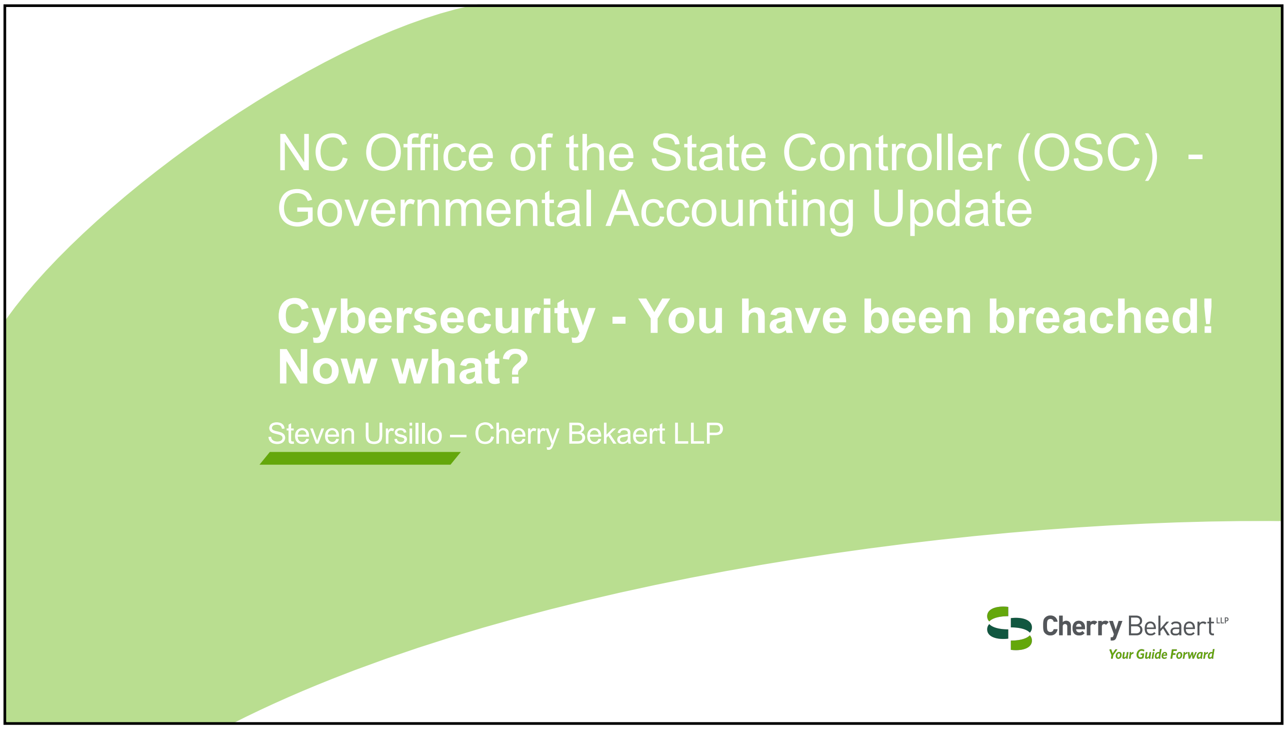


NC Office of the State Controller (OSC) - Governmental Accounting Update

Cybersecurity - You have been breached! Now what?

Steven Ursillo – Cherry Bekaert LLP

Cherry Bekaert LLP
Your Guide Forward

1

About the Speaker

Steven Ursillo Jr, **CPA, CIA, CGMA, CFE, CISA, CISM, CITP, CISSP, CGEIT, CRISC, CEH and CCSFP**
Partner at Cherry Bekaert LLP | National Leader, Information Assurance & Cybersecurity

- Over 20 years of experience specializing in risk management, SOC, information system security and privacy, cybersecurity fraud prevention, detection and response, security and privacy governance, red and blue teaming, IT assurance services and internal control over financial reporting
- Current chair of the AICPA IMTA (Information Management and Technology Assurance) Executive Committee
- Nationally recognized writer and speaker on issues in the forefront of cybersecurity, risk and technology publications
- Past President RISCPA and RICFE
- Past AICPA Council Member

2

2

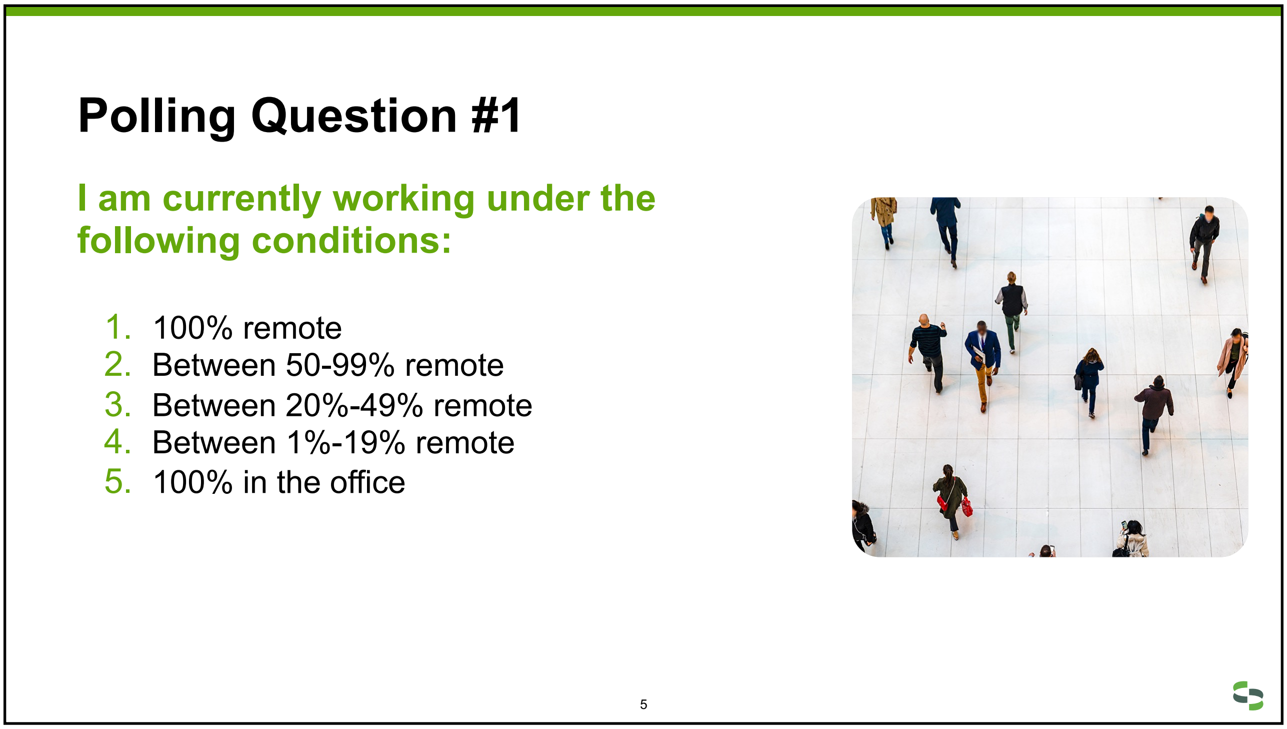
Agenda

- Learning Objectives & Cybersecurity Threat Landscape
- IR Plan Objectives and Considerations
- Security Incident Life Cycle
- Financial Risk Mitigation-Cyber Insurance
- Key Takeaways
- Questions

Learning Objectives

Participants will identify and recognize:

- The latest cyber threat landscape
- Key components when designing, executing and monitoring an incident response program
- Key considerations when responding to a cybersecurity breach
- Cybersecurity risk mitigation strategies

