GLOBAL cyber risk LLC

THE COUNCIL

The Council of Insurance Agents & Brokers

CIAB: The Council Academy

Countering Cyber Attacks: What Good Incident Response Looks Like

Jody R. Westby

CEO, Global Cyber Risk LLC

July 21, 2021

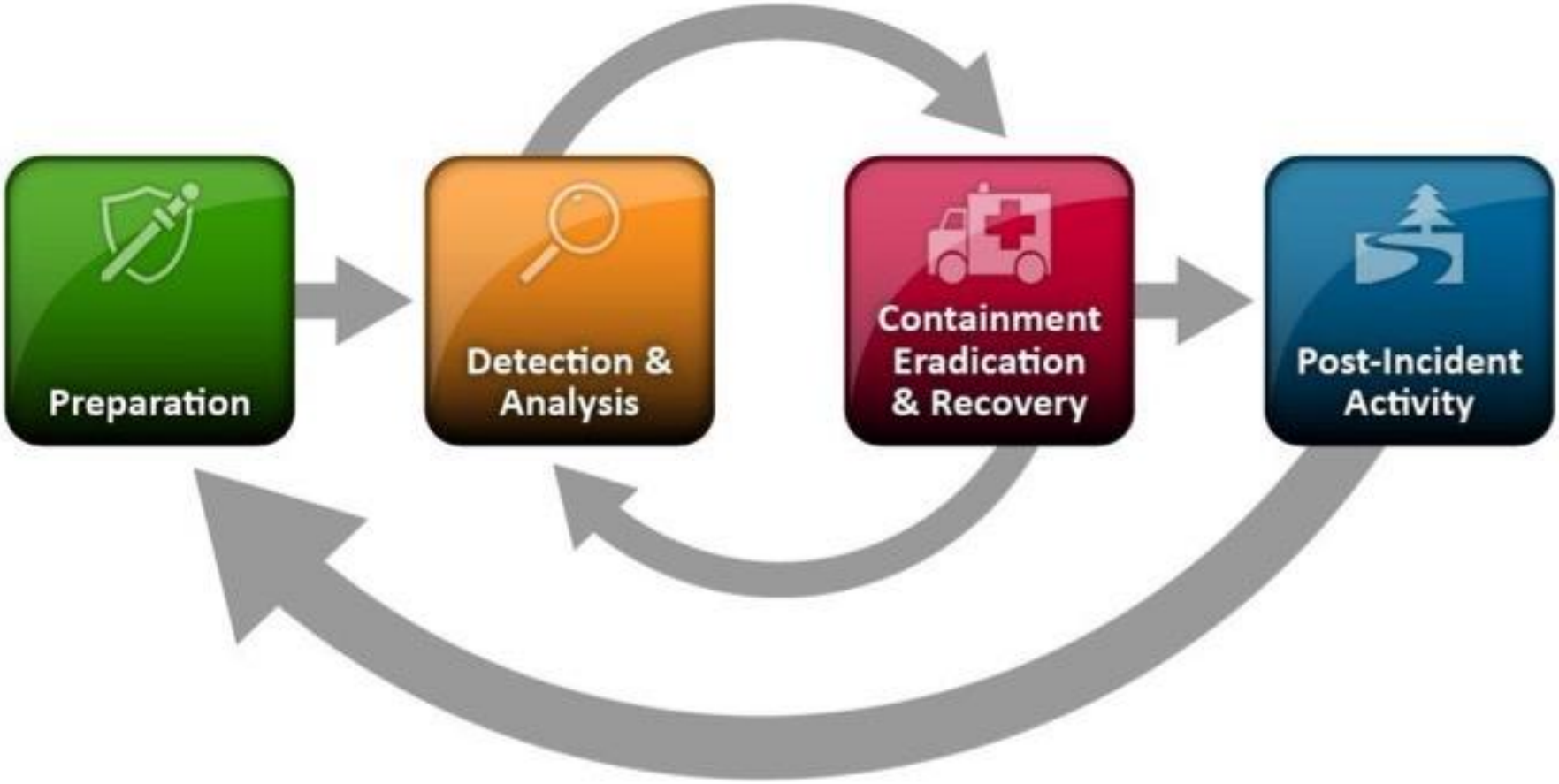
Council Academy: Exploring the Cyber Risk Environment

- 7/20/21 The Current Cyber Threat Environment & Actions to Take
- 7/21/21 Countering Cyber Attacks: What Good Incident Response Looks Like
- 7/27/21 Managing Cyber Risks Associated With The “New Work”
- 7/28/21 Cyber Compliance: Here Come The Regulators And Lawsuits
- 7/29/21 Director & Officer Liability: The Role of Cyber Governance

Importance of Incident Response Planning

- One of the most important activities of a cybersecurity program – and one of the most neglected
- Incident response is an enterprise issue that requires the participation of stakeholders across the organization
- Highly sophisticated threat environment – all data has its market and price
- Multidisciplinary Process (Legal, Business Units, IT, Security, PR, HR, Risk, Finance, Compliance, Sr Management & Board)
- Should adhere to incident response best practices and standards
- External Parties on Team: Forensic investigators, malware experts, outside counsel, crisis communications, notification assistance, credit bureaus, remediation teams
- External Parties Not on Team: law enforcement, communication providers, state attorneys general, FTC & consumer protection agencies, media & social media, regulators, investors
- Success depends upon culture of organization, cross-org participation, testing of plan and linkage with BC/DR planning

