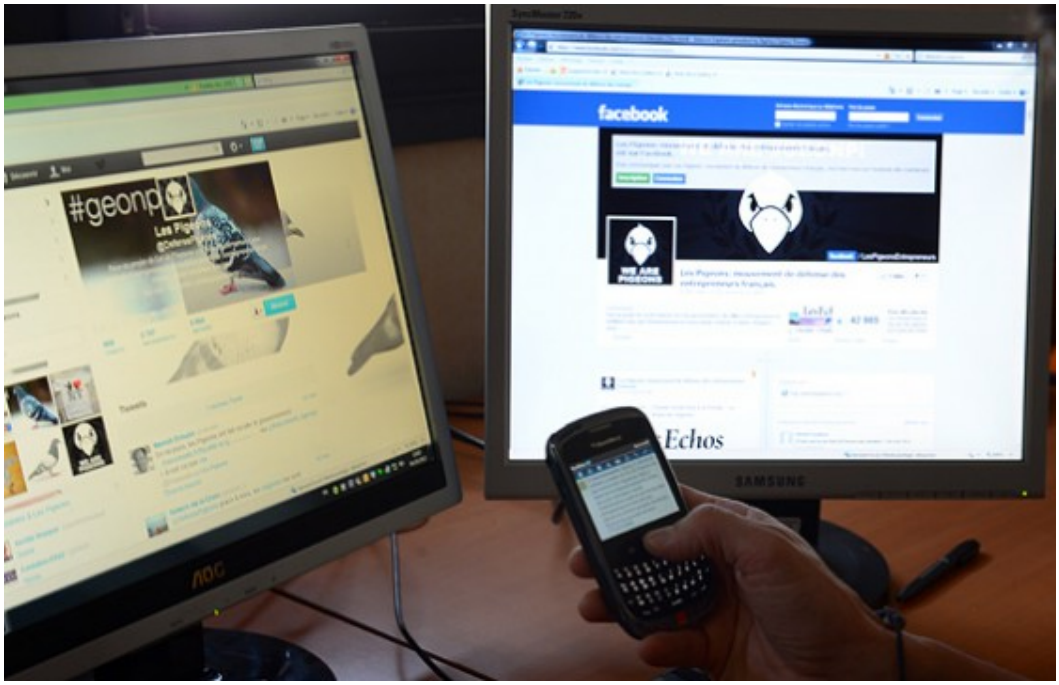
THE HILL

Stop victim shaming in cyber attacks

BY MIRIAM WUGMEISTER - 09/13/16 03:13 PM EDT



Imagine if your neighborhood grocery store welcomed you with a fortified perimeter—barbed wire, tanks and guard towers loomed tall while helicopters and fighter planes scream overhead. The idea that every business would deploy a private army to defend its physical perimeter is, of course, a ridiculous one. But that is precisely what is expected of businesses today in the cyber arena.

Large U.S. businesses are probed by malicious actors all of the time. Employees receive fake emails that look like they are sent by their banks or their bosses, but actually contain malware. All the while, nation state actors are increasingly stealing credentials from employees in order to obtain trade secrets and intellectual property from U.S. companies.

Defending the American people and economy from hostile state or state-sponsored actors is critical for both economic and national security reasons. However, while our state and federal law enforcement agencies vigorously protect people from criminals and assist victims of crimes, companies that publicly disclose that they have been the victim of a cybercrime are not treated like a typical victim by federal and state regulators. Instead, they are investigated by numerous agencies, including the Federal Trade Commission, the State Attorneys General, and

Just In...

We need to strengthen our Arctic security before it's too late
CONTRIBUTORS — 0S AGO

A bridge to the world will keep America afloat
CONTRIBUTORS — 4M 40S AGO

Senators praise decision to halt some Saudi arms sales, urge more action
POLICY — 7M 37S AGO

Graham: Tillerson must say Russia hacked US to earn his confirmation vote
POLICY — 11M 39S AGO

How President Obama can retaliate against Russia
CONTRIBUTORS — 20M 12S AGO

Low marks for the Department of Education
CONGRESS BLOG — 20M 13S AGO

Arnold Schwarzenegger: 'Stop whining' about Trump
IN THE KNOW — 26M 53S AGO

US files trade case against China over grain quotas
POLICY — 30M 12S AGO

VIEW ALL

Related News by


Chomsky: Liberals who didn't vote for Clinton...


McCain: I'll answer 'stupid, idiotic' Trump...


Chrissy Teigen shreds Trump for wanting...


Trump calls for federal employees to sign...

the Security and Exchange Commission,while often simultaneously sued by consumers, business customers, and shareholders. In the face of the onslaught of cyber threats, U.S. companies are charged with defending themselves in cyberspace or facing legal liability. How did we arrive at holding those victimized by a cybercrime liable for the damage inflicted upon them?

In the aftermath of a data security breach—unlike physical assaults or property crimes—a company is likely to be treated as a suspect, not a victim. Federal and state regulators not only examine how the company responded to the attack, but they engage in a full review of its entire data security infrastructure and approach, often dating back to years prior to the inciting incident. Rather than focusing on what the attackers stole and working to find the stolen property and determine how the company can protect itself, the aftermath of a breach sees companies forced to explain whether they had enough “armed guards.” The investigations by enforcement authorities can last for two to three years,costing a company millions of dollars in the process and an untold amount of management attention spent defending their existing data security practices. Thus, when the company should be focusing on remedying any damage done by the attacker and working to protect those who have been impacted by the assault, it instead must spend countless hours, money, and resources defending its data security practices and explaining away its status as a victim.

