Beginning to Understand, Manage and Remedy Cybersecurity and Electronic Data Breaches

BY PHILIP BAUTISTA, AMELIA WORKMAN FARAGO & JONATHAN POLAK

In simple terms, The Merriam-Webster dictionary generally defines "cybersecurity" as measures taken to protect a computer system against unauthorized access or attack. This includes measures to prevent unauthorized access to electronically-stored data. In a world where most data is being stored electronically, cybersecurity breaches are an ever-growing concern for businesses and can result in the compromise and loss of electronically-stored data from a secure environment (a "data breach"), such as the loss of personal data, as well as confidential trade secrets and proprietary information. Cybersecurity breaches can result not only from attacks from external sources, such as hackers or viruses, but also internal sources, such as inadvertent or intentional security breaches by employees, or even businesses' own inferior security infrastructure or inadequate data security policies.

Consider this — hypothetical company ReallySuper-Secur Data Stor, Inc. (ReallySuper-Secur) is in the business of storing electronic data for other businesses, including hypothetical company, WeTrustYou, Inc. (WeTrustYou). WeTrustYou, ignoring idioms like "don't put all your eggs in one basket," contracts with ReallySuper-Secur to process and store WeTrustYou's business information, including confidential trade secrets and proprietary information, as well as WeTrustYou's customer data. The customer data includes personally identifiable information such as customer names and other sensitive information, including credit card and social security numbers. Unfortunately, ReallySuper-Secur loses the data it is storing for WeTrustYou. Perhaps the data loss occurs as a result of a hacker attack or through the misappropriation of data by one of ReallySuper-Secur's employees. Or, maybe, the loss is inadvertent, due to a misplaced mobile device, computer, storage or backup device. In any event, the loss results in disclosure of the data to unauthorized persons. Whatever the reason for the loss, the result is that ReallySuper-Secur and WeTrustYou are now facing possible legal claims from multiple potential plaintiffs.

Not only has ReallySuper-Secur likely breached its contract with WeTrustYou, but WeTrustYou may also choose to assert alternative, non-contract claims against ReallySuper-Secur, some of which are identified later in this article. Additional potential claims by WeTrustYou's customers and governmental and regulatory agencies may be asserted against both ReallySuper-Secur and WeTrustYou.

One of the first areas of focus for businesses upon a cybersecurity and data breach is notification of required persons. Akin to various federal laws and regulations requiring notification, such as the Gramm-Leach-Bliley Act, the Health Information Technology for Economic and Clinical Health Act, and the Health Insurance Portability and Accountability Act, which are sector-specific, most states have laws that impose a legal duty to notify persons whose personal data was accessed or disclosed.[1] For example, Ohio's R.C. § 1349.19 generally requires businesses that own or license computerized data including statutorily defined "personal information" to disclose any breaches of their security systems. Such disclosures must be made to any Ohio resident whose information was or reasonably is believed to have been accessed and acquired by an unauthorized person, if the access and acquisition causes or reasonably is believed will cause material risk of identity theft or fraud. The statute also specifies the timing and types of acceptable disclosures. Failure to comply with this statute's notification requirements could result in the Ohio Attorney General asserting civil actions against businesses, including civil penalties authorized under R.C. § 1349.192, starting at $1,000 for each day of intentional or reckless failure to comply. Penalties can increase based on length of time of non-compliance.

In addition to possible exposure to claims and actions by a state's Attorney General and governmental agencies, and depending upon the circumstances, plaintiffs in the position of WeTrustYou's customers have asserted a variety of other kinds of claims against businesses that lost electronic data or have had electronic data misappropriated. Among those claims are those based upon state unfair trade practice acts and consumer protection laws, as well

as common law claims, such as negligence, misrepresentation, unjust enrichment, invasion of privacy, and emotional distress claims. However, the plaintiffs' ability to demonstrate actual damages resulting from their losses is often a central focus of these cases and defendants, such as ReallySuper-Secur and WeTrustYou, may have meritorious defenses based upon plaintiffs' lack of standing, without proof of actual harm.

Another potential source of claims against businesses that obtain personal data from their customers and potential customers through their websites is the businesses' website privacy policies. For example, if WeTrustYou's website included a privacy policy, through which it warranted the secure storage of its customers' and visitors' personal data, the privacy policy and the customers' claimed reliance on the policy may become a focus of claims against WeTrustYou arising from the breach incident.

