Cis 417 week 9 discussion 1 term paper

Business, Company

Need for an incident response team

Information in organizations is constantly under threat from both internal and external sources. Technology is rapidly changing creating loopholes that attackers may exploit. An organization’s security policy cannot be considered complete until measures are put in place to provide for incident handling and disaster recovery. An incident response team, is a group of well-trained individuals, whose purpose is to correctly handle incidents so that they may be contained and also provide for disaster recovery mechanisms. An incident response team provides the organization with the ability to deal with both potential and real security incidents.

The incident response team and their roles

Manager

The manager or senior level management is responsible for decision making. It is also essential to have a manager on board so as to provide support and co-ordinate the activities of the team.

Information security officer

The role of the information security officer or department is assessing the levels of risk or damages and providing for recovery options.

Human resource manager

The human resource manager is important in handling incidents relating to employees. The manager provides advice on how to best handle employees. This mostly occurs after investigations have been done.

Public relations officer

He or she is charged with the task of ensuring a company's public image, is maintained in case of an incident. In instances where it is mandatory to provide information to the public, he or she advises management of the best message to be portrayed.

Auditor

An auditor is responsible for putting a monetary value to the extent of damage caused by an incident. This is essential for insurance companies and situations where a company needs to press charges.

Security

These are individuals responsible with the physical security of the company. Security is essential to assess the extent of physical damage and carry out investigations.

References

Eugene, S., & Russell, S. (2001). Que. Incident Response. A Strategic Guide to Handling System and Network Security Breaches. Retrieved June 3rd from Google Books.

Kenneth, R., Van, W., & Richard, F. (2001). O'Reilly. Incident Response. O'Reilly Series Internet Computer Security. Retrieved June 3rd from Google Books.

S. Rao, V. (2008). John Wiley & Sons. Corporate Management, Governance, and Ethics Best Practices. Retrieved June 3rd from Google Books.

Julie, L., & Brian, M. (2004). Addison-Wesley Professional. The Effective Incident Response Team. Retrieved June 3rd from Google Books.