Cybersecurity and Incident Management

November 23, 2021

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

The information herein has been provided by CliftonLarsonAllen LLP for general information purposes only. The presentation and related materials, if any, do not implicate any client, advisory, fiduciary, or professional relationship between you and CliftonLarsonAllen LLP and neither CliftonLarsonAllen LLP nor any other person or entity is, in connection with the presentation and/or materials, engaged in rendering auditing, accounting, tax, legal, medical, investment, advisory, consulting, or any other professional service or advice. Neither the presentation nor the materials, if any, should be considered a substitute for your independent investigation and your sound technical business judgment. You or your entity, if applicable, should consult with a professional advisor familiar with your particular factual situation for advice or service concerning any specific matters.

CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances or needs, and may require consultation with counsel, consultants, or advisors if any action is to be contemplated. You should contact your CliftonLarsonAllen LLP or other professional prior to taking any action based upon the information in the presentation or materials provided. CliftonLarsonAllen LLP assumes no obligation to inform you of any changes in laws or other factors that could affect the information contained herein.

Cybersecurity Services

Count on our experienced consultants to help you address cybersecurity risks and recovery. We will help where you need us so that you can feel more comfortable relying on your IT environment and get back to business.

A unique approach. Whether you need a unique individual or a complete team of experienced professionals, we can help you control cracks in your cybersecurity plan. By handing over your IT environment to someone with hands-on knowledge in the field, you can get back to the business of doing business.

Our people. Our 100 cybersecurity professionals each have 10 – 30 years of information security experience. Our team includes Chief Information Security Officers and other security leadership professionals who can help provide the analysis you need and manage projects to address your security requirements.

Some of our focused services

CYBERSECURITY RISK ASSESSMENT AND GOVERNANCE

- AICPA cyber framework risk assessment
- FFIEC cybersecurity assessments
- HIPAA security risk analysis
- Third party service provider risk assessments
- Enterprise risk management input
- Executive / board training
- Staff security awareness training
- Customer security awareness training
- Policy and procedure development

STANDARDS VALIDATION AND COMPLIANCE MONITORING

- NIST
- FERPA
- FFIEC / GLBA
- Red Flags
- NERC / CIP
- HIPAA
- HITRUST
- PCI
- CIS/SANS 20
- General Data Protection Regulation (GDPR)
- SSAE16 SOC engagements

CYBERSECURITY TESTING AND EVALUATION

- RED team testing (breach simulation)
- Penetration testing
- Vulnerability assessment
- Wireless Security assessment
- Web / application security assessment
- Security architecture design evaluation
- Social engineering
  - Email phishing campaigns
  - Pre-text phone calls
  - Impersonation and physical access testing
- Disaster recovery
- Business continuity

INCIDENT RESPONSE

- Incident response program design
  - People
  - Rules
  - Tools
- Incident readiness assessment
- Security incident response (on-call)
- Forensic analysis
- Client executive support
- Retainer services
- Crisis readiness

Presenters

Sundeep Bablani

IT and Cyber Regional Leader – Financial Institution
SAS – Cybersecurity
sundeep.bablani@CLAconnect.com

Barbie Housewright

IT and Cyber Regional Leader – Financial Institution
SAS – Cybersecurity
Barbie.Housewright@CLAconnect.com

Objectives:

- Develop an understanding of cybersecurity challenges
- Develop methodology for cybersecurity risk management
- Establish a plan for responding to cybersecurity incidents

Discussion Categories

- Governance
- Operations
- Regulatory Concerns
- Ransomware
- Incident Response Management
- Cybersecurity Risk Management
- Making a Difference with Cybersecurity

Governance

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

Managed Service Provider (MSP)

- Contracting / Agreement Review
- Continuity Planning of the Vendor

Business Continuity Planning (BCP) Testing

- Planning Practices
- Resources
- Effectiveness
- Work from Home Days
- Variations on Scope

