NEXT CHALLENGE. NEXT LEVEL.

NEXSEN | PRUET

THE BARBARIANS ARE AT THE (ELECTRONIC) GATE

Presented to the Carolinas Credit Union League Compliance Conference 10.23.2018

Marcus A. Manos
Member, Nexsen Pruet, LLC

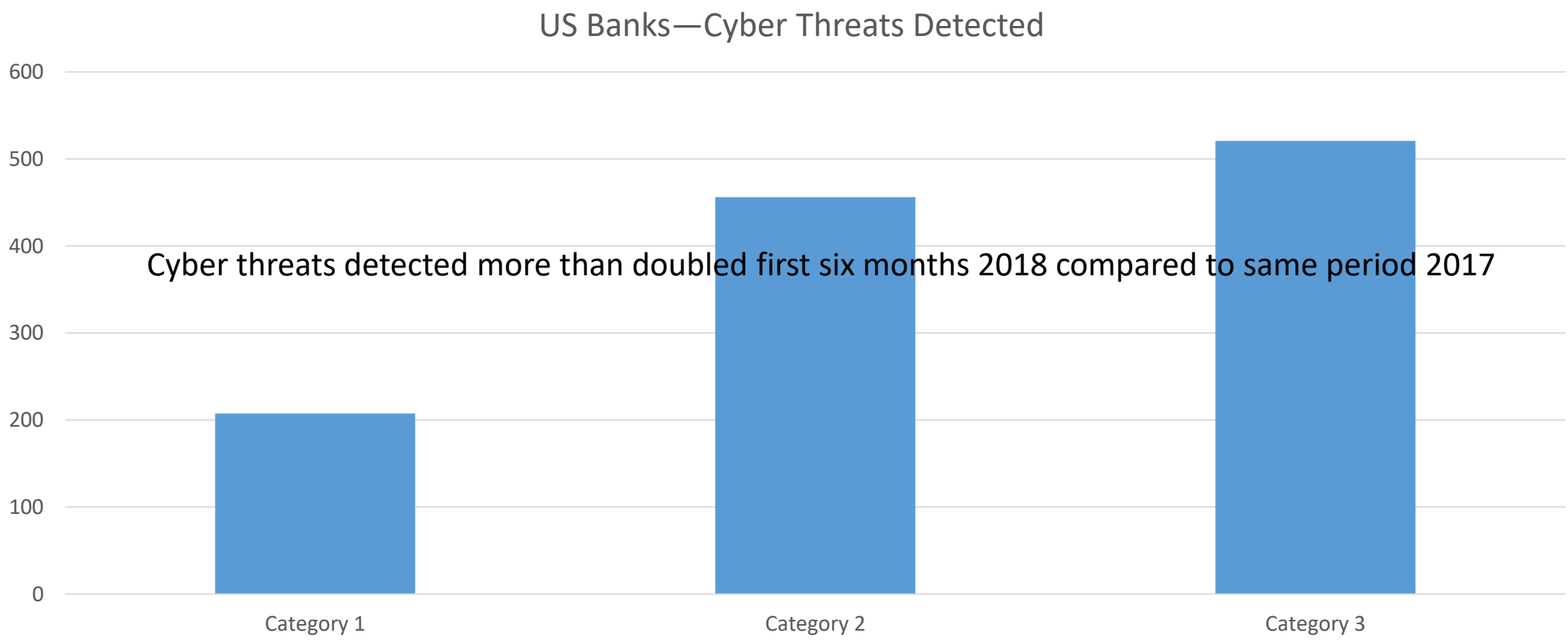
Admitted in SC, DC & NC
803-253-8275
mmanos@nexsenpruet.com

They Want Your Member Data

Cybersecurity and Data Breaches

Threats, Legal Requirements, Prevention, Preparation and Insurance

DATA THEFT AND CYBER ATTACKS ARE ON THE RISE—FINANCIAL INSTITUTIONS ARE THE FAVORITE—Number of threat indicators per U.S. Bank—207.5 first half of 2017, 456 second half of 2017, 520.6 first half of 2018



What is a Cyber Incident or Attack?

