LDR553: **Cyber Incident Management**

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Categorize and scope incidents correctly and the resulting incident management team's objectives
- Design, draft, proof, release and control all communications when managing a serious incident
- Manage a team under extreme pressure and to recognize the natural human responses that will emerge and what they mean
- Lead the team, win the confidence of the execs and exceed the expectations of everyone involved
- Calculate, coordinate, and execute both system and data counter compromise activities
- Strategize and respond to ransomware incidents including how to develop exercises and training around these devastating attacks
- Structure, manage, and deliver briefings to the team, execs and senior leadership or the board
- Organize the transition from active incident to business as usual and how to execute that plan
- Prepare, setup and run cyber incident management exercises

"Great insights, examples and relevant tools. I applied the third-party incident tool within minutes to an ongoing third-party incident. So I can't dream of a more relevant and useful course than this."

—Jonas Roos Christense,
Copenhagen Airports

Open in Case of Emergency

While you can't predict when a major cyber incident will hit your organization, you can control how ready you are to face it. In the aftermath, when incident response teams are engrossed in unraveling the attacker's moves within your networks, they often find themselves overwhelmed. This is where your incident management team steps in, taking charge of managing findings, communications, regulatory notifications, and remediation. With a multitude of tasks and challenges on their plate, many are unseasoned and unprepared for the magnitude of responsibilities.

This course equips you to not just be a member of the incident management team but a leader or incident commander. It ensures a comprehensive understanding of the immediate, short, and medium-term issues an organization might encounter. Beyond familiarizing yourself with the terminology, you'll grasp preparatory actions at different stages to stay ahead of the situation. LDR553 is designed for efficient management of diverse incidents, with a primary focus on cyber, yet its methodology, concepts, and guidance are applicable to various regular major and critical incidents.

What Is Cyber Incident Management

Cyber Incident Management (IM) sits above Incident Response (IR) and is tasked to manage incidents that get too big for the Security Operations Center (SOC) and IR. These tend to be the more impactful or larger incidents that IR is not scaled to handle as it requires significant liaison with internal and external partners to coordinate the investigation, forensics, planning, recovery, remediation, and to brief the corporate comms, C-level staff and board as needed. Less technical and more business focused, the IM team will take the output from IR and relay it to the necessary teams as they coordinate wider investigations and hardening, hygiene and impact assessment as they plan towards recovery. A strong IR lead may fulfill the IM role, but during critical incidents IRs are often shoulder deep in malware, systems, logs and images to process to the point where all technically capable IR staff are kept focused on technical tasks. IMs are more business focused and IR is more technically focused.

Business Takeaways

- Cultivate a workforce adept at leading or contributing to cyber incident management teams
- Streamline incident management processes for quicker resolutions
- Identify and bridge gaps in security incident plans and response strategies
- Elevate the performance of security incident teams to meet evolving challenges
- Strategically plan and navigate through high-stakes attacks, including email compromise and ransomware, fostering a resilient response frameworks
- Promote seamless collaboration between technical and non-technical teams during incident response for a more integrated approach
- Instill a culture of continuous improvement, leveraging lessons learned from incidents to refine future response strategies
- Proactively integrate threat intelligence to anticipate and mitigate potential threats before escalation
- Provide guidance on regulatory compliance and have an awareness of legal considerations, ensuring incident responses align with relevant laws and standards

Section Descriptions

SECTION 1: Understanding and Communicating About the Incident

In Section 1 we will focus on understanding the incident, gathering information from different groups and standardizing the language. To assist in this, we will remind ourselves of some of the common terms to optimize communications. From there we will define what the Incident Management (IM) group will seek to achieve, so we can state and focus on our objectives. This is important as retaining focus can be hard when it gets super busy.

TOPICS: Initial Information Gathering; Defining Your Objectives; Who's on Our Team; Building Our Communications Plan

SECTION 2: Scoping the Damage, Planning the Remediation, and Executing the Plan

After reviewing Section 1, we conclude the communications topic by exploring interactions with attackers. While ransom payment may not be in your plans, engaging in dialogue with attackers can buy time to address issues they've uncovered or prevent potential leaks. Acknowledging the controversy and the diverse beliefs surrounding this approach, it's essential to understand the available options for the organization. The course will delve into how attacker dialogue may occur and the factors influencing response options and processes.

