Disaster Preparedness + Cloud Computing

Jack Newton
CEO + Founder
Clio
WHAT IS A DISASTER?
Law Firms and Other Businesses Slowly Return to Manhattan Following Sandy

Just three months following Hurricane Sandy, law firms that were displaced by the storm have begun to move back into their Manhattan offices. The firm of Fragomen, Del Rey, Bernsen & Loewy, still does not know when it can move back into its location at 7 Hanover Square.
Disasters

“Disruption of business functions and processes.”
Disasters to Others

• Clients undergo disasters for which a lawyer should prepare.
• Courts, Vendors, and Services also suffer disasters
Katrina still threatens 3,000 New Orleans court cases

NEW ORLEANS (AP) — Like the city's crumbled levees and gutted homes, New Orleans' courts have been reduced to shambles — and the chaos could jeopardize many of the 3,000 cases pending before Hurricane Katrina hit.

In his third day back on the bench since the hurricane struck two months ago, Criminal District Judge Benedict Willard opens court by entering a plea of his own — for patience.

"We're going to do as much as we can, with the limited resources," Willard says of this battered city's struggle to resuscitate a justice system crippled by the monster storm.

With the criminal courthouse still mired in muck, Willard presides at the old parish jail in a room once used for witnesses to identify criminal suspects in lineups. One-inch hash marks for measuring height dot the wall behind his small office desk. Attorneys sit in folding chairs.
Bomb Manhunt Closes Courts as Boston Shelters in Place

By Sheri Qualters | Contact | All Articles
The National Law Journal | April 19, 2013

A massive manhunt for a suspect in Boston's Marathon Day bombing forced authorities to place much of the city on lock-down, shuttering businesses including law firms plus federal and state courthouses as a frantic week drew to a frantic close.
Disaster Challenges

- Unworkable Office Location
- Dislocation of Parties
- Closure of Courts & Services
- Destruction of Physical Resources and Data
WHAT IS DISASTER PREPAREDNESS?
Disaster Preparedness

Avoiding Disaster
- Pick tools that are disaster resistant
- Practice due diligence when selecting services and vendors
- Follow industry best practices
- Upgrade systems

Recover from Disaster
- Easy access to data
- Emergency Contact Information
- Clear Recovery Assignments
Cloud Computing

Avoiding Disaster

• Pick tools that are disaster resistant
• Practice due diligence when selecting services and vendors
• Follow industry best practices
• Upgrade systems

Recover from Disaster

• Easy access to data
• Emergency Contact Information
• Clear Recovery Assignments
Cloud Computing

Dynamic, Geo-redundancy, SSAE 16
CLOUD COMPUTING + DISASTER RECOVERY
With the cloud, disaster recovery is finding a laptop and a desk
WHY LAWYERS NEED DISASTER RECOVERY PLANS
“40-60 percent of small businesses simply don't come back to business after a disaster.”

David Paulison, former executive director of the Federal Emergency Management Agency (FEMA)
Clients have increased needs for speedy and accurate representation during crises.
Texas trial lawyer eyes New York storm cases

COMMENT (9)

By Tim Eaton
American-Statesman Staff
From his Austin office, Steve Mostyn looks east. Immediately before him, he sees the Texas Capitol, the domed building in which the state’s most powerful politicians have toiled for more than a decade to hobble the business of trial lawyers like himself.

Much farther east, Mostyn sees potential riches on the horizon. The lure of New York, and all those insurance claims spawned by the destructive wrath of Superstorm Sandy, is irresistible for an ambitious litigator with political connections, piles of money and a fearsome reputation.
During natural disasters, lawyers’ professional and ethical obligations are not suspended.
Lawyers’ Duties on a Good Day

• Competence
  – Awareness of changes in the law & practice
  – Benefits and of relevant technology

• Diligence
  – On behalf of your client

• Communication
  – Respond to or acknowledge client communications

• Continuity
  – Records retention
Ethical Duties

1.1 Competence
1.3 Diligence
1.4 Communication
1.6 Confidentiality
1.15 Safekeeping Property
1.1 Competence

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.
1.3 Diligence

“A lawyer shall act with reasonable diligence and promptness in representing a client.”

