For CEOs: How Safe Is Our Business's Online Data? The 10 Best Questions

Highlight

Think an online security breach won't happen on your watch? Think again and assess your risks with these 10 questions.

The 10 Best Questions

This is the shorthand version. The experts' suggested best answers are below.

1. Are we a target for a data breach event? What kinds of hacks could happen here?
2. What are the consequences if our customers' sensitive information is compromised?
3. How much important, private, or sensitive do we have?
4. What are we doing to prevent or mitigate hacks and natural disasters?
5. Do we have a detailed, concrete, written plan for the worst case scenario of hackers gaining access?
6. How quickly do we need to recover lost data? How often does the data change?
7. Should we develop a protocol to handle an after-hours security breach?
8. If we do get hacked, what data of mine are at risk?
9. Do we need cyber risk insurance?
10. How often do we schedule IT assessments or audits by independent, third-party experts?

The Golden Question

The million-dollar question you almost forgot to ask.

Are we ignoring the warning signs of pending data breaches?

The 10 Best Answers

1. Are we a target for a data breach event? What kinds of hacks could happen here?

Almost certainly yes, Feris Rifai, CEO of security outfit Bay Dynamics told the NBC's Today Show. Breaches may not be preventable, adds Rifai, but their damage can be minimized.

Bob Gregg, CEO of a data breach prevention firm writes for *Forbes* that many companies focus on outside hacking threats, but they should also be alert to less notorious but often deadly breaches caused by a lost hard drive or laptop. The enemy is within, too. "If you have employees that use mobile devices, then your risk of breach is very high," warns Gregg.

2. What are the consequences if our customers' sensitive information is compromised?

Data breaches are much cheaper to prevent than clean up. After a breach, most companies funnel significant unbudgeted funds into cleaning up the mess.

The loss of customer goodwill is one of the highest costs of data breach. According to Gregg, "Sixty-three percent of breach costs are a direct result of lost business. The bottom line is that a data breach can unravel your business and destroy the very fabric of a hard-built reputation."

Related: Reputation Management for Businesses: The 10 Best Questions

3. How much important, private, or sensitive data do we have?

The nonprofit Identity Theft Resource Center reports more than 5,000 breaches and 675 million records have been exposed since 2005. Massive data breaches get the most attention.

Examples include the hacking of 77 million Sony user accounts, Anthem's 2015 loss of 80 million client names and social security numbers, and the loss of 70 million Target customers' financial accounts.

But smaller breaches can also be costly, such as lawsuits about patients' lost medical records or a disgruntled former employee angry over mishandled internal personnel records on insurance, medical or banking accounts. What you may dismiss as a minor breach, could matter tremendously to others.

4. What are we doing to prevent or mitigate hacks and natural disasters?

Proactive strategies include these recommendations from security experts:

- Password protect *everything* worth stealing
- Practice strong password discipline company-wide, no exceptions
- Archive copies of backup tapes and software to restore operational systems off-site
- Offer advanced training for IT managers
- Educating employees on proper procedures for sophisticated threats

Related: How to Hire the Best IT Specialists: The 10 Best Questions

5. Do we have a detailed, concrete, written plan for the worst case scenario of hackers gaining access?

The more detailed, the better. Your company's cybersecurity plan should include procedures for how and when a breach will be publicized, who will be responsible for overseeing the event, and what services and/or protections (such as identity theft or credit protection) will be offered to affected customers and employees.

Once this document is written, don't throw it into your bottom drawer. Assign the task of regular, frequent reviews to your top IT. Personally stay in involved.

6. How quickly do we need to recover lost data? How often does the data change?

The frequency of data change helps to determine your backup schedule. Daily changes require daily backups.

In an article about designing backup strategies, *TechNet Magazine* advises, "Time is an important factor in creating a backup plan. For critical systems, you might need to get back online swiftly. To do this, you might need to alter your backup plan."

7. Should we develop a protocol to handle an after-hours security breach?

This Best Question was suggested by tech expert David Papp, author of *IT Survival Guide: Conquering Information Technology in Your Organization*. This may or may not be relevant for your company's business hours, but don't overlook the potential for natural disasters affecting your location.

Investigate your need for a Business Continuity Plan, drafted either in-house or by external consultants. This plan should include the tools and steps your business will need to bounce back after a cybersecurity breach, a hurricane, and everything in between.

8. If we do get hacked, what data of mine is at risk?

As the CEO, your own accounts and those of your senior staff need special attention.

For example, if you keep your email on company servers a security breach could easily pull in your Outlook emails, cloud accounts, Dropbox folder, Google calendar, and other innocuous daily online tools.

Information security expert Ian Amit told the Today Show: "The human element is critical in cyber security. Security teams need to be educating their people on safe practices and testing their organization for behavioral vulnerabilities."

