Fending Off and Fighting Cybercriminals

Law Week Colorado

September 12, 2016

By Edward J. McAndrew, David M. Stauss, and Gregory Szewczyk

Barely a day goes by without a cybersecurity incident being reported in the news. Retailers, law firms, media organizations, hospitals, the federal government, and the Democratic National Committee, to name a few, have been recent victims of criminal hackers. These criminal attacks come in many different forms such as hackers accessing company servers to steal personal identifying information, credit card information, or emails.

This past year, many companies were the victims of "phishing" scams in which hackers impersonated company executives and convinced employees to wire funds to fraudulent bank accounts or to send the hackers employee W-2s so that they could file fraudulent tax returns. Ransomware incidents, which involve hackers locking businesses out of their computer systems until a ransom is paid, are also becoming commonplace.

Several tools are available to federal and state prosecutors in responding to cybercrimes, and companies can take steps to protect themselves while at the same time assisting federal and state authorities' prosecution of cybercriminals.

Federal prosecutors have at their disposal several statutes to address cybercrime. In addition to federal criminal laws, Colorado state law criminalizes many forms of hacking.

Perhaps the single most important thing a company can do to protect itself from cybercriminals is adequate preparation. Proper employee training is critical for any organization. Further, companies should implement incident response plans and use security measures such as encryption, network segmentation, continuous monitoring, and multi-factor authentication to avoid being attacked, as well as engage outside legal counsel and forensic experts who can be activated as soon as a breach is discovered.

If a breach does occur, it is critical for companies to immediately notify their outside forensic and legal experts so that they can begin an investigation, preserve relevant evidence such as network logs, and notify and coordinate with law enforcement.

Importantly, these schemes often are carried out only after an initial compromise of email accounts has occurred. Hackers often will infiltrate a company's email server and monitor email traffic waiting for an opportunity to strike. Because of this, companies should also work with law enforcement and outside vendors to investigate whether there is a larger problem that needs to be addressed.