



## The Growing Trend of Ransomware:

What You Can Do to Make Your Organization Less Vulnerable

1

## About the Presenter



### *John DiMaggio, Chief Executive Officer, Blue Orange Compliance*

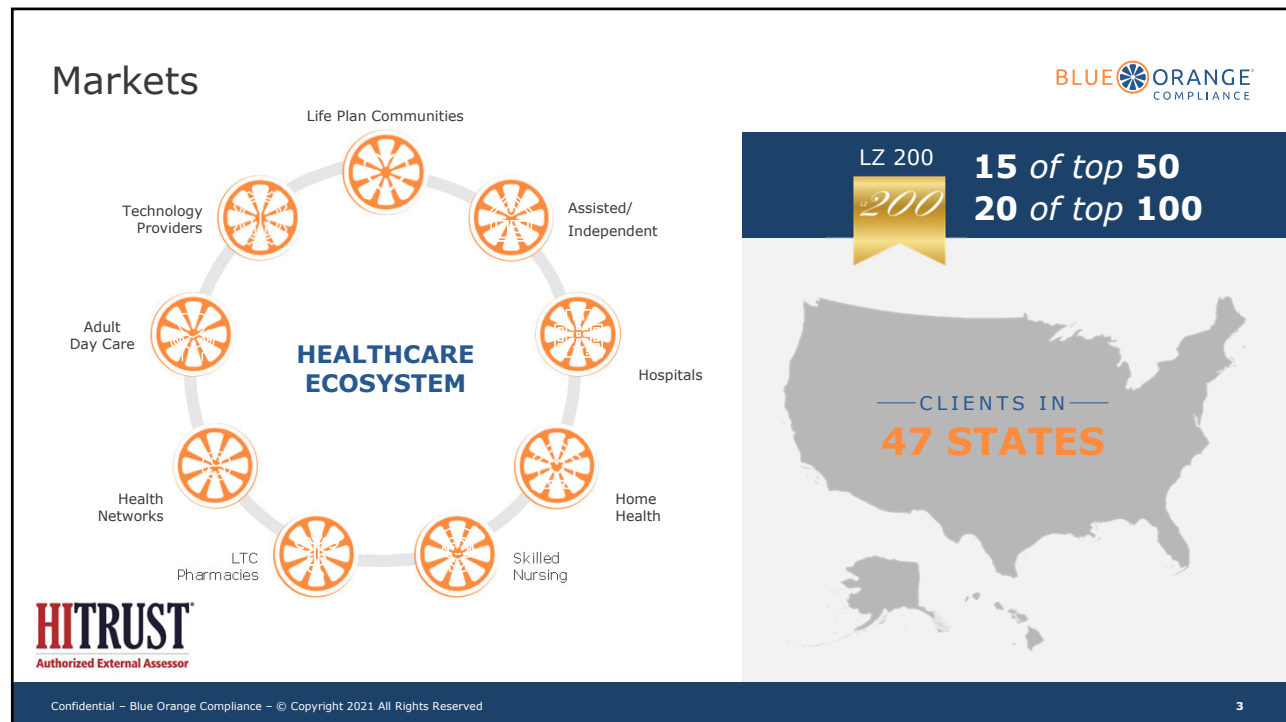
John DiMaggio is the Co-Founder and CEO of Blue Orange Compliance, a cyber-security and compliance firm dedicated to helping health care providers and business associates protect their information and navigate HIPAA and HITECH Privacy and Security regulations.

John is a recognized healthcare information compliance speaker to state bar associations, HIMSS, Health Care Compliance Association (HCCA), and long-term care associations including Long Term and Post-Acute Care (LTPAC), NAHC, Community Oncology Alliance (COA), State BAR Associations, LeadingAge and Argentum. John is also a LeadingAge CAST Commissioner.

