Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response

by Leighton R. Johnson III

Reviewed by A. Krista Kivisild, CISA, CA, CPA, who has had a diverse career in audit while working in government, private companies and public organizations. Kivisild has experience in IT audit, governance, compliance/regulatory auditing, value-for-money auditing and operational auditing. She has served as a volunteer instructor, training not-for-profit boards on board governance concepts; has worked with the Alberta (Canada) Government Board Development Program; has served as the membership director and CISA director for the ISACA Winnipeg (Manitoba, Canada) Chapter; and is a member of the ISACA Publications Subcommittee. Her areas of expertise are cybersecurity, governance, and incident command system/supervisory control and data acquisition systems.

Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response outlines the stages of incident response to ensure that companies are properly prepared to deal with inevitable incidents. The book addresses how to prosecute malicious insiders or external hackers and describes all of the incident response stages that should be followed and completed. The book’s practical approach provides readers with different methods for incident response used in the industry and enables further understanding of the technical and personal skills needed to handle incidents. Johnson also describes many of the incident and forensic tools available today and how they can be used.

The book establishes the importance of having incident response policies and procedures in place so that enterprises can organize and plan strategically with good governance and legal considerations in mind. Setting up a good incident response and forensic team takes a lot of work. While this book provides a good foundation, the legal requirements outlined in the book are not applicable globally. The book also does not discuss the audit function with respect to incident response.

Computer Incident Response and Forensics Team Management covers the management of forensics evidence and chain of custody, which can be used to prepare for incidents that may involve law enforcement. Clarifying roles, responsibilities and reporting relationships for IT staff can help the enterprise better focus on the successful resolution of an incident or investigation, the reporting of resolutions, and the analysis of root causes to best determine the corporate-level course of action, helping to bolster the security of the organization and its information. This clarification leads to individuals better understanding their responsibilities and the actions they need to take when preparing and identifying incidents, which can help them act quickly and take control if an incident occurs.

Effective incident management can protect an enterprise’s critical computing resources and its reputation. Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response is a valuable resource to help organizations better prepare for and respond to computer incidents and attacks.

EDITOR’S NOTE

Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response is available from the ISACA® Bookstore. For information, visit www.isaca.org/bookstore, email bookstore@isaca.org or telephone +1.847.660.5650.