LOEB & LOEB LLP

Privacy Law

ALERT

MARCH 2014

LOEB & LOEB adds Knowledge.

California Attorney General Urges Companies to Be Prepared for Cyber Attacks and Security Breaches

Kamala Harris, California's Attorney General, issued a set of recommendations for preventing and responding to cyber attacks and security breaches. The recommendations, called Cybersecurity in the Golden State, are directed to small and medium-sized businesses, which often lack the resources of a large IT department but are frequently the targets of cybercriminals. According to the Attorney General's office, 50% of all cyber attacks in 2012 were aimed at businesses with fewer than 2,500 employees, and 31% were aimed at those with fewer than 250 employees.

Noting that cybercrime is largely opportunistic, the Attorney General encouraged all California businesses to take the following steps:

1. Assume You're a Target

Any company, whether big or small, can be the victim of cybercrime, so assume you are a potential target and take basic precautions to protect yourself and your company.

2. Lead by Example

Cybersecurity is not simply the domain of the "IT person"; executive management has to get involved. Small business owners should dedicate the time and resources necessary to ensure the safety and security of their information assets.

3. Map Your Data

To protect your data effectively, you first need to know the types of data you have and the location of that data. Next, comprehensively review the data you have stored on your IT systems, both on-site and off, and with third parties (include backup storage and cloud computing solutions in your data mapping project). Once you know what data you have and where it is, get rid of what you don't really need.

4. Encrypt Your Data

Encrypt the data you need to keep. Machines that handle sensitive information, such as payroll or point of sale (POS) functions, ideally should be on networks or systems that are separate from machines involved with routine services like updating Facebook and checking email.

5. Bank Securely

It is essential that small business owners put security first when they engage in online banking. This means that online banking should be performed using only a secure browser connection, and you should erase your web browser cache, temporary Internet files, cookies, and history afterward, so that if your system is compromised, that information will not be accessible by cybercriminals. In addition, take advantage of the security options offered by your financial institution, and set limits on the amounts that can be wired from your accounts.

6. Defend Yourself

Guard against single points of failure in any specific technology or protection method. This should include the deployment of regularly updated firewalls, antivirus software, and other Internet security solutions that span all digital devices, from desktop computers to smartphones to tablets. Useful capabilities include the ability to remotely locate or wipe a device that's gone missing and the ability to identify and block never-seen-before attacks using technologies that analyze behavior and/or employ virtualization tools.

7. Educate Employees

Raise employees' awareness about the risks of cyber threats, mechanisms for mitigating the risk, and the value of your business's intellectual property and data. Your employees are the first line of defense, and good security training and procedures can reduce the risk of accidental data loss and other insider risks.

8. Be Password Wise

Change any default usernames or passwords for computers, printers, routers, smartphones, or other devices. Use strong passwords, and don't let your Internet browser remember your passwords.

9. Operate Securely

Keep your systems secure by using layered security defenses and keeping all operating systems and software up to date. Don't install software you did not specifically seek out, and don't download software from untrusted or unknown sources. Also remember to remove or uninstall software you are no longer using.

10. Plan for the Worst

Every small business should put together a disaster recovery plan so that when a cyber incident happens, your resources are used wisely and efficiently. Pick an incident response team and assign a leader. Make sure the team includes a member of executive management. Outline the basic steps of your incident response plan by establishing checklists and clear action items.

The Attorney General's recommendations also describe the four categories of cyber threats – social engineering scams, network breaches, physical breaches, and mobile breaches – and detailed guidance for responding to cybersecurity incidents.

If you have questions about cyber threats, data audits, or response plans, please contact Nerissa McGinn at nmcginn@loeb.com or 312.464.3130.

