The Court Reporter Industry, Strong Case for Cybersecurity Protection

by Kevin Ribble

E.V.P., Edgewater Holdings

kribble@edgewater.net

Court reporter firms "Guardians of the Record" provide essential services to our legal system. They exchange data with law firms, court systems, businesses and individuals. Depositions contain large quantities of confidential business and personal information; trade secrets, bank information, HIPAA information, SSN, Sexual histories and much more.

If you have not given this issue a great deal of thought, here are a few compelling reasons to employ cyber risk management and risk transfer strategies to protect your firm from litigation and data breach damages.

The court reporter business segment has been quick to capitalize on the new technologies of the 21st century, providing a variety of innovative tools reducing operating costs and expanding productivity from e-mail, online services, such as RealLegal E-Transcripts and CAT are just a few examples. New tools are now being utilized by court reporters including cloud servers and mobile billing options. Unknown to many small professional businesses is the fact that legal responsibilities apply to the storage, transition and management of data.

Court reporter firms are particularly vulnerable to cyber criminals. They are a target rich data environment with business and personal information that has high value to thieves on the dark web. HIPAA information is currently reported to be priced at $10 per discrete record. The following is a summary of the very real exposures to court reporter firms:

- Stream content during depositions to law firm/attorney laptops containing attorney-client privilege, work product, and confidential information (**potential access point and vulnerability**)
- Communicate with parties, attorneys, law firms, and courts (**allowing potential spread of malware/viruses**)
- Accept and process payments from law firms and attorneys (**credit card/bank account info**)
- Travel often (**exposes collected information to theft/unauthorized access**)
- Use technology extensively in performance of job (**vulnerable to hack**)
- Turnover can be high **(various former employees with access to information, passwords, networks**)
- Communicate frequently via email with no personal knowledge of who they are communicating with (**vulnerable to phishing and other scams**)
- Often rely on Wi-Fi networks or portable Wi-Fi hubs (**access point vulnerability**)

Would your agency be ready to respond to a data breach? In a recent case, small business employees showed up on a Monday morning and found they were unable to log into their computers. When the manager investigated, they found their data and systems were being held for ransom by the use of ransomware virus. The access codes had been encrypted and the key was held by criminals demanding payment. They experienced what may be a small business's worst nightmare - they were shut down and unable to conduct business. Loss of revenue and reputation was just the start of the problem. This type of event is up over 300 percent says Kevin Haley director of product management at Symantec Security.

Kevin Haley said his group has seen an average of over 4,000 ransomware attacks per day since Jan. 1, a 300-percent increase over the approximately 1,000 attacks per day in 2015 the company highlighted in its recent Internet Security Threat Report. Haley said the gangs using ransomware have honed their social engineering efforts to target the right people for spear phishing emails. The malware is packaged in a phony email attachment, often a phony invoice.

Scan barcode to fill out an application for insurance to protect your data.

Small professional firms such as courter reporters generally have fewer resources available to monitor and combat cyber threats, making them easy targets for expert criminals. In addition, many of these firms have a false sense of security and believe they are immune from a possible cyber-attack. The data refutes those impressions, Advisen reports:

- The two largest types of data loss are personal privacy and personal financial identity making up more than 80% of cases.
- Small firms make up 57% of the cases, while large firms make up 21% of cases. However, larger firms have 10 times the average number of incidents per company compared to small firms."
- Ransomware 300 percent increase in attacks

Footnotes: FedScoop article Ransomware attacks quadrupled in Q1 2016 Greg Otto

The Choice Is Clear Risk Management and Risk Transfer Strategies Are Essential

The subcommittee heard testimony from a number of professionals from the tech industry on how and why cyber risk is just as much, or even more, of a danger for small companies as it is for larger ones. The overarching theme of the discussion was that the cyber liability landscape is menacing and constantly changing. Cyber policies frequently do not keep up with the expanding methods of hacking attacks, leaving policy holders poorly protected. There are great variations between cyber forms, and some do not adequately address the potential liabilities for an insurance agency. Policies should at a minimum contain provisions for breach response, cost of informing customers, post-attack credit-monitoring, inter- net slander, credit card vendor fines and loss of business from denial-of-service attacks.

The following is a summary of security tips offered as part of the testimony before Congress.

1. Create a written security policy for employees.
When it comes to cyber security, one of the biggest problems is the lack of education among small-business owners and their employees. In your security policy, determine whether employees should be allowed to have personal data on business devices, he said. Conversely, figure out whether business data should be permitted on their personal devices and what to do in case a device is lost or stolen.

2. Use stronger passwords.
This might seem like a no-brainer to some, but business owners have been "dumb" about creating smart passwords. If your password is a common word, or something that can be guessed based on public information, consider changing it to something more difficult to crack.

3. Encrypt your data.
You can't always keep hackers out of your computer systems, so take steps to protect the data contained within those systems. That's where encryption comes in. Disk encryption tools come standard on most operating systems, including BitLocker for Windows PCs and FileVault for Macs. These programs essentially convert the data on your systems into unreadable code that isn't easily deciphered by hackers.

4. **Implement Bluetooth controls, pairing only known, trusted devices.**
5. **Protect against Trojan emails with blacklisting and whitelisting applications.**
6. **Have policy controls over web browser use and website access.**
7. **Install a firewall for mobile devices to restrict inbound connections and prevent use of mobile device as a bridge.**

Small businesses are soft targets for hacker criminals, and the cost to deal with repercussions of a cyber-attack could be disastrous for your agency. Purchasing cyber insurance should be a strong consideration. Purchasing coverage from someone who has the required expertise to ensure your particular business is fully protected is critical.

Footnote: Statement for the Record William Weber, General Counsel, Cbeyond, Inc. Before the United States House of Representatives Committee on Small Business Subcommittee on Healthcare and Technology Hearing on Protecting Small Businesses Against Emerging and Complex Cyber-Attacks March 21, 2013

MERCER
MAKE TOMORROW, TODAY
EDGEWATER HOLDINGS