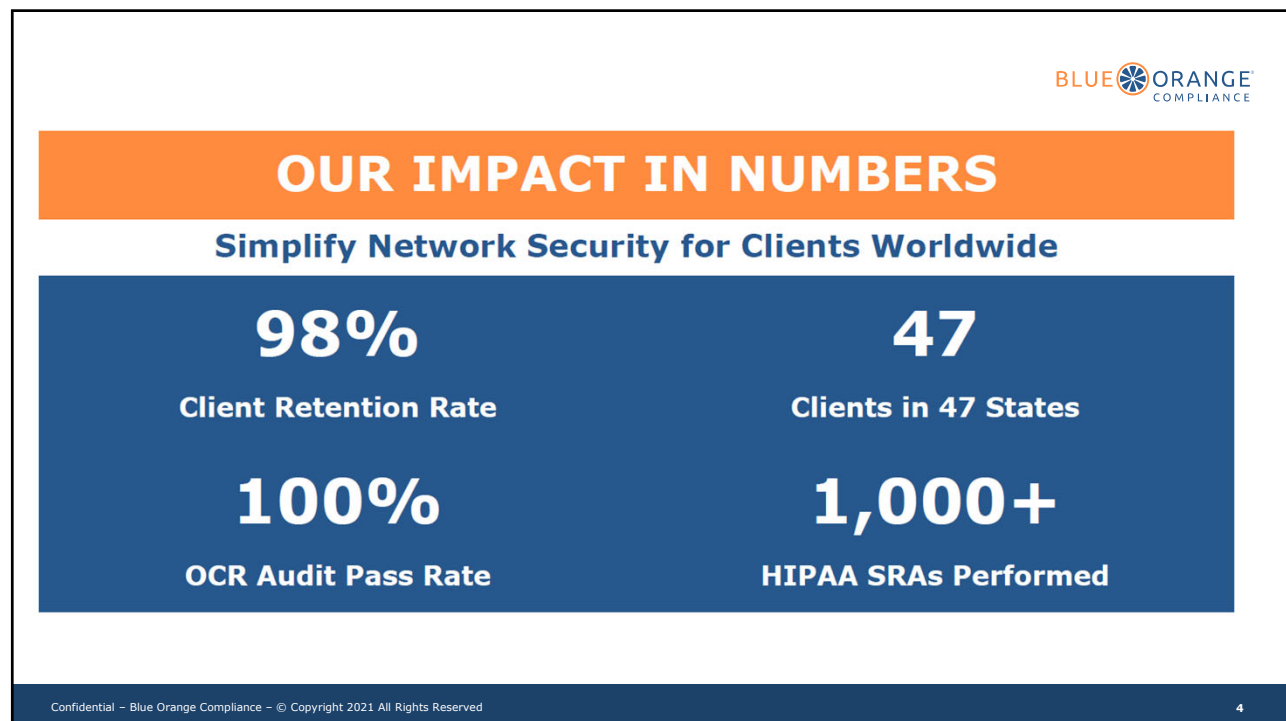
John's extensive healthcare experience includes Chief Information Officer with NCS Healthcare and Omnicare; senior operations roles with NeighborCare, and general consulting to the industry. John began his career as a key expert in Price Waterhouse's Advanced Technologies Group and served on several national and international standards organizations including the American National Standards Institute (ANSI) and the International Standards Organization (ISO).

John is the named inventor for multiple healthcare technology and process patents. He holds an MBA in Finance from Katz Graduate School of Business and a BS in Computer Science from the University of Pittsburgh.

2



3



4

## AGENDA



**Background/  
Groundwork**



**Cyber Security  
Science**



**Ransomware**



**Resilience**



**What to do?**



**Tabletop  
Exercise**

5



## Cyber News

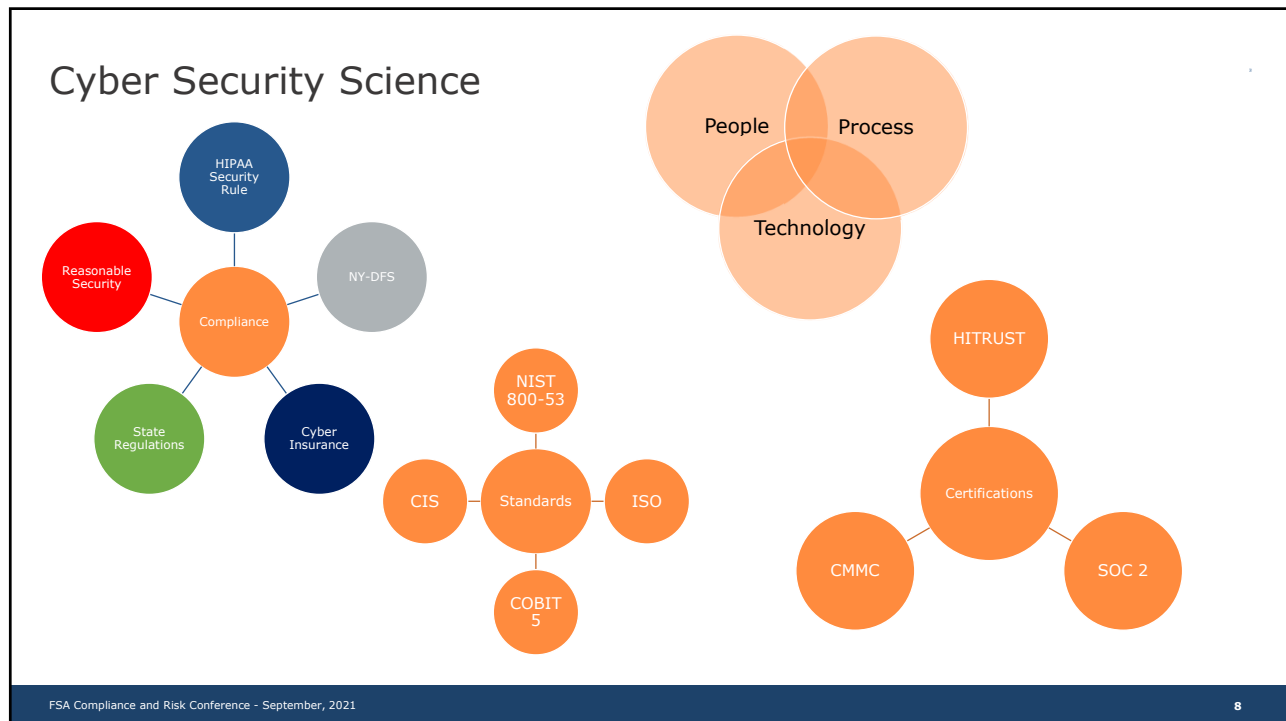
- Ransomware – many
- Downtime
- Exfiltration
- Pipeline attack
- Supply chain -SolarWinds