[1] A lawyer should pursue a matter on behalf of a client **despite opposition, obstruction or personal inconvenience to the lawyer**, and take whatever lawful and ethical measures are required to vindicate a client's cause or endeavor.
1.4 Communication

(a) (2) keep the client reasonably informed about the status of the matter;

(3) promptly comply with reasonable requests for information;

[7] A lawyer may not withhold information to serve the lawyer's own interest or convenience or the interests or convenience of another person.
1.6 Confidentiality

A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation...
1.15 Safekeeping Property

(a) A lawyer shall hold property of clients or third persons that is in a lawyer's possession in connection with a representation separate from the lawyer's own property. Funds shall be kept in a separate account maintained pursuant to Title 16, Chapter 600 of the Maryland Rules, and records shall be created and maintained in accordance with the Rules in that Chapter. Other property shall be identified specifically as such and appropriately safeguarded, and records of its receipt and distribution shall be created and maintained. Complete records of the account funds and of other property shall be kept by the lawyer and shall be preserved for a period of at least five years after the date the record was created.
Lawyers have an ethical duty to have disaster preparation and mitigation plans.
BUILD YOUR OWN DISASTER RECOVERY PLAN
Disaster Preparations

• Plan for disasters and interruptions
• Use available technology prior to disruptions
• Communicate these preparations with clients
Advanced Planning

• Recognize crucial business elements
• Find tools and services that reduce risk or enhance recovery
• Implement plans now
Communications

• Voice over IP (VOIP)
• Call Forwarding
• Email
• Social Media
Backup

• Physical media backups are fragile
• Online backup provides offsite redundancy
Organization

• Practice management services
  – Contact information
  – Notes
  – Documents
  – Billing
Organization

• Online Document Generation

logos: netdocuments, Microsoft Office 365, Google Apps
Finances

• Manage Finances to avoid disruption
• Maintain access to a rainy day fund
• Credit Line
Locum
Communication of Plans

**Client Intake**
- Gather Secondary & Emergency Contact Information
- Communicate Firm Procedures
- Test Systems

**During Disaster**
- Trigger Plans
- Contact Staff First
- Research Disruptions
- Enact Solutions
- Contact Clients and Courts
9+ Steps to Disaster Recovery Planning for Small and Midsize Companies

Smaller companies face significant risk in many kinds of disasters. Plan for disaster recovery now, or risk finding that you're out of business

"A disaster is an event big enough to cause your IT services to be unavailable but small enough that restoring them is important."

"You can't plan for any particular disaster. The one that gets you will be the one you didn't plan for."

Those are the words of Howard Marks, chief scientist of Networks Are Our Lives Inc, and a past contributor to sister bMighty.com publication Network Computing, at last month's Interop New York.

I was so impressed with Marks' presentation titled "Disaster Recovery For The Small and Medium Enterprise" that I decided to interview him on video and lay out some of his key points for our readers.

---

Fredric Paul
Features

0 COMMENTS
COMMENT NOW
Summary

• Lawyers have an ethical duty to plan for disaster
• Disaster plans minimize the chances of business disruption and reduce recovery time
• Disaster preparation should be a part of normal business activity
• Choose tools & services that enhance your practice now and prepare you for disaster.
NEW TYPES OF DISASTERS
“Ransomware”
Your files are encrypted.

To get the key to decrypt files you have to pay **500 USD**. If payment is not made before **13/02/15 - 15:07** the cost of decrypting files will increase 2 times and will be **1000 USD/EUR**.

Prior to increasing the amount left: **167h 57m 43s**

Your system: Windows 7 (x64)  First connect IP: [redacted]

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.

**How to buy CryptoWall decrypter?**

1. You should register Bitcon wallet ([click here for more information with pictures](#))
Ransomware: City of Detroit didn't pay, TN sheriff's office did pay to decrypt

[Image of ransomware screen]

Total costs: 0.5 btc € 164,64
Paid: 0 btc € 0.00

Send bitcoins to this bitcoin address: 1LN8c9mI3k2qaE2yY25u0oA3zc5C7N7DxQ

On IDG Answers ➔
What was the first programming language you learned?
Cryptowall Ransomware Nets $500 Bitcoin Payout From US Sheriff's Office

Stan Higgins  | Published on November 14, 2014 at 20:40 BST

A county sheriff’s office in Tennessee paid a $500 ransom in bitcoin after it became the victim of a cyberattack this week.

As reported by Nashville-based WTVF-TVs, the Dickson County Sheriff’s Office ran afoul of a bug known as Cryptowall, a derivative of infamous ransomware CryptoLocker.

Cryptowall is a Trojan horse program that, once inside a computer, encrypts its contents and triggers demands for a payment in bitcoin. The firm’s estimates suggest that after being discovered earlier this year, as many as 1,000 computers have been infected.

Detective and sheriff’s office IT director Jeff McCliss told WTVF-TVs that a data cache containing sensitive documents, photographs and criminal reports was impacted. Overall, more than 70,000 files were temporarily inaccessible due to the malware infection.
RISKIEST SECTORS for MALWARE & HACKERS

1. Pharmaceutical & Chemical
2. Media & Publishing
3. Manufacturing
4. Transportation & Shipping
5. Aviation
6. Food & Beverage
7. LEGAL
   The legal sector was ranked SEVENTH in Cisco’s 2015 Security Report
Protect Yourself With the Cloud
+
Antivirus
QUESTIONS
Disaster Preparedness + Cloud Computing

Jack Newton
CEO + Founder
Clio