Advanced Media and Technology Department

KENNETH A. ADLER	KADLER@LOEB.COM	212.407.4284
AMIR AZARAN	AAZARAN@LOEB.COM	312.464.3330
IVY KAGAN BIERMAN	IBIERMAN@LOEB.COM	310.282.2327
CHRISTIAN D. CARBONE	CCARBONE@LOEB.COM	212.407.4852
TAMARA CARMICHAEL	TCARMICHAEL@LOEB.COM	212.407.4225
MARC CHAMLIN	MCHAMLIN@LOEB.COM	212.407.4855
MARGARET CHARENDOFF	MCHARENDOFF@LOEB.COM	212.407.4069
CRAIG A. EMANUEL	CEMANUEL@LOEB.COM	310.282.2262
KENNETH R. FLORIN	KFLORIN@LOEB.COM	212.407.4966
DANIEL D. FROHLING	DFROHLING@LOEB.COM	312.464.3122
NOREEN P. GOSSELIN	NGOSSELIN@LOEB.COM	312.464.3179
DAVID W. GRACE	DGRACE@LOEB.COM	310.282.2108
THOMAS A. GUIDA	TGUIDA@LOEB.COM	212.407.4011
NATHAN J. HOLE	NHOLE@LOEB.COM	312.464.3110
MELANIE J. HOWARD	MHOWARD@LOEB.COM	310.282.2143
THOMAS P. JIRGAL	TJIRGAL@LOEB.COM	312.464.3150
IEUAN JOLLY	IJOLLY@LOEB.COM	212.407.4810
ELIZABETH H. KIM	EKIM@LOEB.COM	212.407.4928
LIVIA M. KISER	LKISER@LOEB.COM	312.464.3170
JULIE E. LAND	JLAND@LOEB.COM	312.464.3161
JESSICA B. LEE	JBLEE@LOEB.COM	212.407.4073
SCOTT S. LIEBMAN	SLIEBMAN@LOEB.COM	212.407.4838
DAVID G. MALLEN	DMALLEN@LOEB.COM	212.407.4286
MICHAEL MALLOW	MMALLOW@LOEB.COM	310.282.2287
KATHERINE MASON	KMASON@LOEB.COM	212.407.4898
DOUGLAS N. MASTERS	DMASTERS@LOEB.COM	312.464.3144
NERISSA COYLE MCGINN	NMCGINN@LOEB.COM	312.464.3130
ANNE KENNEDY MCGUIRE	AMCGUIRE@LOEB.COM	212.407.4143
DANIEL G. MURPHY	DMURPHY@LOEB.COM	310.282.2215
BRIAN NIXON	BNIXON@LOEB.COM	202.618.5013
ANGELA PROVENCIO	APROVENCIO@LOEB.COM	312.464.3123
CHRISTINE M. REILLY	CREILLY@LOEB.COM	310.282.2361
KELI M. ROGERS-LOPEZ	KROGERS-LOPEZ@LOEB.COM	310.282.2306
SETH A. ROSE	SROSE@LOEB.COM	312.464.3177
ROBERT MICHAEL SANCHEZ	RSANCHEZ@LOEB.COM	212.407.4173
T.J. SAUNDERS	TSAUNDERS@LOEB.COM	312.464.3174
ALISON SCHWARTZ	ASCHWARTZ@LOEB.COM	312.464.3169
BARRY I. SLOTNICK	BSLOTNICK@LOEB.COM	212.407.4162
REGAN A. SMITH	RASMITH@LOEB.COM	312.464.3137
BRIAN R. SOCOLOW	BSOCOLOW@LOEB.COM	212.407.4872
WALTER STEIMEL, JR.	WSTEIMEL@LOEB.COM	202.618.5015
AKIBA STERN	ASTERN@LOEB.COM	212.407.4235
JAMES D. TAYLOR	JTAYLOR@LOEB.COM	212.407.4895
MICHAEL A. THURMAN	MTHURMAN@LOEB.COM	310.282.2122
JILL WESTMORELAND	JWESTMORELAND@LOEB.COM	212.407.4019
DEBRA A. WHITE	DWHITE@LOEB.COM	212.407.4216
MICHAEL P. ZWEIG	MZWEIG@LOEB.COM	212.407.4960