6

# House Analogy

- Locks – Doors/Windows
- Combination/Key Safe
- Locked closets/cabinets
- Burglar Alarm
- Security Monitoring
- Ring/Video - door bell
- Garage door opener

7



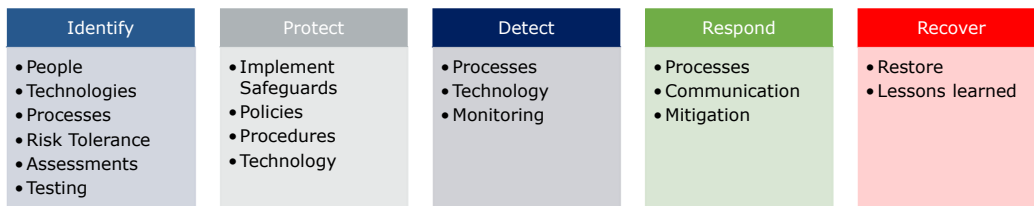
8

# Risk Areas

Areas	Vendors
	Email
	Files/file shares
	E.H.R./Clinical/Operational
	HR
	Remote workers
Sensitive info	ePHI
	Paper PHI
	PII
	Financial
	Marketing competitive
	Employee
Users	Staff
	Management
	Local/Domain Admin

9

## NIST Cyber Security Framework (CSF)



10

# Cyber Attack Techniques



## Motivators

Money  
Fun  
Social/Political Cause  
Information



## Best Practice Stages

Reconnaissance  
Scan  
Gain Access  
Maintain Access  
Clear Tracks

11

# Attack Stages Analogy

Stage	Burglar Your House	Hacker Your Organization
Reconnaissance	<ul style="list-style-type: none"> <li>• Drive by - schedule</li> <li>• Look at county auditor site</li> <li>• Facebook</li> </ul>	<ul style="list-style-type: none"> <li>• LinkedIn</li> <li>• Google</li> <li>• SEC Filings</li> <li>• Website</li> </ul>
Scanning	<ul style="list-style-type: none"> <li>• Check doors, windows</li> <li>• Try garage codes</li> </ul>	<ul style="list-style-type: none"> <li>• Scan ports</li> <li>• Phone calls</li> <li>• Physical visit</li> </ul>
Gain Access	<ul style="list-style-type: none"> <li>• Enter through window</li> </ul>	<ul style="list-style-type: none"> <li>• Phishing</li> <li>• Malware</li> <li>• Social</li> </ul>
Maintain Access	<ul style="list-style-type: none"> <li>• Add garage code</li> <li>• Find spare key</li> </ul>	<ul style="list-style-type: none"> <li>• Create back door</li> <li>• Create user</li> </ul>
Clear Tracks	<ul style="list-style-type: none"> <li>• Leave house as was</li> <li>• Remove fingerprints</li> </ul>	<ul style="list-style-type: none"> <li>• Clear audit logs</li> </ul>

