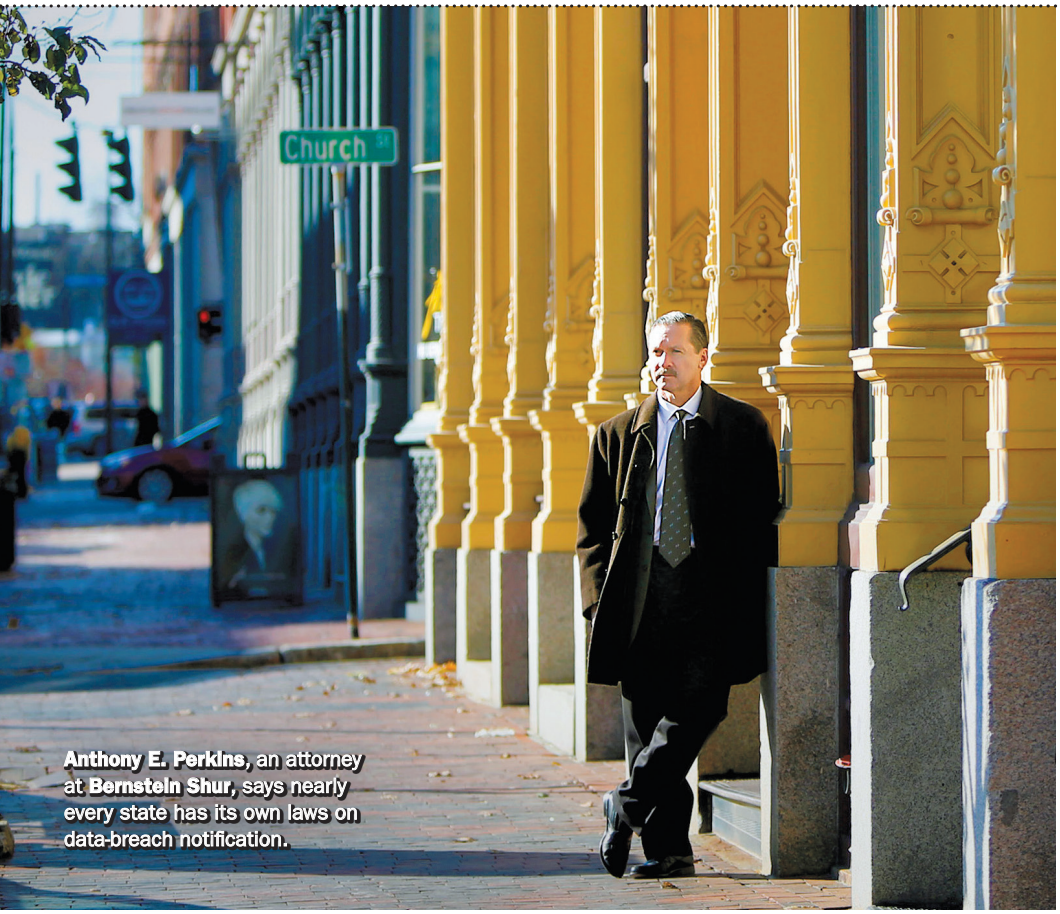
REPRINTED FROM
Mainebiz
MAINE'S BUSINESS NEWS SOURCE
December 1, 2014
VOL. XX NO. XXV
www.mainebiz.biz



Anthony E. Perkins, an attorney at **Bernstein Shur**, says nearly every state has its own laws on data-breach notification.

PHOTO / TIM GREENWAY

Protecting your domain

Big or small, cyberattacks a reality for Maine businesses

BY DYLAN MARTIN

With news of major data breaches hitting corporate giants like Target, Home Depot and Morgan Stanley in the past year, it may be easy to forget that cybersecurity issues are not just limited to big companies — even if the smaller ones believe they're well protected.

Portland-based Otto Pizza, which has grown to nine locations throughout New England in just five years, learned that the hard way when its corporate office received a phone call earlier this year from the Secret Service.

It was the second full week of August and the Secret Service had let the company know that Otto had been the target of a "point-of-sale" attack that impacted systems at its two Portland restaurants, says Eric Shepherd, Otto's director of marketing and communications.

The breach had only impacted about 3% of meal transactions between May 1 and Aug. 13. But that still meant that credit card and debit card numbers of around 900 customers were potentially exposed. So the company put all work aside and focused on the breach.

"Obviously, we were immediately horrified," Shepherd says in recalling the event, which involved working with state and federal authorities, upgrading systems and ultimately issuing communications to customers through several different channels, online and offline.

The breach was a surprise, Shepherd says, because the company had been certified as being compliant with the Payment Card Industry Data Security Standard, known as PCI, a set of protocols originally created by major card companies like Visa and MasterCard.

"We had passed [PCI certification] with no issues. Zero," Shepherd says. "As far as we knew, we were doing everything we needed to do."

As it turns out, Otto wasn't alone in thinking so. According to a report from the U.S. Computer Emergency Readiness Team, a division of the Department of Homeland Security, the Secret Service estimates that more than 1,000 businesses nationwide were impacted by the same malware that infected Otto's POS systems.

"Everyone wants to believe they're always doing what they can," Shepherd says, "but the [hackers] were targeting certain combinations of hardware and software."

Taking responsibility for 'cyber resiliency'

Otto is not alone in facing cyberattacks as a small business. The wave of cyberattacks against businesses across the board appears to be increasing.

A report published in September by Traverse City, Mich.-based Ponemon Institute found that 43% of surveyed U.S. businesses experienced a data breach that involved the loss of more than 1,000 records this year, a 10% increase over 2013. The report, which was commissioned by credit information company Experian, was based on responses from 567 executives.

On the small business side, the National Small Business Association found in its 2013 technology survey that 44% of 845 business owners said their business had been targeted by a cyberattack, whether it was a data breach or other kind of cyberattack.

For Sari Greene, the founder of Portland-based Sage Data Security, the perception that small businesses may not be vulnerable to cyberattacks has to change.

She says that means businesses should adopt the concept of "cyber resiliency," the idea that being targeted by a cyberattack is an inevitability and that businesses should invest in ways to mitigate risk and continue operations when an attack happens.