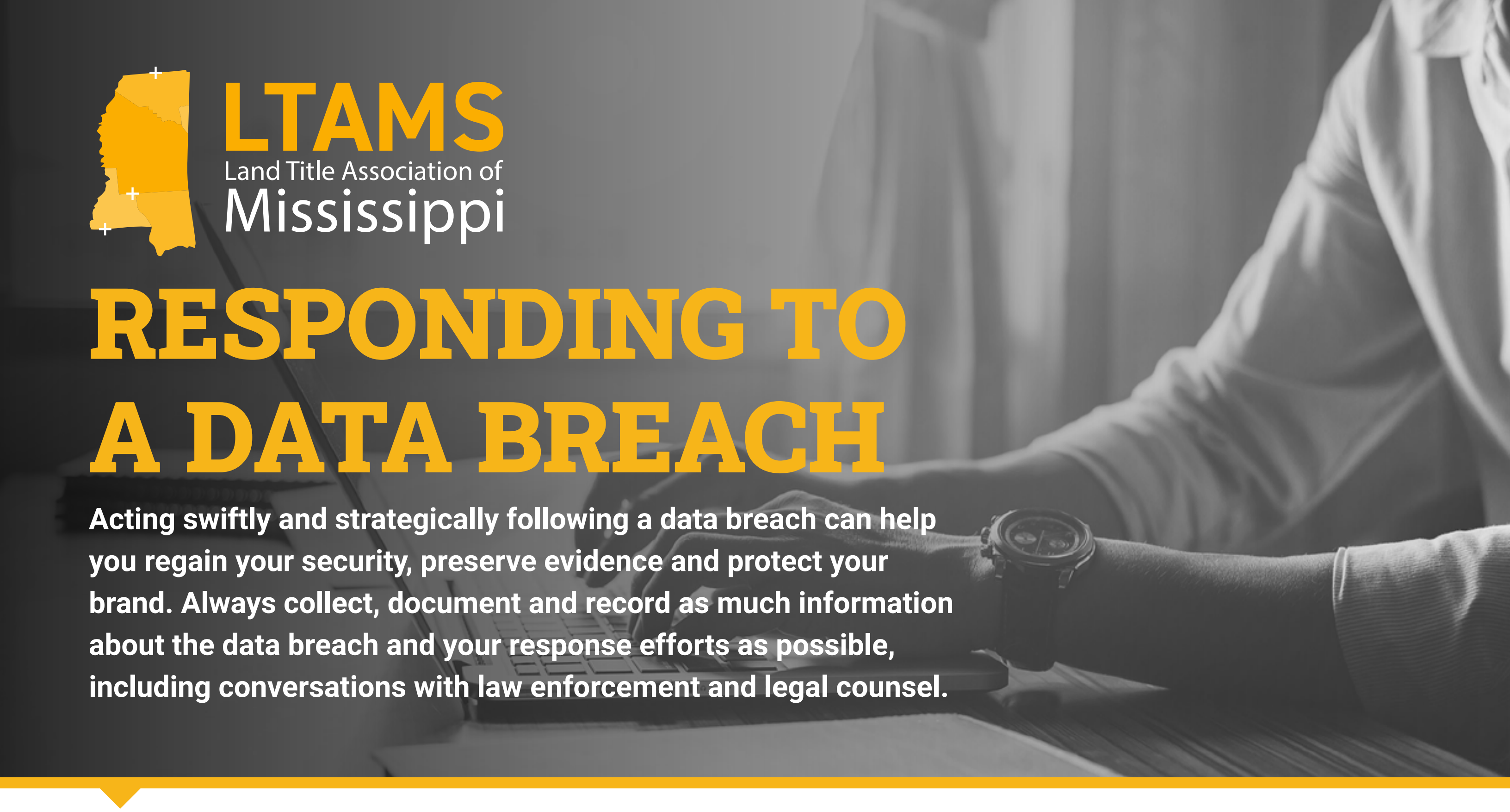

LTAMS
Land Title Association of
Mississippi

RESPONDING TO A DATA BREACH

Acting swiftly and strategically following a data breach can help you regain your security, preserve evidence and protect your brand. Always collect, document and record as much information about the data breach and your response efforts as possible, including conversations with law enforcement and legal counsel.

WHAT TO DO BEFORE A DATA BREACH

1 **FORM A RESPONSE TEAM.** Appoint an appropriate incident lead who has the skills to manage the issues involved with a data breach and who will coordinate response efforts.

2 **REVIEW CYBER SECURITY POLICIES.** Make necessary updates to your plan.

3 **EVALUATE EXTERNAL PARTNERS.** Create a pre-breach agreement with a data breach resolution provider, legal counsel, communications firm, and/or forensics experts to save both time and money after the breach happens.

4 **PRE-BREACH FORENSICS.** Enable processes and systems that will expedite forensics in the event of a breach.

- Perform regular system backups and maintain previous backups for a specific period of time.
- Enable auditing on workstations, servers and network devices.
- Forward audit records to secure centralized log servers.
- Configure mission-critical applications to perform auditing and include the recording of all authentication attempts.
- Maintain a database of file hashes for the files of common operating system and application deployments, and use file integrity checking software on particularly important assets.
- Maintain records (e.g. baselines) of network and systems configurations.
- Establish data retention policies that support historical reviews of system and network activity, comply with requests or requirements to preserve data that are related to ongoing litigation and investigations, and destroy data that is no longer needed.

5 **DISSEMINATE THE RESPONSE PLAN.** Schedule periodic trainings to ensure your staff knows what to do.

