CISOs at Risk

Suffolk County is located on the eastern end of Long Island in the US State of New York. The county is noted for its beaches, vineyards and fishing fleets. And, recently, it has gained some notoriety for a ransomware attack that forced the local government to take all its systems off the Internet. As a result, all agencies were forced to revert to the technology of the 1990s.[1]

> For reasons I do not understand, cyberattacks are crimes for which someone must be blamed, over and above the criminals.

I know nothing about this cyberattack except what I have learned from the media and conversations with fellow information security professionals in the area, none of whom were any better informed than I. But one detail that was reported has been on my mind ever since. In late December, the county government announced that the IT director for one agency, the county clerk, was blamed for enabling the attack and was placed on administrative leave. He was accused of treating his office's cybersecurity in "an incredibly nonchalant manner." The accused individual replied that he had tried to raise awareness that more robust cybersecurity protection was needed and had not been heeded.[2]

Why Blame Anyone?

What keeps rattling in my brain is why was there any reason for anyone to shoulder the blame for the occurrence? Oh, there is certainly someone to blame: some rather nasty individuals who sought to extract a ransom (and a great deal of personal information) from peaceable citizens in a largely rural area. Why should one IT director be held responsible?

There are other troubling examples. The former chief security officer (CSO) at Uber was convicted of not disclosing a hack that had occurred several years before.[3] An IT director in the US State of Florida was fired following a ransomware attack.[4] A credit controller who was scammed at a company in Scotland.[5] An information security officer in California.[6]

For reasons I do not understand, cyberattacks are crimes for which someone must be blamed, over and above the criminals. If thieves broke into someone's home and stole all the valuables, would the homeowner be at fault? There are circumstances in which the answer would be "yes." If the owner were in cahoots with the bandits, it would probably be an insurance scam that would land him in the calaboose. Or if the proprietor left all the doors and windows open, with a sign in the hallway saying, "The jewelry is in the breadbox,"[7] there might be significantly less sympathy for the losses incurred. This thinly veiled analogy is meant to establish the only reasonable reasons for firing or prosecuting any employee for reasons related to a cyberattack. If that person colluded with the attackers, dismissal and prosecution are well called for, though I have never heard of such an attack.[8]

STEVEN J. ROSS | CISA, CDPSE, AFBCI, MBCP

Is executive principal of Risk Masters International LLC. He has been writing one of the *Journal*'s most popular columns since 1998. Ross was inducted into the ISACA® Hall of Fame in 2022. He can be reached at *stross@riskmastersintl.com*.

Contributory Negligence?

But is contributory negligence an apt comparison? I suppose there might *hypothetically* be an information security manager somewhere who cares so little about the data in his care that no identification or authorization is required to access them; viruses are allowed to run riot; and no backups are made. Very hypothetically. If there were such a person, the blame should fall on the managers who hired this dolt in the first place.

Assuming that basic security—however defined—is in place, how can blame be assigned for the actions of malicious outsiders? It is worth noting that cyberattacks have been perpetrated against some businesses and governments that have invested heavily in information security products and personnel. If they had only spent another million or so, would that have succeeded in deterring an attack?

Even then, all that investment might be for naught if the attackers should use trickery to steal the credentials of someone with privileged access to the systems and, therefore, to the data. Compromised credentials are certainly a contributing factor to cybercrimes, though there is considerable controversy as to how great a factor credential theft might be. A simple search reveals statistics that suggest 37 percent[9] to 81 percent[10] of cyberattackers use stolen credentials.

There is little question that phishing and spear phishing are involved in many cyberattacks.[11] Anyone who is fooled by a phish deserves embarrassment, but not dismissal. Let anyone who has never been tricked cast the first stone. I will not.

> Anyone who is fooled by a phish deserves embarrassment, but not dismissal.

Protection Against Blame

Many of the readers of this *Journal* are or may someday be IT directors or chief information security officers (CISOs). Sadly, my friends, your jobs may be on the line should there ever be a cyberattack on your watch. There are, however, some practical recommendations I can make to help you if that day ever comes:

- **Educate your superiors.** They ought to know what practical steps you have taken to prevent, detect and recover from cyberattacks. More important, they should know what their responsibilities for cybersecurity might be.
- **Document the actions you take successfully to deal with any attacks that do occur.** If you ever need to defend yourself, you will have the evidence with which to do so.
- **Apply a standard of due care.** There is no end to the steps that might be taken to protect your systems, but there is an end to budgets. So, determine the best use of the resources available to you and then…
- **Get approval for what you are doing.** Present what you are doing to protect the organization from cyberattacks and then get formal assent from the board and/or the executive committee that these measures are enough. As never before, the IT auditor can be your friend! And if the executives want greater protection, ask them for the resources needed to get to that point.
- **Stand up for any of your staff who might have been tricked into abetting an attack.** There is nothing to be gained from blaming underlings, but you will lose the trust of your people if you turn on one of your own.