- Unauthorized access to a system or machine and its data
- Unauthorized extraction of or damage to data

THESE ARE OFTEN CALLED DATA BREACHES

- Disruption of system availability or integrity of business operations
- Activities causing business or reputation harm

THESE INCLUDE RANSOMWARE AND SYSTEM AVAILABILITY ATTACKS

What's the Impact?

- IBM in its 2017 cost of data breach study found that the average data breach cost the entity breached $3,620,000
- In the financial services industry, the cost per record affected came to $336
- Don't confuse member with record, the credit union holds multiple records per member (driver's license number, social security number, account numbers, etc.)

The Tools are Becoming More Sophisticated

- MoneyTaker – for altering the details of accounts that are about to receive a money transfer
- Metasploit and powershell – for hacking, gaining control and stealing authorizations
- Screenshotter / Keyloggers – for recording keystrokes and screenshots
- LogMeIn Hamachi, UltraVNC, Plink and NirCmd – for gaining remote control and executing orders. The latter tool also enables deleting values and keys from the registry, establishes communications with a VPN, alters files, alters computer definitions, etc.
- ASLRSideChannelAttack – for stealing highly classified authorizations
- Mimikatz – for stealing identification details (usernames and passwords)
- PsExec – for running processes locally through RDP/SMB/RPC protocols
- Banking Trojans – Citadel and Kronos

Why Credit Unions?

- Larger banks and institutions increasing security, becoming more difficult targets
- In 2016, the NCUA reported credit union deposits surpassed $1 trillion
- The personal data of 100 million members resides at credit unions

What are the threats?

Traditional

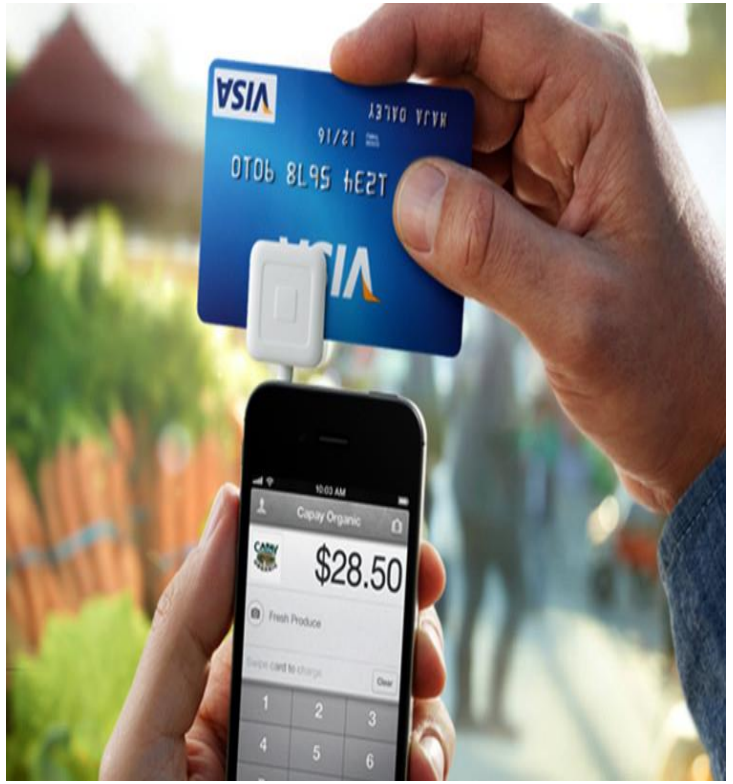
- Card skimming
- User name/password skimming
- Physical theft
- Mail intercept
- Ghost terminals

Relatively New

- Worms and malware
- Data breach
- Cyber extortion
- System control
- Funding redirection

