Advisory

NOVEMBER 2014

If you have any questions about this Advisory, please contact:

JOHN KENNEDY
203.363.7640
jkennedy@wiggin.com

PATRICK LAMONDIA
203.498.4398
plamondia@wiggin.com

MICHAEL MCGINLEY
203.363.7638
mmcginley@wiggin.com

California Reports 600% Increase in the Number of Individuals Affected By Data Breaches

On October 28, 2014, the California Attorney General released a report revealing that more than 18.5 million California residents were victims of data breaches in 2013.[1] That statistic represents a staggering 600% increase over the number of Californians affected by data breaches in 2012[2] and echoes similarly gloomy data breach statistics reported earlier this year by data security researches at Verizon,[3] PwC,[4] and the Ponemon Institute.[5]

Collectively, these reports highlight a national trend: U.S. businesses are struggling to adequately secure the personal information on their networks.[6] Despite the explosion of data breaches, companies generally have not adapted their business practices to prevent breaches or mitigate the harm that they cause to consumers. Further, the reports indicate that companies continue to view and manage cybersecurity risk as an information technology matter and not as an issue mandating direct boardroom attention.[7] This is a dangerous approach.

THE RISK IS UNIVERSAL

The reports illustrate that an alarming wave of cyber-related incidents is occurring throughout the country.[8] In fact, the Ponemon Institute found that 43% of the companies it polled had been involved in a data breach, an increase of 10% over the prior year.[9] The same study found that even though the number of companies with data and privacy policies has improved, most companies believe that they are ill-equipped to deal with the consequences of a data breach.[10]

THE COSTS ARE REAL

The costs associated with data breaches are also on the rise. The Ponemon Institute found that the average cost associated with a data breach increased over the last year from $136 to $145 per record.[11] The average total cost of a data breach for a company in 2014 was $3.5 million dollars.[12]

Data breach costs include both the direct and indirect costs associated with a breach. Direct costs include the cost of investigating the breach, providing credit monitoring services, and paying fines or penalties. Some costs, including fines imposed by state and federal enforcement agencies, are widely publicized and allow companies to engage in purposeful risk evaluation. For example, in October 2014 TD Bank reached an $850,000 multi-state settlement, led by Connecticut's Office of the Attorney General, to resolve a 2012 data breach involving the exposure of the personal data of 260,000 customers resulting from the loss of unencrypted backup tapes.[13] Companies easily can compare their own situations to the facts that led to fines and penalties levied in previous enforcement cases. Companies may be less prepared for the indirect costs associated with a breach, including the loss of current and future customers and the increased cost of acquiring new customers.[14]

CONTINUED ON NEXT PAGE

California Reports 600% Increase in the Number of Individuals Affected By Data Breaches

Together, the direct and indirect costs of data breaches are often substantial. In fact, in 2013, breaches cost organizations doing business in New York more than $1.3 billion dollars,[15] which is itself a conservative estimate because many data breaches are never reported.

RECOMMENDED PRACTICES

These reports illustrate that companies face a growing risk of being confronted with a cyberincident. Given the rising costs associated with these events, businesses must be prepared to prevent and respond accordingly.

Every organization and industry faces unique challenges regarding data breaches. The following recommendations, gleaned from the aforementioned reports and our professional experiences, are best practices that should be considered by all organizations.

ESTABLISH PROPER GOVERNANCE PROCEDURES

- Preparation begins in the corporate boardroom—cyber security cannot be managed solely as an IT matter but rather must be seen as a risk to be managed at the highest levels.
- Board and management oversight and accountability must accompany cyber failures and losses.

ESTABLISH AN INFORMATION SECURITY PROGRAM

- Implement an information security program that includes a written information security plan.
- The NIST Cybersecurity Framework developed is being considered by some industries and the government as a possible unified process benchmark for cyber security—understand what the Cybersecurity Framework is and how it applies to your security program.[16]
- Perform periodic risk assessments and revise your privacy and information security practices based on the results.
- Research which types of threats your industry is most vulnerable to and adapt your practices accordingly.
- Ensure that the hardware and software used by your organization are updated with the latest security patches.

ESTABLISH DATA HANDLING PROCEDURES

- Understand the information that your business collects, where it is stored, how it is used, and who can access it.
- Minimize the collection of unnecessary information.
- Ensure that information is not retained past its useful life.
- Employ strong encryption solutions to protect sensitive information on laptops, desktops, external hard drives, and mobile devices.
- Employ strong encryption solutions to protect data traveling over public and private networks.
- Devalue consumer financial information by using tokenization and encryption technologies.
- Work with your suppliers, especially financial institutions, to ensure that shared consumer information is protected.

PREPARE FOR INCIDENT RESPONSE

- Create and practice executing an incident response plan that emphasizes notifying affected individuals in the most expedient time possible, without unreasonable delay.
- Identify an incident response team that includes members of senior management as well as legal and information technology experts.
- Provide victims of data breaches with free mitigation services such as credit monitoring.
- Improve the readability of breach notices by removing "legalese."
- Consider using substitute notices for payment card data breaches.

The recent spate of cybersecurity incidents plaguing businesses is unlikely to decrease in the near future. Companies today have access to massive amounts of data that must be secured during use, transmission, and storage. For a host of reasons—some malicious, some accidental—portions of this data inevitably will be lost. While there is no method short of ceasing business operations to eliminate this risk, implementing the recommendations above will help manage risk appropriately.

CONTINUED ON NEXT PAGE

California Reports 600% Increase in the Number of Individuals Affected By Data Breaches

[1] Kamala D. Harris, California Data Breach Report, California Dep't of Justice, iv (Oct. 2014), http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf?.

[2] Id. at iii.

[3] 2014 Data Breach Investigations Report, Verizon (2014), http://www.verizonenterprise.com/DBIR/2014/.

[4] Managing cyber risks in an interconnected world, PwC (Sept 30, 2014), http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

[5] Ponemon Institute, 2014 Cost of Data Breach Study, IBM (May 2014) (Ponemon I), http://public.dhe.ibm.com/common/ssi/ecm/en/sel03027usen/SEL03027USEN.PDF.

[6] Breaches at Target and LivingSocial alone were responsible for a combined 120 million exposed records nationwide in 2013. Harris, supra at iv.

[7] According to the PwC report, less than half of corporate boards actively participate in the overall security strategy. PwC, supra at 28.

[8] Like California, the State of New York also had a 'record-setting' year in 2013—data breaches exposed the records of 7.3 million New Yorkers. Eric T. Schneiderman, Information Exposed: Historical Examination of Data Breaches in New York State, New York Office of the Attorney General, 1 (2013), http://www.ag.ny.gov/pdfs/data_breach_report071414.pdf.

[9] Ponemon Institute, Is Your Company Ready for a Big Data Breach, Experian, 1 (Sept. 2014) (Ponemon II), http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf.

[10] Id. at 18.

[11] Ponemon I, supra at 1.

[12] Id.

[13] Attorney General, Department of Consumer Protection Announce $850,000 Multistate Settlement with TD Bank Over Data Breach, State of Connecticut Dep't of Consumer Affairs (Oct. 16, 2014), http://www.ct.gov/dcp/cwp/view.asp?Q=555024&A=4187.

[14] See Ponemon II, supra at 3.

[15] Schneiderman, supra at 1.

[16] NIST Cybersecurity Framework, http://www.nist.gov/cyberframework (last visited Nov. 5, 2014).