



What Not to Do After a Security Breach

Expert familiar with TD Ameritrade, TJX cases discusses the mistakes enterprises often make following a breach

OCTOBER 26, 2007 | 4:00 PM

By Kelly Jackson Higgins
Senior Editor, *Dark Reading*

Step number one after a security breach: Don't immediately bring in the outside forensics team --- get your attorney up to speed on the attack first. And don't assume just because you had a break-in that you have to disclose it publicly -- it all depends on whether data covered under regulatory mandates was exposed.

These are two bits of advice to the security-breached from Kevin Mandia, a forensics expert who has worked on the front line of the TD Ameritrade investigation and is serving as an expert in the TJX breach case. Mandia will testify as an expert witness for the credit- and debit-card issuers if the TJX case goes to trial.

Mandia takes a different view than some breach experts, who encourage enterprises to make swift disclosure of suspected breaches. (See [What to Do When Your Security's Breached.](#))

"Only 'the need to know' should be 'in the know,'" says Mandia, CEO of Mandiant, who for the past 15 years has worked on over 100 computer security breaches with the Fortune 500, FBI, and military. He's seen a lot of mistakes made by victims over the years, he says, as well as major shifts in how companies must respond in today's regulatory and disclosure environment.

Mandia, who couldn't comment directly on the Ameritrade or TJX cases, says over half of the cases that his firm responds to don't actually require public disclosure at all. "This happens a lot -- a database gets compromised and the systems admin pushes back his chair and says 'our database has been compromised,' and the rumor mill starts," he says. "Even if there's no 'covered' [regulated] data on the database, people start talking about it, the *Wall Street Journal* [reports it]."

"I still believe that in over 50 percent of the [incidents] we respond to, disclosure is not required," Mandia says. "Even if there's 'covered' data in the system, it could be encrypted, for instance, and it's unreasonable to think it was compromised."

Attorney-client privilege goes a long way. "The need for counsel is one of the biggest changes I've seen in incident response in the past two years," he says. "But it's very important to have counsel involved before we are -- for attorney-client privilege."

Another big misstep is misjudging whether sensitive data covered by regulatory requirements has been breached. "If I have a computer that's been compromised, I don't have to disclose that my computer has been breached," says Mandia, who will be presenting some of his findings in forensic investigations at the [SecTor security conference in Toronto](#) next month. Only if the data that falls under HIPAA, SOX, PCI, FTC safeguards, and state privacy laws, for instance, has been breached, he says.

Typically, the IT or security technicians in the trenches have to respond and provide their opinions to upper management and counsel on whether data was exposed. "The biggest challenge is technicians are not very good with gray areas, and they're not suited for making opinions" on this, he says. "It's actually better for a layperson to do it."

Another common error companies make is assuming that the attack was an inside job, and focusing only on

that attack vector. "Nine of out 10 think it's an insider... that there's no way their crown jewels could be compromised [by an outsider]," Mandia says. "The catch is that insider investigations are 10 times more costly than external ones because [they must work] surreptitiously -- it's us versus us."

So it can take months to investigate, and it may be all for naught if the breach actually came from outside, he says. Not to mention lost time in catching the real perpetrators on the outside. "Firms need to move as fast as they can for the first five days... If they do that, they are more successful," he says. "But most are making their decisions too damn slowly."

Part of the problem is in most cases, there isn't just one "owner" of the incident response in an organization. The internal investigation often has people going off in different directions and not coordinating their findings, which leads to mistakes and inefficiencies. "You need one guy who handles it appropriately and has enough clout to be a leader," Mandia says. "It needs to be someone no less than two rungs from the top."

Meanwhile, the process of forensic data collection has changed: Due to the nature of today's malware, companies now must also acquire and analyze system memory as well during their investigations, he says. "You have to inspect within the memory," he says.

And most organizations today are running in fear of kernel-level rootkits, he says. "Everyone is chasing that ghost, although they are not finding a lot of them," he says. "Everyone wants to do rootkit detection when responding" to a breach, he says.

The attack techniques, however, are basically same old, same old, he says. "The vulnerabilities are generally going to be in Office and PowerPoint and they are still coming in via email," he says, and users are still being duped into clicking infected attachments with trojans and keyloggers, for instance.

Have a comment on this story? Please click "Discuss" below. If you'd like to contact Dark Reading's editors directly, [send us a message](#).

- [Mandiant](#)