MGT553: **Cyber Incident Management**

2 Day Course	12 CPEs	Laptop Not Needed

You Will Be Able To

- Perform a complete risk assessment
- Inventory an organization's most critical information assets
- Assign a data owner and custodian to an information asset
- Assign classification values to critical information assets
- Prioritize risk remediation efforts as a result of performing a risk assessment
- Evaluate risk management models for use in their own organization

Skills Learned

- How to make sense of different incident response frameworks
- Understanding the importance of scoping incidents correctly
- The ability to define the incident management team s objectives
- Recognition of the importance of managing a team under extreme pressure
- Awareness of human responses to facing catastrophically impactful urgent changes
- How to structure, manage, and deliver briefings to upper management and the board
- Planning and controling communications when managing a serious incident
- Communicating with attackers and the pros and cons thereof
- Where and how to track the incident
- Planning, coordinating, and executing counter compromise activities
- Understanidng types and contents of incident resports both during and post closure
- Steps on how to close the incident and return to business as usual

Open in Case of Emergency

You can't predict or pick when your organization will face a major cyber incident, but you can choose how prepared you are you when you face it. While there are broad technical aspects to cyber incidents there is also a myriad of other activities that generally falls to executives, managers, legal, press, and human relations staff. These include communicating both internally and externally, considering the battle rhythm and a look at methodologies for tracking information gathered and released to the public.

This course empowers you to become an effective incident management team member or leader; ensuring you fully understand the different issues facing incident commanders in the immediate, short and medium term. As well as becoming comfortable with terminology, you will understand what preparatory work you can undertake at different stages to help you get ahead of the situation. MGT553 was developed to ensure efficient management of a diverse range of incidents with a focus on cyber; however, the methodology, concepts and guidance will apply to many regular major and critical incidents.

This course will help your organization:

- Develop staff that know how to lead or contribute to a cyber incident management team
- Manage your incidents more effectively and thus resolve them quicker
- Understand the gaps in your security incident plans and response strategies
- Create higher performing security teams

Author Statement

"Of my 28 years in cyber security, I ve spent over 11 of them in incident response and later incident management. During that time, I ve seen a wide range of approaches to handling cyber incidents, some good and others less so. One common issue was that most people on the Incident team had never been part of a major incident and thus they lacked confidence, forward planning, and were easily stunned when the incident took a turn they had not predicted.

"This course is designed to demystify incident management, to provide attendees with a framework to not only deal with the matters at hand, but also to plan for the subsequent phases, so they are technically ready and mentally prepared. Cyber incidents, such as ransomware, can be devastating, not only to the networks, but also the team charged with investigating, mitigating, reporting and remediating the damage. In addition to the core incident management aspects, we cover the mental health of the team, the operational tempo and how to spot people suffering under pressure. I believe that this course, enriched with the anecdotes of the SANS incident response instructors own toe-curling incidents will prepare your team for anything attackers and bots throw at them. When you are prepared and ready, you can respond better, faster and get control of the situation quicker facilitating a rapid return to business as usual."

—Steve Armstrong

Section Descriptions

SECTION 1: Building Your Security Program

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.

With the objectives defined we then turn to initial tasks and delegating those to the team; this is to give us some breathing space to plan the next steps. Our initial tasking output will be based on one of the core tools in the Cyber Incident Response Tool Kit (CIMTK) the "IM Starting Grid". This detailed list of Yes/No questions outputs a list of core IM tasks that aide rapid response. By identifying these tasks early, concurrent activity can be initiated for both support teams (Incident Response (IR), Information Technology (IT), Human Resources (HR), Legal etc.) and the IM team. As IM is totally dependent upon a good team, we will assess team composition and what different groups need to contribute to the mission. Finally, we dig into communication and how to interact with different stakeholders. Tracking activity, tasks, and communications is a big theme throughout this course.

TOPICS: Initial Information Gathering; Defining Your Objectives; Building and Managing our Team; Building our Communications Plan; Tracking the Message

SECTION 2: Technical Security Architecture

After reviewing Section 1, we conclude the communications topic by looking at communications with the attackers. While you may have no plans to pay any ransom, by entering into dialogue with attackers, you can gain time to fix issues the attackers have uncovered, discovered, or could leak. While controversial and possibly contrary to your own beliefs, it is important to understand options are available to the organization. We will cover how attacker dialogue may occur and what factors will influence the response options and process.

We will look at what incident information should be tracked and options or ways to achieve that. We review both commonly available products as well as bespoke options (including those for on prem and cloud hosted solutions).

Getting into the remediation of the network and data damage, we have a large section on categorizing the damage the attackers have inflicted and then mapping to the necessitated remediation work that will need to be prioritized and tracked to ensure that all possible vulnerabilities have been removed. A much-overlooked aspect, we discuss secrets that are included in stolen data and systems and consider how this might affect our future operations.

In the reporting and documenting of the case, we review some of the outputs from the IM process. While a solid IR report is always useful, we will cover what aspects could be added to expand it to cover IM. This is important as the direction of the Incident Response is often mandated by Incident Management, so linking the two into one report makes for a more structured reading while outsourcing some aspects to others.

In planning the closure of the incident, we discover what remediation and vulnerability closure tasks should be moved to non-incident mainstream projects and what reflection meetings should be held to ensure root causes are captured and lessons are identified and tracked.

In developing the wider team, we examine some of the training you can give those outside of the regular IR and IM staff to improve their awareness of issues and to help smooth future incidents. To assist this, we explore tabletop exercises and how you make them. We then both build one as a lab and close out the section by running one.

TOPICS: Talking to or Working with the Attackers; Tracking the Incident, Tasks, People and Progress; Remediation of Network and Data Damage; Reporting and Documenting the Case; Planning the Closure of the Incident; Developing the Wider Team; Summary and Closure

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 responsibility to support cyber incidents and who 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

"Brilliant insight. Excellent content. An absolute must course for anyone dealing with incident management."

—Gary Smith

"All was very relevant and well delivered. All extremely useful information."

—Peter Leonhardt