MAINE BANKERS Association

MONARCH ISC
INFORMATION SECURITY CONSULTING

John Hill Rogers, CISSP
john@monarchisc.com
Senior Consultant

Expo 2021

Cybersecurity for the Marketing Department

MONARCH ISC
INFORMATION SECURITY CONSULTING

Session Agenda

- Why Are We Talking About Cybersecurity and Marketing?
  - Applicable Cybersecurity Principles
  - The “Extrovert” of the Organization
- Two Faces of Marketing Cyber Risk
  - Inbound
  - Outbound
- Protect!
  - Culture First (People & Process), Always!
  - Email / Messaging
  - Website Presence
  - Social Media Channels
  - Supply Chain / Marketing & Advertising Vendors

MONARCH ISC
INFORMATION SECURITY CONSULTING

Why Are We Talking About Marketing?

General Principles – Setting the Table

- Cybersecurity is Everyone's Job!
- Cybersecurity is not an "IT problem."
- Social Engineering / Cybercriminal methodologies target and leverage:
  - Low criticality / low privilege functions of an organization.
  - All available information.
- Dark web marketplaces have rich stores of information.
- Ever increasing awareness in the marketplace equates to elevated importance of cybersecurity being expected part of customer experiences. (Seriously, it's happening!)
- Reputation Risk is often guilt by association for FIs

MONARCH ISC
INFORMATION SECURITY CONSULTING

Why Are We Talking About Marketing?

General Principles – Setting the Table

- There is no such thing as “innocuous” information.
  - Personal information associated with the bank:
    - Travel plans.
    - Photos of family.
    - Detailed Bios on websites.
  - Work information on personal social media.
    - Position, tenure, reporting structure(s).
    - For LinkedIn, limit what contact and personal information is available.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Why Are We Talking About Marketing?

General Principles – Setting the Table

- Family details
- Social media quizzes and un-sourced memes asking for “fun” information about preferences, background, etc.
- Network and friend requests. Restrict/limit the Attack Surface
  - Is this person already on my friend’s list?
  - Are they legitimate?
  - Will this connection benefit my institution / professional life?

MONARCH ISC
INFORMATION SECURITY CONSULTING

Why Are We Talking About Marketing?

The Extrovert of the Organization

- Multiple streams of inbound and outbound communication.
- Multiple sites containing useful social engineering information.
- Use of hyperlinks (Links ARE the Internet. It's how we use them that matters).

MONARCH ISC
INFORMATION SECURITY CONSULTING

Why Are We Talking About Marketing?

The Extrovert of the Organization

- Use of vanity domains. Do staff know those are in use?
- Use of multiple “plug-in” website analytics, social media, and other tools.
- Fundamental purpose is to talk with the market.
- High volume of inbound email attachments.
- Use of cyber-immature vendors in marketing and advertising.
  - Lax authentication controls for perceived “low priority” targets.
- Desire to personalize customer experiences by sharing personal information.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Why Are We Talking About Marketing?

I'm Not Asking You To Stop This Behavior!

MONARCH ISC
INFORMATION SECURITY CONSULTING

Why Are We Talking About Marketing?

MONARCH ISC
INFORMATION SECURITY CONSULTING

“What you risk reveals what you value”

Jeanette Winterson

MONARCH ISC

Two Faces of Marketing Risk

Inbound

- Email
- Website forms data
- Customer and vendor queries
- Social Media

MONARCH ISC
INFORMATION SECURITY CONSULTING

Two Faces of Marketing Risk

Outbound

- Email
- Social Media
- Pubic / Market Communications Channels
- Vendors

MONARCH ISC
INFORMATION SECURITY CONSULTING

Protect!

Reach-out from a secure position.

MONARCH ISC

Protect: People's Behavior

Culture First (People & Process) - Always

- There are no IT systems to prevent 100% of the impact of human failure. Period, end of story.
- Train staff to be aware of risk and always employ mindful use techniques.
- Reward security performance.
- Provide frequent and novel reminders and new information.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Protect: Process

Culture First (People & Process) - Always

- Include security and risk professionals early in innovation plans.
- Research risks of new techniques, technologies, and campaigns.
- Use security and risk professionals to review activity often.
- Support culture of “know” over “no”.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Protect: Public Information

Protection for Public Information

- Inventory all public information, including flows and endpoints.
- Policy requirement for review and approval of all content publishing and modification.
- Scheduled review of inventory.
- Rigorous vendor due-diligence

MONARCH ISC
INFORMATION SECURITY CONSULTING

Security Layers for Email Service

Protect: Email Communications

- Use email marketing service – tools to control human error.
- DomainKeys Identified Mail (DKIM).
- Sender Policy Framework Record (SPF).
- Domain-based Message Authentication, Reporting and Conformance (DMARC)
- Transport Layer Security (TLS) or Secure Messaging System.
- Anti-malware scanning and sandboxing
- Multi-Factor Authentication (Esp. for MS 365)

MONARCH ISC
INFORMATION SECURITY CONSULTING

Protect: Email Communications

Security Layers for Email Service

- Use email marketing service
  - Tools to control human error
  - Tracking of activity
  - Simplification of consistent information made publicly available
- When including links
  - Be clear with link destination and purpose
  - Include information for potential “clickers” about the risks of clicking links
  - “Seed your ground” with regular value-add educational information for customers –
    - How will they know it is you?
    - How will they know it is NOT you?

