The Academy
The Health Management Academy

CONSUMER ANALYTICS | CYBERSECURITY

Jarrett Lewis | Executive Director, Consumer Research | The Health Management Academy
Corey Aferiat | Senior Director, Financial Forums | The Health Management Academy

A recent string of attacks waged on hospitals and large health systems has elevated the focus on cybersecurity in healthcare. While health systems are clearly beginning to understand the extent of cybersecurity as an enterprise risk, little information is available on how consumers view the impact of cyberattacks in healthcare. In order to shed light on this issue and understand the potential reputational damage associated with an attack, The Health Management Academy/RBC Capital Markets first quarter *Consumer Health & Information Technology* survey measured consumer attitudes and perceptions around cyberattacks on hospitals and health systems.

Cyberattacks have become one of the top business threats for companies globally. According to a Center for Strategic and International Studies (CSIS), companies worldwide are losing $445 billion a year due to cybercrime.[i] Liability issues, loss of key business information, productivity, and revenue all stand as potentially detrimental consequences of an attack.

Key Findings

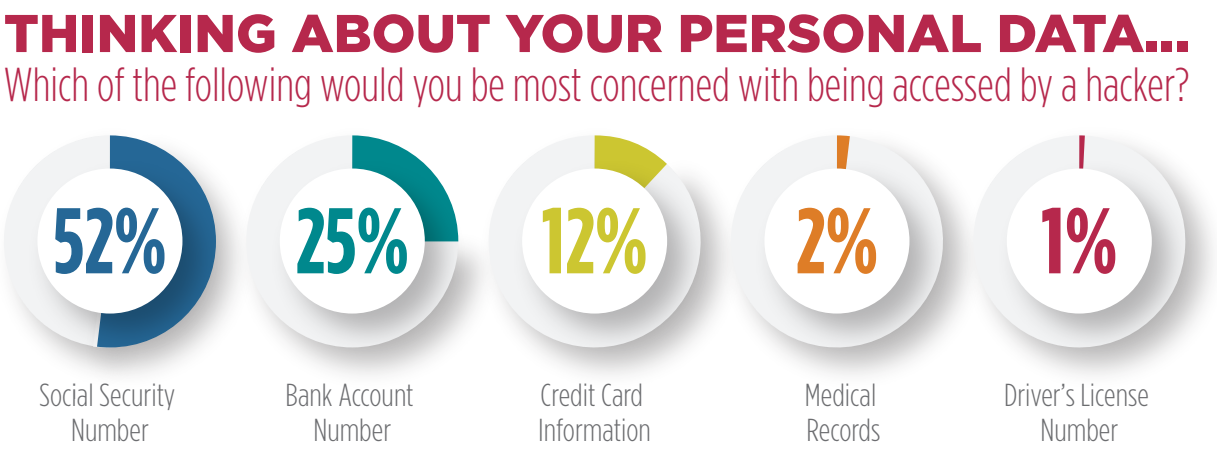
- Consumers are not nearly as concerned about a breach of their medical record information as their banking or social security information. (Figure 1.)
- However, nearly one-half (45%) of Americans say they would be less likely to return to a provider if it was the subject of a security breach. (Figure 3.)
- Only 1 in 10 Americans are aware of their medical records ever being hacked or exposed, despite the fact that nearly 1 in 3 Americans have had their medical information hacked, breached or exposed. (Figure 2a & Figure 2b).

Medical Record Security: Perception Versus Reality

Perhaps an extension of the lack of transparency in healthcare broadly, Americans largely have misconceptions about the level of protection and relative importance of their personal medical information. It is well documented that medical records are among the most valuable pieces of information exchanged on the black market – some estimates suggest they are 10 times more valuable than the cost of stolen credit card or banking information.[ii]

However, when respondents were asked whether they were more concerned with losing their social security number, financial information, or medical records, they overwhelmingly feared the loss of their social security number and financial information. As Figure 1 illustrates, 52% of consumers were most concerned about their social security number, 25% their bank account number, 12% their credit card information. Only 2% of respondents were most concerned about losing their medical records to a hacker, statistically even with concern over the loss of a driver's license number.

Figure 1. Top Hacking Concern



According to the U.S. Department of Health and Human Services, more than 100 million records were hacked or exposed in 2015. In the case of the breach at health insurer Anthem, the personal information of up to 78.8 million individuals was exposed.[iii] While nearly 1 in 3 Americans have had their medical information compromised (Figure 2b), The Academy survey found just 1 in 10 Americans aware of their medical information ever being hacked or exposed (Figure 2a).

Figure 2a.