12

# What is Ransomware

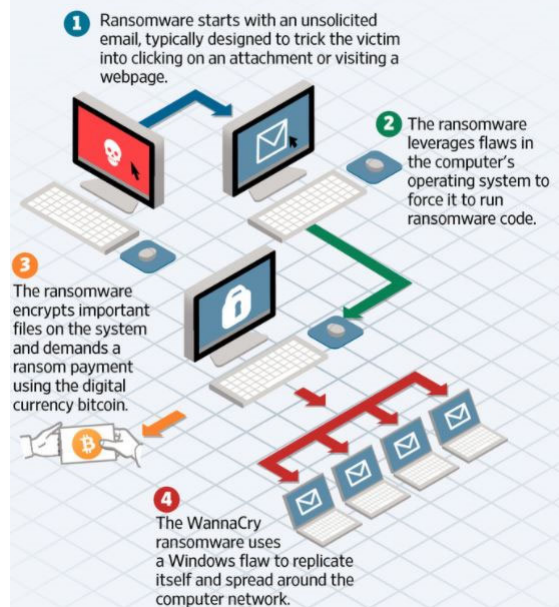


- A malicious software that gains access to files or systems and blocks user access to those files or systems.
- The first documented and purported example of ransomware was the 1989 AIDS Trojan, also known as PS Cyborg.
- Files or entire devices are held hostage using encryption until the victim pays a ransom in exchange for a decryption key.
- Ransom is usually paid in crypto currency like Bitcoin.
- Ransomware varieties have grown increasingly advanced in their capabilities for spreading, evading detection, encrypting files, and coercing users into paying ransoms.

13

# How Ransomware Works

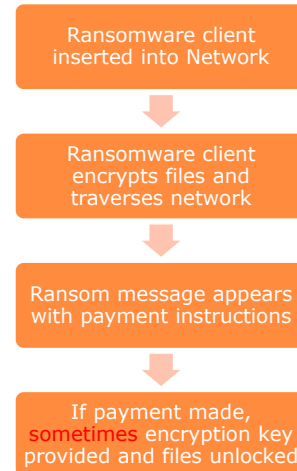
## How Ransomware Works



14

## Ransomware Components/Process

Encryption Client/Script  
 Encryption Algorithm  
 Encryption Key  
 Ransom Message  
 Optional Command and Control Server (CCS)  
 Bitcoin Wallet Id  
 Price



FSA Compliance and Risk Conference - September, 2021

15

15

## Ransomware Entry Points

BLUE ORANGE  
COMPLIANCE

- Network Configuration
  - Exposed Server Message Block (SMB)
  - Remote Desktop Protocol (RDP)
- Unpatched Software
- Malicious Website
- Phishing email link or attachment
- USB Drive
- Weak passwords
- Internet of Things (IoT)
- ....

16



**1. You should register Bitcoin wallet** ([click here for more information with pictures](#))

**2. Purchasing Bitcoins** - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

**Here are our recommendations:**

- [LocalBitcoins.com \(WU\)](#) - Buy Bitcoins with Western Union
- [Coincave.com](#) - Recommended for fast, simple service. Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person
- [LocalBitcoins.com](#) - Service allows you to search for people in your community willing to sell bitcoins to you directly.
- [btcdirect.eu](#) - THE BEST FOR EUROPE
- [coinmr.com](#) - Another fast way to buy bitcoins
- [bitquick.co](#) - Buy Bitcoins Instantly for Cash
- [How To Buy Bitcoins](#) - An international directory of bitcoin exchanges.
- [Cash Into Coins](#) - Bitcoin for cash.
- [CoinJar](#) - CoinJar allows direct bitcoin purchases on their site.
- [anxpro.com](#)
- [bitylicious.com](#)
- [ZipZap](#) - ZipZap is a global cash payment network enabling consumers to pay for digital currency.

**3. Send 1.79 BTC to Bitcoin address:**

**4. Enter the Transaction ID and select amount:**

Transaction ID:  1.79 BTC ≈ 700 USD

Note: Transaction ID - you can find in detailed info about transaction you made.  
(example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)

**5. Please check the payment information and click "PAY".**

\*Image from bleeping computer

FSA Compliance and Risk Conference - September, 2021 17

17

## What to Do

- Assessments
- Testing
- Plan/Remediation
- Monitoring
- Processes

FSA Compliance and Risk Conference - September, 2021 18

18

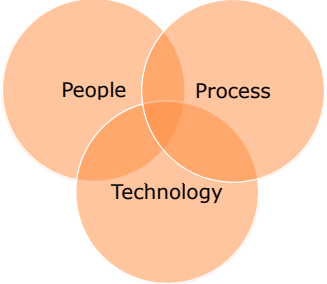
# What to Do

- Assessments
- Testing
- Plan/ Remediation
- Monitoring
- Processes
- Training
- Cyber Insurance

19

## Security Assessment

- HIPAA Security Risk Assessment – NIST
  - All areas of Security Rule
  - Against relevant NIST Controls (90+)
  - Interviews
  - Materials Review
  - Policies and Procedures
  - Evidence
  - Physical Controls
  - Tech Eval



