A Judge Approved a Lawsuit Against Target. His Reasoning is Good News for Business.

By Chris Cronin | ISO 27001 Auditor | Governance & Compliance Services

Business and legal journalists have been expressing disappointment at Judge Paul Magnuson's decision to allow third party banks to sue Target Corp after their cardholder data breach. Both journalists and expert commentators have argued that allowing third parties to sue for damages after a data breach unfairly increases a hacked organization's liability. But these journalists and commentators are missing a larger point about the decision: Judge Magnuson showed us the underpinnings of a business-friendly formula that can protect hacked companies from liability.

When news of a data breach goes public, the hacking victim is often subjected to criticism from both the public and the business community alike. We predictably hear speculation that the hacked victim was sloppy, not vigilant, insufficiently talented, or just plain negligent. We can also predict that the victim will be sued as a result of the breach. After all, didn't they let the breach happen? Shouldn't someone pay? Or is it possible that a hacking victim is just a victim, just like the people whose personal information was stolen?

Judge Magnuson's U.S. District Court decision regarding the Target case implied that sometimes a victim is just a victim after all. Magnuson made a decision that allowed banks to sue Target for damages after Target's payment card breach in 2013. He stated that Target's negligence should be evaluated based upon the foreseeability of the threat, the impact to others, and the reasonableness of safeguards that could have prevented the breach.

Translated, this means that if Target had safeguarded cardholder data using controls that were appropriate for the risk, yet were not overly burdensome, then even if data was subsequently breached by sufficiently talented hackers, Target would not be negligent.

Magnuson did not invent this standard of care on-the-fly. Most states and federal courts consider a similar "duty of care balance test" to determine whether someone is responsible for harm that comes to others.

Here are three critical concepts for businesses to understand about the Target case and how it relates to their information security programs and liabilities:

1. **Look for "reasonable safeguards."** The duty of care balance test that was applied to Target is a common standard in negligence cases, and appears as the phrase "reasonable safeguards" in information security regulations such as the HIPAA Security Rule, the Gramm Leach Bliley Safeguards Rule, and regulatory actions such as FTC orders.
2. **Risk assessments are opportunities.** Information security standards require risk assessments which use the same logic as the duty of care balance test; considering foreseeable threats, likelihoods, impacts, and effective safeguards that are not overly burdensome. Businesses should think of their risk assessments as opportunities to set their level of "reasonable security" or "due care" in preparation for the tough discussions that follow a security breach.
3. **Find your own balance.** Because the duty of care balance test, regulations, and risk assessments all require that safeguards provide a balance between safety and burden, and because organizations each have unique situations, you must find your unique balance point. This will help you plan security controls and programs that make sense to your business.

In order to take advantage of this duty of care balance test, businesses should adopt a risk assessment methodology such as ISO 27005, NIST 800-30 and 800-37, or ISACA's RISK IT method. Each of these require that organizations think through foreseeable threats to information assets, that they consider likelihood and impact, and that they devise security safeguards that are appropriate to the risk, and the burdens that the safeguards create.

While designing your risk assessment, think through impacts to your organization and to others, and define levels of impact that would be considered "acceptable" or "not acceptable." When you evaluate your risks and your safeguards in terms that are considerate of you and others, you are creating the underpinnings of a security plan that is meaningful to judges, regulators and business managers alike. ■

"Target's negligence should be evaluated based on the foreseeability of the threat, the impact to others, and the reasonableness of safeguards that could have prevented the breach."