6 **PRACTICE YOUR PLAN.** Test preparedness across all departments by conducting breach simulation exercises.

7 **SCHEDULE REVIEWS.** Set calendar dates for regular reviews of your response plan to make adjustments and address any new risks.

WHAT TO DO AFTER A DATA BREACH

FIRST HOUR:

1 **RECORD THE MOMENT OF DISCOVERY.** Also mark the date and time your response efforts begin, i.e. when someone on the response team is alerted to the breach.

2 **ALERT AND ACTIVATE EVERYONE.** Include everyone on the response team, including external resources, to begin executing your preparedness plan.

3 **STOP ADDITIONAL DATA LOSS.** Take affected machines offline, but do not turn them off or start probing into the computer until your forensics team arrives.

FIRST THREE HOURS:

4 **SECURE THE PREMISES.** Ensure the area where the data breach occurred and surrounding areas are secure to help preserve evidence. Also obtain any offsite devices that were involved.

5 **DOCUMENT EVERYTHING.** Record who discovered the breach, who reported it, to whom it was reported, who else knows about it, what type of breach occurred, etc. Interview those involved with discovering the breach and anyone else who may know about it – then document the results.

6 **BEGIN AN IN-DEPTH INVESTIGATION.** Your forensics team should begin analyzing preserved or reconstructed data sources to determine size and type of information compromised.

FIRST 12 TO 24 HOURS:

7 **REVIEW NOTIFICATION PROTOCOL.** Review those that touch on disseminating information about the breach for everyone involved in this early stage. Based on the advice of legal counsel, notify your customers about the breach. Open, honest communication is critical. Your post-breach letter will help customers understand what they must do. Your actions will establish how you begin rebuilding trust with your customers. External breach management partners can assist in managing communications with your customers.

8 **NOTIFY LAW ENFORCEMENT.** Based on the advice of legal counsel, law enforcement may need to be notified.

9 **EXECUTE THE TERMS OF YOUR PRE-BREACH PLAN.** Bring in your forensics firm to begin an in-depth investigation.

AFTER THE FIRST 24 HOURS:

10 **FIX THE ISSUE THAT CAUSED THE BREACH.** Your forensics team should have now investigated the network and any affected machines and systems. In the process it will likely have discovered the cause of the breach. Have the team delete any hacker tools and determine if you have any additional vulnerabilities or security gaps. The team should also replace any affected machines with new ones before taking them back online. Be sure to document everything so you can learn from this situation in the future.

11 **CONTINUE WORKING WITH FORENSICS.** In addition to fixing what caused the breach, you'll need your forensics team to take stock of what exactly was stolen. This means analyzing backup, preserved or reconstructed data sources, figuring out the number of customers or employees that were affected and the type of information that was compromised and then aligning those affected with the stolen data so you can begin notifying people.

12 **IDENTIFY ANY LEGAL OBLIGATIONS YOU MAY HAVE.** Once forensics has a full picture of what was compromised and who that affects, have your legal team take a look at any state and federal regulations that govern the industry and the type of data that was lost. Determine who you need to notify and what timetables you have and then ensure that you actually follow through on those notifications. This isn't fun, and it's probably going to hurt consumers' trust in your company or organization in the meantime. But, not notifying people could lead to even bigger problems.

13 **REPORT TO UPPER MANAGEMENT LEVELS.** Chances are that the upper management and executive levels in your company are aware of the breach, but they're going to want detailed reports on it. You should be keeping them informed of all the facts, including causes, resolutions and potential ramifications. It's also good to continue to give regular updates on the progress of investigations and the overall response.

14 **IDENTIFY ANY POTENTIAL CONFLICTS.** You'll need to look at any and all upcoming business initiatives that could potentially interfere with your investigation of and response to the data breach, and make sure both the response team and upper management are aware of them. In some cases, you may need to postpone some things while the response carries on.

15 **IMPLEMENT IMPROVED TRAINING PROGRAMS.** Based on lessons learned, implement new training programs that would help prevent future data breaches.

SOURCES:

- ALTA Best Practices Pillar III – Protecting NPI “When a breach is detected, Company should have a program to inform customers and law enforcement as required by law”
- Data Security Guide From FTC (June 2015): www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business
- Data Breach Guide From FTC (September 2016): www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf
- Data Breach Resolution Checklist From Experian (2017): www.experian.com/assets/data-breach/white-papers/experian-2017-2018-data-breach-response-guide.pdf
- Data Breach Partner Services – Experian: www.experian.com/data-breach/data-breach-resources.html and www.experian.com/assets/data-breach/brochures/Data-Breach_TurnKey_SellSheet.pdf
- NAR Data Security and Privacy Toolkit: www.nar.realtor/educsess.nsf/9f710ae7a91142f8862569a60067238b/06e2acfc47397493862577c200564989/$FILE/Raynolds.pdf
- The Center for Internet Security (CIS) Critical Security Controls V6.0: www.sans.org/media/critical-security-controls/SANS_CSC_Poster.pdf
- Overview of Digital Forensics: www.isaca.org/
- Internet Security Threat Report From Symantec 2017: digitalhubshare.symantec.com/content/dam/Atlantis/campaigns-and-launches/FY17/Threat%20Protection/ISTR22_Main-FINAL-JUN8. pdf?aid=elq_

This information is being provided by LTAMS for reference purposes only and is not intended to represent a standard best practice or the only approach to any particular issue. This information should not be construed as legal or business advice from or on behalf of LTAMS. Users should consult their own legal counsel if necessary to ensure that any policies adopted or actions taken meet the unique security requirements of their company.