuse of vulnerabilities, 0-day vulnerabilities	Adversarial												Pending		Pendi
	Access of web sites through chains of HTTP Proxies (**Obfuscation**)	Adversarial												Pending		Pendi
	Access to device software	Adversarial												Pending		Pendi
	Alternation of software	Adversarial												Pending		Pendi
	Rogue hardware	Adversarial												Pending		Pendi
	Manipulation of information	Adversarial												Pending		Pendi
	Repudiation of actions	Adversarial												Pending		Pendi
	Address Space hijacking (IP prefixes)	Adversarial												Pending		Pendi

MARCUM TECHNOLOGY

22

0420026N

Vendor Risk Assessment

- Inventory of current vendors with access to relevant data.
- Assess security risk and compliance for each.
  - Perform penetration testing if necessary.
- Obtain missing or updated confidentiality, security, and other data-handling agreements.
- Obtain evidence vendor meets internal risk requirements.
- Implement processes to manage the collection and review of vendors as they are on-boarded, and, regularly thereafter.

MARCUM TECHNOLOGY

23

0420026N

Update Security and Privacy Awareness Training

Key Attributes to Include Within Training:

- Include 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.
  - 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

24

0420026N

Monitoring and Tracking

Knowing where risks exist, having endpoints inventoried and protected, are more important than ever.

- SIEM Monitoring / SIEM Challenges
- Monitoring various areas of the Defensive Layers
- Strategically placed defensive layers to accommodate remote workers
- Monitoring remote and cloud workforce
- Insider Threat Monitoring
- Data Loss Prevention
- Possible credential sharing
- Monitor for suspicious logins
- Multifactor authentication requirements
- Security Events Collection from the ground, up.
- Security Event Correlation
- Event retention for behavior monitoring
- Monitoring workforce productivity.

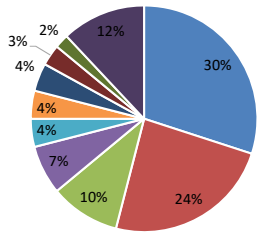
MARCUM TECHNOLOGY

25

0420026N

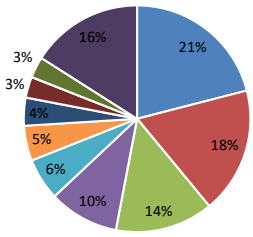
What Losses Happen and To Whom

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

MARCUM TECHNOLOGY

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

26

0420026N

Don't Think If – Think When and How You Recover

MARCUM TECHNOLOGY

Recent Compromises / Investigations

- Large publicly held insurer's **mobile app** leaking PII - no credentials or permission to test, publically held, client is a hedge fund. What would you do next?;
- Law firm **rogue access point** - wireless survey identifies rogue access point hidden within the casing of a carbon monoxide alarm;
- Kryptolocker **ransomware** downloaded after email phishing exploit drives user to malicious website - ransomware used by extortionists for financial gain - 36 systems in 2 days = $250,000 cost to clean up;
- Admin level staff member at a Fortune 500 technology company misconfigures **Google Drive** allowing unauthenticated access to all files (many including PII) to anyone on the using the site;
- **Social Media** - adversary posing as a trusted insider gains access to trusted business/social media networks of legitimate users. Collects PII and gains access to insider info. Also delivers at least one malicious payload (key logger) via IM;

MARCUM TECHNOLOGY

28

0420026N

Recent Compromises / Investigations

- Trusted insider leaving to join competitor - exfiltrates **proprietary software** via email to private email accounts and removable storage devices. Company is using Apple products and employee remotely wipes his returned iPhone and MacBook post termination..
- **Celebrity email** compromise (Gmail) leads to stolen home made adult video and extortion;
- High profile entertainer being spied on by ex-husband via her **devices** including her laptop, smartphone, television, automobile, kids gaming console and physically with cameras.
- **IoT devices** are similar to computing systems yet lack antivirus and other security controls;
- **Wireless Key Logger** - Off the shelf devices doing major damage in theft, espionage marital cases and the like. Controls often do not detect; and
- Media company receiving abusive **anonymous requests** from self proclaimed "whistle blower."

MARCUM TECHNOLOGY

29

0420026N

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

30

0420026N

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

31

0420026N

Our Solutions

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

MARCUM TECHNOLOGY

32

0420026N

Questions?

Jeffrey Bernstein
Director, Marcum Technology
732-640-3690
jeffrey.bernstein@marcumtechnology.com

Jaike Hornreich
Director, Marcum Technology
813-397-4865
jaike.hornreich@marcumtechnology.com

NEXT in Marcum Technology Webinar Series:

April 30 at 1 pm EDT: Improving Cybersecurity by Influencing Good User Behavior
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

www.marcumllp.com/coronavirus

MARCUM TECHNOLOGY

33

0420026N