CYBERRISKS+LIABILITIES

IN THIS ISSUE

5 Key Takeaways From Ponemon's 2016 Cost of Data Breach Study

Ponemon's 2016 Cost of Data Breach Study is out. Read on to learn five key lessons gleaned from the report.

Circuit Court Rules That Password Sharing Violates Federal Law

The 9th U.S. Circuit Court of Appeals upheld the conviction of a man who used a borrowed password to access a database. Does that mean sharing passwords for Netflix is criminal?

48 Percent of People Traded Their Passwords for Candy From Strangers

Researchers at the University of Luxembourg used social engineering—and chocolate—to get people on the street to turn over their passwords.

BALDWIN KRYSTYN SHERMAN

5 Key Takeaways From Ponemon's 2016 Cost of Data Breach Study

According to the 2016 Cost of Data Breach Study from the Ponemon Institute, the average total cost of a data breach for a U.S. company is now $7 million. There are a number of key takeaways from this report:

- **The average cost of a data breach hasn't fluctuated much in recent years.** While this year's average cost is nearly double the average cost in 2006, the average total cost of a data breach has averaged just below $6.5 million since 2008.
- **Lost business costs companies more than costs directly related to the data breach itself.** On average, stolen records cost a company $221 per record. Of that, $76 represents direct costs like technology or legal fees, while $145 is allocated to indirect costs, like abnormal turnover or churn of customers.
- **Malicious attacks remain the most common cause of data breaches.** Roughly half of all data breaches are the result of malicious attacks. As a result, these data breaches are more costly than those that are the result of other causes, like system glitches or human error.
- **Data breach costs vary by industry.** The health care sector's per capita cost for each stolen record was $402, well above the $221 average. By contrast, the per capita costs for those in government or hospitality were $148 and $86, respectively.
- **Costs can be either increased or reduced by taking certain measures.** Having an incident response team can lower the per capita cost by almost $26 dollars. In contrast, third-party breaches increased the per capita cost by just over $20 dollars.

FBI Director Recommends No Charges be Filed in Clinton Email Case

FBI Director James Comey recommended that the Department of Justice (DOJ) not file any charges against Hillary Clinton regarding the possible mishandling of classified materials on her personal email server while she served as secretary of state. Comey clarified that, while he wouldn't recommend any charges be filed, Clinton engaged in behavior that was "extremely dangerous."

He further claimed that someone in a position like Clinton's should have known better than to discuss sensitive and classified materials in unsecured email exchanges, and that doing so while traveling abroad could have exposed sensitive materials to hostile parties. Still, given the scope of the exposure, lack of intent to expose secrets and lack of evidence of a cover-up, Comey said that prosecuting such a case would be highly unusual.

Hackers Selling Access to the Computer Systems of 70,000 Companies

Cyber security firm Kapersky Lab announced last month that it had uncovered an online marketplace where criminals were selling access to more than 70,000 corporate and governmental computer systems—some for as little as $6 each.

They suspect that the hackers behind xDedic, the name of the online forum, are likely Russian-speaking hackers who've transformed their business model from selling passwords themselves to hosting a forum and allowing others to sell, while collecting a small commission on each transaction. Such a marketplace, experts warn, signals a continuing evolution in the cyber crime community—one where marketplaces like this one allow low-skill criminals to purchase system access directly from more sophisticated criminals.

DHS and DOJ Issue Final Guidance for CISA

Last month, the Department of Homeland Security (DHS) and the Department of Justice (DOJ) released procedures for federal entities pertaining to the Cybersecurity Information Sharing Act (CISA). Additionally, they released guidance for non-federal entities, to assist in their sharing of records with federal entities. Both documents reflect the interim guidance that the agencies released in February.

Circuit Court Rules That Password Sharing Violates Federal Law

In a ruling that appears to declare password sharing a federal crime, the 9th U.S. Circuit Court of Appeals recently upheld the conviction of a man who used a borrowed password to gain access to his former employer's database.

The case involved a man named David Nosal, a former employee of Korn/Ferry International, a research firm. Nosal was convicted under the provisions of the Computer Fraud and Abuse Act (CFAA) when he used a former co-worker's password to access one of the firm's databases. The CFAA—a piece of legislation designed to combat hacking—makes it a crime to access a system without "authorization." The court ruled that, since Korn/Ferry didn't authorize Nosal to use the password, his access was unauthorized, and the court upheld the conviction.

However, some analysts are worried that the court's ruling could set a dangerous precedent. As a dissenting opinion in the ruling notes, CFAA doesn't define who has the authority to authorize access to a system or the use of a password. Civil liberties advocates warn that if the company issuing the password—rather than the user of that password—determines "authorized" use under CFAA, millions of Americans could theoretically be jailed for sharing accounts for things like Netflix, Facebook or Spotify.

The ruling will be binding for other decisions in the 9th Circuit—which covers much of the West Coast and includes Silicon Valley—and will likely be consulted by judges in other courts around the country.

48 Percent of People Traded Their Passwords for Candy From Strangers

A pair of psychologists from the University of Luxembourg—armed with nothing more than University of Luxembourg bags and a large supply of chocolates—convinced nearly half of those who received the candy to turn over their personal passwords.

The psychologists did so to study the effects that giving a small gift—in this case, the chocolate—would have on achieving compliance. Gift-giving is one tactic that falls under the umbrella term "social engineering," and has been a tool that is gaining more popularity among hackers.

For more information on social engineering and how to guard your organization against it, contact Baldwin Krystyn Sherman Partners today.

Baldwin Krystyn Sherman Partners
4010 W. Boyscout Blvd., Suite 200
Tampa, FL 33607
813-984-3200
http://www.bks-partners.com/