Incident Response Realities – Not a Linear Process



NIST 800-61 Graphic

Incident Response – Key to Staying in Business

- Incident Response Plan
- Incident Response Policy
- Incident Response Procedures
- Incident Response Training
- Incident Response Scenarios & Testing
- Incident Response Review Process
- CSIRT Team
- External Entity Points of Contact – Roster of contact info
- Linkage to BC/DR
- Incident Response Checklist

Incident Response Policy Elements

- Statement of management commitment
- Purpose and objectives of the policy
- Scope of policy (who/what it applies to & circumstances)
- Organizational structure, definition of roles/responsibilities, levels of authority
- Definition of cyber incident and related terms
- Handoff / escalation points in incident management process
- Prioritization or severity ratings of incidents
- Reporting requirements
- Requirements & guidelines for external communications & info sharing
- Performance measures
- Reporting and contact forms

Incident Response Plan

- Mission
- Strategies and goals
- Senior management approval and governance process
- Organizational approach to incident response
- Preparation for a major cyber incident (documentation, configurations)
- Identification of the incident
- Incident analysis, linkage with inventories (apps and data)
- Event management across organization
- Communications management (internal and external)
- Response to and containment of the threat, including documentation
- Eradication of the threat and identification of remediation
- Continuance of operations and recovery from the breach
- Analysis of lessons learned
- Scenario planning and testing
- Training and ongoing awareness
- Plan reviews and maintenance

IRPs & Business Continuity & Disaster Recovery

- Linkage between IRP & business continuity and disaster recovery (BC/DR)
- Often overlooked, underfunded, two areas most immature in development
- Response and recovery can be chaotic without tested IRP and BC/DR plan
- DR is more than restoring a backup file; it involves recovering operations
- Best practices and standards for IRP and BC/DR:
  - NIST 800-61: Incident Response
  - NIST 800-184: Cybersecurity Event Recovery
  - NIST 800-86: Integrating Forensics Techniques into Incident Response
  - NIST 800-34: Contingency Planning
  - ISO 27035: Incident Response
  - ISO 27031: IT Business Continuity
  - ISO 24762: IT Disaster Recovery

Planning for Disaster Recovery

- Begins in enterprise security program with
  - Business Impact Assessment and business continuity requirements (RTO/RPO)
  - Asset inventories (applications, data)
  - Data classification & risk categorization (apps)
  - System configuration and controls
  - Policies and procedures
  - Monitoring & logging
  - Incident response
  - Backup/recovery plans
- DR requires a budget, specialized expertise, and close working relationships with IT, cybersecurity, business units, and vendors
- Written Disaster Recovery Plan with annual testing

Elements of Disaster Recovery Plan

- Authority – Personnel who can activate the plan
- Recovery team – Identification of DR team members and full contact info
- System recovery details and procedures – documented system details on restoration (backup servers, failover site, RTO/RPO, system architecture diagrams, etc.)
- Crisis communications plan, external and internal, including escalation)
- Offsite storage details
- Operational workarounds if system can't be restored within RTO
- Facility recovery details (communication circuit details, access, alternate location)
- Infrastructure, hardware & software (ID management system, recovery network, staging to validate the recovery)
- Vendors necessary for recovery & Service Level Agreements
- Reporting and escalation requirements
- Post-mortem analysis
- Metrics to be tracked

Summary

- Environment more sophisticated than ever: 1 in 4 companies can expect nation state sponsored attack
- Current remote working environment is a boon for cybercriminals
- Cybercriminals will take advantage of every gap and deficiency in your organization's cybersecurity program
- Three areas that generally have lowest maturity scores:
  - Asset inventories (especially applications and data)
  - Incident Response Planning
  - Business Continuity & Disaster Recovery
- Companies without developed and tested IRPs and BC/DR are high risk for insurance companies

CIAB Resources from Leader's Edge

- Ripple Effects of Cyber Attacks, June 1, 2021, https://www.leadersedge.com/p-c/ripple-effects-of-cyber-attacks
- Ransomware Continues to Lead Cyber Attacks, Mar. 26, 2021, https://www.leadersedge.com/p-c/ransomware-continues-to-lead-cyber-attacks
- Put Incident Response Front and Center, Feb. 28, 2021, https://www.leadersedge.com/p-c/put-incident-response-front-and-center
- Forgiveness After An Attack, Jan. 14, 2021, https://www.leadersedge.com/p-c/forgiveness-after-an-attack
- 2020 vs. 2021, Nov. 30, 2020, https://www.leadersedge.com/p-c/2020-vs-2021
- You Thought COVID-19 Was Bad, Sept. 24, 2020, https://www.leadersedge.com/p-c/you-thought-covid-19-was-bad
- 20 for 2020, Jan. 14, 2020, https://www.leadersedge.com/p-c/pay-now-or-pay-later
- Ransomware: It Doesn't Have to be This Hard, Nov. 21, 2019, https://www.leadersedge.com/p-c/ransomwareit-doesnt-have-to-be-this-hard
- Pay Now or Pay Later, July 11, 2019, https://www.leadersedge.com/p-c/pay-now-or-pay-later

Thank You!

Jody R. Westby, Esq.

westby@globalcyberrisk.com

202.255.2700