TOPICS: Talking To or Working With the Attackers; Tracking the Incident, Tasks, People, and Progress; Remediation of Network and Data Damage; Root-Cause Analysis Methods and Outcomes; Reporting and Documenting the Case; Planning the Closure of the Incident

SECTION 3: Training, Leveraging Cyber Threat Intelligence, and Bug Bounties

In this session, our focus is a deep dive into the training of Incident Response (IR) and Incident Management (IM), not only within our own teams but extending to the wider organization. We'll explore the imperative need for training, considering the type of training required based on organizational maturity. Engaging in hands-on labs, including an exercise exemplifying the onboarding of non-IR personnel to cyber incidents, we aim to provide practical insights.

TOPICS: Developing the Wider Team; Developing the SOC/IR/IM Team; Leveraging Cyber Threat Intelligence; Third-Party Supply-Chain Compromise

SECTION 4: Cloud Incidents, Business Email Compromise, Credential Theft Attacks, and Incident Metrics

In response to the escalating complexity of incidents, our focus turns to visualizing key facts, with timelines emerging as a powerful tool. However, we stress the importance of careful scoping, as a poorly conceived timeline, not tailored to the target audience, risks confusion and fails to convey the intended message. Our exploration delves into the art of scoping timelines, exploring various styles, and drawing insights from case studies that exemplify different perspectives on the same incident.

TOPICS: Timelines for Visualization; Defining Cloud Attacks; Credential Theft Attacks; Business Email Compromise; Cloud Asset Attack; Cloud Management Console Attacks

SECTION 5: AI for Incidents, Attacker Extortion, Ransomware, and Capstone Exercise

In this last session we will look at some of the bigger issues facing the organizations. We start by looking at how to improve the team by working with others, linking to other teams and groups. ChatGPT is now a common word in the press and is used by tech and non-tech people alike. With organizations seeming to rush to invest and claim they are using AI, we will take some time to understand what they are talking about. Ransomware is headline news almost every day. It's the one thing that keeps more CISOs and Boards awake each night, so we will take a deep look at its history and where it is now in terms of development. We will look at the stages of a ransomware compromise and what detections points were missed as the attackers moved from initial access to the final closing blow of encryption. Finally, we will look at the need to investigate the network compromise in parallel to the remediation so the organization can repel a further attack that may come depending upon their decisions to pay/no-pay.

TOPICS: Improving IR/IM; Leveraging IA for IM; Ransomware; Summary and Review of the Sessions; Capstone Exercise

Who Should Attend

- Security managers
  - Newly appointed information security officers who will be leading incidents
  - Recently promoted security leaders who want to understand incident management better
- Security professionals
  - Technically skilled security staff who have recently been given incident commander responsibilities
  - Team leads with the responsibility to support cyber incidents and whom may need to remediate systems
- Managers
  - Managers who want to understand how to manage technical people during an incident
  - Leaders who need an understanding of cyber incidents from a management perspective
- Legal/HR/PR staff
  - Staff who are new to cyber incident management but may be called upon to provide critical support in tense situations and who want to understand better what may be expected from them

NICE Framework Work Roles

- Knowledge Manager (OM-KMG-001)
- Cyber Legal Advisor (OV-LGA-001)
- Privacy Officer/Privacy Compliance Manager (OV-LGA-002)
- Information Systems Security Manager (OV-MGT-001)
- Communications Security (COMSEC) Manager (OV-MGT-002)
- Cyber Policy and Strategy Planner (OV-SPP-002)
- Executive Cyber Leadership (OV-EXL-001)

"It was awesome to have the opportunity to apply existing and newly learned skills to the labs. It is obvious that a significant amount of time had been invested in them."

—Andrew Kempster, **DXC Technologies**

"The labs were perfect. Today's capstone exercise brilliantly brought together the elements we had learned, adopting tools to help deliver the products required. And while its goal was to deliver the final exercise of the course, it really has sparked the imagination of everything we can do with what we have learned. Excellent work."

—Lee T., **Law Enforcement**