# MITIGATING DATA BREACHES

BY MARK GERLACH

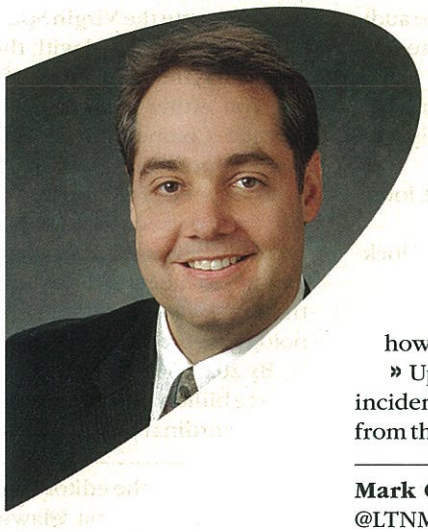
Emergencies, including data breaches, are best handled with three steps: prepare, prevent, recover. That was the message of a panel at the 2014 International Legal Technology Association conference. Speakers included Robert Newman, an associate at Winston & Strawn; Deena Coffman, CEO of IDT911 Consulting, a subsidiary of IDT911; and Tedrick Housh III, a partner at Lathrop & Gage.

## PREPARE

Cybercriminals target law firms, Housh said, because they have key information about clients—their intellectual property assets, pending merger and acquisition deals, litigation that could impact stock prices, and more. Companies should inventory, prioritize and understand their obligations for owning and maintaining sensitive data, and create a data response team before a breach erupts, he said.

"You never see a football team that gets the playbook on game day," Coffman observed.

But the poll of the 50+ people in attendance (taken via ILTA's conference app) revealed that 60% of respondents said their organization does not have a data incident response plan in place. Of those who did, 33% said they tested the plan annually; quarterly 22%; occasionally 30%; and never 10%.



"First, stop the breach and identify the compromised data."
—TEDRICK HOUSH

An important tip for preparing is to assess points of exposure (e.g., unencrypted email, laptops, hard drives or smartphones) and manage those areas to ensure (or try to ensure) that they are secure. "Make security manageable and affordable," Coffman said after the panel. "Breach events are far, far less expensive to prevent or mitigate than they are to correct."

The biggest risk areas are not always where the most information is housed, said panelists. Risks can include data located in a legacy system or backup drive, said Newman to LTN.

"Simple human error is also the source of many incidents," he said.

Panelists suggested elements that an incident response plan checklist should include:

- An assessment of data risks and policies.
- An incident response team and written plan.
- Employee training policy.
- Vulnerability and penetration testing.
- Incident response procedure drills.
- A system to manage and transfer risk.

## RECOVER

Panelists offered tips on how law firms could recover:

- First, stop the breach and identify the compromised data, said Lathrop & Gage's Housh after the panel. Next, check with legal counsel to discuss how to respond to clients and regulators, he said.
- Outside communication must be accurate, Housh cautioned. The public might be understanding of a breach, he said, but will have less tolerance for a poorly handled incident.
- "You can either strengthen your brand or decimate it; how you respond can make the difference," said Coffman.
- Update and revise both the internal security policy and incident response plan after a breach with information learned from the incident, said Newman.

---

**Mark Gerlach** is a staff reporter for Law Technology News. @LTNMarkGerlack.

instantiate processes such as staff hires, candidate recruitment, and more.

- Catalyst Repository Systems has upgraded its technology-assisted review platform **Insight Predict**. It enables continuous, active learning, ranking and training by large teams. Filters offer visual navigation for constructing complex queries.

- KCura Corp. has updated its legal hold and collection software in **Relativity 8.2**. Customized monthly and daily summary reports for active holds can be delivered via email. Relativity's **Scout** can remotely analyze a custodian's computer and display available data for collection.

- Kroll Ontrack Inc.'s **Remote Data Recovery** remotely accesses disks, RAID systems, virtual machines, storage area networks and logical unit numbers—so the devices stay on the customers' premises.