ATM and Point of Sale Attacks

- The majority of cyber attacks still come through ATM machines
- 50 ways to skim your data
  - Separate device
  - Overlaid device
  - Internal device
- Ghost terminals—unlikely here due to lack of concentrated activity but remote locations attract



The oldest methods are still a data breach

- Physical theft of cards
- Physical theft of statements or mail giving information
- Mailing information to the wrong place
- Emailing it to the wrong place
- Single customer phishing, vishing, smishing, and the like

What we have here is a need for communication

- Some of these types of fraud are susceptible to credit union installed defenses
  - Tamper trackers in ATM terminals
  - Inspection by those loading and unloading ATM terminals
  - Viewing (automated selections or samples) of ATM security videos
  - Automated scans of ATM systems
- Others rely on communication and outreach to the community
  - Member communications
  - Merchant forums
  - Contact with local media crime prevention segments and similar show
  - Outreach only improves the credit unions community profile

The Tools of the Trade

- The more sophisticated cyber attacks often use more sophisticated versions of classic fraudster social engineering
  - The ..ishings—phishing, spear phishing, vishing, smishing
- Malware, worms and virus implants
  - Redirect transactions
  - Access and transmit/copy data
  - Interrupt operations
    - By overloading the system
    - Or isolating and cutting off the data
- Three goals—to secretly redirect funds from members, seize member Personal Identification Information (PII) for imposter fraud, or to black mail the credit union for payment

Phishing Ain’t What it Used to Be

- Phishing
- Spear Phishing
- Pharming
- Vishing
- Smishing
- OH MY!
- Practiced against members directly and against credit union employees/contractors

Phishing

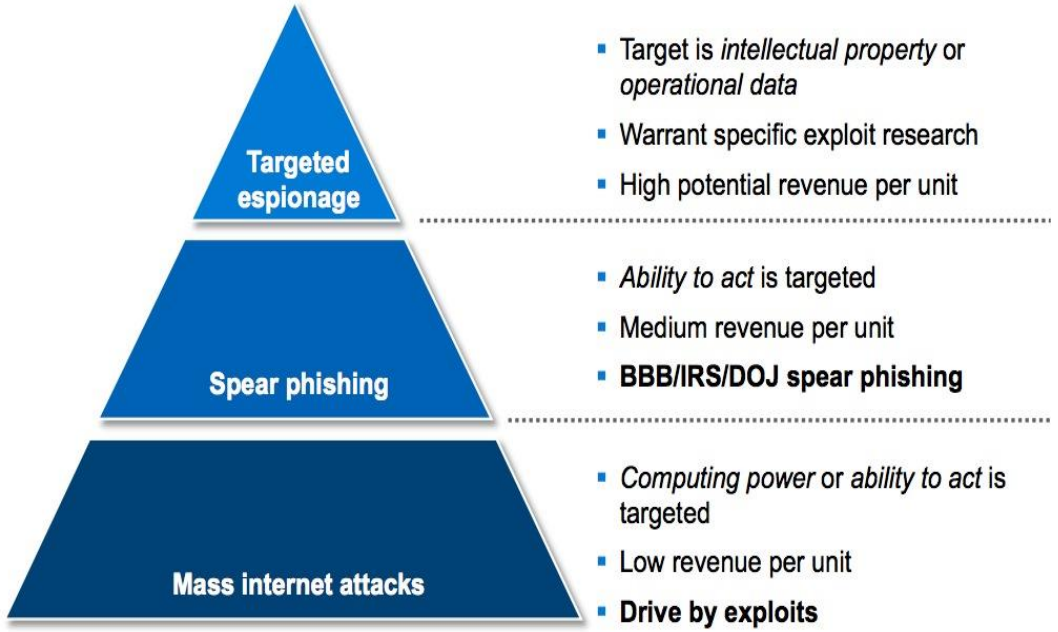
- An email or web redirect seeking to have the person put in their username and password to allow a criminal to access an account or system
- Also used to get account numbers and zip codes for more traditional mail order fraud
- Web redirect can be sophisticated

No Phishing in these waters!

