ALM | LAW.COM

New York Law Journal

Hacking the Contract: How Cybersecurity Failures Can Be a Business's Best Bargaining Chip

By Charles Nerko and Xun Chen

Cybersecurity failures dominate headlines, topple CEOs, and fuel billion-dollar compliance bills. Companies treat them as the cost of doing business—or even as existential threats. But what if we have it backward? What if security weaknesses weren't mere risks to manage but profitable opportunities to exploit?

Businesses track vendors on price, performance, and delivery. Security should be no different. Most security problems originate from culpable vendors and other third parties. When they fail to safeguard information, that failure can be a financial liability. Or it can be an elegant tool to hack the underlying business relationship—providing leverage to escape a bad deal, extract better terms, restructure contracts, or drive more value.

The real power move isn't just reacting to reported breaches. It's unearthing a counterparty's security weaknesses before they become your problem.

Cybersecurity as a Core Contract Deliverable

For years, companies have treated cybersecurity as a compliance issue, something to check off a list. Contracts bury confidentiality promises deep in boilerplate, and customers rarely challenge them. That's a mistake. What if companies stopped viewing cybersecurity solely as a risk and started seeing it as a strategic asset?

Charles Nerko cnerko@barclaydamon.com

Xun Chen xchen@barclaydamon.com

Cybersecurity is a contract deliverable, just like timely shipments or product quality. If a supplier delivers defective parts, the customer has recourse. Security failures merit the same scrutiny. Yet businesses assume counterparties will self-report security lapses. Many will not.

Even leading companies fail independent audits. A 2024 study by Cybernews found that 84% of analyzed Fortune 500 companies scored a D or worse for their cybersecurity efforts, with 43% receiving an F rating. If industry leaders can't satisfy security standards, why assume others do?

The solution is obvious: assess security just like any other contract obligation. Just as companies inspect the goods they purchase, they should review their counterparties' security posture. Proactive security reviews turn vague guarantees into actionable business leverage. This strategy is particularly valuable for businesses negotiating with high-cost service providers, SaaS vendors, and legacy technology firms.

Think of it as a quality control inspection. If products don't meet specifications, you reject them or demand a credit. Why accept subpar cybersecurity?

The Case for Commissioning Security Reviews on Counterparties

Most companies wait for an incident before examining a counterparty's security posture. That's like waiting for a bridge to collapse before checking its foundation.

If you suspect you're overpaying—or stuck in an unfavorable contract—commissioning a security review on the other party might be the best way out. An independent security review can reveal substandard security practices. The results can provide documented evidence of problems that provide leverage to renegotiate, exit, or demand concessions.

This strategy is particularly valuable for companies tethered to disadvantageous agreements: ones with steep early termination fees, outdated pricing structures, unfavorable service terms, or that are no longer competitive. If a contract is otherwise ironclad, a cybersecurity failure may be the legal crowbar for a renegotiation or exit.

Yahoo's sale to Verizon is a textbook case of turning cybersecurity failures into business leverage. As Verizon was pursuing the acquisition, Yahoo disclosed two data breaches. Rather than walk away, Verizon renegotiated the deal and knocked $350 million off the purchase price.

Verizon strategically used the breaches to gain the upper hand in negotiations and extract additional value. There, the security problem wasn't just a risk; it was a bargaining chip.

The same strategy applies to ordinary commercial contracts. A counterparty suffering a breach or failing an audit shifts bargaining power in your hands. A security failure can justify an exit without termination fees, trigger renegotiated pricing, or force service improvements. Every cybersecurity failure has a price; the only question is who foots the bill.

Security Failures as Contract Killers

Business-to-business contracts often cap damages, restricting liability when things go wrong. But security failures often bypass those limits through claims of gross negligence, fraud, or trade secret misappropriation. Courts recognize that security lapses are not just a compliance issue; they can void contract protections entirely.

Courts, particularly in New York, routinely strike down liability caps when red flags of security problems are ignored—opening the door to full damages. In *Abacus Federal Savings Bank v. ADT*, 18 N.Y.3d 675 (2012), the Court of Appeals rejected an alarm company's liability cap in a business-to-business contract.

The case arose after burglars emptied a bank vault without triggering an alarm. Because the alarm company disregarded warning signs of a faulty system, the Court of Appeals found sufficient allegations of gross negligence, nullifying the liability cap.

The First Department reached the same conclusion in *Tillage Commodities Fund v. SS&C Technologies*, 151 A.D.3d 607 (2017). There, an investment fund's administrator ignored cybersecurity red flags and processed fraudulent wire transfers. The First Department found that the plaintiff's allegations of the vendor's gross negligence overrode the contract's liability cap.

For businesses seeking to escape unfavorable contracts, these cases provide a clear roadmap: if a counterparty's security lapses amount to gross negligence, contract protections may collapse.

Fraud claims can also dismantle contract limitations and provide powerful legal leverage. If a counterparty knowingly misrepresents certain security controls are in place, or that a security problem has been fixed, those misstatements could engender a fraud claim, providing ground to exit a contract or recover punitive damages.

In *IS Chrystie Management v. ADP*, 205 A.D.3d 418 (2022), a payroll company assured its customer that payroll system errors had been fixed. They hadn't. Relying on these misrepresentations, the customer continued using the flawed system, resulting in costly wage overpayments. The First Department found that the customer had a valid fraud claim, stripping away the contract's liability limitations and consequential damages waiver.

Misrepresentations about cybersecurity can also trigger claims under trade secret laws. In *Bessemer System Federal Credit Union v. Fiserv Solutions*, 472 F. Supp. 3d 142 (2020), a financial institution sued its technology provider for falsely representing that its security controls met federal banking standards. The court found that this stated a fraud claim, as well as a claim under the Defend Trade Secrets Act for improperly acquiring the financial institution's customer information.

The ruling signaled that misrepresentations relating to cybersecurity can expose counterparties to fraud and trade secret claims—opening powerful legal avenues to not only exit a contract, but also recover punitive damages, statutory damages, and attorneys' fees.

For businesses, the takeaway is clear: cybersecurity failures aren't just IT problems; they can be contract killers. They open the door to claims that strip away contractual limitations of liability, exposing counterparties to high-stakes claims. Faced with that risk, adversaries may rather settle, renegotiate, or offer financial concessions.

Businesses have long seen cybersecurity as a cost center, a compliance burden to be managed. It's time to rethink that equation. Proactively auditing counterparties and enforcing security obligations turns cybersecurity into a tool to reshape relationships and extract value. Security failures can justify renegotiating deals, terminating unprofitable contracts, and even seeking compensation.

The next time a counterparty causes a breach or fails to meet its security commitments, don't just treat it as bad news. Capitalize on the business opportunity it is.

Charles Nerko *leads the data security litigation team at Barclay Damon LLP.* **Xun Chen** *is an associate at the firm. Charles represented Bessemer System FCU in its data security litigation.*

BARCLAY DAMON LLP