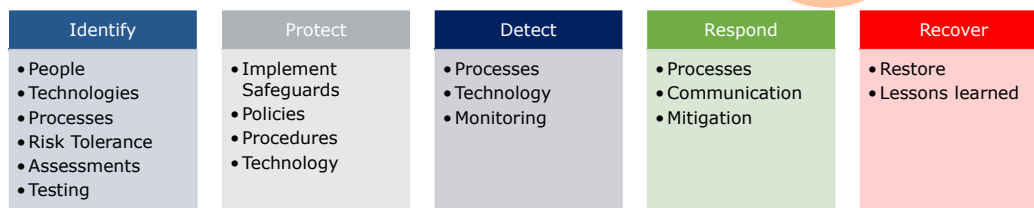
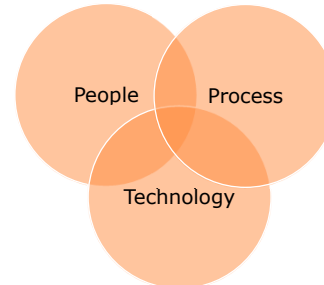
Identify	Protect	Detect	Respond	Recover
<ul style="list-style-type: none"> <li>People</li> <li>Technologies</li> <li>Processes</li> <li>Risk Tolerance</li> <li>Assessments</li> <li>Testing</li> </ul>	<ul style="list-style-type: none"> <li>Implement Safeguards</li> <li>Policies</li> <li>Procedures</li> <li>Technology</li> </ul>	<ul style="list-style-type: none"> <li>Processes</li> <li>Technology</li> <li>Monitoring</li> </ul>	<ul style="list-style-type: none"> <li>Processes</li> <li>Communication</li> <li>Mitigation</li> </ul>	<ul style="list-style-type: none"> <li>Restore</li> <li>Lessons learned</li> </ul>

FSA Compliance and Risk Conference - September, 2021

20

## Testing – Vulnerability Scanning

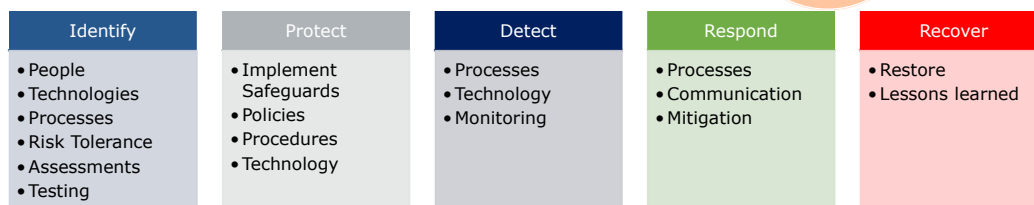
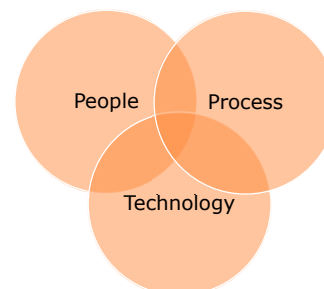
- Internal
- External
- Known Vulnerabilities
- Validates Patching
- Light Configuration
- Perform Regularly - > annual



21

## Testing – Penetration Testing

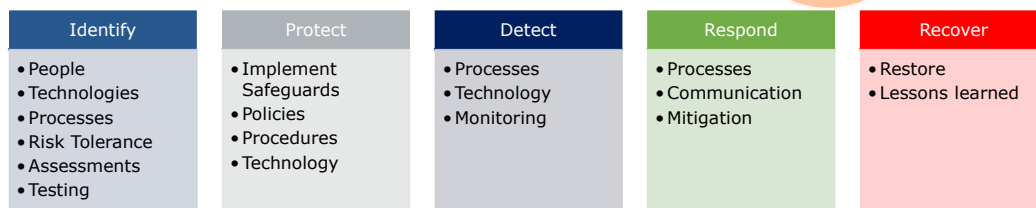
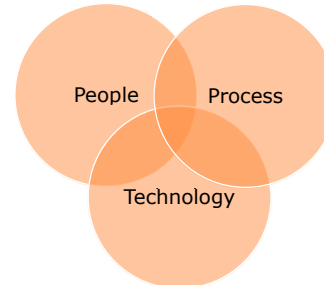
- Internal
- External
- Offensive
- Social
- Configuration
- More
- Perform Regularly - Annual



22

## Testing – Phishing

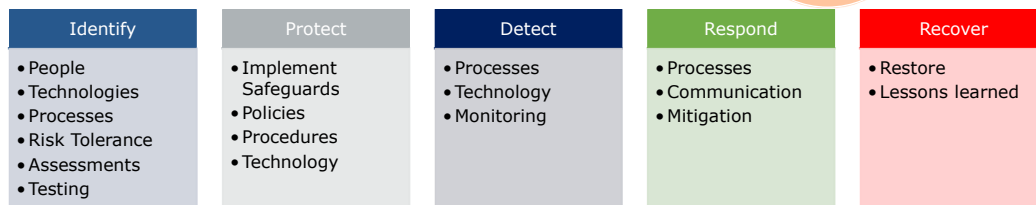
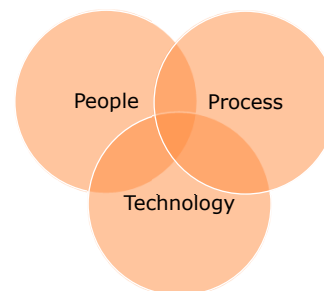
- Campaigns
- Metrics
- Training
- Discipline
- Perform Regularly - Monthly