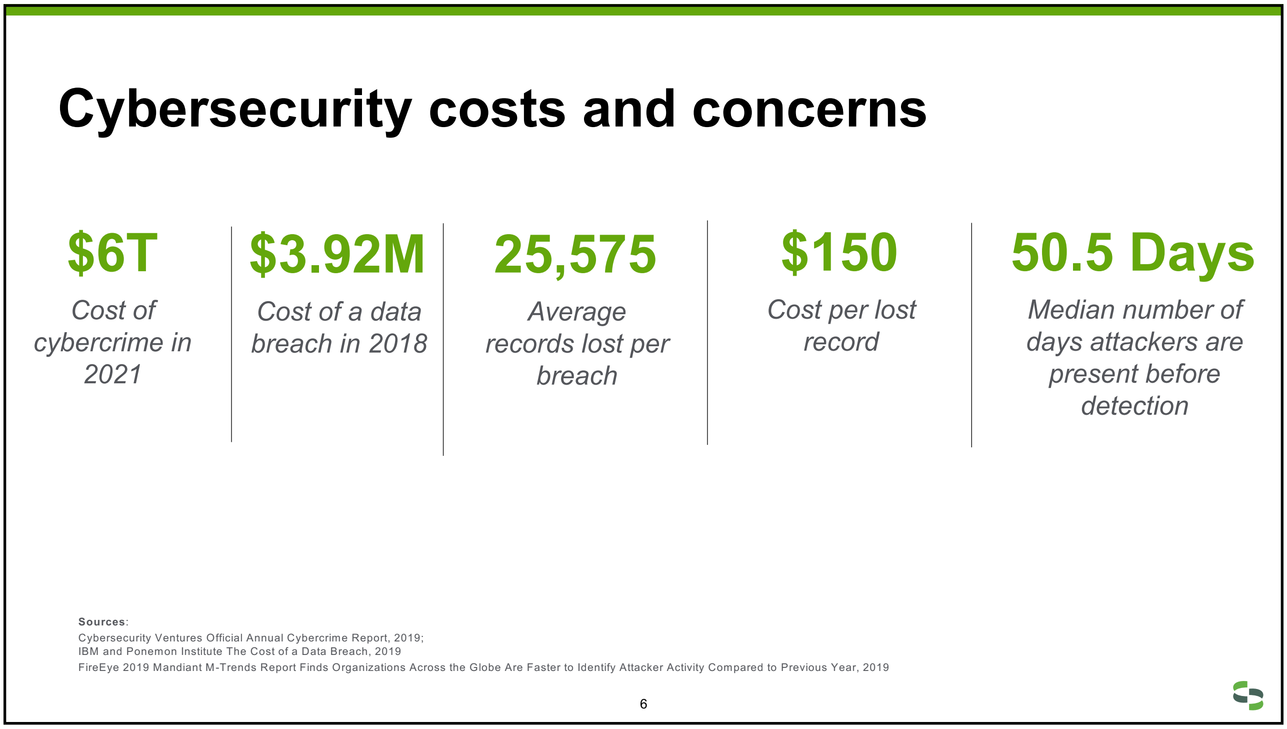


Polling Question #1

I am currently working under the following conditions:

1. 100% remote
2. Between 50-99% remote
3. Between 20%-49% remote
4. Between 1%-19% remote
5. 100% in the office

5

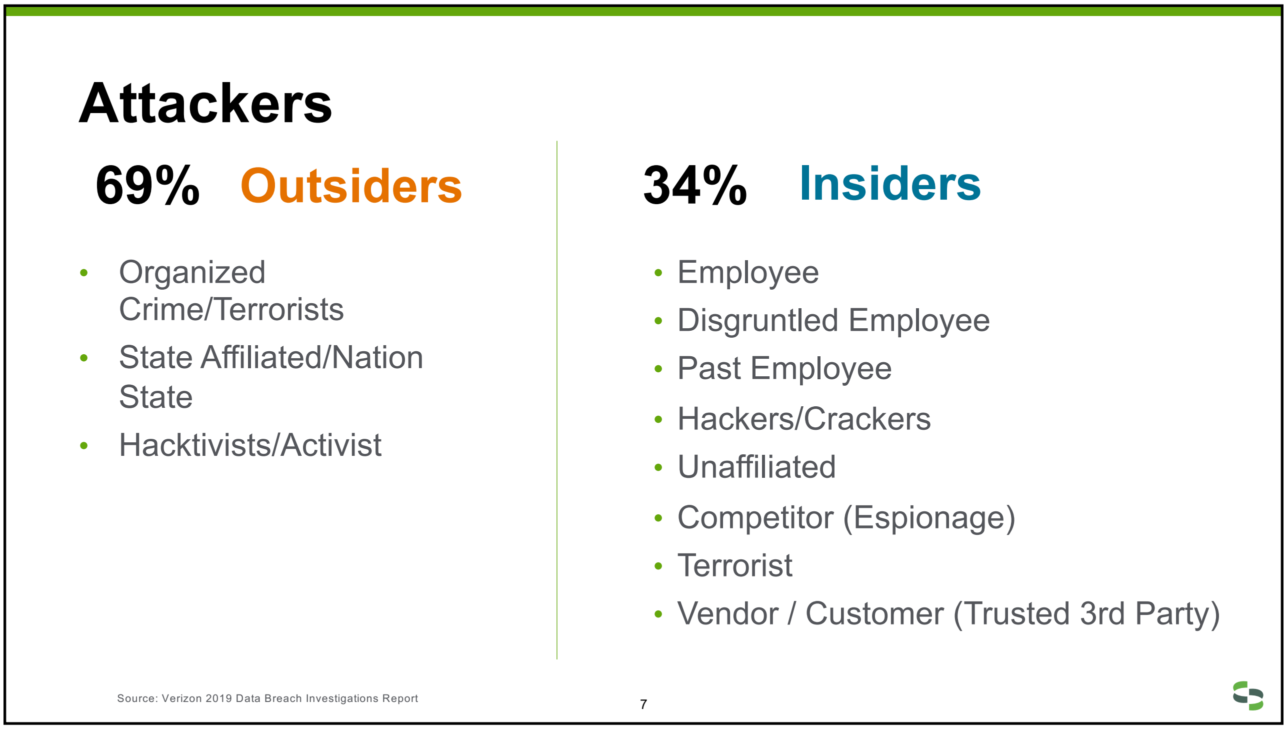


Cybersecurity costs and concerns

$6T	$3.92M	25,575	$150	50.5 Days
Cost of cybercrime in 2021	*Cost of a data breach in 2018*	*Average records lost per breach*	*Cost per lost record*	*Median number of days attackers are present before detection*

Sources:
Cybersecurity Ventures Official Annual Cybercrime Report, 2019;
IBM and Ponemon Institute The Cost of a Data Breach, 2019
FireEye 2019 Mandiant M-Trends Report Finds Organizations Across the Globe Are Faster to Identify Attacker Activity Compared to Previous Year, 2019