It is small consolation, but the job and reputation of everyone in your position is on the line. Alas, no matter how many times you win the war against the attackers, sometimes the bad guys win. Losing just one time is going to be painful. But it is the organization's pain, not yours to bear alone.

LOOKING FOR MORE?

- Read *Reporting Cybersecurity Risk to the Board of Directors. www.isaca.org/reporting-cyberrisk-to-bod*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Endnotes

1 Maslin Nir, S.; "How a Cyberattack Plunged a Long Island County Into the 1990s," *The New York Times*, 28 November 2022, *https://www.nytimes.com/2022/11/28/nyregion/suffolk-county-cyber-attack.html*

2 Maslin Nir, S.; N. Schweber; "How Hackers Used One Software Flaw to Take Down a County Computer System," *The New York Times*, 21 December 2022, *https://www.nytimes.com/2022/12/21/nyregion/suffolk-county-cyberattack.html?searchResultPosition=1*

3 Metz, C.; "Former Uber Security Chief Found Guilty of Hiding Hack From Authorities," *The New York Times*, 5 October 2022, *https://www.nytimes.com/2022/10/05/technology/uber-security-chief-joe-sullivan-verdict.html*

4 Waterfield, P.; "IT Director Fired Following Lake City Ransomware Attack," *InfoSecurity*, *https://www.infosecurity-magazine.com/news/it-director-fired-lake-city-1-1/*

5 Staff, "Peebles Media Group v. Patricia Reilly: Full Case Report," *Scottish Financial News*, 19 November 2019, h*ttps://www.scottishfinancialnews.com/articles/peebles-media-group-v-patricia-reilly-full-case-report*

6 Blumenthal Nordrehaug Bhowmik De Blouw LLP, "Alleged Hack: Fired Employee Sues SF State for $1M," 26 September 2016, *https://www.bamlawca.com/california-labor-laws/alleged-hack-fired-employee-sues-sf-state-for-1m*

7 A box once found in every home (in the United States, at least) for storing bread and other baked goods. Also used for sizing, hence "bigger than a breadbox." I just thought readers ought to know.

8 I make a distinction between collusion and attacks by trusted insiders. I know of no instance in which an employee worked with external attackers to steal money or information assets. One-person breaches of trust are, alas, still occurring. I am most familiar with the data breach at Canada's Caisse Desjardins, in which an employee stole the personal information of millions of the bank's customers. Benessaieh, K.; "Vol de données chez Desjardins: la catastrophe, un an plus tard", *La Presse de Montréal*, 19 June 2020, *https://www.lapresse.ca/affaires/entreprises/2020-06-19/vol-de-donnees-chez-desjardins-la-catastrophe-un-an-plus-tard*

9 Jones, C.; "Fifty Identity and Access Security Stats You Should Know in 2023," Expert Insights, 6 January 2023, *https://expertinsights.com/insights/50-identity-and-access-security-stats-you-should-know/*

10 Staff, "Over 80 Percent of Hacking Related Breaches Were Related to Password Issues: Cybersecurity Trends," CloudNine, *https://cloudnine.com/ediscoverydaily/electronic-discovery/80-percent-hacking-related-breaches-related-password-issues-cybersecurity-trends/*. This is actually a misrepresentation of figures in Verizon, *2022 Data Breach Investigations Report*, USA, 2022, *https://www.verizon.com/business/resources/reports/dbir/*, but it does illustrate the confusion around this subject.

11 Stone, A.; "Phishing Attacks Are What Percentage of Cyber Attacks?" Safeguard Cyber, 19 March 2021, *https://www.safeguardcyber.com/blog/security/phishing-attacks-are-what-percentage-of-cyber-attacks*. This blog post says that phishing was used as an entry point for almost one-third of all cyberattacks, yet another useless and unsupportable statistic.