23

## Testing – Ransomware Simulator

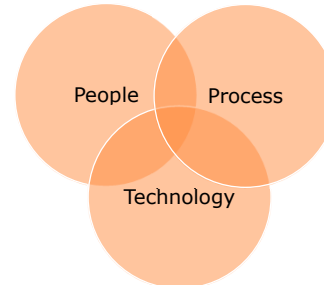
- Non-destructive simulation
- Tests detection



24

## Testing – Incident Response

- Tabletop Exercise – Various incidents
- Multidisciplinary – Execs/I.T., etc.
- Test/create Playbooks
- Test Backup/Recovery

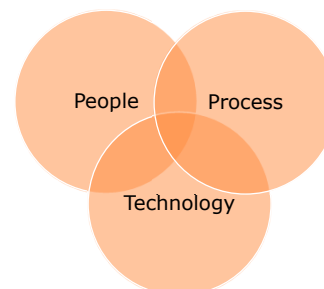


Identify	Protect	Detect	Respond	Recover
<ul style="list-style-type: none"> <li>• People</li> <li>• Technologies</li> <li>• Processes</li> <li>• Risk Tolerance</li> <li>• Assessments</li> <li>• Testing</li> </ul>	<ul style="list-style-type: none"> <li>• Implement Safeguards</li> <li>• Policies</li> <li>• Procedures</li> <li>• Technology</li> </ul>	<ul style="list-style-type: none"> <li>• Processes</li> <li>• Technology</li> <li>• Monitoring</li> </ul>	<ul style="list-style-type: none"> <li>• Processes</li> <li>• Communication</li> <li>• Mitigation</li> </ul>	<ul style="list-style-type: none"> <li>• Restore</li> <li>• Lessons learned</li> </ul>

25

## Employee Training

- Regular Security Awareness Training
- Policy and Procedure Training

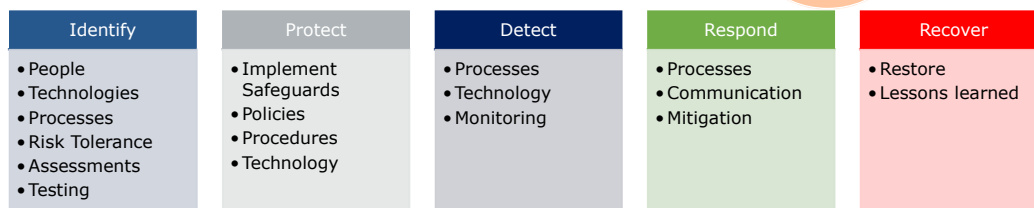
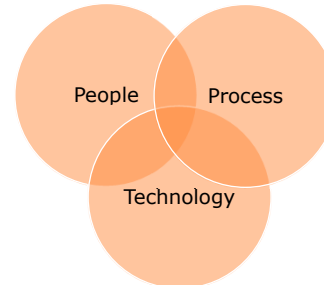


Identify	Protect	Detect	Respond	Recover
<ul style="list-style-type: none"> <li>• People</li> <li>• Technologies</li> <li>• Processes</li> <li>• Risk Tolerance</li> <li>• Assessments</li> <li>• Testing</li> </ul>	<ul style="list-style-type: none"> <li>• Implement Safeguards</li> <li>• Policies</li> <li>• Procedures</li> <li>• Technology</li> </ul>	<ul style="list-style-type: none"> <li>• Processes</li> <li>• Technology</li> <li>• Monitoring</li> </ul>	<ul style="list-style-type: none"> <li>• Processes</li> <li>• Communication</li> <li>• Mitigation</li> </ul>	<ul style="list-style-type: none"> <li>• Restore</li> <li>• Lessons learned</li> </ul>

26

## Log Management

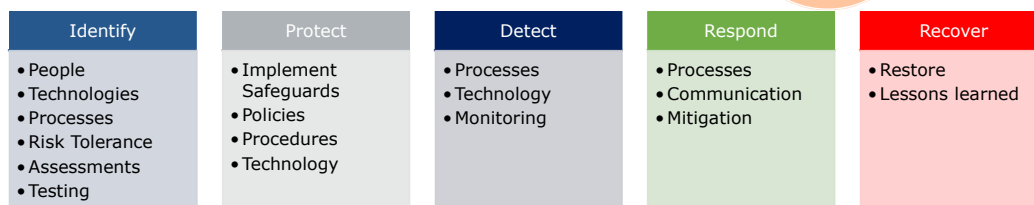
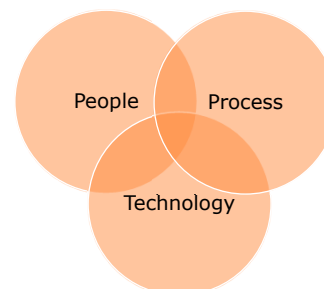
- Ensure logging turned on
- Ensure sufficient space/storage > 6 month
- Required for Forensics



