



Volume 7, Issue 9 – September 29, 2015

Managing cyber security risk

Highlights

- Agency leaders ultimately own their agency's cyber security risks.
- MN.IT Services helps agencies manage cyber security risk.
- Employees are targets for hackers, as employee computers are often gateways into other systems and data.

Hardly a day goes by when we do not hear about another large data breach. Many organizations, such as Target, Home Depot, Anthem, and even Harvard University, have been hacked. Advanced cyber-attacks are becoming more sophisticated and more common. These attacks test the limits of any organization's existing controls.

The cyber threat is enormous for governments. Governments collect and store vast amounts of sensitive data, which is valuable to hackers. Much of that data is now stored electronically, rather than on paper, which increases the risk. These factors have forced the state to develop stronger and better cyber strategies.

Three groups have responsibility for cyber security within the state. They are MN.IT Services, agency leaders, and all state employees.

MN.IT Services operates twelve distinct services as part of its Enterprise Security Program. Most focus on *proactive risk management*, hoping to prevent security incidents from happening. Examples of proactive services include policies and standards, security awareness training, and vulnerability scanning of computers.

MN.IT also has advanced monitoring and other security services designed to maintain *situational awareness* across state IT networks. MN.IT security professionals use state of the art monitoring tools to analyze millions of events in MN.IT's Security Operations Center each day, searching for potential incidents.

Finally, MN.IT has security services to help agencies *respond and recover* from incidents, which are an unfortunate reality in today's interconnected world.

Managing cyber security risk is a joint effort between MN.IT Services and agencies. Agency leaders are the ultimate owners of cyber security risk. Agency leaders must understand what MN.IT Services does to decrease cyber risk. They also must realize, however, that decisions they make about the design, implementation, and monitoring of their agency's systems affects those systems' risk posture.

Ultimately, though, cyber security is everybody's business. Compromised employee computers often serve as an internal launch point to attack other more lucrative systems and data.

Ongoing security training is one of the best ways to help employees avoid costly and embarrassing security incidents. All employees must realize they are the target of hackers, who are always watching for ways to gain a foothold into government systems. Employees also should be familiar and comply with policies and standards established to protect critical government systems and data.

Employees can serve as an important resource by reporting suspicious activity to MN.IT cyber security professionals. If you see something, say something by emailing the Security Incident Response team (mnit.isirt@state.mn.us) or by contacting your local service desk.

Suggested action steps: October is National Cyber Security Awareness month. MN.IT Services coordinates awareness efforts throughout Minnesota state government. Watch for upcoming announcements from MN.IT on ways you can get involved.

If you have questions, please contact Jeanine Kuwik at Jeanine.Kuwik@state.mn.us or (651) 201-8148. Special thanks to Chris Buse, MN.IT Chief Information Security Officer, who contributed to this bulletin.