6



Attackers

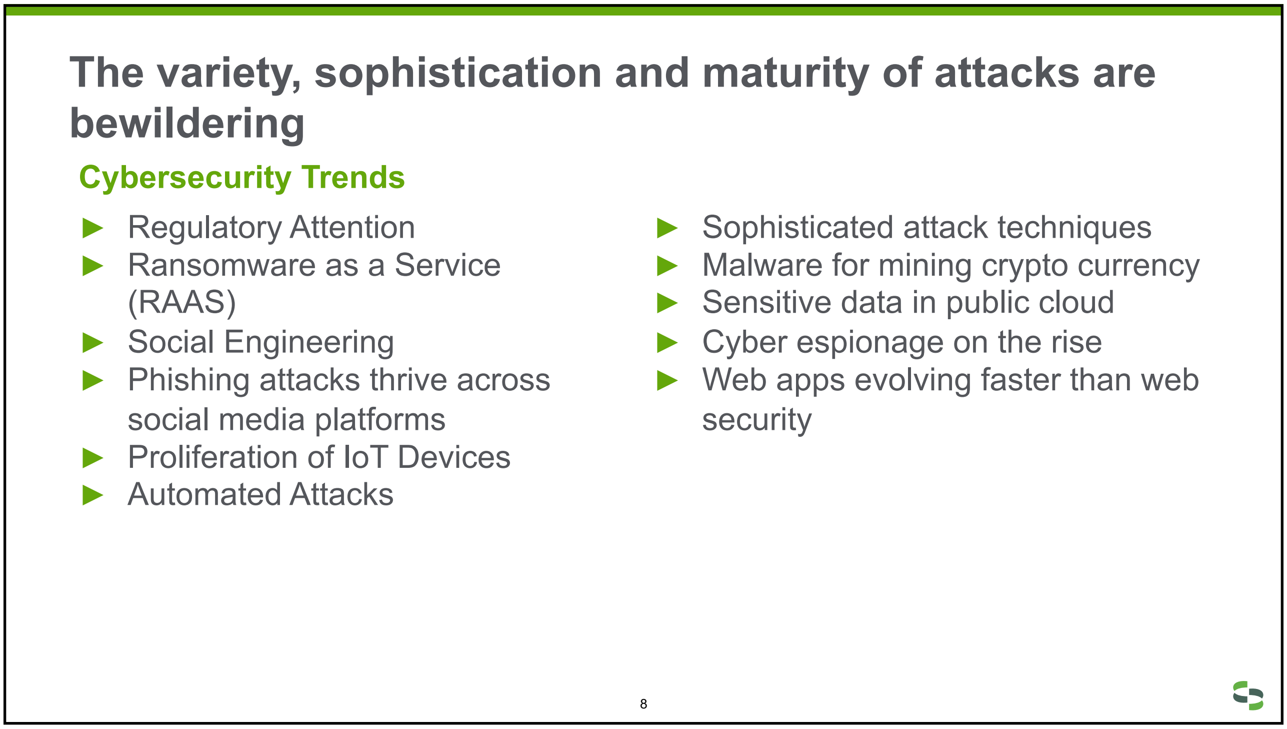
69% Outsiders

- Organized Crime/Terrorists
- State Affiliated/Nation State
- Hacktivists/Activist

34% Insiders

- Employee
- Disgruntled Employee
- Past Employee
- Hackers/Crackers
- Unaffiliated
- Competitor (Espionage)
- Terrorist
- Vendor / Customer (Trusted 3rd Party)

Source: Verizon 2019 Data Breach Investigations Report



The variety, sophistication and maturity of attacks are bewildering

Cybersecurity Trends

- ▶ Regulatory Attention
- ▶ Ransomware as a Service (RAAS)
- ▶ Social Engineering
- ▶ Phishing attacks thrive across social media platforms
- ▶ Proliferation of IoT Devices
- ▶ Automated Attacks
- ▶ Sophisticated attack techniques
- ▶ Malware for mining crypto currency
- ▶ Sensitive data in public cloud
- ▶ Cyber espionage on the rise
- ▶ Web apps evolving faster than web security

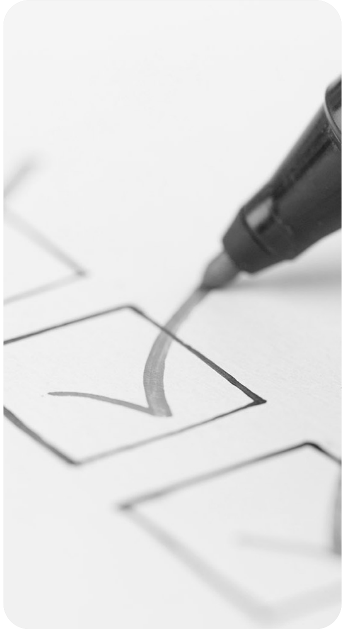
The variety, sophistication and maturity of attacks are bewildering (Continued)

Top Threats

- Phishing/variants
- Targeted Ransomware
- No footprint malware
- Password spraying
- Business email compromise
- Advanced persistent threats

Top Risks

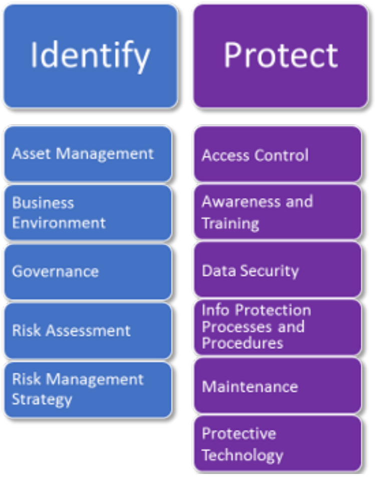
- Consolidation and M&A
- Outsourcing/supply chain
- Cloud apps/email/social media
- Poor patching processes
- Badly coded applications
- Failing to Plan



Cybersecurity Governance Quick Hit Checklist

- Strategy (objectives, resources, business strategy)
- Governance
- Critical Data and Asset Identification
- Risk Management
- Vulnerability Management
- Third Party Risk Management
- Monitoring and Reporting
- Incident Response and Breach Notification
- Awareness and Training

NIST Cyber Security Framework

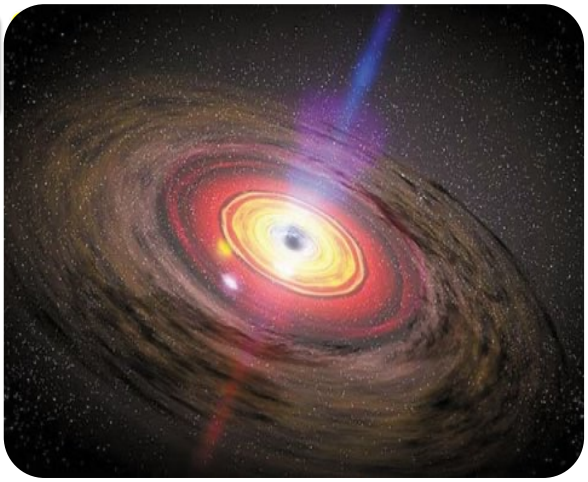


Identify

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

Protect

- Access Control
- Awareness and Training
- Data Security
- Info Protection Processes and Procedures
- Maintenance
- Protective Technology



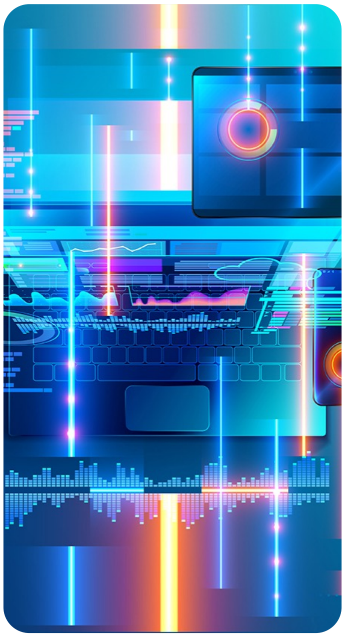
Polling Question #2

I work in the following area:

1. Accounting
2. Technology Risk
3. Cyber/Tech Risk
4. Other
5. I have decided not to work for a while/ever

IR Plan Objectives and Key Considerations

13



Objectives of an IR Plan

- ▶ Safeguarding of covered and protected information
- ▶ Identify an attack
- ▶ Contain the damage
- ▶ Eradicate the root cause
- ▶ Timely and effective restoration of business operations and service level agreements

