[HPS] LEADING THINKING

Hamilton Place Strategies
www.hamiltonplacestrategies.com
202-822-1205

Cybercrime Costs More Than You Think

Findings:

- **The median cost of cybercrime has increased by nearly 200 percent in the last five years and is likely to continue growing**
- **The reputational risk associated with cybercrime extends well beyond monetary damages**
- **Having a plan in place for how to respond to a cyberattack could save millions**

In an increasingly interconnected world fueled by the expansion of digital technology, cybercrime has become a big business. How big? Cybercrime costs the global economy about $450 billion each year (Fig. 1), a value that exceeds the market capitalization of such corporate powerhouses as Microsoft Inc. and Exxon Mobil Corp., and it's nipping at the heels of Apple Inc. Put another way, cybercrime would rank as the world's 23rd largest economy – beating out countries like Austria and Iran. And if cybercrime were a U.S. industry, it would be bigger than the entire farming or oil and gas extraction industries.

If cybercrime were a U.S. industry, it would be bigger than the entire farming or oil and gas extraction industries.

In the last five years, the median cost of a cyberattack has increased by nearly 200 percent (Fig. 2). And cybercrime's not just getting bigger, it's becoming more frequent and far reaching.

Consider:

- Since 2005, 828 million individual records have been exposed by data breaches – the equivalent of every person in the U.S. having almost three records stolen.
- In 2014 alone, data breaches exposed over 85 million records in the United States.

Reputations At Risk

While the direct cost of a cyberattack can be significant, the reputational damage can be even more impactful to the bottom line. In the Target data breach of 2013, which affected millions of U.S. customers, the company incurred $252 million in data breach-related expenses, with only $90 million of that expected to be offset by insurance recoveries. In its 2015 10-K filing, the company referred to the data breach as "an example of an

Tucker Warren
Jared Favole
Scott Haber
Emily Hamilton

incident that affected our reputation and negatively impacted our sales for a period of time."

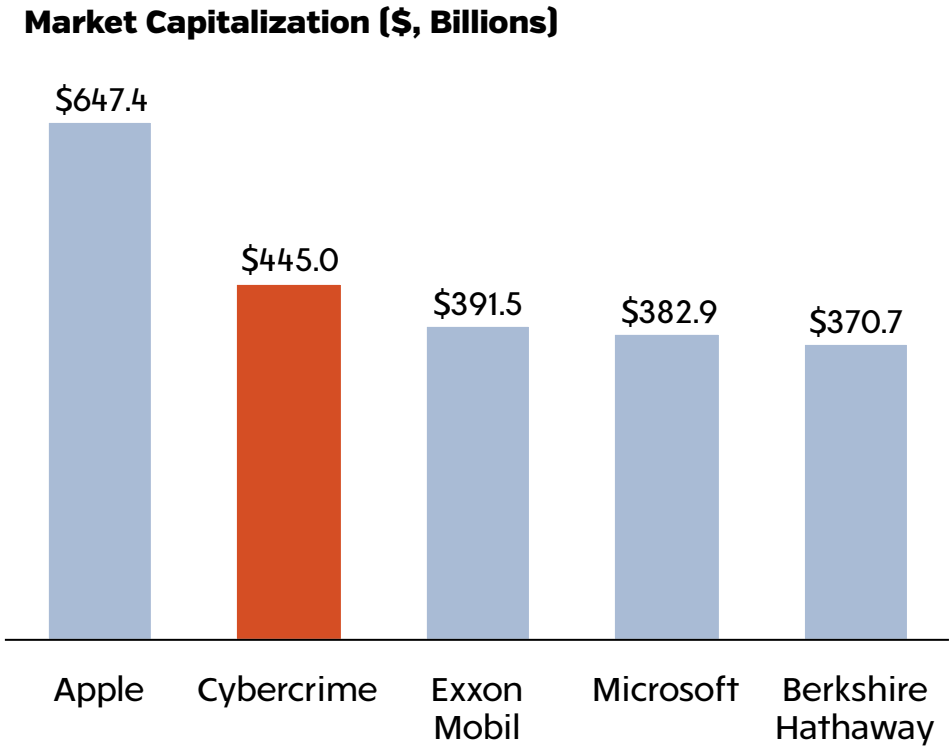
Cybercrime also carries with it a "ricochet effect" where simply sharing an industry with a victim is enough to impact your business. In the case of Target, its data breach brought other retailers into the spotlight, with headlines like "Retail Industry Security Hacks May Surge In 2014." This ricochet effect shows that even if your company avoids a cyberattack, you could be harmed if a less-prepared industry player lets its defenses down.

U.S. CEOs are more concerned about cyber-related threats and attacks than fiscal crises, asset bubbles, and energy prices.

Business leaders seem to have taken notice. The World Economic Forum's recent report on Global Risks of 2016 found U.S. CEOs are more concerned about cyber-related threats and attacks than fiscal crises, asset bubbles, and energy prices.

Despite the attention cybercrime has among people tasked with protecting the reputations of the largest companies in the world, the costs of attacks and the frequency with which they occur are rising. This shows that a lot more needs to be done to protect the reputations of businesses.

