Cybersecurity Risks In The Courtroom

By **Daniel Garrie, David Cass, Joey Johnson and Richard Rushing**

Law360, New York (July 31, 2017, 10:23 AM EDT) --

Daniel Garrie

Though courts are traditionally open to the public through physical access, or electronic filing systems such as PACER, courts around the country are routinely tasked with administering justice in a confidential setting. Because of the level of accessibility of courts, security has traditionally focused on aspects of physical security such as the guidance published by The National Center for State Courts. We are now in the time where companies have seen devastating cyberattacks. In order to protect the integrity of the judicial process, courts also need to focus on cybersecurity. These confidential proceedings arise in a wide variety of contexts, spanning trade secret disputes, national security issues, settlement results, and cases involving minors, just to name a few. While there have not been many publicized breaches of court-situated information, as cybercriminals continue to look for easy targets, the court system will surely enter their crosshairs. If judges and court personnel do not maintain proper data security and cyber hygiene, confidential litigant information can fall into the hands of a wide variety of bad actors. This article will outline some of the risks posed to courts and offer some guidance for managing those risks.

David Cass

Consider the following hypothetical. A federal judge is presiding over a multibillion-dollar intellectual property case. The plaintiff seeks a preliminary injunction, and that ruling, regardless of outcome, will have an outsize effect on the parties' bottom lines and future viability. Accordingly, if an individual were to know the judge's preliminary injunction ruling, even a day early, he or she would be able to generate windfall profits by trading on that information — a practice that is becoming more and more common for cybercriminals.

Joey Johnson

Now consider that the judge, his or her clerks, or other courtroom personnel use their smartphone for both work and personal use. As often happens, a child or significant other gets hold of the smartphone and downloads a game or application that has malware code attached to it. When the judge later logs in to check his or her email, the malware infiltrates the court's email server. This silent intrusion allows cybercriminals to monitor all emails related to the dispute. The cybercriminals would then be able to see the court's ruling in advance of its issuance, creating a potential windfall of the cybercriminals, while causing serious harm to the litigants and the integrity of justice system as a whole.

Another way that cybercriminals can gain unauthorized access to potentially confidential information is the courtroom itself. A courtroom is full of computer and connected devices, all equipped with microphones and webcams. If a cybercriminal was able to compromise even one connected device, they would be able to listen in on all court proceedings, whether or not they were open to the public. This information, whether it be trade secrets or sealed indictments, could then be sold to the parties with interests in the information.

Richard Rushing

Notably, the type of data breach outlined above occurs frequently. Many organizations are not even aware when it is happening. But are courts aware of this risk?

This example is not meant as a prompt for courts to radically overhaul their policies and procedures. Nor is it meant to scare the arbitration and mediation communities from engaging in important work. What this example should do is highlight the risk of bad cybersecurity and serve as a reminder that no one is immune to cyberattacks. It is important for the courts to start thinking about how to develop a good cybersecurity infrastructure in order to protect litigants' confidential information and the court system as a whole.

Here are three suggestions that can assist the courts in becoming secure. While there is no silver bullet, these three suggestions and increased awareness can be of value to the courts.

1. Create and develop secure communications and data management frameworks.

- Understand the differences between standard data classifications and the level of security required of each.

- Consider the extent you are in receipt of personally identifying information in the context of a litigation or other court proceeding.

- Identify and separately protect critical data and systems.

- Ensure that email encryption services are available to you, and know when you need to use them to protect the data or conversations exchanged.

- On a quarterly basis, implement and update appropriate controls, systems and processes to protect these systems.

- Verify, validate, and test security systems on a quarterly basis to ensure the continued protection of critical data in the most effective manner.

2. Develop and practice strong "cyber hygiene" — i.e., develop the habit of routinely improving and maintaining the security of one's information systems.

- Implement robust passwords or other advanced means of multifactor authentication, and update them every three months.

- Ensure security of computing and communication devices, especially when traveling abroad.

- Consider creating secure areas for dealing with sensitive matters that do not allow computing and communication devices inside.

- Utilize surveillance and malware detection and "detonation" software.

- Assess the security needs for encrypted phones, laptops and smart devices and ensure that all devices are duly protected.

- Be aware of "spear-phishing" schemes and how to avoid them.

- Use regularly conducted scenario based penetration tests to see how sensitive information may be compromised and abused.

- Keep up-to-date on relevant incidents, causes and consequences.

3. Develop and regularly test an incident response plan.

- Create an incident response plan for your practice that outlines your policy for handling a cyberbreach if one occurs. This must include your plan for assessing a breach, dealing with the potential media fallout, and any corrective actions that may be needed in the wake of a breach.

- Identify appropriate contacts within law enforcement and applicable regulators before a cyberattack.

- Comply with privacy laws, and work with counsel to protect the confidentiality of the information you receive, maintain and exchange with others.

There is no one-size-fits-all approach to cybersecurity. However, it would be prudent for courts and court administrators to implement, and continually update in order to secure their chambers.

As a practical point, judges should also develop standard approaches to data management and protection within each case they preside over. While some of this may need to be subject to party negotiations, this could also serve as a tremendous value to litigants who might otherwise not appreciate the potential susceptibility of their data.

As the world becomes more and more sensitive to the threat of cyberattacks, the court system should be ready to demonstrate to litigants and other stakeholders that they are acting to prevent or contain cyber-attacks, and preserve the integrity of the confidential and valuable data that has been entrusted to it.

Daniel B. Garrie is an arbitrator, forensic neutral and technical special master at JAMS, available in Los Angeles, New York and Seattle. He is executive managing partner of Law & Forensics LLC, and head of its technical computer forensics and cybersecurity practice groups, with locations in the United States, India and Brazil. He is also a partner at Zeichner Ellman & Krause.

David Cass is the vice president and global chief information security officer of IBM Cloud and SaaS Operational Services.

Joey Johnson is the chief information security officer of Premise Health Inc.

Richard Rushing is the chief information security officer for Motorola Mobility LLC.

The authors would like to thank Benjamin Dynkin and Michael Mann at Law & Forensics for contributing to this article.