- From within, train, train, train and make sure the policies are documented
- Clicking on a suspicious link or providing information must carry consequences in the disciplinary process
- For members, education—account opening packets, hand outs, bill flyers, community outreach meetings and media reminders
- Look for the tell tales, poor grammar, unknown email, requests information never asked for before

Spear Phishing

- Different methods and different targets
- Will come from your contact list or from a prior transaction
- Appears to be someone you know
- May even be in the form of an instruction from a superior on vacation or similar where verification is difficult



Pharming (not the genetic modification kind)

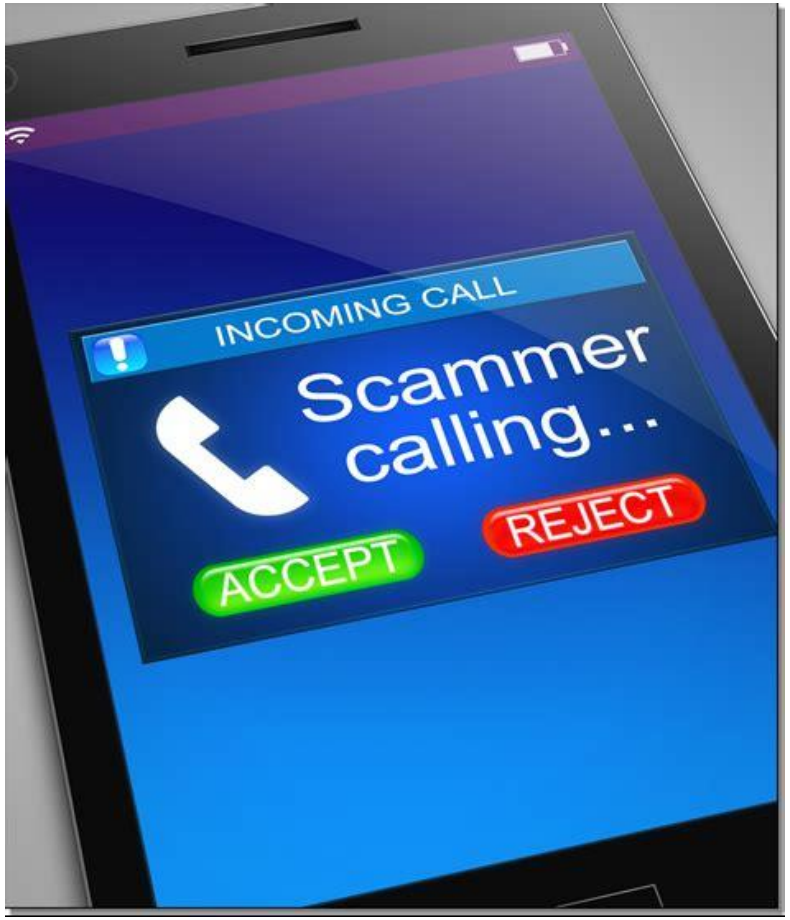
- The fraudulent communication—email, pop up, redirect site—guides the use to what appears to be a genuine website requiring entry of data like user name, password, account number
- Can be a fake goods or services for sale website

Don’t Buy the Pharm

- Updated anti-malware programs catch many pharming operations. As will be stressed later, updating and being current on versions is vital to effective prevention
- Do not use shopping or other purchasing sites you’ve never heard of
- Do not click on links in email from unknown persons
- Carefully view the site—does it have the claimed company’s logo and other information—is it consistent with the sites you normally use?
- Training of employee and information for members and the business community are very important.
- Make sure site names are spelled correctly in your browser and the transaction is occurring on an https:// URL
- Look for certificate errors on the https:// secure page of the site