14

14

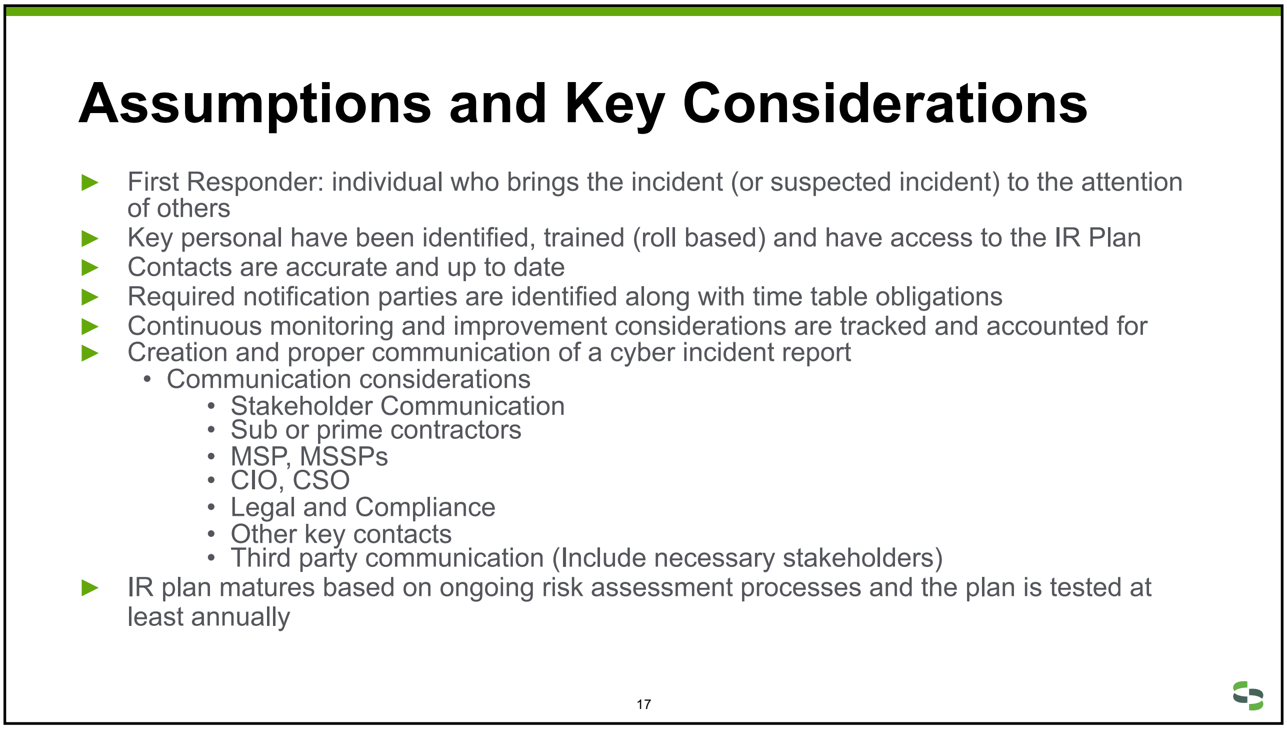
Breach Notification Requirements

- State law
- Federal law
- Global requirements (GDPR, etc.)
- Regulatory requirements (ex. HIPAA, CMMC, PCI, PCAOB, etc.)
- Third-Parties (customers, vendors, partners)
- Individuals

Data Breach Response Considerations

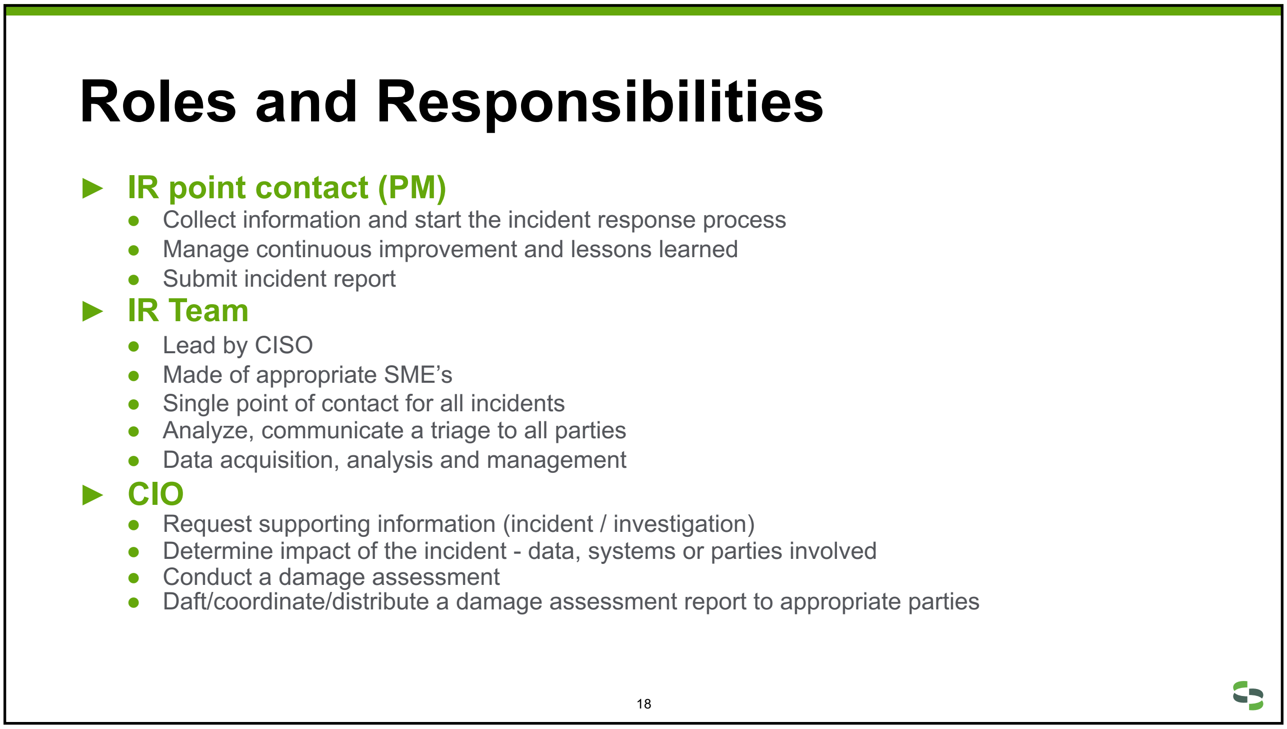
- Breach notification may be specified by your state or federal law
- Include information about the compromise-do not mislead
- Describe how the breach happened
- What assets were compromised
- How the adversaries used the information (if available)
- What remediation steps have been taken
- What actions have been done or are being performed to protect individuals (i.e. credit monitoring)
- How to contact the designated individual(s) in your organization for support

Source: https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business



Assumptions and Key Considerations

- First Responder: individual who brings the incident (or suspected incident) to the attention of others
- Key personal have been identified, trained (roll based) and have access to the IR Plan
- Contacts are accurate and up to date
- Required notification parties are identified along with time table obligations
- Continuous monitoring and improvement considerations are tracked and accounted for
- Creation and proper communication of a cyber incident report
  - Communication considerations
    - Stakeholder Communication
    - Sub or prime contractors
    - MSP, MSSPs
    - CIO, CSO
    - Legal and Compliance
    - Other key contacts
    - Third party communication (Include necessary stakeholders)
- IR plan matures based on ongoing risk assessment processes and the plan is tested at least annually



Roles and Responsibilities

- **IR point contact (PM)**
  - Collect information and start the incident response process
  - Manage continuous improvement and lessons learned
  - Submit incident report
- **IR Team**
  - Lead by CISO
  - Made of appropriate SME’s
  - Single point of contact for all incidents
  - Analyze, communicate a triage to all parties
  - Data acquisition, analysis and management
- **CIO**
  - Request supporting information (incident / investigation)
  - Determine impact of the incident - data, systems or parties involved
  - Conduct a damage assessment
  - Daft/coordinate/distribute a damage assessment report to appropriate parties