Phase Activation Criteria and Planning

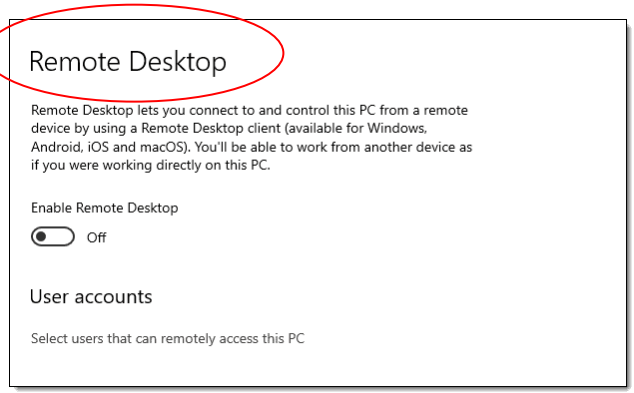
- Planning
- Preparing
- Responding
- Recovering

Operations

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

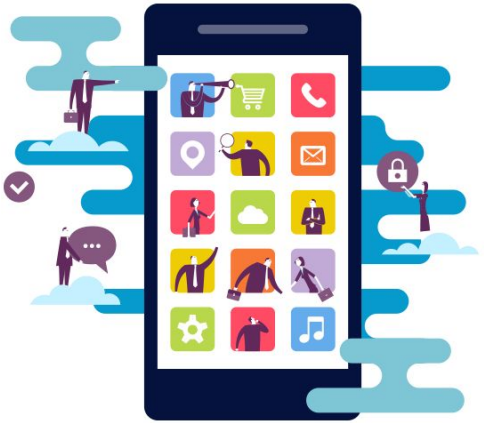
Remote Access

- High-Reliance on Telecommuting
- Remote Access
  - Capacity, bandwidth & authentication mechanisms
  - Capability and Technology
    - Infrastructure / application
- Security Considerations



Mobile Device Management

- Utilizing Mobile Device Technology
  - Bring Your Own Device
  - Organization owned
  - Mobile device management
    - Technology
    - Governance



Vendor Relationship Management

- Technology Vendors
  - Provisions for pandemic
- Supply Vendors
- Vendor Continuity Planning
- Subcontractors

Communication Methods

- Alternative Contact Information
- Employee Collaboration
  - Virtual meetings
- Customer Communication
  - Branch closures
  - Procedure changes

Service Delivery Technology

- Online Account Opening
- Online Application Procedures
- Electronic Signature

Electronic Alternatives to Automate Manual Processes

- Reliance on manual processes for conducting daily business
- Limitation of Personnel Resource
- Streamlining
- Checklists and Policies
  - Centralized repository

Limitation of Access to Hardware, Software Licenses and Supplies

- Purchasing
- Additional Inventory
- Licensing
- Lack of centralized repository of daily checks

Third Party Applications and Cloud Access

- Ease of Access
- New Technology Implementation
- Limitations relating to third party application and cloud resources

Disaster Recovery as a Service

- Technology
- Resources
- Access
- Service

Regulatory Considerations

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

Avoid Compromising Security to Meet Business Objectives

- No Reduction in Regulatory Responsibility
  - Protection of Customer information
- Confidentiality
- Integrity
- Availability

Temporary System and Application Access Modification

- Access Management
  - Temporary
    - Elevation of privilege
    - Access to additional resources
    - Remote access
    - Mobile access
  - Access termination

Budget and Resource Considerations

- Emergency Implementation Budget
  - Hardware
  - Software
  - Access
    - Security

Telework and Protection of Customer Information

- Telecommunications
- Printing
- Data Destruction

Testing Worst Case Scenarios

- Scope
- Severity
- Loss of Staff
- Quarantine
- Branch Closure

Ransomware

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

Ransomware

Ransomware (old fashioned)

- Caused by a computer “malware” introduced into the environment
- Encrypts all files accessible by computer
  - Computer internal hard drive
  - Network drives
- Ransomware options
  - Pay ransom for decryption key
  - Restore files from backup to state prior to encryption

Ransomware Evolved

- As companies did a better job with backups, ransomware evolved
- Double extortion
  - Encrypting files is not the only activity
  - Data exfiltration
  - Demand payment not to release data
- Triple extortion (newer)
  - Calling clients to increase pressure
- • Ransom Amounts