Related: Protect Your Personal Information from Online Identity Theft: The 10 Best Questions

9. Do we need cyber risk insurance?

Cyber and data breach insurance is an exploding industry as a hacker counterattack. But Gregg warns that policies vary widely and coverage may be less than ideal.

He says, "The very insurance policy you purchase may be at odds with your organization's culture of protecting customers. There are limitations on serving customers' needs and protections from customer lawsuits. None will cover lost business from defecting customers."

Related: What to Consider When Purchasing Business Insurance: The 10 Best Questions

10. How often do we schedule IT assessments or audits by independent, third-party experts?

Keep the possibility of a serious breach on your radar. Even if you have a crackerjack internal IT team, data security requires an objective outsider's assessment. This process will help you understand the scope of potential problems, lock down data, and look at regulatory and compliance requirements.

Gregg recommends, "External experts can inventory all of the private, sensitive information in your organization and create a breach response plan that will protect you."

The Golden Question

The million-dollar question you almost forgot to ask.

Are we ignoring the warning signs of pending data breaches?

Gregg believes that businesses and senior managers need to listen to the concerns raised by their IT personnel, in-house privacy specialists, and security officers.

Target's handling of its 2014 massive breach illustrates the consequences of not asking this question. Bloomberg BusinessWeek reports that Target ignored warnings about a possible intrusion, according to interviews with Target's own data security operation personnel.

A Target spokesperson said at the time, "We are investigating whether, if different judgments had been made, the outcome may have been different."

Related: The 10 Worst Questions You Can Ask About Your Business's Cybersecurity

QDoc's Q-Tipsters

Deny digital dangers and be damned. What you don't ask can hurt you.

References

1. American Society of Pension Professionals & Actuaries, “Ask Yourself About Online Security,” January 15, 2015, http://www.asppa-net.org/News/Browse-Topics/Sales-Marketing/Article/ArticleID/4099

2. Bankrate.com, “10 Tips to Computer Security,” by Cheryl Allebrand, http://www.bankrate.com/finance/financial-literacy/10-tips-to-computer-security-1.aspx

3. *Blast Magazine*, “Tips to Keep your Private Mobile Data Private,” by Adam Morley, December 12, 2013.

4. *Bloomberg BusinessWeek*, “Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It,” by Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack, March 13, 2014, http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

5. Business 2 Community.com, “5 Real Computer Security Disasters,” by Mitz Pantic, May 24, 2013, http://www.business2community.com/tech-gadgets/5-real-computer-security-disasters-0503539

6. *The Business Insider*, “Here's A Great Idea For Creating Passwords That Are Easy To Remember But Hard To Hack,” by Julie Bort, December 6, 2013.

7. The Canadian Institute of Chartered Accountants (The Information Technology Advisory Committee), “20 Questions Directors Should Ask about IT Security,” http://www.cica.ca/focus-on-practice-areas/information-technology/it-advisory-committee/publications/item46763.pdf

8. *CIO*, “10 Disaster Preparedness Questions to Ask Your Cloud Services Providers,” by Stephanie Overby, July 19, 2012, http://www.cio.com/article/711450/10_Disaster_Preparedness_Questions_to_Ask_Your_Cloud_Services_Providers

9. ComputerWeekly.com, “Supercharging Cyber Security Protection: Questions to Ask When Hiring a Managed Services Provider,” by Dragana Vranic and Kim Cuthbert, October 2015, http://www.computerweekly.com/opinion/Supercharging-cyber-security-protection-Questions-to-ask-when-hiring-a-managed-services-provider

10. *Consumer Reports*, “7 Online Blunders: Common Mistakes Can Ruin Your Computer or Invite Identity Theft,” September 2008, page 26.

11. *Consumer Reports*, “Boom Time for Cybercrime,” June 2009.

12. *Consumer Reports*, “Online Exposure: Social Networks, Mobile Phones and Scams Can Threaten Your Security,” June 2011.

13. *Consumer Reports*, “Six Ways to Stay Safer,” June 2011.

14. *Consumer Reports*, "Your Info: At Risk Everywhere," July 2014.