Security Incident Lifecycle

Cherry Bekaert LLP
Your Guide Forward

19

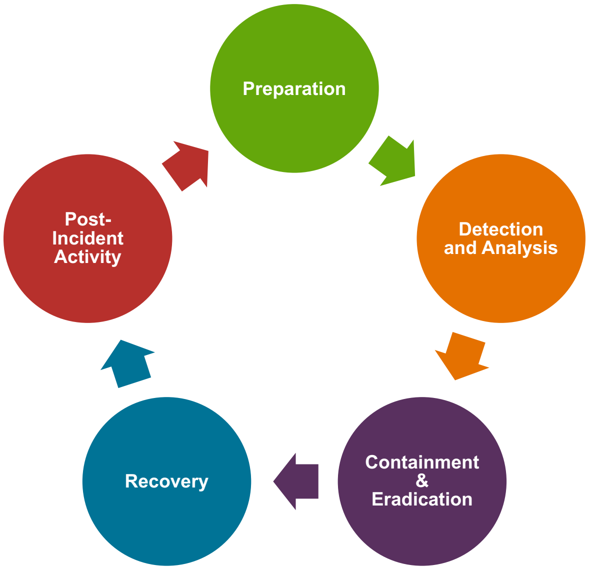
Polling Question #3

When it comes to a potential material cybersecurity incident, my organization:

1. Is well prepared, bring it on!!!
2. Is fairly mature and has tested the plan on a few occasions
3. Procedures are ad-hoc but can respond based on the circumstances
4. Has not performed any preparation
5. Not sure

20

Security Incident Lifecycle (SILC)



Security Incident Life Cycle - Preparation

- Identify and designate the owner and responsible party for all incidents
- Identify team of experts (operations, security, forensics, legal, IT, investor and public relations, corporate communications, HR, management, etc.)
- Provide a communication outlet to report an incident to employees, contractors, third parties to report suspicious or suspected breach activity
- Focus efforts based on risk assessment results
- Ensure detection and monitoring controls are properly designed and operating effectively (firewall, IPS, anti-malware, logging, NTP)
- Provide media training to data acquisition and management team

Security Incident Life Cycle – Preparation (Continued)

- Identify a secure repository for evidence collection and management
- Provide company wide training on breach awareness responsibility and reporting protocols
- Evaluate the adequacy of cybersecurity insurance coverage
- Additional steps taken to prepare:
- Testing of the IR plan
- Collection and implementation of lessons learned
- Update contact and escalation lists on the IR plan
- Plan distribution - make sure the IR plan is available to key personnel
- Identify and address precursors of the incident
- Verify resources available - tools and subject matter experts (SME’s)

23

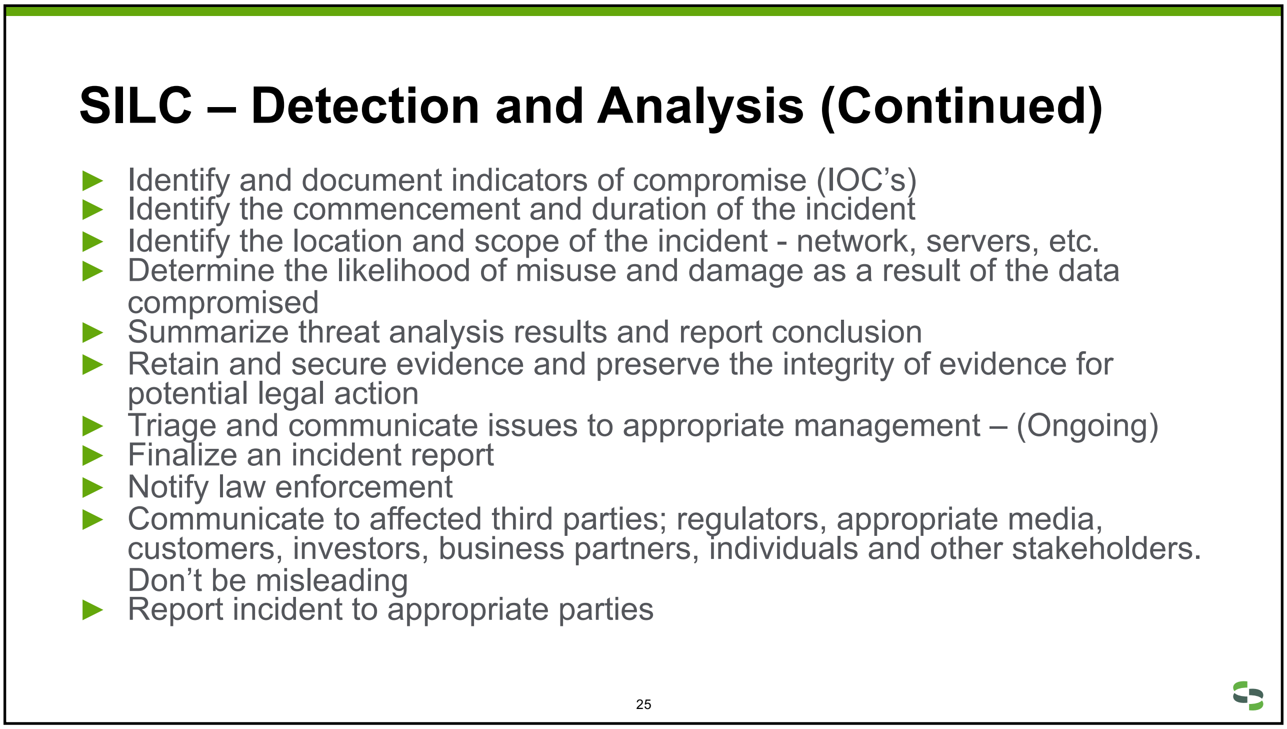
23

SILC – Detection and Analysis

- Create/open and incident ticket
- Prioritize incident based on business impact
- ID affected resources and potentially affected resources
- Incident classification - considerations
- Gather the appropriate team
- Set up technical contacts for operational restoration
- Consult with insurance carrier
- Consult with legal (internal and/or external) specializing in data security regulatory requirements, state and federal law
- Set reoccurring meetings for status updates and next steps (remain agile)
- Perform necessary technical investigations (assessment, network, system and device forensics, etc.)
- Interview relevant individuals related to the incident
- Identify initial cause (patient zero) and coordinate the required specialist to help restore operations
- Identify the nature and classification of the data/assets affected