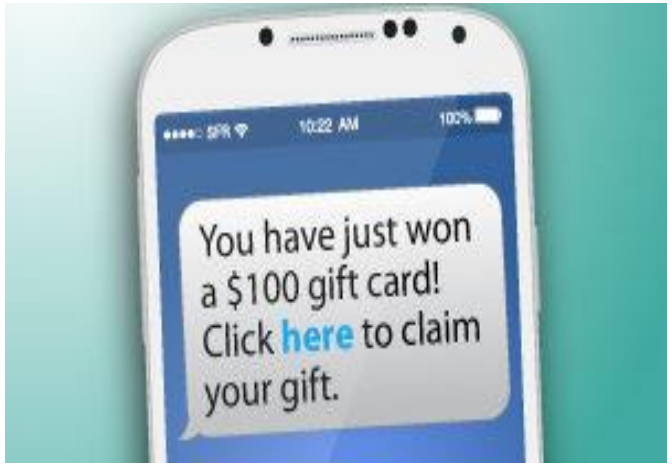
Vishing

- Another rebirth of an old method
- Classic telephone fraud
- Phone contact or voicemail from the IRS, the credit union, etc.
- Please update your information and….
- Social engineering
- NO ONE ASKS YOU TO DO THIS ON PHONE



Smishing (who makes these up anyway?)

- Same technique but using SMS messaging on your cell phone
- As more and more security is routed through your cell phone, this can be dangerously deceptive
- The more deceptive ones look like security checks or prizes for filling out a survey



Solutions and Prevention All the …ishings

- Training and awareness
- Suspicion and caution
- Automated solutions do exist to detect and shut down these scams, including shutting off call back numbers and websites
- Among those that appear effective based on literature in the market
  - IBM Trusteer® Rapport
  - PhishLabs
  - AppRiver®
  - ESET®
  - CSC Cyber Security Services
  - FraudWatch International

Source of Legal Duties and Regulations

- Federally charted credit unions must protect data and give notice as required by Graham-Leech Bliley Act of 1999 (15 U.S.C. §§ 6801-6809)
- The NCUA provides implementing regulations including guidelines for data security and data breach notice/remediation 12 C.F.R. § 748 and Appendices A and B
- FTC red flag regulations under FACTA apply to state chartered credit unions.
- North Carolina and South Carolina data breach acts would apply to credit unions charted in each state.

Federal Programs

- Every federally insured credit union must develop and implement:
  - Administrative
  - Technical
  - Physical—safeguards to protect the security, confidentiality and integrity of member information.
- Must include
  - Comprehensive written information security program that
    - Ensures security and confidentiality
    - Protects against anticipated threats
    - Protects against unauthorized access that could result in substantial harm or inconvenience
    - Ensure proper disposal of member and consumer information

Federal Information Security Program

- Board of Directors involved
- Assess risks
- Manage and control risks
- Oversee vendors/service providers
- Gather data and update the plan
- Report to the Board
- Appendix B guides what goes in the notice if a breach occurs, but also much more

North Carolina

- Regulations and statutes governing credit unions require they maintain the safety and integrity of the credit union's finances
- These flexible statements change with the times and likely include taking steps to protect member information against data breaches and the credit union against cyber attacks on its electronic systems
- No specific standards regarding the safe guarding of member data or the procedures necessary to develop and implement a program exist
- The credit union must give notice of a breach, however, including notice of steps taken to protect the information from further unauthorized access. N.C.G.S. § 75-65.
- A violation results in liability under the unfair trade practices act

South Carolina

- South Carolina's data breach statute goes further than North Carolina's
- In addition to the immediate notice requirement with greater detail than NC, it provides for liability for failure to abide by the statute
- The SC statute implies that the business will have security of some sort
- Essentially state chartered credit unions should consider following federal guidelines substantively and to the extent affordable as they are likely to be argued as the industry standard in the event of a breach
- If the credit union acts as an insurer, then it must follow the new Insurance Data Security Act in SC

