In February, we released a new BitSight Insight, examining the cyber health of the U.S. economy, and found that 82% of the 460 companies assessed had an externally observable security compromise in 2013. Examples of security events observed include communications …

Cyber Security Risk: Perception vs. Reality in Corporate America

By Sonali Shah, BitSight Technologies

03.10.14
1:48 PM

Are you confident in your risk assessment? Share your thoughts in the comments section below.
Image: CJ Schmit/Flickr

In February, we released a new BitSight Insight, examining the cyber health of the U.S. economy, and found that 82% of the 460 companies assessed had an externally observable security compromise in 2013. Examples of security events observed include communications between compromised computers inside an organization and external computers known to be under the control of an attacker, distribution of malware, and propagation of malicious email. Although these security events do not necessarily equate to data loss, each one is an indication that the organization has been compromised in some manner.

However, in spite of this evidence of widespread compromise among America's largest companies (our analysis was based on a subset of companies in the S&P 500), corporate and IT leaders seem to feel quite confident about their security posture.

Take for example the 2014 Global State of Information Security Survey, conducted by PriceWaterhouseCoopers and CSO Online, that found executives to be quite confident in the robustness of their security initiatives. Seventy three percent of the North American executives surveyed believe that their security programs are effective. Then there is also the 2013 (ISC)2 report on the information security workforce, developed in partnership with Booz Allen Hamilton and Frost & Sullivan, which found that the majority of respondents believe that their organizations would perform better or the same relative to 12 months earlier. Respondents with C-level and officer job titles were more optimistic on readiness than respondents with lower job titles. And lastly, the Trustwave 2014 Security Pressures Report found that 72% of respondents in the U.S. feel safe from IT security threats. Nearly 60% of the respondents were CIOs, CISOs, VPs or Directors.

Optimism Bias Leads to False Confidence in Security

So why are America's corporate and IT leaders so confident in their security posture? Optimism bias is one reason. According to the famous cognitive neuroscientist Tali Sharot, 80% of people have optimism bias. They overestimate the likelihood of experiencing good events and underestimate the likelihood of experiencing negative events. "We're optimistic about ourselves, we're optimistic about our kids, we're optimistic about our families, but we're not so optimistic about the guy sitting next to us," she says in her TED Talk. People tend to believe that their desired outcomes will indeed happen and that their goals will be met. They know that bad things do happen, but assume these bad things will happen to someone else. This is why, in spite of knowing that 40% of marriages in the western world end in divorce, newlyweds almost always say their chance of divorce is 0%.

Another reason for this false confidence is that many business leaders simply do not understand cyber security risk. A report issued in January 2014 by Lancope and Ponemon Institute titled Cyber Security Incident Response: Are we as prepared as we think? found that corporate leaders in the U.S. and U.K. are often in the dark on cyber security issues. Only 20% of survey respondents said their executives are frequently briefed on cyber threats.

How to identify, quantify, and mitigate cyber risk are questions often left to the "techies" in the company. Executives believe that they have hired the right management team, and they in turn have hired the right people to manage security risk. In addition, security spending in most North American companies has grown from 2012 to 2013 and will likely increase again in 2014. Therefore, many executives believe, the company's security posture must be good.

When it comes to cyber risk, the mismatch between perception and reality is great. Natural optimism bias combined with a lack of understanding of cyber risk can lead business executives believing that their businesses are secure. While cyber risk may never go away, understanding the reality can help many companies take action to lower this risk.

Are you confident in your risk assessment? Share your thoughts in the comments section below.

Sonali Shah leads marketing and product development as Vice President of Products at BitSight Technologies.

Sonali Shah

View original post

WE RECOMMEND

RECOMMENDED BY

When Will the Tablet Become the Desktop?

The Easiest Path to Online Riches Is Good Ol' Buying and Selling

Tags: cyber, insurance, management, risk, security

Post Comment | 2 Comments | Permalink

Back to top

Share on Facebook

50 shares

Tweet 156 g+1 7 1

Reddit Digg Stumble Upon Email

2 Comments Wired: Innovation Insights Login

Sort by Best Share Favorite ★

Join the discussion…

Andy Bochman · 14 days ago

Great article and I share your observations about wishful thinking. It's hard to imagine anyone, let alone a corporate officer with loads of official responsibility, feeling super confident on security in 2014, unless they entirely avoid all news sources and never interact with security advisors outside their company. Glad capabilities are emerging to surface (the likely tip of the iceberg of) their security gaps in hard-to-refute empirical form.

• Reply • Share ›

Quince30 · 14 days ago

One way to mitigate risk, especially among a small group of senior staff handling sensitive information is to create a two-tier email model. I've found the execs doing this anyway with their gmail or hotmail accounts due to a distrust of internal systems that can be accessed by IT staff (in-house or with third parties) and its better to formally set something up with some assistance (e.g. education on strong passwords). There are various encrypted email systems and I'm currently testing out a new one called xcapsa as I can use it with existing email clients on laptops and phones but its also encrypted. However it's bitcoin only, hopefully something that won't be too edgy for the budget board!

• Reply • Share ›

Subscribe Add Disqus to your site