Foster Garvey

Duff on Hospitality Law

New Reports Offer Key Insights into Data Breach Patterns and Costs – Hospitality Industry Remains a Primary Target

on 4.17.15 | Posted in Data Privacy

Benjamin Lambiotte, technology and data privacy attorney in Garvey Schubert Barer's D.C. office, shares key points from two significant survey reports analyzing trends in data security breaches during 2014 that were released this week; one from Verizon, and the other from IBM and the Poneman Institute. It should come as no surprise to anyone that once again, the hospitality industry is featured prominently in both reports. Thank you, Ben! – Greg

The Verizon report studies in depth the industry sectors most frequently targeted and affected, the nature of current threats, and causes and consequences of actual data breaches. The Poneman report focuses on costs associated with successful attacks. Both are worth a close read. Together, the reports starkly illustrate the increasing pervasiveness, complexity and costs associated with preventing and responding to data breaches. The good news is that they also provide guidance on effective preventive and cost control measures.

Here are some of our key takeaways and observations from these fascinating reports:

No Organization or Business is Immune from Attack, but Some are More Frequent Targets Than Others

- In terms of volume of security incidents by sector, the top ten (in order) were government entities, information, financial services, manufacturing, retail, hospitality, professional services, health care, and other services.
- Actual data breaches (attack succeeds; data lost or compromised) occurred most frequently (in order, by sector) in: government, financial services, manufacturing, hospitality, retail, professional services, health care, information, education, and other services.
- In certain industry sectors, cyber criminals more frequently breach smaller businesses. Smaller hospitality businesses, by far and away, ranked number one, with retail second. Financial services remains the number one large business target, followed by large retail,

and health care.

- Certain industry sectors are more frequent targets of certain types of threats. For example, the hospitality industry is particularly susceptible to Point of Sale (POS) intrusions. Verizon reports that 91% of data breaches in that sector were POS intrusions. The POS credit card systems used in that industry have of late been plagued by a new breed of malware (including PoSeidon) that burrows deep into the system and "scrapes" card data momentarily stored in RAM. "Insider" threats (errors and abuse of access privileges) are more prevalent in health care than other industries. Financial institutions are particularly vulnerable to "crimeware" and web application hacks. Businesses should calibrate their risk management approaches to the specific types of threats they face.

Dealing With a Data Breach is Expensive -- the More Records Compromised, the More it Costs

- Poneman predicts that the average per record mean cost of a data breach will be $201 per record, an increase over the past two years. Such costs include lost customers, and expenses of dealing with the breach. Relative costs depend on the scale of the breach. Verizon predicts that breaches of 1,000 records will result in losses between $52,000 and $87,000, and that breaches of 10 million records will result in losses of between $2.1 to $5.2 million.
- Certain industries have higher data breach costs than others, with regulated industries having a higher per capita record costs than non-regulated businesses. The highest relative per capita data breach costs (in order) are in the health care, transportation, education, energy and financial sectors.

The Most Frequent Ways Cybercriminals Gain Access is Through Dumb Stuff We Do or Don't Do

- In order to steal or compromise sensitive data, cybercriminals have to get at it. The most common way they breach the castle continues to be "phishing" and "spearphishing." "Phishing" involves baiting a system user to respond to an official-looking e-mail asking for a reply "verifying" a password or account number. "Spearphishing" is a variation where the e-mail also resembles a routine communication from a trusted sender, but invites the recipient to click on a web link or open an attachment whose payload is malware. The stats are sobering. Fully 23% of e-mail recipients open phishing e-mails, and 11% click on the malware payload. 50% of the time, this happens within an hour after the "seafood" e-mail arrives. A phisher who sends out this kind of chum generally only has to wait 1.22 seconds before some sucker somewhere takes the bait.

- Another prevalent way cybercriminals get at sensitive data is an organization's failure to install "patches" for known security vulnerabilities. The stats here are also depressing. In 2014, half of exploited vulnerabilities were defeated within less than a month after becoming known. But in 99% of the cases where a known vulnerability was exploited, a patch had been available for a year or more! Due to failure to implement available fixes, hackers continue to be able to exploit well-known "oldie but goodie" vulnerabilities.
- Plain old human error is another major inroad for hackers. 60% of incidents were caused by internal staff sending sensitive information to the wrong person, putting sensitive data on publicly accessible servers, or disposing of sensitive medical or personal data in insecure ways. Also, people forget or lose mobile devices containing sensitive data in an insecure environment all too frequently.
- While technological countermeasures are necessary, a focus on human factors – the loose nut behind the keyboard – is at least as important. Training and awareness, and practices designed to mitigate our natural tendencies to make the type of mistakes that frequently give hackers keys to the castle, are a key part of any data breach risk management strategy.

Certain Specific Measures Can Reduce the Cost of a Data Breach When it Occurs

- The Poneman report documents that certain types of expenditures can reduce the overall cost of data breach. Having in place before the breach a strong security posture, a Chief Information Security Officer with responsibility for data protection, and a defined incident response plan all reduce the per capita record cost of a breach. It makes sense that planning and investing resources before an incident occurs can save money when it happens.

If you have any questions about these reports, or for more information on data security, please feel free to contact me or Ben, directly.

Tags: Data Breach, data privacy, Poneman institute, Verizon