CIO Insights: Data Security

With "data security tactics resembling counter-terrorism," how can your company protect its data?

Monday, May 20, 2013 at
Coca-Cola Consolidated in Southpark

A panel of experts brought together by Apparo and its corporate partners assembled to discuss the pressing topic of data security in the global environment we live in today. Below are key takeaways from the event which not only cover the modern day challenges of data security, but how a company can input a forward-thinking strategy to ensure the safety of its information.

What are the modern day challenges of data security?

- Reinforced by a recent article in the Wall Street Journal that focuses on an interview with Shawn Henry, a 20-year FBI veteran, panelists stressed the reality that corporations are simply unprepared to handle relentless computer hackers who spend their days thinking of ways to break down the newest security just as soon as it's created.
- Many times the adversaries are so skilled they "leap right over the fence, and you don't ever hear an alarm go off.'' Companies can attempt to slow them down by constantly hunting inside the perimeter of their network.
- However, having simply a defense-minded strategic approach to data security will undoubtedly fail. Companies need to prepare for what happens when/if the systems fail, and be sure their focus is not only protecting data, but internal systems as well.

What is the motivating factor behind many of the attacks on data?

- While data security has been an economic and business concern for more than 15 years, the difference today is it's driven by economic and political strategies of competing global markets. These strategies seek intellectual capital and property to create their development both internally and in developing markets.
- To better protect companies, executives need to understand the economic motivations behind the cyber-attacks. If you understand that market manipulation is a key factor, we can input strategies that focus on as-close-to-instantaneous-as-possible responses to false information – versus expensive manipulations which will ultimately be re-hacked.
- Excellent case study is the hacking of an Associated Press (AP) twitter account that tweeted false information about an attack on the White House; $136 billion was lost in the resulting market swing. The AP saw the tweet and within four minutes had counter-tweeted that the information was false and the financial markets righted themselves. Although $136 billion is

a tremendous loss, imagine how much worse it could have been had the AP taken hours to assess, lock down their systems and waited to understand the attack before responding.

What are key ways corporations can reduce security threats to both data and systems?

- Full corporate support, from top to bottom, for security programs is the best deterrent.
- Internal awareness programs, especially at the Executive levels, to ensure security is part of the organizational culture.
- Security teams should be front and center, not isolated in their work. They should be incorporated into the business – not just outside peering in – and accessible to all employees.
- Invest in security people who are trained and dedicated – do not cut expenses here. You need technology smarts as well as people and business skills and these do not come inexpensively.
- Be aware of how your network is used so you will see anomalies more quickly.

Special Thanks to the Following Panelists:

Featured panelists:

- Paul Stein, Partner
  Ernst & Young, LLP
- Mike Brannon, Director
  National Gypsum Company
- Jeffrey Z. Johnson, Executive Director, CISSP
  Ernst & Young LLP

- Chad Smith, Security Specialist
  CISCO
- Jeff Stovall, Chief Information Officer
  City of Charlotte
- Tammy Moskites, CSIM, Chief Information & Security Officer; *Time Warner Cable*

CIO Insights Presented By:

Contact Information:

For more information about CIO insights, please contact Karen Pierce at kpierce@apparo.org.