Cyber Security Awareness Update – The Threat Continues

(Through Q1 2022)

Instructor:

Colleen M. Capossela, Esq.

CATIC
AGENT DRIVEN. INSURING RESULTS.

CATIC PRO INC.
PROFESSIONAL SOLUTIONS FOR YOUR BUSINESS

Cyber Security Awareness - What's happening?

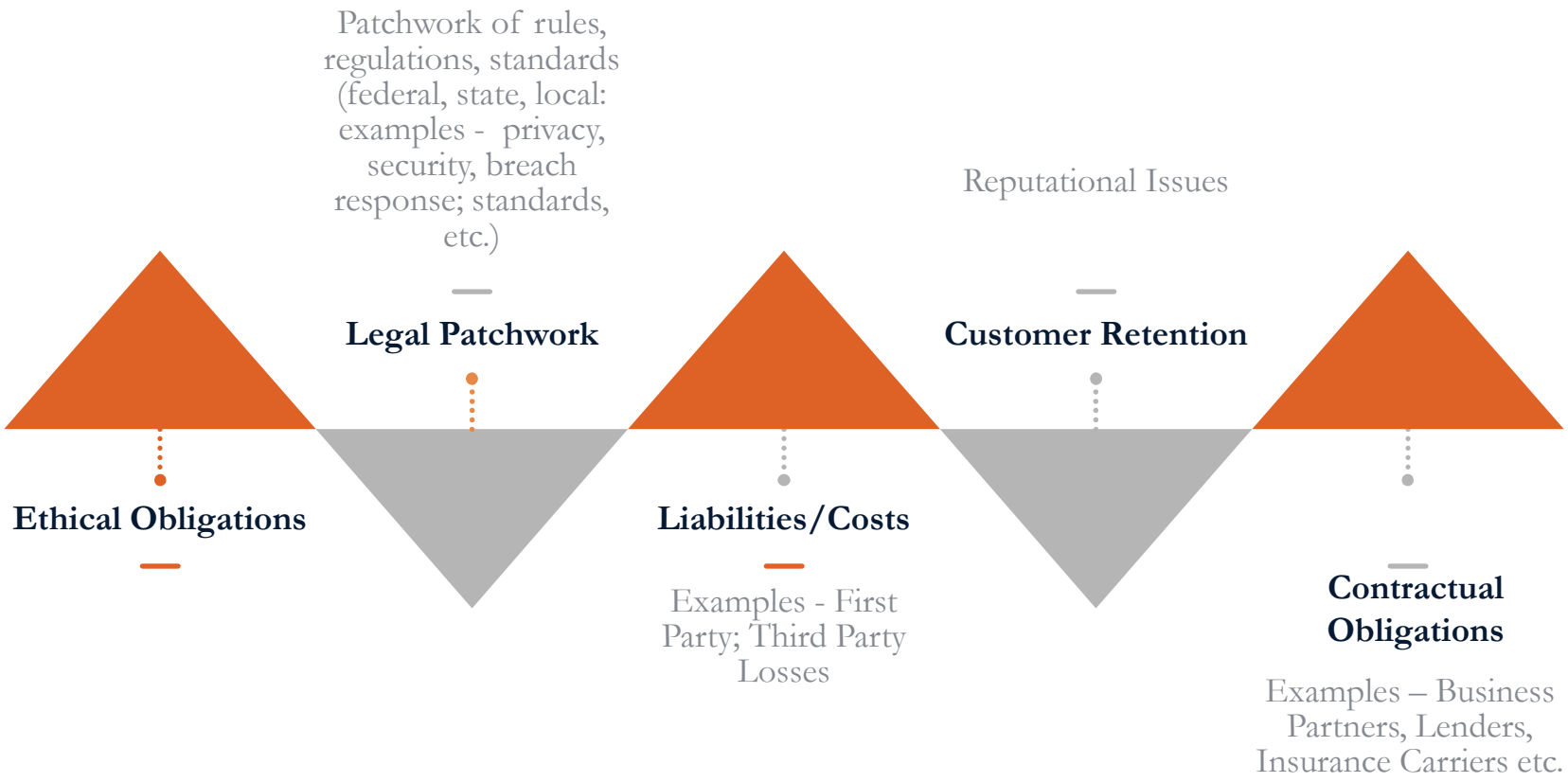
Industry as a whole is a target

One of Biggest Risks Businesses Face; Ever Changing, Ever Evolving

All impacted regardless of size

Awareness & Planning is key!

