Buckle up for cybersecurity

BY MICHAEL KOKAL

Remember when cars didn't have seat belts and kids piled into the back seat? Today, that could be considered child abuse.

Our attitudes about wearing seat belts changed. We are now seeing a similar transformation in the area of cybersecurity. Cybercrime is a growing problem, and new laws, regulations, and lawsuits are going to make cybersecurity measures for computer networks as commonplace as using seat belts.

We really don't have a choice but to change our attitudes. Cybercrime is the fastest growing criminal enterprise on the planet. Last year, more than two billion records were lost or stolen, amounting to a global cost of $500 billion. That number is expected to quadruple in the next three years. The ultra-sophisticated criminal enterprises and nation states behind the crimes have been reaping profits in excess of the global drug trade. Surprisingly, small businesses with fewer than 200 employees have been the hardest hit.

Being the victim of a cybercrime may be only the start of your woes. When the department store Target suffered a well-publicized data breach, it was then hit by more than 140 lawsuits from consumers and banks whose personal and financial data were compromised. And it's not just large retailers or financial institutions which are potentially liable to customers: it is any company or business that possesses or safeguards confidential client information or customer data.

Chicago law firm Johnson & Bell was recently sued in what was believed to be the nation's first data security class action lawsuit against a law firm brought by its clients. The lawsuit alleged that Johnson & Bell's internal VPN (virtual private network) and email systems were prone to "man-in-the middle" or "DROWN" cyberattacks which could allow hackers to eavesdrop and steal confidential client information. Interestingly, the Johnson & Bell lawsuit did not allege that any actual data breach occurred.

In response to cybercrime, the state of New York just enacted unprecedented requirements for financial firms and insurance companies to protect their networks and customer data from hackers and to disclose data breaches to state regulators. Other states are expected to follow suit. Last year, Illinois passed the Personal Information Protection Act, which placed requirements on "data collectors" – broadly defined to encompass corporations, financial institutions and retail operators to use "reasonable security measures" to protect customer information from disclosure. The failure to do so could constitute an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.

Depending on the nature of your business, there may already be industry self-regulation and governmental cybersecurity guidelines that apply to you. For instance, financial services have the Financial Industry Regulation Authority (FIRA), retail has the Payment Card Industry Data Security Standard, healthcare has several standards like HIPAA and HITECH, banking has the Federal Financial Institutions Examinations Counsel (FFIEC), and insurance has the NAIC Model Cybersecurity Law.

Indeed, compliance with the myriad overlapping industry, state and federal statutes and regulations presents a daunting task for any business looking toward the future. But make no mistake: it's only a matter of time before we all are "buckled up" with cybersecurity. ◆

Michael Kokal is a partner at the lawfirm of Heyl, Royster, Voelker and Allen P.C. in Springfield.