The basic legal requirement that companies must have “reasonable” security is enforced by State Attorneys General and the Federal Trade Commission, as well as other federal regulators and private litigants.In other words, a company is expected to protect its business and customers against the types of basic, foreseeable threats that can be reasonably managed by an enterprise. But what is reasonable in the face of a foreign nation state actor?

While regulators insist that all that is required is “reasonable” security to combat reasonably foreseeable threats, their expectations have increased as attacks have evolved. It was one thing when using passwords, basic encryption, and Internet firewalls would stymie all but the best attackers, and were effectively the equivalent of the store security guard. Today, “reasonableness” rests on a faulty premise that each company can defend itself on its own. No one expects a small town in the Midwest to be able to defend itself against the army of another country, so why do we expect a company to able to defend itself against national state cyber attackers? What percentage of revenue is it reasonable for a company to spend to defend itself? How many people should a small company be expected to employ to run the network infrastructure in order to protect itself? Given that the federal and state governments seem unable to protect the information they hold despite vastly greater resources and insight, why are companies expected to do this on their own? Companies are justifiably starting to ask, “why isn’t my government protecting me?”

This approach by regulators fails to account for the increasing sophistication and organized, strategic approach taken by the malicious cyber attackers. Cyberattacks come in many forms -- the attackers may be an arm of a national government or a state-sponsored group, they may have the encouragement or implicit support of a regime, or they may merely be organized criminal hacking rings. The targets and modus operandi vary as much as the threat actors. They include apparent cyber-espionage efforts such as the theft of sensitive personal information held by U.S. government agencies; stealing financial information (such as

credit card numbers) held by major retailers, restaurant chains, or hotels; theft of trade secrets and intellectual property in order to gain an economic advantage; seeking to embarrass or cripple an organization that shares a different ideology or has offended a state actor; disrupting business operations by wrecking enterprise computing networks; stealing or leaking sensitive operational information; and even holding companies "hostage" for ransom.

Defending against these sophisticated threats requires dedicated efforts and skilled personnel, significant funding, carefully designed networks and controls, the deployment of sophisticated technologies, and the expertise to govern these various threads together in an effective manner. As the reports regarding breaches in the last few years indicate, in spite of formidable efforts and a thriving private cyber defense sector, both the U.S. public and private sectors continue to be victimized.

Unlike regulators and litigants, we have seen a dramatic shift by federal law enforcement in its efforts to stop re-victimizing the victim of a cybercrime. In the past year, the FBI, Secret Service, and the Department of Justice have made enormous strides in working with companies to share information and gently gather the information they need to prosecute malicious actors. Perhaps this is because federal law enforcement truly understands what we are up against and the imperative that we work together to stop the cyber criminals.

Regulators, however, fail to understand that the aftermath of a breach is a tremendously chaotic, disruptive time for a company. The company may be trying to stop or understand the nature of the attack (often with the assistance of, or in coordination with, law enforcement agencies), trying to reassure staff and customers, or simply trying to get the business up and running again. Being a suspect at the same time— meaning having to respond to regulatory inquiries and deal with the threat of litigation or stiff penalties—has deleterious effects. It is not only distracting, but it curbs the willingness of companies to share information with law enforcement.

Ironically, companies that know that they have been attacked and have sufficiently sophisticated systems to detect a breach are likely the companies with the best security. Thus, when regulators commence enforcement actions based on a publicly announced breach, they are typically investigating the companies that have the best security and the best systems for identifying a problem. Thus the regulators are going after the wrong targets. This second guessing by regulators as to a company's security practices following a cyber attack creates an adversarial relationship between the private companies and the government, which is charged with protecting the nation and its citizens from criminals and hostile nations, at exactly the time when companies should be able to rely on the government for support and when the information that the companies have is of most use to law enforcement.

While there is a lot that businesses can do to make it harder for hackers, we are losing ground in cyberspace as a nation, and the spate of hacking cannot be ended by regulatory changes or press releases reminding companies of the importance of implementing good security practices. Sophisticated hackers abound—elite, dedicated teams that exist solely to wreak havoc to further criminal, economic, political, or military strategic objectives. The notion that it is reasonable for every company to successfully defend itself from sophisticated cyber attacks is outdated and unhelpful. Just because a company has been the victim of a cyberattack does not mean that it has unreasonable security *per se*. It

means it was a victim. Enforcement authorities in the United States should follow the lead of the FBI and the Secret Service and treat companies that have experienced such breaches as victims rather than suspects. Our only hope of stopping cyber attackers is if companies, law enforcement, and regulators work together effectively, rather than passing around blame.

Wugmeister is a partner at Morrison & Foerster, a leading global law firm, and is co-chair of the firm's global privacy and data security practice. Follow her on Twitter @MWugmeister

---

TAGS **CYBER SECURITY** **CYBER CRIME** **CYBER ATTACKS** **LAW ENFORCEMENT**