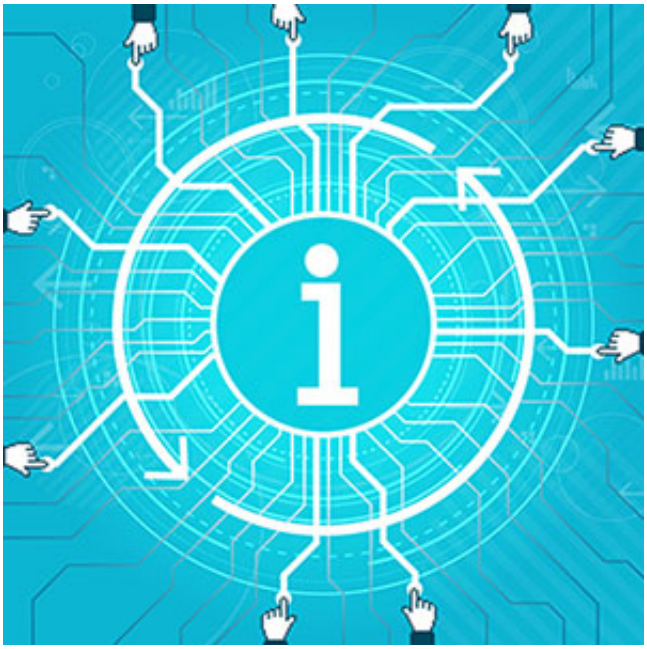
Sharing threat information before, during, and after a cyber-attack

November 11 2014, by Evelyn Brown



Credit: idspopd/Fotolia.com

Time is not your friend when your information systems are under cyber attack, but sharing threat information before, during, and after an attack with a trusted group of peers can help. Not only does it alert the other members of your community to a potential attack, it can provide critical actionable information to speed and bolster your own defenses. Participating in a formal information sharing group can greatly enhance an organization's cybersecurity capabilities.

But for all the potential benefits, sharing operational information outside an organization presents a unique set of challenges. To help, the National Institute of Standards and Technology (NIST) has prepared a Guide to Cyber Threat Information Sharing that provides organizations with the key practices they need to consider when planning, implementing and maintaining information sharing relationships. NIST is requesting comments on the draft document by November 28, 2014.

An organization that has faced an attack has valuable information to share with others. "By sharing cyber threat information, organizations can gain valuable insights about their adversaries," says lead author Christopher Johnson. "They can learn the types of systems and information being targeted, the techniques used to gain access and indicators of compromise. Organizations can use this information to prioritize defensive strategies including patching vulnerabilities, implementing configuration changes and enhancing monitoring capabilities."

Information sharing within business sectors is particularly advantageous because the organizations often face similar threats.

The NIST publication presents a deeper treatment of the information-sharing concepts presented in Section 4 of the Computer Security Incident Handling Guide, Revision 2. The guidance also references the Framework for Improving Critical Infrastructure Cybersecurity's Framework Core, which is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors.

The guide examines the benefits and challenges of coordinating and sharing, presents the strengths and weaknesses of a variety of information sharing models, explores the importance of trust, and addresses specific data handling considerations.

Appendix A provides a collection of scenarios that demonstrate the value of information sharing by describing real-world applications of threat intelligence sharing and coordinated incident response. These include an email phishing attack on people who attended a conference and how an investigation by credit card companies revealed that a retailer was unknowingly under attack.

More information: DRAFT Guide to Cyber Threat Information Sharing: csrc.nist.gov/publications/dra … /sp800_150_draft.pdf

Provided by National Institute of Standards and Technology