24

24

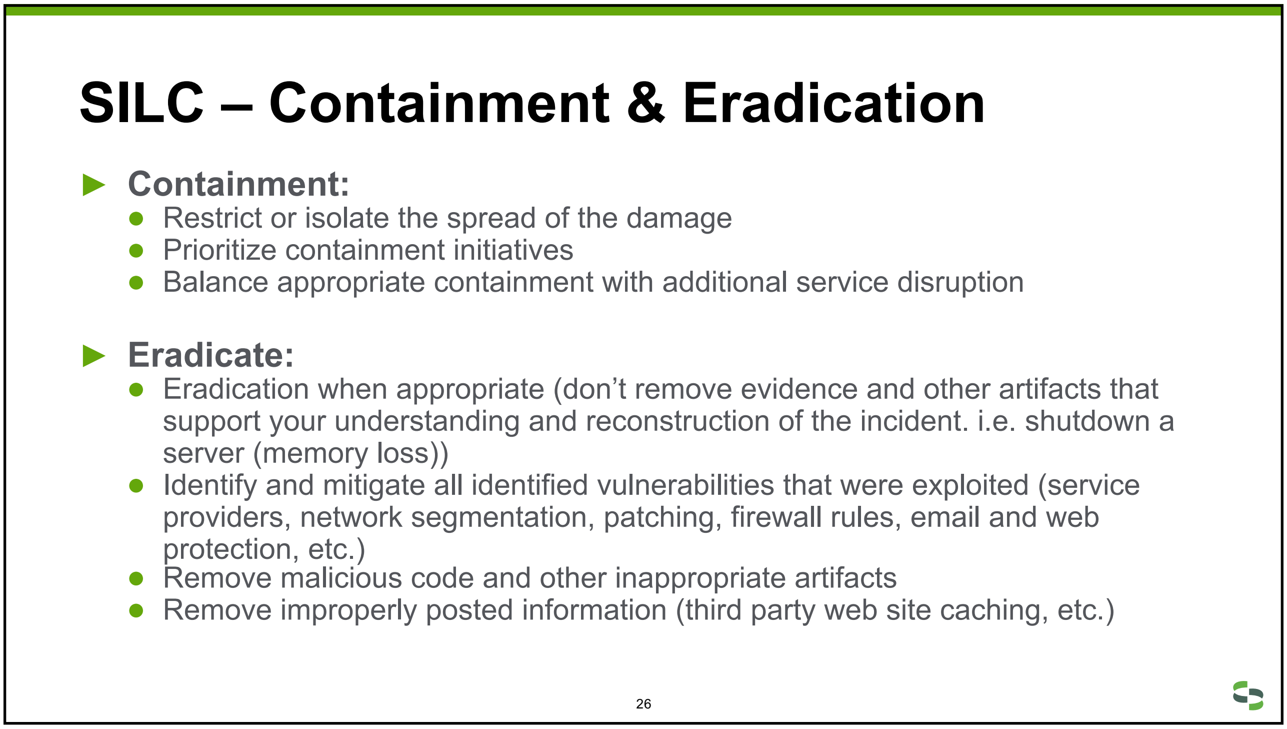


SILC – Detection and Analysis (Continued)

- Identify and document indicators of compromise (IOC's)
- Identify the commencement and duration of the incident
- Identify the location and scope of the incident - network, servers, etc.
- Determine the likelihood of misuse and damage as a result of the data compromised
- Summarize threat analysis results and report conclusion
- Retain and secure evidence and preserve the integrity of evidence for potential legal action
- Triage and communicate issues to appropriate management – (Ongoing)
- Finalize an incident report
- Notify law enforcement
- Communicate to affected third parties; regulators, appropriate media, customers, investors, business partners, individuals and other stakeholders. Don't be misleading
- Report incident to appropriate parties

25

25



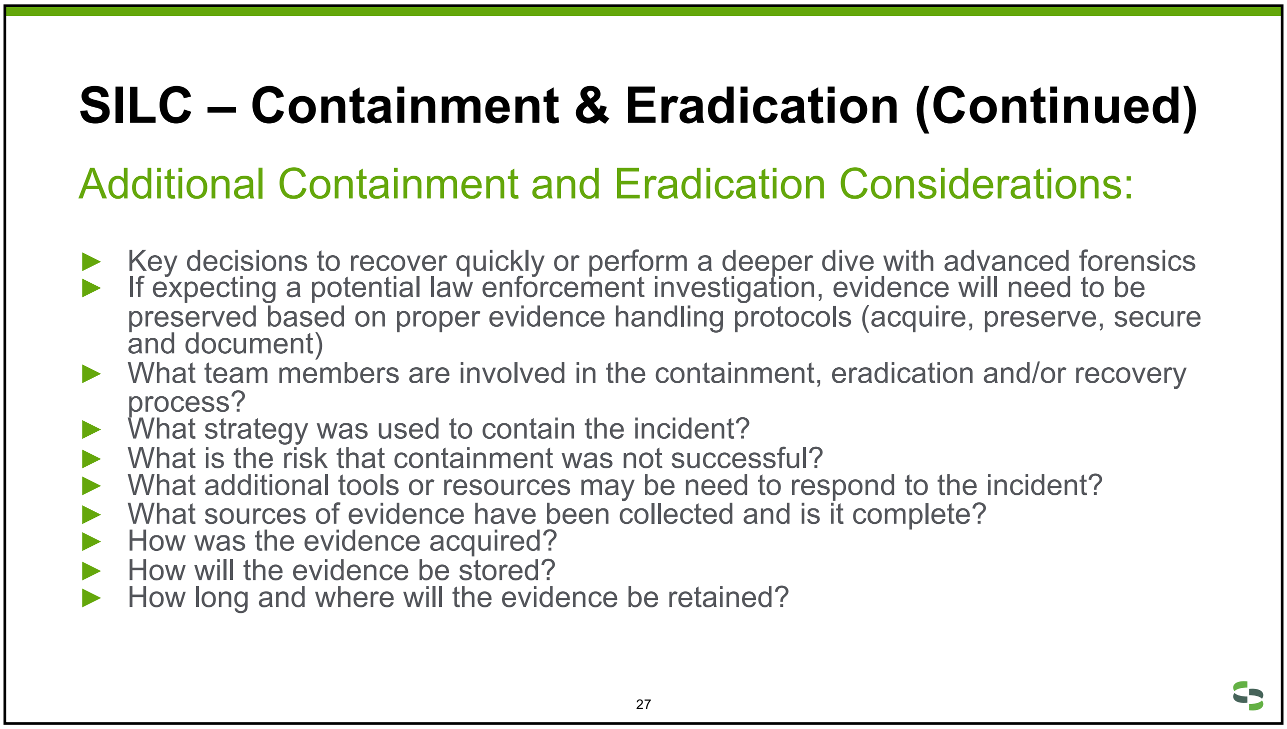
SILC – Containment & Eradication

- **Containment:**
  - Restrict or isolate the spread of the damage
  - Prioritize containment initiatives
  - Balance appropriate containment with additional service disruption

- **Eradicate:**
  - Eradication when appropriate (don't remove evidence and other artifacts that support your understanding and reconstruction of the incident. i.e. shutdown a server (memory loss))
  - Identify and mitigate all identified vulnerabilities that were exploited (service providers, network segmentation, patching, firewall rules, email and web protection, etc.)
  - Remove malicious code and other inappropriate artifacts
  - Remove improperly posted information (third party web site caching, etc.)