While both ReallySuper-Secur and WeTrustYou have significant exposure, they may possibly assert other causes of action arising from the data loss. For example, if they determine that one of their employees, a hacker, or other third-party intentionally accessed their computer system without or in a manner that exceeds authority, they may have a claim under the Computer Fraud and Abuse Act (CFAA), 18 U.S.C.§ 1030, which is also a criminal statute.

As discussed in our hypothetical above, WeTrustYou not only lost electronically-stored personal data of its customers but also its trade secrets and proprietary information. In addition to the ReallySuper-Secur scenario, sources both internal and external to businesses may also cause losses of electronically-stored trade secrets and protectable proprietary information. For example, employees may download and copy electronically-stored trade secrets and proprietary information in preparation for new employment, with the intent to use them for their own personal benefit or for the benefit of their new employers. Hackers may also breach businesses' cybersecurity in order to access and misappropriate its trade secrets and proprietary information. Businesses that fall victim to such acts may raise claims for misappropriation of trade secrets and proprietary information, including claims under states' versions of the Uniform Trade Secrets Act, such as Ohio's Trade Secrets Act, R.C. § 1333.61 *et seq.*, and states' versions of the Deceptive Trade Practices Act, such as Ohio's Deceptive Trade Practices Act, R.C. § 4165.01, common law unfair competition, and the CFAA, as discussed above. In addition to criminal penalties that may be imposed on the misappropriating party, victims may obtain restitution if the Justice Department prosecutes the misappropriation under the Economic Espionage Act, 18 U.S.C. § 1832.

As with most legal problems, an ounce of prevention is worth a pound of cure when it comes to avoiding cybersecurity and data breaches. In addition to ensuring appropriate technical infrastructure to avoid breaches, businesses can manage risk and mitigate the impact of cybersecurity and resulting data breaches by developing and implementing thorough written compliance and response plans. These written compliance and response plans should be tailored to the specific risks and legal requirements of the individual business and must take into account any sector-specific laws governing the type of data collected and stored. Businesses should train, hire, or contract with personnel to oversee their plans. Compliance officers and response teams should be established to oversee and execute the plans.[2]

Once the plans are in place, an important aspect of cybersecurity planning and risk mitigation is the regular review and updating of those plans. In particular, procedures relating to businesses' notification and reporting obligations upon data breaches should be regularly analyzed and modified, as the failure to make timely notifications and reporting could result not only in the imposition of penalties, but may also lead to increased damages to potential plaintiffs whose data has been disclosed. To that end, businesses should consider including basic customer notification communications that comply with applicable laws and that can be quickly updated to provide to customers within required time limitations. Cybersecurity breach planning may further include the procurement of cyber risk insurance policies, as standard business or liability insurance policies may not cover losses under cybersecurity breaches.[3]

The days of storing and warehousing large amounts of paper information are gone and businesses have adapted to a new world of electronic data storage. Businesses, and the lawyers that counsel them, must understand how to best manage electronic data, the risks involved with cybersecurity breaches, and how to avoid and respond to incidents of cybersecurity and data breaches.

[1] *See* U.S. Congressional Research Service. Data Breach Security Notification Laws (R42475; April 10, 2012), by Gina Stevens. http://www.law.umaryland.edu/Marshall/crsreports/index.html (last visited October 10, 2013).

[2] *See* concepts at *Cyber Attacks: Prevention and Proactive Responses*, Vince Farhat, Bridget McCarthy and Richard Raysman, Holland & Knight LLP, Practical Law Publishing Limited and Practical Law Company, Inc. (2011), *available at* http://www.hklaw.com/publications/cyber-attacks-prevention-and-proactive-responses-11-28-2011/.

[3] Id.

Philip R. Bautista is a partner in Taft Stettinius & Hollister, LLP's Cleveland Office and is a member of the firm's Litigation, Intellectual Property, Cybersecurity and Data Privacy, and Construction groups. He can be reached at (216) 706-3957 or pbautista@taftlaw.com.

Amelia Workman Farago is an associate in Taft's Cleveland Office and is a member of the firm's Litigation, Cybersecurity and Data Privacy and Appellate groups. Amelia represents clients in commercial disputes, including matters involving intellectual property and technology issues. She can be reached at (216) 706-3907 or afarago@taftlaw.com.

Jonathan G. Polak is a partner in Taft's Indianapolis Office and is a member of the firm's Litigation, Intellectual Property, Business and Finance, and Cybersecurity and Data Privacy groups. He can be reached at (317) 713-3532 or jpolak@taftlaw.com.