MONARCH ISC
INFORMATION SECURITY CONSULTING

Security Layers for Email

Protect: Email Communications

- DomainKeys Identified Mail (DKIM)
  - A record to demonstrate to the incoming mail server that the sender has the right to send mail from that domain.
  - Email includes a digital signature to provide assurance it is not spoofed or altered in transit.
  - End-users are not aware of these verifications; they are performed by the infrastructure (mail and Domain Name Service (DNS) servers).

Security Layers for Email

Protect: Email Communications

- Sender Policy Framework Record (SPF)
  - Detects forged sender addresses during email delivery. Works best in conjunction with DMARC.
  - Works with DNS to ensure mail senders IP Address is authorized by that domain's Admins.
- Domain-based Message Authentication, Reporting and Conformance (DMARC)
  - Extends ability of DKIM and SPF.
  - Provides policy guidance from administrative owner of a domain to receiving servers/domains.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Security Layers for Email

Protect: Email Communications

- Transport Layer Security (TLS)
  - Provides encryption to establish confidentiality and data integrity.
  - Can be forced between domains.
  - Now default between domains exchanging email on the MS 365 platform
- Secure Messaging System
  - Invoked by user to send encrypted email.
  - Recipient receives message that a secure message is available.
  - Requires authentication

MONARCH ISC
INFORMATION SECURITY CONSULTING

Security Layers for Email

Protect: Email Communications

- Anti-malware scanning and sandboxing
  - Layered onto email server service.
  - Scan all incoming and outgoing email.
  - “Explode” links in a protected space (sandbox) before email is delivered to ensure they are legitimate.
- Multi-Factor Authentication (Esp. for MS 365)
  - Absolutely ESSENTIAL!!!
  - Every logon, every user

MONARCH ISC
INFORMATION SECURITY CONSULTING

Protect: Website

Website Security

- Secure forms – Input validation and encrypted transmission.
- Limit personal information shared about your team(s).
- Comprehensive due-diligence for hosting provider.
- Use of service to monitor and detect spoof sites.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Website Security

Protect: Website

- Digital Certificates (HTTPS).
- Web Application Firewall (WAF).
- Regular External Penetration Testing.
- Regular Web Application Penetration Testing.
- Rigorous vendor due diligence.
- Daily review of published site.
- Policy requirement for content publishing and modification.
- Limited use of plug-ins and APIs, control of those in use.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Social Media Controls

Protect: Social Media Channels

- Limit use to authorized individuals and implement least privilege.
- Again, policy requiring process with review and approval of all content published and modified.
- Use third-party aggregation tool that can monitor, alert and flag risky activity, e.g., Kadince
- Use MFA – ALWAYS.
- Strong passwords.
- Stay on-top of what customers/public are posting and consider a review/approve/publish strategy.
- Encourage staff and leadership to omit work information from Facebook and Twitter personal accounts, and limit what is published on LinkedIn.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Protect: Supply Chain / Vendor

Third-Party Security

- If application, plug-in vendor:
  - Know how they code! Is a secure framework in use? Which one? Are developers trained and certified?
  - Know how they manage the source code.
  - Do they perform complete code reviews regularly?
  - Know how they patch / update the code, including when and how patches and updates are deployed.
  - Know their internal general security practices.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Protect: Supply Chain / Vendor

Third-Party Security

- Other vendor types (Marketing/Advertising)
  - Consider them medium-high risk vendors.
  - Low operational criticality does not equate to low-risk.
  - Limit information shared to least necessary for function.
  - Review ad account/data ownership.
  - Establish controlled processes for information transmission, publishing and modification of content.
  - Do not permit shared accounts for remote access.

Recap

- It’s not an IT Problem
- There is no such thing as innocuous information
- Departmental partnerships support the “Culture of Know” over “No!”
- Secure IT platforms provide safety to take rewarding risks.
- Limit social media sharing, interaction, and monitor activity.
- Know more about third-parties, especially those considered “low priority targets.”

MONARCH ISC
INFORMATION SECURITY CONSULTING

MAINE BANKERS Association

Questions?

Thank you!

John Hill Rogers, CISSP
Senior Consultant
john@monarchisc.com
www.monarchisc.com

MONARCH ISC