26

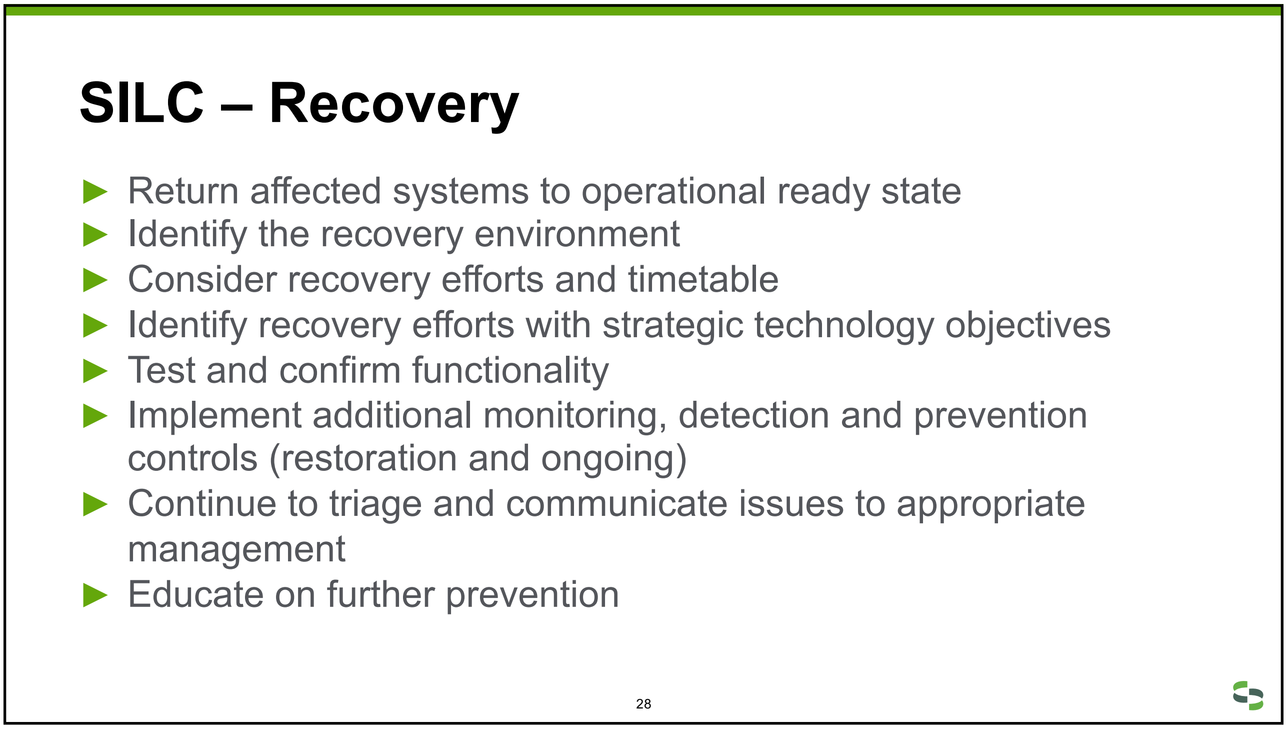
26



SILC – Containment & Eradication (Continued)

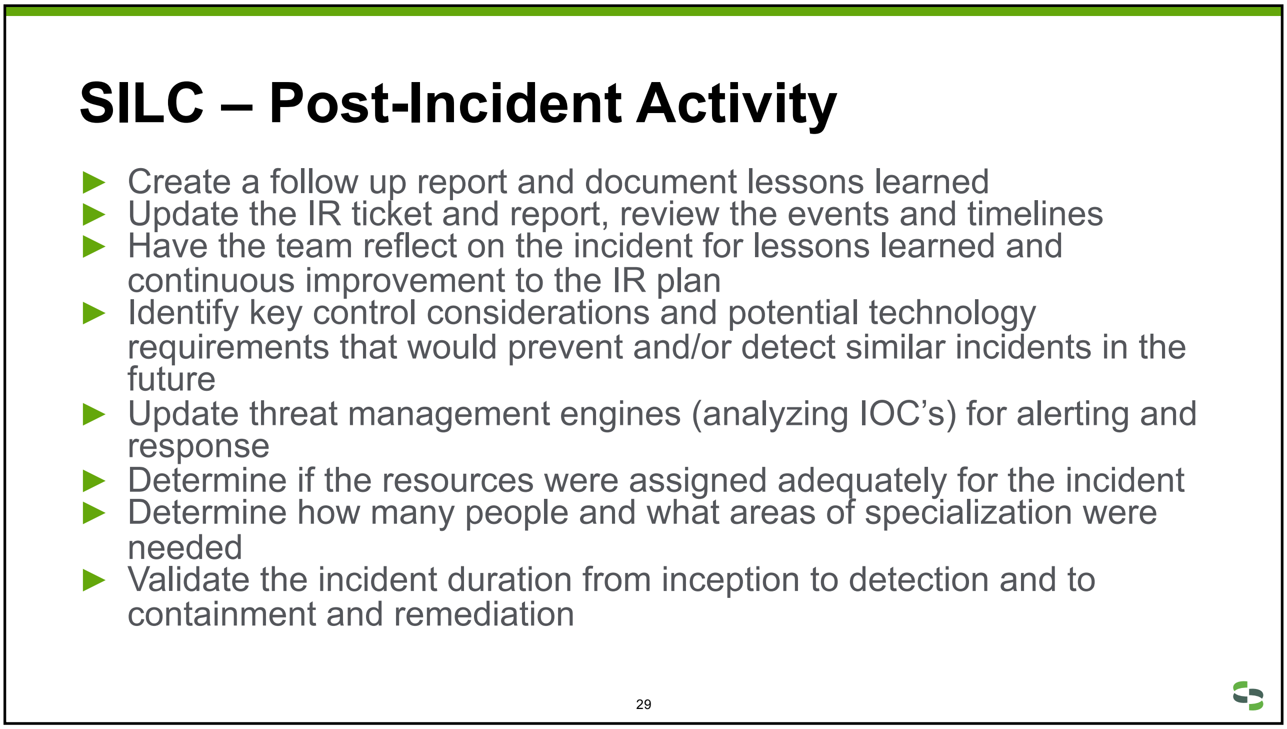
Additional Containment and Eradication Considerations:

- Key decisions to recover quickly or perform a deeper dive with advanced forensics
- If expecting a potential law enforcement investigation, evidence will need to be preserved based on proper evidence handling protocols (acquire, preserve, secure and document)
- What team members are involved in the containment, eradication and/or recovery process?
- What strategy was used to contain the incident?
- What is the risk that containment was not successful?
- What additional tools or resources may be need to respond to the incident?
- What sources of evidence have been collected and is it complete?
- How was the evidence acquired?
- How will the evidence be stored?
- How long and where will the evidence be retained?



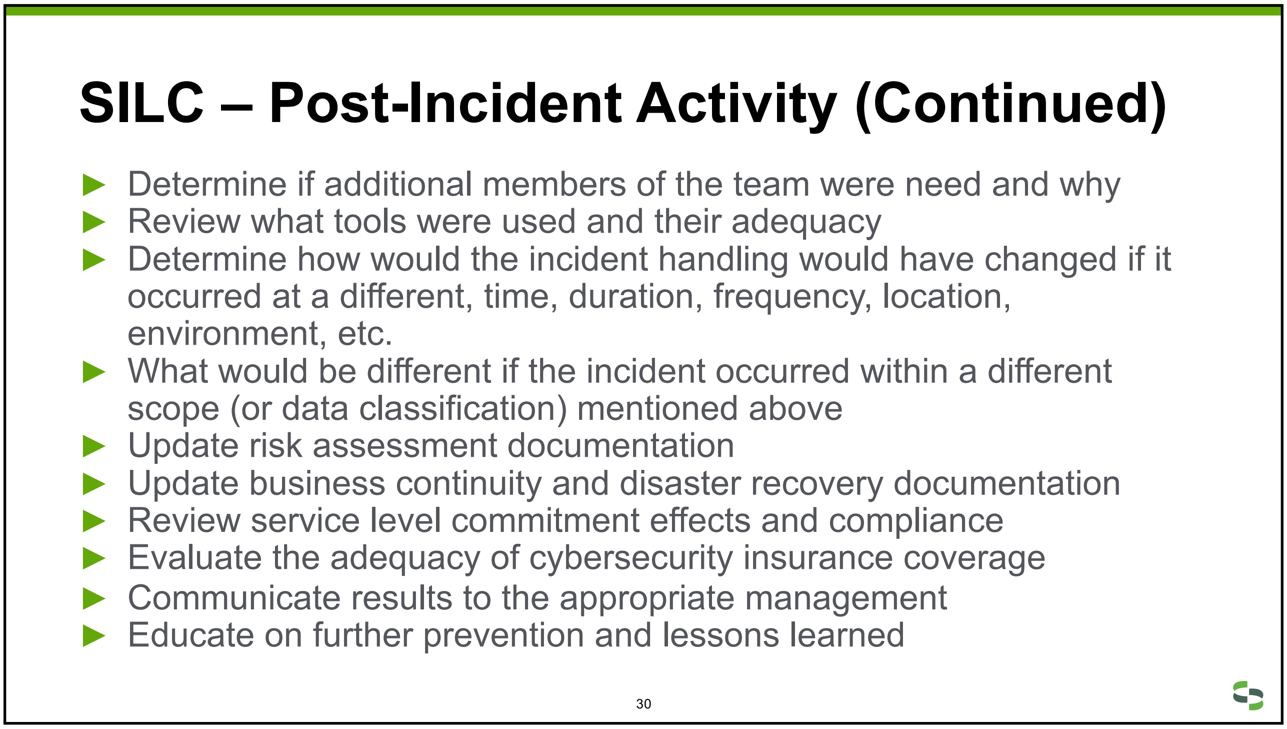
SILC – Recovery

- Return affected systems to operational ready state
- Identify the recovery environment
- Consider recovery efforts and timetable
- Identify recovery efforts with strategic technology objectives
- Test and confirm functionality
- Implement additional monitoring, detection and prevention controls (restoration and ongoing)
- Continue to triage and communicate issues to appropriate management
- Educate on further prevention