HOW TO BUILD THE DEFENSE

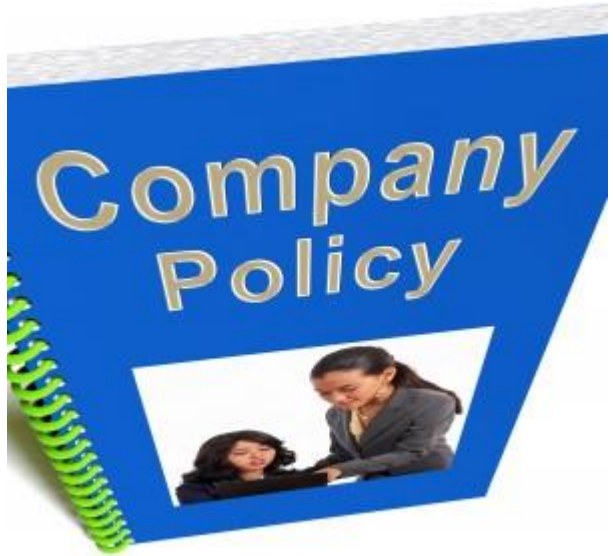
- Some easy steps
- Stay up to date—upgrade versions and perform patches regularly as available
- Require the creation of strong passwords and frequent changes
- Use two factor idetnification
- Battered1776!Fish
- Regular penetration testing of he system—internal and external

More Defensive Moves

- Have malware detection/removal, anti-virus and firewall software updated often—this is more than software upgrades and patches, the definitional tables change quickly
- Perform cybersecurity assessments
- Use encryption
- Detailed written policies approved by the Board
- Frequent and refreshed training in privacy and cybersecurity policies and procedures

Policies and Procedures Development

- Board directed with full management buy in
- Participation from every sector of the credit union
- Must include training and awareness standards
- Must be regularly evaluated in light of experience and refreshed
- Information Security Forum's Standard of Good Practice for Information Security (2018) a good resource



Policies and Procedures--Technology

- What do you require—malware detection/removal, anti-virus, threat detection, email and other filters with phishing and virus alerts, monitoring and testing software etc.
- Standard for vendors providing these goods and services
- Any outside standards the credit union decides to adopt
- There must be a Chief Information Security Officer or equivalent—this person should have the technical lead for security
- There must be a Chief Privacy Officer whose concern is the data itself and breach response

Policies and Procedures—the Ongoing Thought Process

- Information Asset Identification
- Where Does the Information Come From? (Collection Sources)
- Organization

Organizational Thoughts

- Board involvement and oversight
- CEO and general counsel involvement and oversight
- Internal management task force or committee overseeing information security and privacy
- Cybersecurity incident response team
- Privacy incident (non-cyber or limited cyber) response team
- Who is responsible for insurance?
- Vendor consultant management
- Member outreach and education
- Data retention and destruction policies