Cybersecurity Data Breach — By the Numbers

- IBM's 2021 Cost of a Data Breach study conducted by the Ponemon Institute noted:
- $9.05m – Average cost of a data breach in the United States ($4.24m global average)
- 44% - Share of breaches that included records containing Customer Personally Identifiable Information (PII), at an average cost of $180 per record
- $2.98m –Global average cost of a breach for organizations under 500 employees; $5.33m at enterprises over 25K employees
- $1.07m- Cost difference where remote work was a factor in causing the breach
- 38% - portion of breach costs due to lost business

Behind the Statistics

- Hackers can do a lot in and to your network in 207 days (Global Average) o Learn everything about your business
  - Find you crown jewels and take them
  - Disable backups and security systems
  - Create numerous back doors
- Public portrayal of ransomware creates a false sense of security
  - Ransomware is usually coupled with other acts and just the most visible part of the attack
  - These days, ransomware coupled with data exfiltration
  - Resuming operations is just the first step
  - Legal and business ramifications of a data breach can persist

Business Email Compromise

- Using the compromised (or guessed) credentials, they connect to your email server and download the contents.
  - What do you have in your email?
  - This by itself is a data breach
- Leverage the information learned from the emails
  - Email connections (CC vs. BCC)
  - Specific names of friends/family
  - Travel schedule
- Send out very convincing emails for other fraud schemes