27

## Monitoring

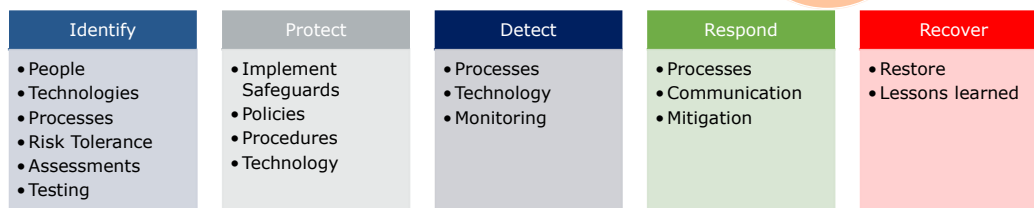
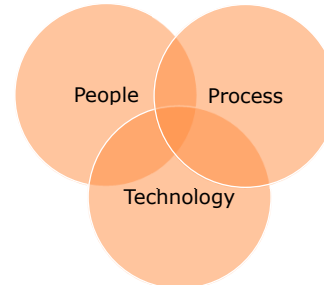
- Examine activity from multiple sources
- Risk-based Alerts based on playbook



28

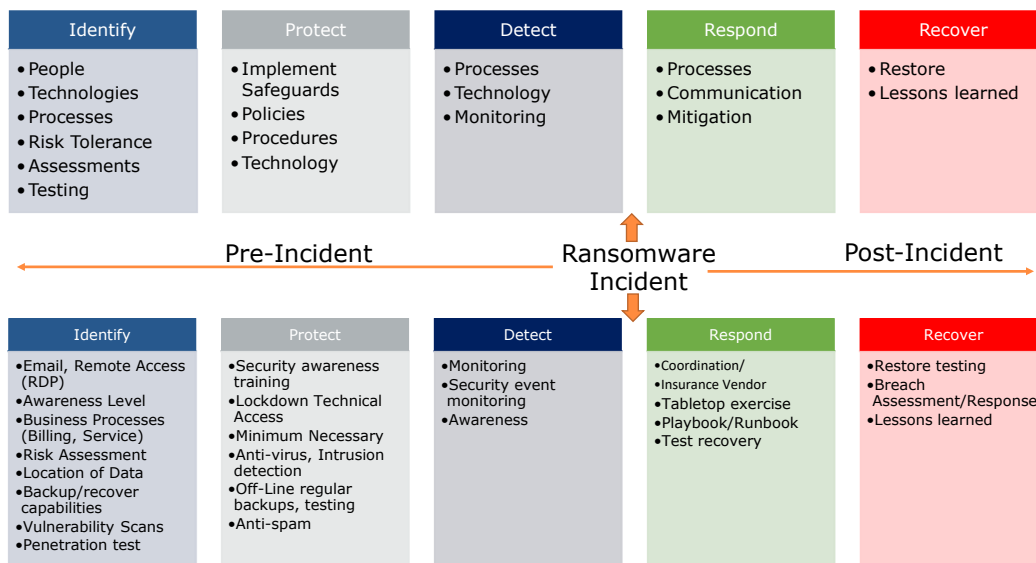
## Plan/Remediation

- Develop and Manage Active, Prioritized Plan
- Socialize Plan to Management/Board



29

## NIST Cyber Security Framework (CSF)



30

## Cyber Insurance

- Evaluate Policy
- Market Changes

### ▪ INSURABILITY REQUIREMENTS

- Multi-Factor Authentication
- Secured Remote Connectivity - No Public RDP
- Segregated Backups
- Employee Training
- Cyber Incident Response Policy
- EDR / IDS and NextGen Antivirus tools deployed
- Patch Management
- Penetration Testing/ Vulnerability Assessments
- Identifying key IT and non-IT vendors

31

## Incident Response Definition

An organized approach to addressing and managing the aftermath of a security breach or cyberattack, also known as an IT incident, computer incident or security incident. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

"Source: SANS Institute"

32



## Incident Response HIPAA Requirements

- Policies & Procedures
- Training
- Testing/Exercises
- Handling
- Monitoring
- Reporting
- Assistance

33

## Incident Response Tabletop- Goals

- Understand I.T./Security and interaction with other parts of the organization
- Understand importance of emergency response procedure from all areas with an organization
- Provide insight into the response capabilities to ransomware or other incidents
- Discuss effectiveness of internal/external communication
- Test your Playbook/Runbook

34

## Tabletop Exercise

Test your ability to

- Classify incidents based on severity and impact
- Notify appropriate individuals
- Collect artifacts
- Escalate when necessary
- Respond technically and organizationally

Injects

- Scenario twists - Affects scenario potentially causing it to spawn or change course

Usually lasts approx. 2 hours

Recommended annually or system changes

35

## Incident Response Tabletop-Who

### **REQUIRED:**

Exercise Leader(s)

Security Team

This consists of any individuals likely to be responsible for responding to a security incident, part or whole.

