KATZ, MARSHALL & BANKS, LLP

Study Finds Gap Between Executive Awareness and Cybersecurity Reality

By Alexis Ronickher
February 5, 2016

No business executive will deny that maintaining cybersecurity is critical for business success, particularly given the headline-grabbing cyber breaches of the last few years. Lax cybersecurity can result in the loss of critical business assets, the breach of customer information, the violation of state and federal cybersecurity laws and regulations, and all the associated legal ramifications.

A new cybersecurity study from Dimensional Research, however, finds what our whistleblower clients have been only too aware of: there is a lack of understanding and attention about cybersecurity at the top level of business.

Cybersecurity Professionals Face Uninformed CEOs

The December 2015 report found "more than half of security professionals today believe their company's security can be compromised. Yet, one third of CEOs are not regularly briefed on cybersecurity and related business risks."

The report surveyed IT professionals worldwide to capture hard data on visibility and support of cybersecurity programs at the executive level. More than 300 IT professionals responded and reported the following:

60% felt that their company's security could be breached today;
Over half of CEOs make decisions without regard to cybersecurity;
Over one-third of CEOs aren't regularly briefed on cybersecurity risks;
61% of CEOS do not know enough about cybersecurity; and
Only 39% feel they are fully supported by executives.

What Executives Don't Know Can Hurt You

These findings support our clients' experiences in raising cybersecurity issues internally. An organization's tone is set from the top, and it is no different with regard to cybersecurity. When a CEO lacks the necessary knowledge and interest in cybersecurity to adequately factor it into business planning, lower-level executives and managers know that cybersecurity is not a true priority and act accordingly.

When a whistleblower raises a cybersecurity vulnerability or threat that will be disruptive or expensive to address, those lower-level executives and managers are not willing to do the hard work of educating the CEO (or C-suite in general) as to why additional, unplanned costs and resources are required to address the problem. Instead, they all-too-often try to silence the whistleblower. If the cybersecurity whistleblower refuses to jeopardize the company's (and customers) security by letting the problem drop, the whistleblower often faces retaliation, not infrequently culminating in losing their job.

Education Can Prevent Costly Whistleblow

In our experience, when CEOs and boards of directors become aware of cybersecurity problems and related whistleblower retaliation, they take action. Unfortunately, it is usually too late to avoid liability for the unlawful retaliation, and frequently the delay also has meant that the company was needlessly vulnerable to security risks for a prolonged period of time.

CEOs can change this dynamic by doing the following:

> Cybersecurity professionals need to know that they are fully supported by their CEO, both in their day-to-day activities and when they raise serious vulnerabilities and risks internally—even when those problems may be expensive and inconvenient to fix.
>
> CEOs also need to take the time to educate themselves about cybersecurity and make decisions with cybersecurity in mind. If lower-level executive and midlevel managers know that cybersecurity really matters to a company—on a day-to-day basis—they will be less likely to quash internal reports by whistleblowers.
>
> Finally, CEOs need to make clear that retaliation against cybersecurity whistleblowers is unacceptable and puts the company at risk. A zero-tolerance policy for retaliation against whistleblowers is key, as is a company showing that it is committed to actively addressing the cybersecurity problems raised by whistleblowers.

By protecting whistleblowers, the company will have a more robust cybersecurity posture and avoid significant legal liability under the anti-retaliation provisions of statutes like the Sarbanes-Oxley Act and the Dodd-Frank Act, as well as state wrongful termination laws.