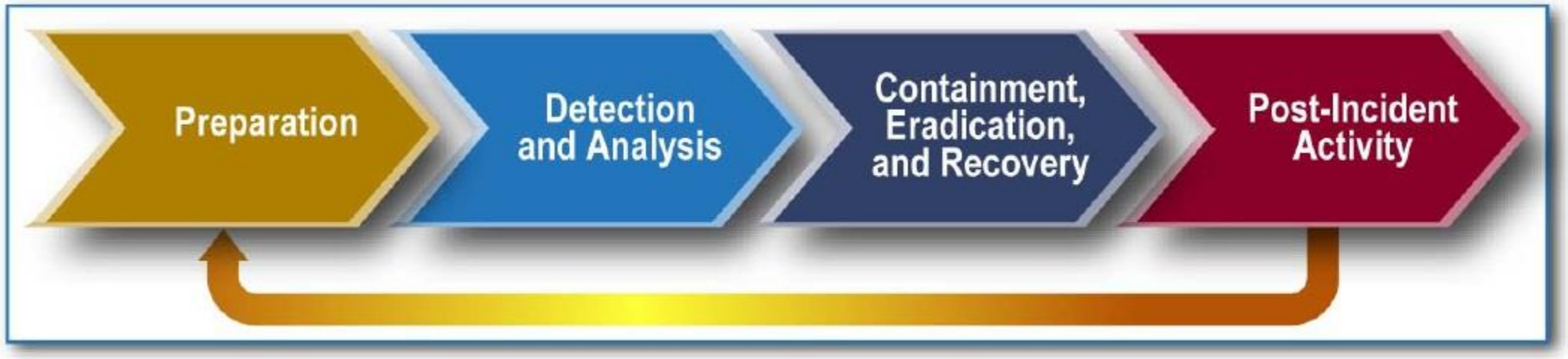
Policies to Consider

- Information Security Policy (must have)
- Data Breach/Cyber Incident Response Policy (must have)
- Privacy and Cybersecurity Training Policy
- Relevant portions of Employee Manual/HR Polices—privacy rights and obligations, data security monitoring, dangers of phishing etc., email use policy, internet use policy, password and dual authentication policies all intertwine with the above and need to be consistent
- Contractor/vendor/consultant required terms policy for data and system security and incident response
- Marketing and data sharing policy if needed

What is your Incident History?

- Whose organization suffered a non-cyber privacy breach?
- Whose organization suffered an electronic data breach?
- Whose organization suffered another type of cyber incident?
    - Ransomware
    - System availability
    - System error
    - System hijack

Despite all Your Efforts, the Incident Occurs



Be Prepared

- Prepared to respond to members, regulators and the press
- Prepared to stay in operation
- Prepared to minimize the damage to the credit union and its members
- Prepared to respond to lawsuits and claims

Response Team and Immediate Legal and Forensic Investigation

- The credit union must know the team it will have on the ground during a major incident and the support it will have on the phone. First, internal resources must be committed and on instant response. IT, human resources, finance and customer service must be involved.
- Second, the credit union needs to know and have agreements in place with vital vendors needed to stay in operation. These vendors need to be ready to come to the operations center or participate by phone, whichever the credit union needs.
- The credit union's outside counsel needs to be on call to be on the ground within 24 hours of notice. The legal team should hire a forensic investigative firm.

The Public and Governmental Phases

- Once security is restored and ongoing operations assured
- Report to and cooperate with law enforcement—outside counsel should take the lead
- Public relations/crisis management consultant needs to be part of the team
- Counsel drafts notice response, input from management and PR
- Same with regulatory responses—remember these will not be permanently confidential due to FOIA
- Media management key at this point to minimize reputational harm

Preparation for the Cost--Insurance

- Cyber risk policies still written manuscript meaning no industry wide set of a few forms
- Differs by insurer and by industry insured
- Tends to be expensive
- Mixed first and third party coverage with governmental response component as well

Coverage to Explore

- Privacy breach response costs, notification expense, and credit monitoring expense coverage
- Systems Asset Protection
- Cyber Extortion/Terrorism Protection
- Media Exposures
- Data Security and Privacy Liability Protection
- Privacy Regulatory Investigation, Defense and Penalty Coverage

Where to Look for Coverage

- CUNA Mutual provides a policy
- The top ten writers of cyber risk insurance are
  - AIG (American International Group)
  - XL Group, Ltd. (Axa XL)
  - Chubb, Ltd.
  - The Travelers
  - Beazley Ins. Co.
  - CAN Financial Corp.
  - BCS Ins. Co.
  - Axis Capital Holdings, Ltd.
  - Liberty Mutual Ins. Co.
  - Allied World Assurance

QUESTIONS? COMMENTS?

Marcus A. Manos

Nexsen Pruet, LLC

mmanos@nexsenpruet.com