15. *Consumers' Checkbook*, "Healthy Computing Habits: Taking Care of Your Computer and Keeping It Safe from Intrusion," Fall 2013/Winter 2014, http://www.checkbook.org/cgi-bin/memberonly/tips/computer_safety/wdc/article.cfm

16. DataCenterKnowledge.com, "Seven Questions to Ask Service Providers Before Signing Your Next Contract," by Bhavesh Patel, January 28, 2015, http://www.datacenterknowledge.com/archives/2015/01/28/seven-questions-ask-service-providers-signing-next-contract/

17. EIN News.com, "Six Important Questions to Ask on International Data Privacy Day, January 28," January 28, 2015, https://www.einnews.com/pr_news/246846180/six-important-questions-to-ask-on-international-data-privacy-day-january-28

18. *Entrepreneur*, "10 Questions to Ask When Creating a Cybersecurity Plan for Your Business," by Kim Lachance Shandrow, April 23, 2013, http://www.entrepreneur.com/article/226456

19. *Forbes*, "5 Questions Boards Should Ask About Data Privacy Risks," by Bob Gregg, November 4, 2011, http://www.forbes.com/sites/ciocentral/2011/11/03/5-questions-boards-should-ask-about-data-privacy-risks/

20. Global Technology Resources, Inc., "Five Cyber Security Tips for Computer and Online Safety," by Dave Herrald on October 23, 2013, http://www.gtri.com/five-cyber-security-tips-for-computer-and-online-safety/

21. *Harvard Business Review* Blog, "Three Questions You Should Ask About Your Cyber-Security," by James Kaplan and Allen Weinberg, March 5, 2012, http://www.ceo.com/flink/?lnk=http%3A%2F%2Fblogs.hbr.org%2Fcs%2F2012%2F03%2Fthree_questions_you_should_ask.html%3Fcm_mmc%3Dnpv-_-AWAREN-_-KAPLANWEINBERG_POST-_-030512

22. *The Herald* (Rock Hill, SC), "ISACA: Nine Questions to Ask to Improve IT Risk Management," January 28, 2015, http://www.heraldonline.com/2015/01/28/6743135_isaca-nine-questions-to-ask-to.html?rh=1

23. IT Business Edge.com, "Nine Questions to Ask When Selecting a Security Vendor," by Will Irace, http://www.itbusinessedge.com/slideshows/nine-questions-to-ask-when-selecting-a-security-vendor.html

24. *ITworld*, "How IT Leaders Can Best Prepare for Disaster," by Thor Olavsrud, November 7, 2012, http://www.itworld.com/311640/how-it-leaders-can-best-plan-disaster

25. Massachusetts Institute of Technology, “Information Services Technology, Top Ten Safe Computing Tips,” http://ist.mit.edu/security/tips

26. NetworkWorld.com, “How to Respond to an Unexpected IT Security Incident,” by Joan Goodchild , March 12, 2009, http://www.networkworld.com/news/2009/031209-how-to-respond-to-an.html

27. NewsFactor.com, “10 Questions To Help Optimize Your Data Center Investment,” by Fortrust.com, June 9, 2015, http://www.newsfactor.com/news/Optimize-Your-Data-Center-Investment/story.xhtml?story_id=021000D8BWRL

28. Papp, David, *IT Survival Guide: Conquering Information Technology in Your Organization*, PFH Publishing, 2011.

29. *PC Magazine*, “Target Ignored Data Breach Warning Signs,” by Chloe Albanesius, March 14, 2014, http://www.pcmag.com/article2/0,2817,2454977,00.asp

30. *The Practical Accountant*, “The Right Questions for New Disasters,” January 2002, page 10.

31. PR Newswire, “11 Foolproof Security Tips for PC Users,” February 21, 1995.

32. PRWeb.com, “10 Key Questions to Ask Your IT Department to Avoid Corporate Catastrophes,” http://www.prweb.com/printer/5259284.htm

33. *Reader’s Digest*, “7 Things Your Computer Person Won’t Tell You,” http://www.rd.com/advice/saving-money/7-things-your-computer-person-wont-tell-you/

34. *Reader’s Digest*, “13 Things Your Computer Person Won't Tell You,” by Adam Bluestein, http://www.rd.com/advice/saving-money/13-things-your-computer-person-wont-tell-you/

35. States News Service, “Consumer Corner,” by Kansas Attorney General Derek Schmidt, October 29, 2012.

36. *TechNet Magazine*, “9 Questions You Must Ask Yourself When Planning a Backup Strategy,” http://technet.microsoft.com/en-us/magazine/dd767785.aspx

37. TechNewsWorld.com, “Technology News: Disaster Recovery: Disaster Recovery: It's More Than a Plan,” by Adam Montella, April 16, 2011, http://www.technewsworld.com/story/72285.html

38. TechSling.com, “Clear Reasons Why Your PC At Home Or Work Needs Security,” December 27, 2013, http://www.techsling.com/2013/12/clear-reasons-why-your-pc-at-home-or-work-needs-security/

39. Today.com (The Today Show, NBC News), “Sony Hack: Questions to Ask Your Employer About Data Security,” by Devin Coldewey, December 23, 2014, http://www.today.com/money/questions-ask-your-employer-wake-sony-hack-1D80380969

40. *Wired*, “Burning Question: How Much Computer Security do I Really Need?” by Cliff Kuang, October 2008.

by Dr. Dede Bonner, The Question Doctor
10 BQ Document # BUS114-03