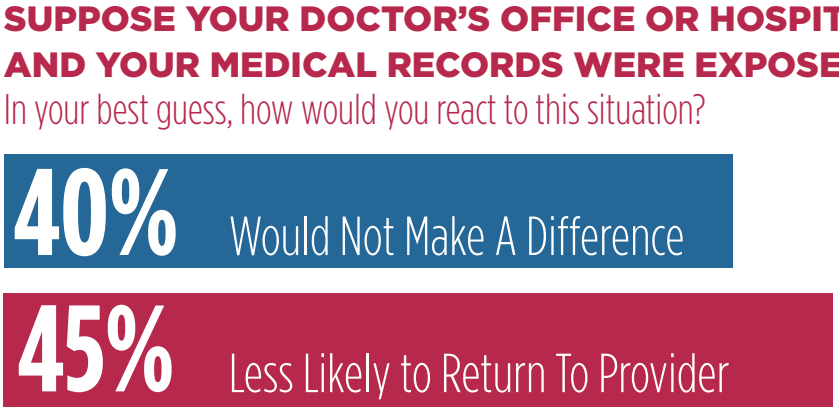
Figure 2b.

What is the Reputational Risk to Providers?

In 2015 more than 95% of the exposed medical records stemmed from attacks on health insurers. As a result, consumers generally believe their healthcare provider is doing a good job of protecting their medical records from cyberattacks, as 80% of the survey respondents said their medical provider was doing well to protect their medical records. However, high expectations bring harsh reactions in the event of a breach.

As Figure 3 illustrates, an astonishing 45% of Americans say they would be less likely to go back to their doctor's office or hospital in the event of a hack of that provider.

Figure 3. Impact of Medical Record Hack



Self-insured consumers and younger consumers are among the most likely to depart from their providers. Conversely, patients with a chronic disease and consumers living in rural areas are less likely to switch providers (Figure 3), given more frequent contact with providers and potential access issues, respectively.

Figure 4. Impact of Medical Record Hack By Groups

	18-34	35-44	45-54	55-64+	65+	White	Hisp.	AA
Less Likely	57%	56%	51%	36%	24%	41%	54%	53%
No Difference	31%	31%	34%	41%	61%	42%	34%	34%

	Parents	Non-Parents	Urban	Suburban	Rural	Chronic Disease	No Chronic Disease
Less Likely	55%	40%	48%	45%	37%	38%	50%
No Difference	36%	42%	36%	39%	47%	49%	35%

For organizations outside of the healthcare industry, it is clear major data breaches have caused severe reputational damage. Target's customer traffic fell by nearly 25% in the month following its 2013 breach and its 4th quarter net income fell 45% from the year before. The attack against eBay in 2014 was one of the largest ever, with data of 145 million customers exposed. A YouGov survey taken shortly after the hack revealed a significant drop in the brand's reputation.[iv]

Both of these retailers (and others) eventually rebounded from their data breaches. However, unlike the retail business, healthcare patient provider relationships are unique and represent a sacred trust. Accordingly, providers are held to the highest standard. Surveys consistently show nurses and doctors are among the most trusted professions and hospitals are among the most trusted institutions. Accompanying that trust are elevated expectations. Consumers simply expect more from their doctor and their hospital. While a data breach would be costly due to HIPPA fines and legal fees, these data reveal an additional and potentially severe cost of reputational damage and patient defection.

Conclusion

The legal, financial, and operational risks of cyberattacks are becoming better known but the reputational risk of a severe attack is largely unknown.

Consumer misinformation regarding the value of medical information could elevate the reputational risk to providers in the event of an attack or breach. When consumers better understand the extent to which valuable information might be obtained from their medical records, they are likely to grow more concerned.

Consumers have high expectations for their providers when it comes to both their medical care and the security of their medical records. If a breach occurs, they may not hesitate to switch providers. As they become more informed, the risk to the enterprise will continue to rise.

Methodology

The Health Management Academy conducted a national survey of 1,500 adults, April 5-9, 2016. The survey was conducted using a blend of live landline telephone interviews and web-based interviews. The data were weighted to approximate a national sample of adults based on gender, age, ethnicity and region.

The survey has a margin of error of ±2.53% at a 95% level of confidence. Results based on smaller sample sizes of respondents—such as gender or age—have a larger margin of error.

References

[i] Center for Strategic and International Studies. Net Losses: Estimating the Global Cost of Cybercrime. Report. June 2014. Accessed April 18, 2016. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

[ii] "Your medical record is worth more to hackers than your credit card." Reuters. 2014. Accessed April 20, 2016. http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

[iii] "Anthem: Hacked Database Included 78.8 Million People." Wall Street Journal. 2015. Accessed April 21, 2016. http://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364

[iv] "Here's who's been hacked in the past two years." Fortune. 2015. Accessed April 20, 2016. http://fortune.com/2015/10/02/heres-whos-been-hacked-in-the-past-two-years/