DON'T BE A YAHOO: IDENTIFYING AND MANAGING CYBERSECURITY THREATS

By Steven C. Kerbaugh and Katie Zuroski

CYBERSECURITY THREATS ARE EVER-PRESENT

The recent Yahoo! data breach, which affected more than 500 million accounts, has companies of all sizes particularly attuned to cybersecurity issues and looking for solutions. Cybersecurity – which can generally be defined as security from attacks against, or unauthorized access of, computer networks and/or data – should be on every business executive's mind. Ignoring the threats could prove disastrous.

According to IBM and the Ponemon Institute, the average cost of a data breach in the United States is $7.01 million, and the global average cost per lost or stolen record containing sensitive information is $158. Among other things, such costs result from post-breach investigation expenses, legal bills, identity protection services, regulatory compliance measures, and the implementation of new technology.

Moreover, one of the biggest financial consequences of a data breach is customer turnover due to lost trust. Lost trust and concerns about continuing security issues may also prompt civil lawsuits and government investigations. Knowing and complying with cybersecurity laws should be a top priority for any company seeking to avoid such consequences.

THE COMPLEX LEGAL FRAMEWORK SURROUNDING CYBERSECURITY BREACHES

There is a patchwork of overlapping laws and regulations relating to cybersecurity issues. For example, there are specific cybersecurity breach reporting laws in certain industries, including the health care and financial services industries. Forty-seven states have some type of breach notification laws, though they vary between states. And agencies such as the Department of Justice, Office for Civil Rights, Federal Trade Commission, and Food and Drug Administration all have the ability to investigate data breaches.

Indeed, one of the most concerning court cases affecting corporate liability for cybersecurity issues involved a government agency. *F.T.C. v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015). The FTC sued Wyndham Worldwide Corporation for failing to adequately safeguard its computer network, thereby allowing hackers to access customer information. The Federal Court of Appeals for the Third Circuit upheld the FTC's authority to sue under a provision of the FTC Act. The practical impact of the case is that the FTC can sue companies for data practices that it deems "unfair" to consumers.

This holding is problematic for corporations because "unfair" data security practices are difficult to define in the ever-changing technology sector. For example, if a company fails to fix an application vulnerability, is it unfair to consumers even if the company exceeds security expectations in other areas? Who is properly liable – the application developer, the contractor who built the website using the application, the corporation whose name is on the site, or some combination? Such questions are not settled.

In addition to agency investigations and lawsuits, companies often face private litigation, including class action lawsuits, when there has been a security breach. Typical claims asserted in such cases include negligence and bailment.

BEST PRACTICES FOR HANDLING CYBERSECURITY THREATS

Companies can and should take proactive steps to protect against cybersecurity threats. Having the appropriate safeguards and companywide processes in place will help a technology team detect breach attempts before they happen.

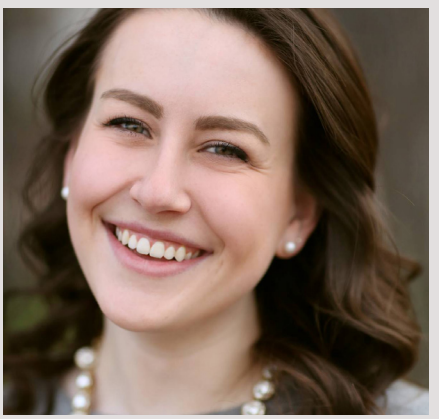
According to IBM and the Ponemon Institute, encryption decreases per-record loss by $13, and appointing a chief information security officer decreases the loss by $7 per record. The ability to prevent cyber threats can also be enhanced by increased employee awareness training, limitations on access to sensitive data sites/equipment, and forms of monitoring online activity. Such actions have been shown to decrease per-record losses as well.

Another important safeguard is insurance. Cybersecurity costs are often excluded from general liability and property insurance policies, making cybersecurity insurance essential. Having cybersecurity insurance decreases the per-record breach loss by $5.

Since hacking methods often evolve faster than companies can adapt, data breaches are virtually inevitable. It is thus crucial to have an effective breach response team. Developing procedures for detecting and responding to data breaches decreases the per-record loss due to a breach by $16.

It is also important to retain appropriate outside professionals. A public relations firm can help manage a company's image, consumer relations, and communications with the media in the event of a cybersecurity breach. Finally, it is essential for a company to have a knowledgeable legal team that is well-versed in cybersecurity laws to both provide advice regarding the state of the law and best practices, and to assist during any lawsuit or investigation should a breach occur.

Steve Kerbaugh is an attorney at Anthony Ostlund Baer & Louwagie P.A. He regularly advises businesses and represents clients during all phases of commercial litigation. Katie Zuroski is a law clerk at Anthony Ostlund Baer & Louwagie P.A. and a third-year law student at the University of St. Thomas School of Law.



TRANSFORM YOUR ORGANIZATION BY FOCUSING ON EFFECTIVENESS, IMPROVEMENT AND DEVELOPMENT OF PEOPLE AND PROCESS.

TALON
Performance Group

For change and shifts using practical expertise with transformational cheer, leaders turn to Jodi at Talon.

Jodi Standke, CEO of Talon Performance Group, is an award-winning talent management expert and entrepreneur. She has been helping entrepreneurs, professionals and leadership teams succeed for over 15 years.

Contact Talon Performance Group for a Free Consultation:
612-827-5165
www.TalonPerformanceGroup.com