HealthManagement
Promoting Management and Leadership

Volume 17 - Issue 2, 2017 - Best Practice

When a Cybercrime Takes Place - Who's to Blame?

Ajay K. Gupta
******@***healthsolutionsresearch.org
Health Solutions Research, Inc - Rockville, MD, USA
Twitter

Mansur Hasib
******@***umuc.edu
Programme Chair of Cybersecurity Technology - The Graduate School of University of Maryland University College (UMUC) & Cybersecurity and Healthcare Speaker & Author
Twitter

When cybersecurity is breached and sensitive data is compromised, who should be held responsible - the hacker or the victim?

When money is deposited into a U.S. bank and someone steals it, the money remains secured and the bank must honour its obligation to return the funds. Even if the bank goes out of business or into bankruptcy, each customer is protected by the federal government (i). This set up works because the law clearly backs the consumer. Even though the company may have been the victim of a crime, the bank cannot absolve itself of the responsibility to protect depositor accounts.

In a similar case, if a person gets injured on the job due to the employer's failure to perform due diligence in providing safe working conditions, the company remains liable for damages. Once again the law sides with the non-corporate party. Even if the employer is the victim of a crime which causes the employee's physical injury, they cannot wriggle out of the liability.

Contrarily, in the case of digital harm, similar situations remain murky. Who is to blame? Major companies argue that they perhaps should not be held liable for a client's digital harm or subsequent financial harm stemming from a cybercrime. They consider themselves a victim as well.

While the laws for financial harm and physical harm appear to provide some reasonable level of protection, the laws for digital harm are almost non-existent or weak.

Who is to Blame for Cybercrime?

Clearly, compromising the security of a network is a criminal act conducted by the hacker/s involved. These actions can include gaining unauthorised access, stealing or altering data, or any other abuse of a network and its resources. The cyber-criminals are responsible for their illegal actions and, in most people's minds, should shoulder all the blame. In this area, though, the question of liability remains just that: a question. So who carries the legal liability for the cybercrime?

Can a Company be Held Liable for Having Been Compromised?

Let's consider an example. If a company is compromised and the intellectual property of a business partner gets exposed to the wild, can the holder of that IP sue for damages?

Two schools of thought are at play here. The first view believes that companies whose systems have been compromised should not be held responsible for breaches and the impact of the breaches. They consider themselves to be victims of the crime. Others suggest that if those companies did not exercise due care or due diligence with regard to the protection of their IT assets, then the victim argument does not fly. Instead corporate leadership (board members and executives) should be held responsible and accountable for the breaches. This second approach concludes that holding companies liable is the only way the industry—and the digital world as well—will truly make progress toward better security.

Should the Victimised be Liable?

Two additional questions emerge from the discussion of cybercrime liability and victimisation:

- Does being a victim absolve the person or company of all blame?
- Can holding the leadership of victimised companies accountable actually improve the security?

Can Victims be Guilty?

People generally don't like to blame victims. That action seems counterproductive and at some level just simply wrong. The reality is, however, that we often do. In several cities, when graffiti finds its way onto buildings, the government fines the owners if the graffiti isn't cleaned up quickly enough. Even though no one suggests that the building owners are guilty of vandalising their own property, they are the ones who are punished nonetheless.

Additional cases illustrate this point. If executives do not monitor the financial health of their company and it's revealed that the books have been cooked, the CEO can expect to be in trouble. The boss may make the argument that he/she didn't alter any financial statements because, or perhaps, they were focused on product development or client delivery. In those cases, the inattention to the company's financial health happened due to neglect, if not willful action. This negligence doesn't absolve the CEO of any liability; in fact it confirms it. The widely accepted view is that CEO s are responsible for the accuracy of the company's financial statements

See Also: 10 Ways to Enhance Cybersecurity Protection

What Happens to Leaders Who Follow Due Care?

This last example also speaks to the value of holding leadership accountable. The logic goes that if executives are liable for the wrongdoing of their companies, they will proactively ensure their firms take security seriously. That attitude and, hopefully, resulting actions actually may bring those companies closer to being effective in protecting their networks in the first place.

This case also offers the executive leadership an out. If they follow cybersecurity best practices and standards for their industry in a demonstrable and auditable way, then leadership is not negligent and can perhaps avoid or at least reduce their liability. In such a scenario, the victim argument applies.

In our current time, the murky arena of corporate/executive responsibility persists because no definitive standard of due care exists. Fortunately, progress toward this end is underway:

- National Institute for Science and Technology (NIST) Special Publications subseries 800 (csrc.nist.gov/publications/PubsSPs.html#SP%20800) speaks to civilian federal agencies and is a baseline for most others (ii).
- The Health Information Trust Alliance (hitrustalliance.net) has produced the HITR UST Cybersecurity Framework for the Healthcare industry.
- The Payment Card Industry Data Security Standard (pcisecuritystandards.org/pci_security/maintaining_payment_security), managed by the Payment Card Industry Security Standards Council, established security best practices for the credit card processing industry.
- The ISO 27000 series (iso.org/iso/iso27001) sets security standards for commercial businesses.

There are others as well.

As we get closer to clarity and widespread acceptance on a set of cybersecurity practices that constitute due care, a set of practices that can be clearly implemented and followed, companies and their leadership may be exempt from liability in a cyber-attack. When companies cannot make such a claim, perhaps leadership should be culpable.

What about Partial Blame for Companies?

The above-mentioned situation implies that, if reasonable attempts to meet recognised security standards and best practices have been met (eg, as can be documented through an audit), then company leadership should be in the free and clear when they become victims of a cyber-attack.

It seems everyone bases guidance on cybersecurity controls and operations on the NIST SP 800 Series. If a company follows the guidance issued for their industry and is certified for having followed that guidance to a high degree by a recognised audit firm—and yet are still compromised—does this imply that some liability would accrue to either or both the standards body for creating a false sense of security, or to the auditor? Can the company and its clients, who may have suffered losses in the hack, such as the loss of their identity information, sue the auditor or NIST ?

And what happens when a company can clearly demonstrate its level of effort even when no standard or widespread agreement of proposed standards yet exists (which is closer to the case today)? Or if the company simply hasn't followed existing standards, because of the unique nature of its business operations or out of a disagreement with accepted standards? If companies in such situations are hacked, should their leadership still be held liable?

Conclusion

More questions than answers currently remain in this new area of cybersecurity and digital harm. However, it is paramount that these queries be asked and that we address them publicly and legally.

Notes

i. T he Federal Deposit Insurance Corporation protects bank accounts up to a certain bank balance.

ii. NIST has been designated by Congress as the agency to establish cybersecurity guidelines for the federal government. The NIST Special Publications (SP) 800 Series are these guidelines. They serve as the basis for many standards bodies and industry best practices in both the public and private sector.

Published on : Sun, 7 May 2017