Incident Management

Incident Response Management

DETECT

DIAGNOSE

CONTAIN

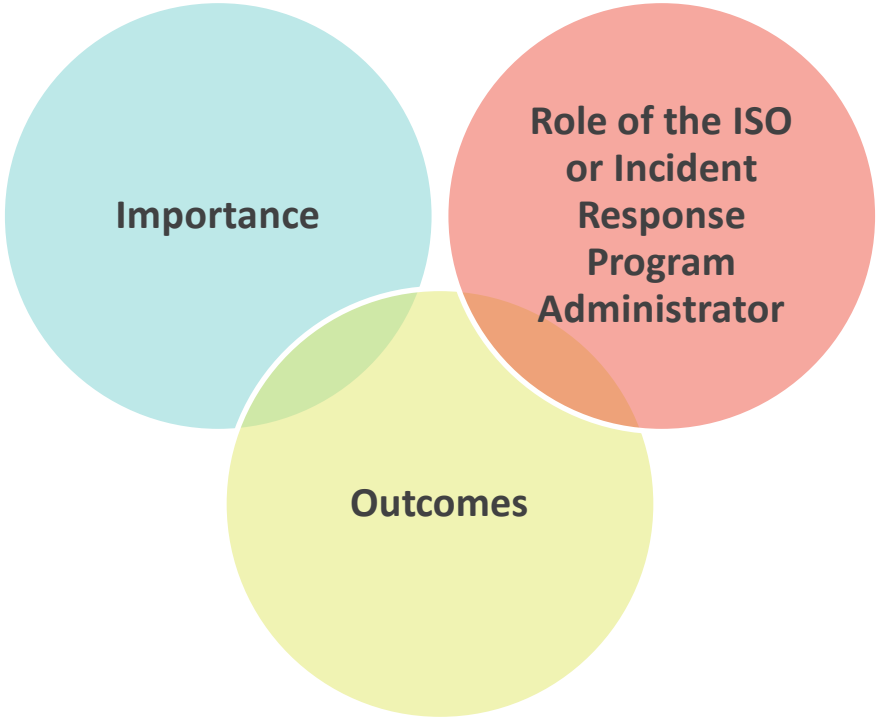
RESTORE

ROOT CAUSES

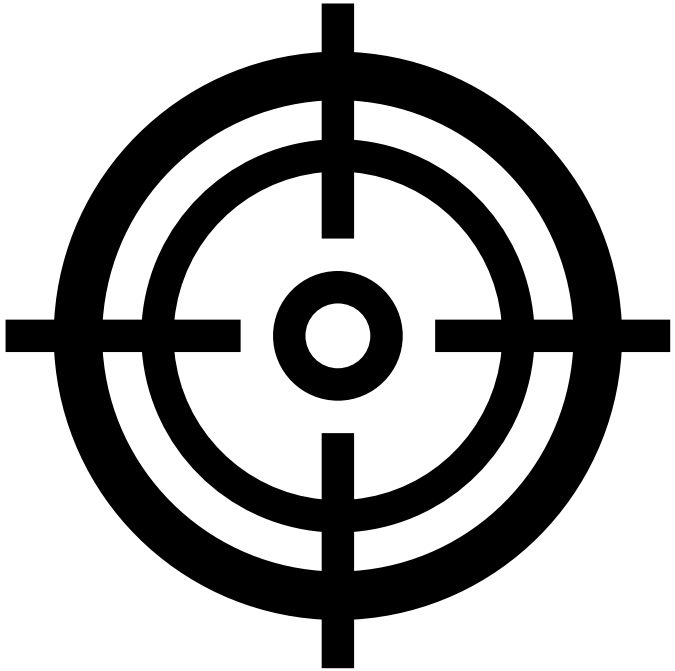
PREVENT

DOCUMENT

Incident Response Procedures



Effective Incident Response



- Handling of Incidents
- Detection and Monitoring
- Escalation and Notification
- Response Capabilities
- Proactivity
- Performance Measurement
- Incident Categorization
- Communication and Lessons Learned

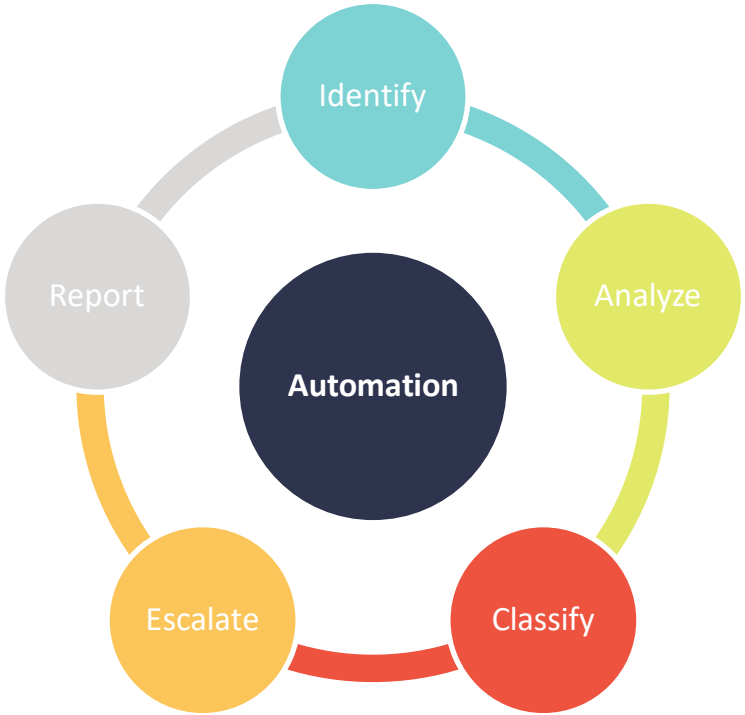
Concepts

INCIDENT HANDLING

INCIDENT MANAGEMENT

AUTOMATION

Incident Management Systems



Responsibilities

- Developing the Plan
- Handling Incidents
- Verifying and Reporting
- Planning and Budget

