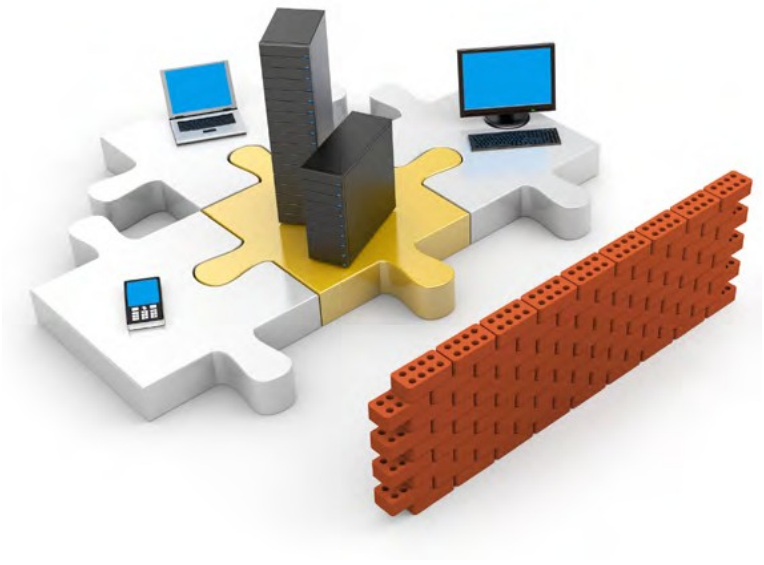
Administrative Office of the U.S. Courts
Department of Technology Services

Court IT Security: Is Your Data Safe?

February 2018



Understanding the Big Picture

Government information systems are under attack by a hacker community that continues to increase in size and sophistication. Federal judiciary systems have not been immune from such incidents. The effort to protect judiciary information and systems is not an isolated event, but an ongoing process. You can assist by working with your IT staff to ensure that actions such as scanning court systems for vulnerabilities and subscribing to security alerting resources occur on a regular basis.

Questions to Ask

Sometimes, the greatest risk facing an IT system is the level of unknown risk. If you do not know your weaknesses or risks, then they cannot be effectively managed and remedied. The following questions will facilitate a discussion with your court unit executives and IT leadership about the health of your local IT security program.

What are your Top Three Security Concerns?

Based on judiciary trends data, most courts face challenges pertaining to patches, configuration, and asset management, including software and hardware inventories. You may want to consider requesting a no-cost IT security assessment or a server vulnerability scan from the AO-IT Security Office (ITSO). Information about these services is published on JNet.

What routine checks are run to make sure systems are not vulnerable to attacks?

A formal vulnerability management process identifies, analyzes, and mitigates risks to the court's local area network. Several no-cost security products and services are available both to assess and to strengthen a court's local security profile.

What security policies are in place and where do users locate them?

Often, local security policies exist, but are not documented. Policies for the management, operation, and use of judiciary systems should be written and available on the court's intranet. If you need help with developing local security policies, visit the Building Local IT Security Policies Service page on JNet. Additionally, all users should formally acknowledge (in writing) their obligation to adhere to all local and national policies. The Judiciary's national policies are codified in the *Guide to Judiciary Policy*.

What types of IT security training and awareness programs are available for local staff?

Users are often called the "first line of defense" against IT security incidents. To successfully contribute to securing judiciary information, users must understand and follow effective IT security practices.

An effective security training and awareness program, which includes both general and more focused awareness training on specific topics, helps foster this understanding. Many materials are published on JNet to assist local courts in developing these programs.

How are mobile devices protected?

Mobile devices, such as laptops, tablets, thumb drives, and smart phones, are inherently vulnerable to loss or theft. To make sure the data stored on them is not accessible to unauthorized users, they should be password protected and, if possible, configured so that data stored on them can be remotely erased if lost or stolen.

Court management of these devices, using judiciary-supported software (Airwatch, the Judiciary's enterprise mobile device management service) that is available from the AO, helps ensure a consistent and secure configuration. Court users should be prohibited from storing sensitive judiciary information on a mobile device unless the information is encrypted.

Are judiciary employees allowed to use their personal devices for judiciary business?

Yes. However, to maximize the benefits and minimize the risks, be sure to have in place a Bring Your Own Device (BYOD) policy and program that:

- Clarifies what *is* and *is not* allowed
- Provides for local court management of these devices, using the tools described above
- Explicitly obtains the user's consent to fulfill certain obligations, such as not tampering with the device.

Judiciary-wide licensing is available for courts to more easily manage and keep an inventory of all court and personal mobile devices.

Has the court IT staff practiced responses to likely security incidents, such as a virus infection or lost laptop? Do court personnel know what to do?

"In the moment" decision making is stressful and can lead to mistakes. Knowing ahead of time how to respond to an incident prepares IT staff to respond more effectively in detecting, containing, and eradicating the problem sooner, resulting in less system damage and recovery expense to the court. Be sure annual security training provides tips to help all end users recognize and respond appropriately to suspicious activity.

What security tools are available and in use in the courts?

The Judiciary follows a model in which security protections are implemented at the local and national levels. To help courts improve their local security program, several no-cost tools are available from the AO. This includes using the Vulnerability Scanning Service (VSS) to help manage vulnerabilities, host-based intrusion prevention systems to protect the court's public sites, Symantec Endpoint Protection to defend against and detect malicious software, and KACE (to manage configurations, patches, and assets, among others.

Judiciary users can contact the Security Operations Center (SOC) at SOC@ao.uscourts.gov or (202) 502-4370 for assistance with these tools.

Information Technology Security Office (ITSO) Contacts:

Visit the Department of Technology Services (DTS) ITSO website on JNet at *Information Technology* and click on the ***Security*** heading.

For questions or comments contact the AO-IT Security Office at (202) 502-2350 or email: AO_ITSO@ao.uscourts.gov

Original Date Published: 2012