Digital Documents and Cyber Security

By Richard P. Howe Jr.

Since its inception in seventeenth century America, the mission of the registry of deeds has been fourfold: (1) take in documents related to the ownership of real estate; (2) make and preserve official copies of those documents; (3) create an index to allow people to find relevant documents; and (4) make those records and indexes available to the public. About ten years ago, a centuries-old paper-based system gave way to digital record storage. The new technology allowed greater access to the records while increasing efficiency and cutting costs.

As digital documents, storage, and communications have evolved, so has cybercrime. Early email scams like the friend stranded in Hong Kong without money or a generous Nigerian prince anxious to share his fortune with you almost seem quaint by today’s standards. Whoever hacked the emails of the Democratic National Committee and John Podesta (Hillary Clinton’s campaign chair) reminded us that theft of information is still part of the dark tool box of bad actors, but the most significant threat to digital records today comes from ransomware.

Ransomware is a software program that is surreptitiously inserted into your computer and then migrates laterally to other machines on your network and onto your servers. Once the program is remotely activated by the bad guys, it encrypts the data on your computer and on your server, if it has traveled that far. When you log onto your computer, post-ransomware attack, you are confronted by a strange screen displaying a stranger message:

Your files have been encrypted and the only way to decrypt them is to pay us a certain amount via Bitcoin. If you pay, we will send you the private key needed to decrypt your files. This offer is only good for 72 hours. If you haven’t paid by then, your files will be inaccessible to you forever.

(continued on page 2)
Two things have contributed to the rise of ransomware. First is the easy availability of strong encryption programs that are unbreakable. Second is the invention of Bitcoin which is an untraceable, anonymous payment method. The FBI reports that there are more than 4000 successful ransomware attacks each day, but that number is probably much greater because many organizations just quietly pay the ransom in the hopes of regaining access to their data.

How does the ransomware get on your computer in the first place? Usually by someone in your organization clicking on a link in an email and launching the program. Because we live in a click-happy culture, this is an effective delivery system. But employee education – “don’t click on any links if the email is from someone you don’t know” – is not enough, because the bad guys have grown increasingly sophisticated in crafting emails that look like they are from a friend or colleague.

So what is an organization to do? Continuous user education is a big part of it. While it may be inevitable that your computers will be infected, don’t make it easy for the bad guys. Make sure all the updates and patches on your computer software are current. Those updates usually are a response to the newest attack, so delaying their installation leaves you vulnerable. Most importantly, continuously backup your data. After an attack, the only way to recover your information short of paying the ransom is to wipe clean your computer and restore your files from backup. Finally, have frequent “what if?” discussions with key personnel, and include ransomware response in your disaster recovery plan.

After learning of the threat posed by cyber criminals, envisioning a return to a paper-based system may seem attractive, but with proper training and procedures, ransomware can be placed in context of all the other obstacles your organization may encounter.
Helping Owners Comply with the Mass. Lead Law

By Toni Snow

It is well known that the impacts of lead poisoning on children under age 6 may include learning problems, hyperactivity and other behavior problems, as well as damage to kidney function, hearing and speech. What is not as well known is that children do not usually become lead poisoned from eating paint chips. In fact, it is much more common for a child to become lead poisoned by coming in contact with lead dust from living in homes built prior to 1978 (when lead paint was finally banned in the U.S.). Lead dust can be generated by home renovations that do not follow state and federal lead safe work practices or from the daily “wear and tear” of opening and closing old lead painted windows and doors. The child “ingests” lead contaminated dust through normal hand to mouth activity and, over time, prolonged exposure can result in elevated levels of lead in the child’s blood. With continued exposure, the child may become lead poisoned. Lead poisoning in Massachusetts is identified as a lead level >25 micrograms per deciliter of blood, but lower blood lead levels do not necessarily indicate less damage to the developing child’s body and brain. The Centers for Disease Control has stated explicitly that: “No safe blood lead level in children has been identified.”

Massachusetts, a national leader in addressing childhood lead poisoning and prevention, sponsored the first and most comprehensive Lead Law in the country. The Massachusetts Lead Law, drafted into legislation in the 1970s and regularly updated since, requires owners of properties built before 1978, where children under age 6 reside, to have the apartment or home deleaded. The deleading must be done by certified and licensed deleading contractors and all inspections must also be done by certified and licensed lead inspectors. Failure to comply with the Lead Law may result in costly fines and lengthy litigation for property owners, contractors and real estate agents.

The Lead Law also broadly addresses additional key issues related to childhood lead poisoning prevention by requiring the following: blood lead testing of children at ages 1-3; Tenant Notification prior to rental or leasing; Lead Paint Notification by the Seller or Real Estate Agent prior to the sale of a home, non-discrimination of families with young children when renting or buying a home; and the certification and licensing of lead inspectors and deleading contractors.

While childhood lead poisoning poses a serious burden for affected families, the cost of lead paint abatement, which sometimes exceeds $8,000 per unit, may pose a significant financial burden for property owners and landlords. Fortunately, there is financial help available to residential property owners in most local communities. Programs offering financial and technical assistance in the Merrimack Valley include the City of Lowell (978-674-1439), the City of Lawrence (978-620-3523), and the Town of Nashua, NH (603-589-3071) all of whom are recipients of federal funding for Lead Hazard Control. Statewide, Mill Cities Community Investments, 450 Merrimack St., Lowell (978-970-0600 x5), administers the MassHousing “Get the Lead Out” program. The terms of these programs vary, call for more information.

*This article was previously published in the October 2014 Issues of the Merrimack Valley Housing Report
ATTENTION HOMEOWNERS, LANDLORDS AND TENANTS

The Lowell Lead Paint Abatement Program Welcomes New Clients!

Lead-Safe Lowell offers Lowell homeowners 0% interest, FORGIVABLE loans for lead paint removal in residential properties. No payments are required and the loan is fully discharged after 3 years! Occupants of dwellings must be low-to-moderate income to qualify.

- Up to $15,000 available for single family homes
- Up to $12,000 available, per unit, for multi-family homes
- FREE Lead Inspection and Project Management
- FREE Soil Testing

Contact:

Philip Ferreira, Program Manager TODAY!
978-674-1410
Pferreira@lowellma.gov