Resources

Policies and Standards

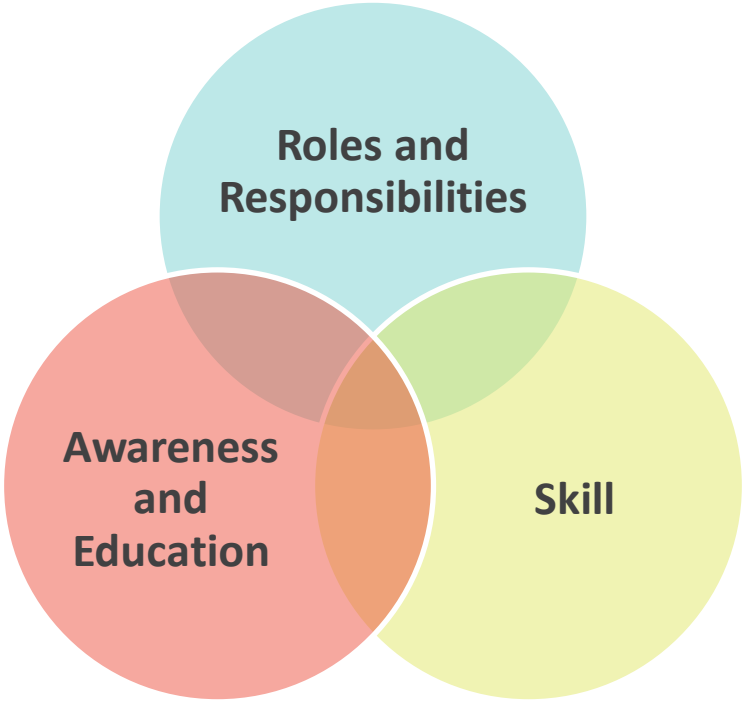
Technology

Technology Concepts

SECURITY PRINCIPLES

SECURITY VULNERABILITIES / WEAKNESSES

Personnel



Program Components

Audit and Assessment

Outsourcing

Risk Management

Risk Management

Assurance

Value

Resources

Incident Response Capability

Assessment of the Program

History of Incidents

Threats

- Environmental
- Technical
- Man-Made

Vulnerabilities

Elements of an Incident Response Plan

PREPARATION

IDENTIFICATION

ERADICATION

RECOVERY

LESSONS LEARNED

Developing an Incident Response Plan

- Gap Analysis
- BIA
- Escalation Process
- Help/Service Desk Process
- Incident Response Team
- Training

Developing an Incident Response Plan

NOTIFICATION REQUIREMENTS

SUPPLIES

INSURANCE

Challenges Incident Response Planning

MANAGEMENT BUY-IN

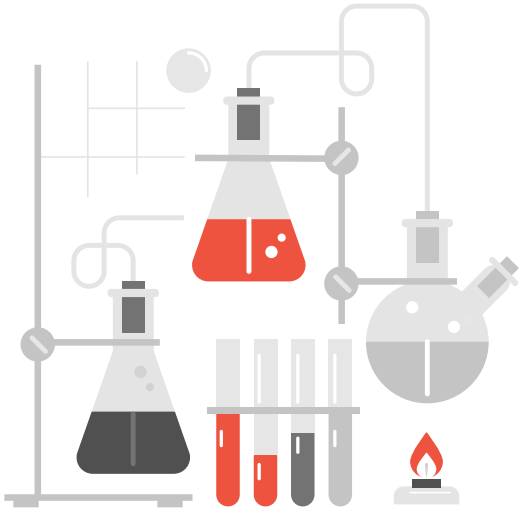
GOALS AND STRUCTURE

INCIDENT RESPONSE TEAM TURNOVER

COMMUNICATION

COMPLEX AND BROAD

Testing



Entire Plan

- Gaps
- Assumptions
- Timelines
- Effectiveness
- Performance
- Accuracy
- Currency

Collaboration/Coordination

Documentation

Post Incident Activities

CAUSE AND CORRECTIVE ACTION

DOCUMENTATION

PROCEDURES

EVIDENCE

FORENSIC EVIDENCE

Polling Question

- How formal is your Incident procedure documentation?
  - a. The procedures are in our heads.
  - b. We have notes somewhere.
  - c. The IT Department keeps a procedural document.
  - d. We have a formal, documented plan that establishes recovery procedures based on the type and scope of various events.