Fig. 1: If Cybercrime Had Been A U.S. Company In 2014, It Would Have Been The Second-Largest



Source: Bloomberg, cybercrime cost from Allianz Cyber Risk Guide

Plan For It, Communicate About It

While cybercrime seems to be becoming an inevitability, the ensuing reputational damage doesn't have to be. Companies spend a lot of time and money to protect their business and by extension their customers. But what about investing in and preparing for how to handle the communications response? It's not just about protecting your company. Your company's efforts will benefit the industry too. The less companies talk about cybercrime, the more they'll be feeding into worst-case-scenario thinking. Here are some things every company in every industry should do:

Cybercrime also carries with it a "ricochet effect" where simply sharing an industry with a victim is enough to impact your business.

Know your story: Find out how likely your business is to be attacked. Develop a list of five things your company does right now to prevent cybercrime and get

clearance for how to discuss those details externally.

Media train experts: Cybercrime is complex and confusing to the general public. Establishing credibility will likely take more than just a communicator. A technological expert, possibly even a chief technology officer if your company has one, should be trained well before an attack on how to interact with the media.

Internal navigation: In a crisis, navigating internal communications channels can be as tricky as external ones. Understand who in your company would need to be involved in internal and external communications in the aftermath of a cyberattack and where the technical cyber expertise lies within the company.

Create a playbook: Develop a plan for how your team and the company will react to a cyberattack. This can streamline your company's response, ultimately saving time and money.

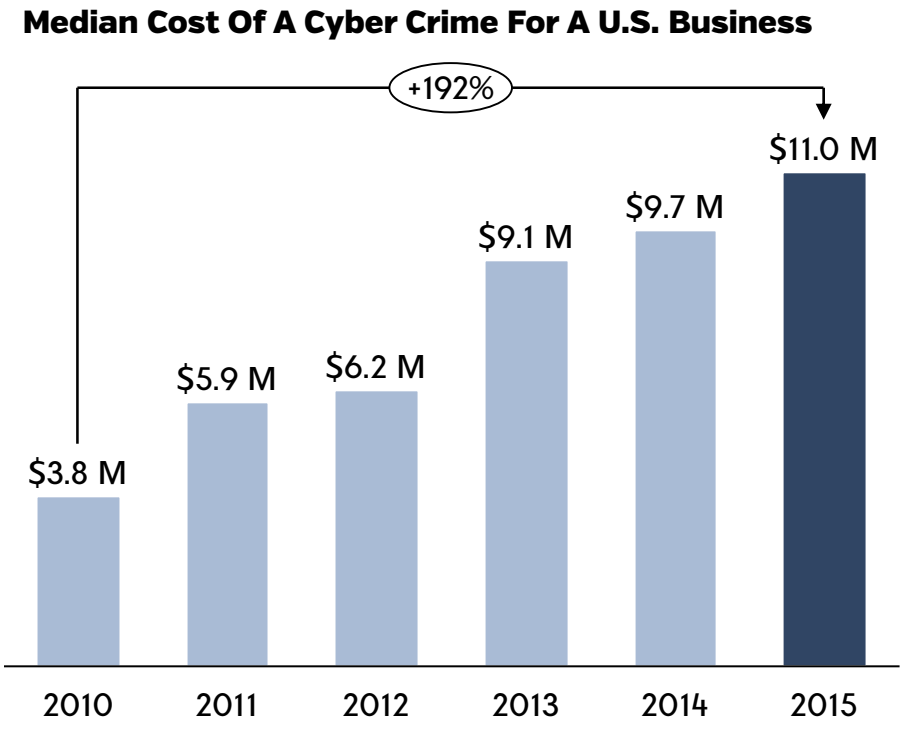
Brief the board: Ensure the board understands that a cyberattack is likely to happen in this day and age, and inform them of the planning in place to prevent and recover from an attack.

Engage stakeholders: Done well, proactively communicating with stakeholders about your company's cybersecurity risk and plans isn't a risk. Given the realities all industries are facing with cybercrime, doing so will help ensure your company is ready and prepared. And after all, being thought of as ready and prepared is what every business wants for their reputation.

Know the media: Identify key reporters and create working relationships in advance of an attack so you aren't introducing yourself to the reporter who covers your attack in its aftermath.

War gaming: Lay out a few of the most likely cyber scenarios that would impact your business and game out how you and your colleagues would respond, what everyone's roles would be, external dependencies, and who needs to know what, when in the first 24-48 hours inside and outside of the company.

Fig. 2: The Cost Of A Cyber Attack For U.S. Businesses Has Increased By 192% Since 2005



Source: 2015 Cost Of Cyber Crime Study: United States

You can't control it, but what you can control is whether you're prepared to respond

These are just a few steps that will help your company contextualize the threat of a cyberattack, and how to mitigate its damage. Unfortunately, if you're in business today, it's nearly a guarantee you'll be hacked at some point over the next couple of years. You can't control it, but what you can control is whether you're prepared to respond when it happens. [ ]