SILC – Post-Incident Activity

- Create a follow up report and document lessons learned
- Update the IR ticket and report, review the events and timelines
- Have the team reflect on the incident for lessons learned and continuous improvement to the IR plan
- Identify key control considerations and potential technology requirements that would prevent and/or detect similar incidents in the future
- Update threat management engines (analyzing IOC's) for alerting and response
- Determine if the resources were assigned adequately for the incident
- Determine how many people and what areas of specialization were needed
- Validate the incident duration from inception to detection and to containment and remediation



SILC – Post-Incident Activity (Continued)

- Determine if additional members of the team were need and why
- Review what tools were used and their adequacy
- Determine how would the incident handling would have changed if it occurred at a different, time, duration, frequency, location, environment, etc.
- What would be different if the incident occurred within a different scope (or data classification) mentioned above
- Update risk assessment documentation
- Update business continuity and disaster recovery documentation
- Review service level commitment effects and compliance
- Evaluate the adequacy of cybersecurity insurance coverage
- Communicate results to the appropriate management
- Educate on further prevention and lessons learned

Polling Question #4

When it comes to cybersecurity incident response communication, my organization:

1. Unfortunately had to report an incident that lead to a breach
2. Has had one or more incidents, but has not suffered a breach needing communication
3. Has never had an incident
4. Not sure

Cybersecurity Insurance

Cherry Bekaert LLP
Your Guide Forward

Cyber Insurance: Factors that Effect Coverage

- Adequate coverage for the incident (scope and limits)
- Risk assessments can be a valuable tool to assist
- Timing of coverage
- Type of policy (claims based, occurrence, retroactive coverage)
- Gap/buffer period coverage (Extended Reporting period)
- Change of ownership (tail policy, name additional assured)(optional extension period)
- How did the breach occur?
- Who is responsible for committing the breach?
- What type of information was stolen? (Personal (ePHI, PHI, PII), Confidential (1st and 3rd Party), Secrets, Classified, Source Code, Copyrighted, Proprietary, System, Financial

Typical / Endorsements Loss Coverages –Insured

- **Breach Response / Crisis Management:** Responds to a network or privacy breach including breach notification, public relations, forensic consultants and credit monitoring costs.
- **Privacy Breach Responses Costs:** Includes all reasonable legal, public relations, advertising, IT forensic, call center, credit monitoring, identity theft restoration and postage expenses incurred by the insured in response to a privacy breach.
- **Extortion Loss:** Responds to a threat by a third party to commit a network security or privacy breach.
- **Business Interruption / Extra Expense Loss:** Loss of income resulting from a network security breach or a network attack and extra expenses incurred to restore network to original condition.
- **Data Loss:** Cost to restore data destroyed or altered as a result of a network security breach. This is sometimes included in branch response.

Typical / Endorsements Loss Coverages – Insured (Continued)

- **Network Asset Protection (including Non-physical Business Interruption):** Coverage for all reasonable and necessary sums required to recover and/or replace data that is compromised, damaged, lost, erased or corrupted. Coverage also includes business interruption and extra expense coverage for income loss as a result of the total or partial interruption of the insured's computer system
- **Regulatory Defense & Penalties:** Coverage for defense costs and fines/penalties for violations of privacy regulations, including, but not limited to, HIPAA, Red Flags Rule, and the Hi-Tech Act.
- **Multimedia Insurance:** Coverage for both online and offline media. Including claims alleging copyright/trademark infringement, libel/slander, advertising, plagiarism, and personal injury.
- **Cyber Extortion:** Will pay extortion expenses and extortion monies as a direct result of a credible cyber extortion threat.

Typical / Endorsements Loss Coverages - Liability (Third Party)

- **Network Security & Privacy Insurance:** Covers third party claims arising out of a breach of the insured's Network Security or other private information. Includes coverage for both online and offline information, virus attacks, denial of service, and failure to prevent transmission of malicious code.
- **Network Security Liability:** Provides coverage for actions when you are legally liable for claims made against you for a Network Security Breach.
- **Privacy Liability:** Provides coverage for actions when you are legally liable for claims made against you for a Privacy Breach of Personally Identifiable Information, Personal Health Information or Non-Public Corporate Information.

Typical / Endorsements Loss Coverages - Liability (Third Party) (Continued)

- **Regulatory Coverage:** Provides coverage for actions/proceedings and fines/penalties against you by a regulatory agency resulting from a violation of a Privacy Law.
- **Website Media Content:** Provides coverage for actions that you are legally liable for claims made against you for content on your website.
- **Multimedia Insurance:** Coverage for both online and offline media, including claims alleging copyright/trademark infringement, libel/slander, advertising, plagiarism, and personal injury.
- **Third-Party Coverage:** Broad Coverage for data that is stored with a third party including, but not limited to, IT outsourcers and Independent Contractors.
- **Worldwide Coverage:** Claims can be brought outside of the U.S.

Coverage – Additional Topics & Considerations

- **Nation/state, terrorism, cyber terrorism, acts of God:** Coverage for income loss and interruption expenses as a result of the total or partial interruption of the insured’s computer system due to a cyber terrorism attack or act of God.
- **Payment Card Industry:** Data Security Standards endorsement available to qualified applicants. Provides $ sub-limit for fines & penalties levied by an acquiring bank and also includes $ for legal expenses.
- **Social Engineering:** Protection against damages sustained from social engineering crimes, could be a separate policy or an additional endorsement to a cyber policy.

Coverage – Additional Topics & Considerations (Continued)

Wire Transfer / Funds Transfer Fraud

Protection against unauthorized wire transfers or fund transfers. Could be part of a cyber policy or a crime policy.

Others

Financial Fraud, telecommunications fraud, phishing attack coverage.

Potential Key Exclusions / Sub-limits

Portable electronic device exclusion, intentional acts exclusion, negligent computer security exclusion, vicarious liability/vendors.

Polling Question #5

When it comes to cybersecurity insurance, my organization:

1. Has a comprehensive cybersecurity policy
2. Has a policy, but I am not sure of the completeness of coverage
3. Does NOT have a cybersecurity policy, but has other insurance protection (business interruption, crime, etc.)
4. Does not believe in insurance
5. Not sure of the insurance coverage

Key Takeaways

- Cyber Crimes are consistently occurring and the related costs are increasing
- Cyber attacks are becoming more and more sophisticated
- It's a Business Problem
- Stop focusing on "if" we get breached and focus on "when"
- Incident Response Procedures should be reviewed with all employees
- Understand the significance of Executive, Board Level and Audit Committee involvement for Information Security Governance
- Insist on a reasonable level of transparency to the organizations security incident response program including risk management and incident response testing methodology, measurements and metrics
- Stay involved and include information security / privacy governance high level strategic initiatives and performance metrics as regularly reviewed artifacts

Resources

- AICPA Cyber Security Resource Center
- Cyber Risk Management Reporting Framework
- Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program
- https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

How Can I Help?

Steven J. Ursillo, Jr.
National Leader, Information Assurance & Cybersecurity

401.250.5605
sursillo@cbh.com
@StevenUrsilloJr