Some Major Concerns



CYBER SECURITY AWARENESS

CRIMINAL's GOAL: Hack Technology or Hack People

Cyberattacks – Some Methods

- Social Engineering Tactics, for example –
    - Phishing/Smishing/Vishing/Pharming/Spoofing Etc.
    - Spear Phishing/Smishing/Vishing/Spoofing Etc.
    - Whaling

…and fax, mail etc.!

CYBER SECURITY AWARENESS

EXAMPLES:

- **Phishing/Smishing/Vishing** - Urgent bank request for verification of account information.

- **Spear Phishing/Smishing/Vishing** -

    - Request from your boss – access accounts; send funds; click on link.
    - Request from employee to redirect direct payment.
    - Email, text or call from customer, attorney, other party to transaction wanting you to wire funds; even calling you to confirm receipt to stop you from acting.
    - Emails, text or calls from Associations – click on link or provide information.
    - Posing as a vendor, for example of popular business applications, or security vendor.

- **Whaling -** Email to executive on major case included a link for more details.

…fax, mail etc.

You provide funds or valuable information to the criminal, or allow access, for example, infecting your systems with malware.

Cyberattacks – Some Methods Continued

- More on Spoofing
- Deepfakes
- Guessing and/or Stealing Common Passwords
- Internet Use/Wi-Fi Free Spots
- Baiting
- Theft or Loss of Physical Equipment
- Tapping Into Unpatched Software Vulnerabilities
- Exploiting Flaws in Security Systems
- Third Party Vendors
- Forensic Recovery
- Insiders – Rogue Employees

CYBER SECURITY AWARENESS

- ASSESS & PLAN WITH YOUR EXPERTS
- Doing Nothing is not an option
- There is no “One size fits all” Plan
- MULTI-LAYERED & ENTERPRISE WIDE
- Continually Review with Your Experts/Revise and Update
- Test

CYBER SECURITY AWARENESS

- **Some helpful hints for your review with your experts (not all inclusive):**
  - Establish Your Team for Planning and Responding
  - Evaluate Your Operations – People, Systems, Processes, Data Etc.
  - Put Technology and Security Programs in Place, for example (not all inclusive):
    - *Some Technology Considerations:*
      - Proper back up and testing
      - Regular/automatic, patch & update
      - Proper Firewalls
      - Anti-virus/Anti-malware/Anti-pharming
      - Intrusion prevention/Intrusion detection/Monitor systems
      - Multi-factor authentication
      - Encryption (data in rest and in motion)
      - Virtual Private Networks

CYBER SECURITY AWARENESS

- *Some Technology Considerations:*

  - Secure Communication Systems
  - Network Segmentation; Mapping
  - Consider Spam Filters
  - Consider Application Whitelisting
  - Lock down physical computer ports – restrict media
  - Penetration Tests/Vulnerability Assessments/Security Testing
  - Establish Reporting on Relevant Items and Monitor

  Etc.

CYBER SECURITY AWARENESS

- *Some Security Program Considerations (not all inclusive list):*

  - Use of Company's Systems Requirements – For example:
    - ✓ Proper password management, for example:
      - Require strong effective passwords/password phrases
      - Do not use same passwords/password phrases
      - Do not reuse passwords/password phrases
      - Do not share passwords/password phrases
      - Update
      - Lock out plan
    - ✓ Prohibit use of automatic login features

CYBER SECURITY AWARENESS

- *Some Security Program Considerations:*

  - ❖ Use of Company's Systems Requirements – For example:

    - ✓ Restrict use and access (Work Related/Job Needs)
    - ✓ Restrict use and access of Internet (Business only)
    - ✓ Restrict downloads and installations (Gatekeeper)
    - ✓ Mobile Devices/ Laptops/Remote Systems – apply security, examples:
      - Password protect/Multifactor Authentication
      - Encryption
      - Safeguard/Lockdown
      - Prohibit use of free Wi-Fi/Public access
      - VPN

Etc.

