STROZ FRIEDBERG

Defending Post-Breach Class Actions: What the General Counsel Needs to Know

After a data breach or cyberattack, companies face audit committee-driven reviews, regulatory scrutiny, and class action lawsuits. General Counsel (GC) must often defend against claims of poor pre-breach security and deficient response post-breach.

THE GC SHOULD TAKE ACTION PRIOR TO AN INCIDENT

Increasingly, GCs are using their powerful positions to help companies proactively improve security and incident response readiness. The unique ability of a GC to understand how a company's security posture will be judged, post-breach, will improve security, help to identify and eliminate hard-to-defend vulnerabilities, and as a result improve companies' post-breach posture.

HOW CAN THE GC HELP? BECOME A POSITIVE VOICE IN CORPORATE CYBERSECURITY

In Stroz Friedberg's experience, post-breach claims normally allege the company did not:

Identify and remediate known vulnerabilities	Detect the full scope of a breach fast enough	Practice pre-breach IT security with due care
Kick the attacker out as quickly as it should have	Accurately report the number of customers affected	Provide customers with timely notice

THE GC SHOULD ASK THE CISO AND CIO:

- How has the company assessed cybersecurity?
  - Are there written security assessments? (Review them – they are post-breach fodder)
    - How did the company fare on these assessments? Assessments are often more harsh than IT management's own summary representations.
    - What standards were used?
    - Are assessments risk-ranked with prioritized mitigation fixes?
- Have the vulnerabilities identified in assessments been remediated or is there a mitigation program in place?
  - It's easier to defend a delay in remediation of low risk security gaps, if more critical vulnerabilities were addressed first.
- Is the company adequately prepared and defended?
  - Has the company implemented all necessary security layers? What layers of security and staffing has the CIO asked for in the past and not been able to secure funding?
  - Does the company have adequate plans, technologies, technical responders, and data breach counsel in position to facilitate incident response?
    - Some technologies take a long time to position, so this is best dealt with prior to a breach.
    - Outside counsel and technical responders should have similar approaches to incident response to avoid conflicts during an incident.
    - The GC should also ensure the company 'table-tops' (i.e., practices) its response in simulated breach drills, and that these rehearsals include all relevant stakeholders.

An outside expert's view can be an invaluable aid to determine whether pre-breach security is taken seriously overall, and to benchmarking the company against best practices.

CONTACT Americas: +1 212.981.6540 EMEA: +44 20.7061.2200 Asia Pacific: +852 3187.8800

strozfriedberg.com