Security Management

Security Management is required if not acting as exercise leaders or members of the security team.

Risk Management Representative

Emergency Preparedness Representative

### **RECOMMENDED:**

Executives

Minute/Note keeper (if exercises leaders are not prepared to take notes)

36

## Security Incident Examples

Ransomware  
Business Email Compromise  
Lost Laptop  
Keyloggers  
Crypto-jacking

37

## Ransomware

- Malware
- Enters through infected Ads or files
- Encrypts files
- Ransom demanded for key
- Usually no data is stolen

38

## Incident Response Stages

Detect  
Respond  
Recover

39

## Scenario Information

- Time: 9:33am
- Event: Help desk ransomware call
- Description: At 9:33am John Doe calls the help desk stating that there is a ransomware note on his screen. He was recently browsing a the web just prior to receiving the notice. He cannot get it to close.

40

## Inject

- Time: 10:32 – 10:45 am
- Event: Help desk ransomware calls
- Description: Between 10:32am and 10:45, the helpdesk gets multiple calls reporting a similar message. Once call is from Sally Smith in HR who recently opened an invoice and the other is from the SNF clinical staff at your new campus 2 hours away. Neither can access any files or get the message to close.

41

## *Detection*

- How would this alert be detected and reported in your organization?
- Are we confident in our alerting, logging, and reporting structure?

42

## Correlation

- Were the affected users performing same activities?
- What things do these users have in common?
- Are there shared local admin passwords?
- Any unusual traffic or other indicators?
- What was the user doing?

43

## *Impact*

- What type of data does this employee have access to?
- What is the employee's organizational role?
- Is there a risk of spreading or pivoting throughout the environment?
- Are any files accessible?
- Is ePHI involved?

44

## *Event Notification*

- Is the business owner/manager notified?
- Who else is initially notified of the event?
  - Users?
  - Employees?
  - Residents?
- How are notifications communicated?

45

## Inject

- Time: 12:01 pm
- Event: Inquiry calls on general number
- Description: A nurse involved at the other campus is married to someone that works at the local newspaper. A reporter is calling to ask about the incident.

46

## *Incident Declaration and Prioritization*

- Incident Declaration
  - How was it determined that there was an incident?
  - How did the organization invoke the IRP?
  - Was it possible to correlate other information?
  - What immediate actions will prevent the spread of ransomware?
- Prioritization
  - How is priority determined?

47

## *Notification/Escalation and Analysis*

- Notification/Escalation
  - Who gets notified of the incident
  - How are the notifications communicated?
- Who performs the analysis
- Who owns this incident? What type of incident are you going to declare?
- How is this prioritized?
- Do any additional resources or stakeholders need to be notified?
- Who performs the analysis?
- What are options to deal with the outage?

48



## *Incident Eradication*

- How can the ransomware be prevented from spreading to additional systems?
- What is the process for connecting a previously compromised system to the network again?

49

## *Incident Recovery*

- On or offsite backups?
- How often are backups taken
- How long to restore from backup?
- Who is responsible?
- How often is the restore process exercised?
- How long to wait before removing defenses?

50

## *Incident Communication*

- Is the rest of the organization notified of the incident?
- Is there any external communication?
- Who is responsible for notifications?
- Is an after action review performed?
- Is the incident response plan updated with information obtained from this incident?

51

## The After-Party- HIPAA Breach

Definition: "The acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E ("HIPAA") which compromises the security or privacy of the protected health information."

Breach Risk Assessment

OCR Investigation

52

## Management/Board Level Discussion Items

- When was the last time we practiced our cyber incident response capability?
  - What is my role in a particular incident?
- If an incident happened right now could we continue operations?
  - Pay Ransom vs Recovery
- What is OUR determined difference between a short term incident and a long term incident – as defined by the business
  - Corporate environment vs subsidiaries
- Do we have retainers in place for Legal, PR, and Cyber Security
- Do we have cyber insurance to cover this? What does it cover?

53

*Thank You*



## *Contact Info and Additional Information*



*John DiMaggio, CEO  
Blue Orange Compliance  
john.dimaggio@blueorangecompliance.com  
614.567.4109*

54



55