What is your business critical data? And where do you think it lives?

How framing data security as a risk management problem leads to better results.

by Rockie Brockway, GSEC, GCIH, GSNA, Information Security and Business Risk Director for Black Box Network Services

Imagine that you are heading up a renewable energy technology program in a rising nation state. Before you launch, another country announces the same technology at a much lower cost. An investigation determines that the specifications were stolen by hackers and sold.

Now picture yourself as the CIO of a mid-level chemical company that suffers an employee theft of intellectual property. The illegal transfer of trade secrets results in $400 million of revenue lost to the competition.

These are scary scenarios. But they are not imaginary.

Irreplaceable Data

All organizations have data. Those that have irreplaceable data are the most at risk of having that data compromised. They may be in the science, pharma, manufacturing, legal or financial industries. They all have something in common, the secret sauce that, if stolen, would have an enormous business impact.[1]

Companies in other industries such as retail have data that is replaceable, but may nonetheless suffer big hits to revenue and reputation with a data security breach.

Recent events convince us that data security threats and the corresponding risks to business are increasing. And we fear that our secret sauce is less secure than it was just a year ago. Yet, one in three companies doesn't have a written information security policy.[2]

Are You Prepared?

Cloud computing, remote access and mobile devices all increase the vulnerability of systems to attack. And the Internet of Things will bring new risks, where it may be possible for hackers to directly cause physical harm. Perhaps it will be a wirelessly controlled artificial heart that is compromised, or your car's autopilot sensors that are disabled.

As Internet technology permeates devices and business processes, the surface area exposed to attack is increasing. And you can be sure that hackers will be stepping up their efforts to take advantage of the opportunity.

The big question for every CIO is this: Am I confident that I will not lose millions of dollars in a data security breach? Or in Harry Callahan's vernacular, "Do I feel lucky? Well, do ya?"

Your Business Critical Data

Your business critical data is probably unique. It might be a formula for a chemical process or plans for a sonic screwdriver. It could be architectural drawings, pending medical and pharma patents, or details of a potential merger or acquisition.

The more valuable the data, the more motivated someone will be to steal it, and the more sophisticated their attempt to subvert your existing security technology.

Understanding your adversary is the key to understanding the risk. Asking, "What would this data be worth to someone else, and who would that be?" helps you understand how to protect it. How do you think the Coca-Cola Company guards the formula for Coke so well?

If we think in terms of data security technology rather than

business risk we may fail to provide the appropriate protection. Hackers, on the other hand, who recognize the value of the data, will take extraordinary measures to obtain it, including compromising key employees to get around the technology.

Step 1: A C-level Responsibility

Identifying your business critical data and its value is the first step toward minimizing the risk. C-level executives and above are in the best position to have this conversation. The CFO, being accountable for the purse, understands the value. His inclusion in the discussion is critical.

If the risk analysis is left to someone below the CIO level, having technology-focused discussions becomes likely. Overlooking the most valuable data, which may be on the CEO's smartphone or a scientist's tablet, could be the result.

When IT staff is focused on boxes, it takes suffering a breach to tighten security. However, a reactive approach is doomed. Another hacker, or insider, may already be planning an attack on an enticing target thought to be secure.

When the value of the data is large, the means employed to obtain it will be large as well. The business risks must be accurately assessed to match the level of protection to the potency of the threat.

Step 2: Where Does Your Business Critical Data Live?

Understanding where your business critical data resides is the second step in minimizing the business risks. In the Home Depot breach, the sensitive data was in the registers. People could profit by stealing it. And Home Depot didn't sufficiently protect their network perimeter.

Business critical data might be found in your CRM application or in an email, in a database or in transit, on the company's server or in a smartphone. The popularity of BYOD and emerging technologies makes the location more nebulous, increasing the difficulty of pinning it down.

A very common risk scenario is insider theft in a manufacturing company. Usually, a handful of really smart employees and a demand for talent create the circumstances where knowledge workers take intellectual property with them when they leave.

In a financial company, analysts determining a merger valuation may be motivated to leak insider information for profit via email or a voice call. To minimize losses, systems must be designed that can recognize these situations, understand where the data is located and protect it.

Step 3: Having the Right Conversation

Talking in terms of "business risk", rather than "data security" gets the right people involved. Conversing with the data owners about risks to the business yields a more accurate assessment of the data, its value and location.

Knowing the value of the data informs an organization of potential adversaries and the level of their capabilities. Thus informed, organizations can decide to remediate, mitigate or accept the risk, prepare an appropriate defense, and allocate resources accordingly.

Otherwise, the Target, JP Morgan Chase, AIG, Home Depot, HP, and Snapchat breaches will repeat along with less public but more catastrophic losses in an increasing number of companies.

So, how confident *are* you that you won't lose millions in a data security breach?

A competent risk assessment team can guide the business conversations. "Where does my business critical data live?" is a tough question to answer. An experienced consultant employs an effective process for satisfying both the "what" and the "where" questions, as well as determining the value of the data, potential adversaries and the strength of existing defenses.

After recent events and breaches, it's time to start the conversation. Over time, our fears diminish, but the risks are constant. A very public breach may create a window of opportunity to muster the support required to complete the process. Framing the issue as a risk management problem will yield better results.

To Learn More

Talk to Black Box about your business critical data and steps to minimize your risks. Email cisco@blackbox.com.

About Black Box

Black Box is a leading technology solutions provider dedicated to helping customers build, manage, optimize, and secure their IT infrastructure. Black Box delivers high-value products and services through its global presence and over 4,000 team members. To learn more, visit the Black Box Web site at www.blackbox.com

[1]Corman, J. (10/24/11). A Replaceability Continuum [Blog post]. Retrieved from http://blog.cognitivedissidents.com/2011/10/24/a-replaceability-continuum/

[2]Dipietro, B. (9/19/14). Survey Roundup: Cyber Gaps Keep Companies at Risk, The Wall Street Journal, Risk & Compliance Journal. Retrieved from http://blogs.wsj.com/riskandcompliance/2014/09/19/survey-roundup-cyber-gaps-keep-companies-vulnerable/