CYBER SECURITY AWARENESS

- *Some Security Program Considerations:*

  - Email Plans – For example:
    - ✓ Do not rely on
    - ✓ Do not email sensitive/confidential information
    - ✓ If using email, APPLY PROPER SECURITY & ENCRYPT
    - ✓ Be ***suspicious*** of "all" emails
    - ✓ Require "You" to call for example, **verify** and ***confirm*** with known independent valid source
      - No opening of attachments
      - No clicking on links
      - No providing sensitive/confidential information/credentials
      - No transferring funds
    - ✓ REQUIRE REPORTING
    - ✓ Add warning statements to emails (but not the only warning…)
    - ✓ Need to do much more to warn customers!
  - Etc.

CYBER SECURITY AWARENESS

- *Some Security Program Considerations:*

  - Records Retention Program – For example:
    - ✓ Business records to retain (Legal/Necessary)
      - Electronic, Hard Copies, Etc.
      - Email, Instant Messaging, Etc.
      - Office, Home, Etc.
    - ✓ Retention period
      - Not "Everything Forever"
    - ✓ Safeguard/Lockdown/Clean Desk Plan, especially Personal Identifiable Information, but also Confidential
    - ✓ Restricted Access
    - ✓ Destruction/Deletion/Scrub/Purge – Consider Sensitivity Etc.

CYBER SECURITY AWARENESS

- *Some Security Program Considerations:*
  - ❖ Funds Transfer Plan – For example:

    - ✓ Communicate Upfront
    - ✓ Checks and Balances
    - ✓ Establish proper verification and confirmation protocol
    - ✓ No reliance on non-face-to-face receipt
    - ✓ "You" ***verify*** and ***confirm*** by for example calling known independent reputable source (valid payee)
    - ✓ Implement a "No Change Program" (Initial Letter)
    - ✓ Implement a "No Wire Program" (Initial Letter)
    - ✓ Access lender's website by typing URL/no links/due diligence
    - ✓ Prohibit use of free or public Wi-Fi to lenders' sites
    - ✓ "You" confirm receipt of funds
    - ✓ Etc.

CYBER SECURITY AWARENESS

- *Some Security Program Considerations:*

  - Lender Security Programs (ACH, International, Positive Pay, Etc.)
  - Initial Letters/Agreements
    - ✓ Identify processes followed
  - Third Party Vendor Plans – i.e. SOFTWARE PROVIDERS, CLOUD PROVIDERS, Etc.
  - Incident Response Plans – Key breaches that could affect you – HOW WILL YOU RESPOND (Remember – Business Continuity Plan/Disaster Recovery Plan As Well) **AND TEST**
  - Employee Discipline/Termination

CYBER SECURITY AWARENESS

- **What else?**
  - *AWARENESS*
  - Educate, Train, Test and Enforce Regularly – Make important
  - Quiz; Surprise Test

CYBER SECURITY AND OTHER RISK AWARENESS

- **What else?**
  - Monitor and Keep Up on Changes
  - Modify When Necessary
  - Obtain "PROPER" Cyber and Crime Coverages
  - With all, GET WITH YOUR EXPERTS

Sample Resources & Disclaimer

- **Some Resources – For Example: CATIC, and :**
  - FBI – www.ic3.gov; www.fbi.gov
  - DOJ – www.justice.gov/criminal-ccips/cybersecurity-unit
  - CISA - https://www.cisa.gov/
  - FINRA – www.finra.org/industry/cybersecurity
  - FCC – www.fcc.gov/general/cybersecurity-small-business
  - SBA – www.sba.gov/managing-business/cybersecurity
  - FTC – www.ftc.gov/tips-advice/business-center

- **Disclaimer – All contents of this presentation and related material are provided for informational purposes only. It does not purport to address every possible circumstance, practice, measure, standard, obligation, hazard, loss potential, etc., and specifically disclaimed is any warranty or representation that compliance as noted herein will make any person, business, premises, property or operation safe or in compliance with any law, rule, regulation etc. Please be sure to contact your experts (for example, IT Security, Legal, Insurance experts etc.) to assess your obligations and needs.**

QUESTIONS


INSURANCE
BONDS
VOLUNTARY EMPLOYEE BENEFITS
SUCCESSION PLANNING

Thank You

101 Corporate Place, Rocky Hill, CT 06067
860-513-3131
email@CATICPro.com

www.CATICPro.com

CATIC
AGENT DRIVEN. INSURING RESULTS.

CATIC PRO INC.
PROFESSIONAL SOLUTIONS FOR YOUR BUSINESS