Managing Cyber Risks

Managing the risk

- As always, prevention is the first step
- Cyber threats evolve rapidly so organizations need to anticipate successful attacks

Prepare yourself for a potential cyber attacks

- Risk assess, classify, and inventory systems
  - Determine if industry standards are required (NIST, CMMC, CIS Critical Controls)
  - If not required, are they desired?
- Conduct a Cyber Security Risk Assessment to determine how you measure against a standard
- Develop an immediate, short and long-term strategy for remediating findings identified as part of the review.
- Consider penetration testing as part of your verification strategy

User Education and Testing

- Malware typically needs a helper to do its job.
- Educate users on common phishing scenarios as well as how to identify masked links and spoofed sender addresses.
- Implement a cyber awareness training program

Cyber Awareness Training Program

- Training program is an HR function, not IT
- All employees must participate
  - Initial onboarding
  - Quarterly updates
- Conduct phishing “tests” to determine employee readiness
- Employees who do not pass the test take remedial training
- Document every employee’s training history and performance
- A documented program makes for a good legal defense

Good IT Administration and Design

- Staff should not have local administrator rights to their workstations
- Network and domain administrators use two sets of credentials (general use and elevated privileges).
- No email, browsing, or general computer use when using administrator level credentials.
- Implement a policy and practice that stipulates administrators do NOT log into workstations with domain administrator rights.

INCONVIENENT!

Incident Response Preparedness

- Unfortunately, data breach can still occur despite implementing all the best security precautions
- When that occurs, organizations need to ensure they are ready to respond to a data breach.

Have a plan, practice the plan, prove the plan

Polling Question

- Show of hands, which of these roles should be responsible for staying on top of an organization's cyber security?
  - CEO/Owner
  - CFO/COO
  - Internal IT team
  - Outsourced IT provider

Cyber Security as a Specialty

- An entire army of hackers results in rapidly changing threat landscape
- Cyber security is rapidly evolving
- Cyber security has become its own area of specialization, separate than IT operations and administration
- Most IT departments are staffed to keep systems operational leaving little time for staff to
  - Stay up to date on threats
  - Implementing proactive measures

Knowledge and Independence

- Important to have someone focused full time on cyber security. Doesn't need to be dedicated to you.
- Should be independent of operations and report to leadership independently from operations
- Accountant vs. Auditor

Adequate Insurance

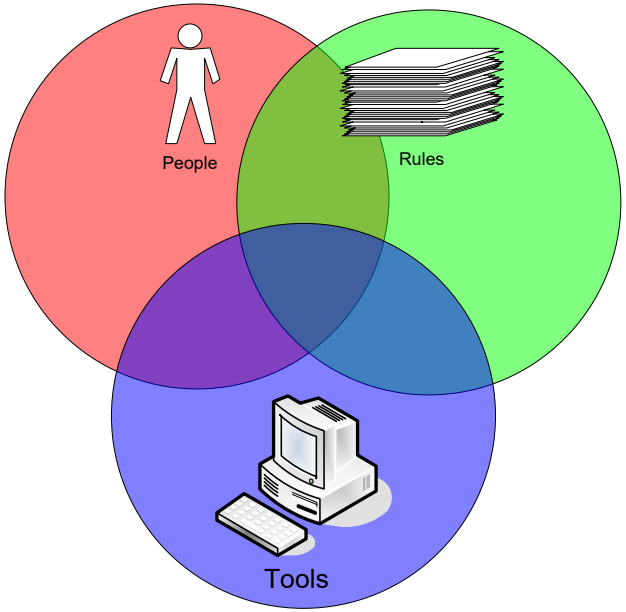
- Cyber insurance is as important as E&O and General Liability these days.
  - Covers cost of response and damages
  - Provides privacy attorneys, forensic responders and communications experts
  - Covers ransom payment
- Riders to general liability polices are not adequate
- Verify coverage is adequate every year

Cyber Security Can Make a Difference

Properly Managing Cyber Risks makes a Difference

- Technical tools are only as good as the people behind them

- Proper management requires a combination of leadership, technology and philosophy



Resources

- www.stopransomware.gov
- https://www.csbs.org/ransomware-self-assessment-tool
- https://www.ffiec.gov/press/PDF/FFIEC%20Statement%20on%20Pandemic%20Planning.pdf

Thank you!

Do you have questions? Please feel free to reach out.

Sundeep Bablani
Director
SAS – Cybersecurity
sundeep.bablani@CLAconnect.com

Barbie Housewright
Manager,
SAS – Cybersecurity
Barbie.Housewright@CLAconnect.com

CLAconnect.com

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING