Cyber Attacks: Is the ‘Big One’ Coming Soon?

DAN LOHRMANN

MARCH 13, 2021

In the past 90 days, the world has witnessed a serious escalation in cyberattacks. Some experts are still predicting that the worst is yet to come. Are we prepared?

Many CSO, CTOs, military leaders, and even some global company CEOs, are now saying yes.

Quick Recap

2020 was the year that the COVID-19 crisis also brought a cyber pandemic.

Late last year, the security industry’s top experts from global cybersecurity company leadership predicted even worse cybersecurity outcomes for 2021 compared to what we saw in 2020.

And in December, we learned about how SolarWinds’ Orion vulnerability was compromised, causing one of the worst data breaches in history that is still evolving for about 18,000 organizations.

Earlier this month, Microsoft said there were vulnerabilities in its Exchange Server mail and calendar software for corporate and government data centers. The vulnerabilities go back 10 years and have been exploited by Chinese hackers at least since January, according to CNBC and others who see more serious attacks coming from criminals based on these issues.

Taking a Step Back

What we now know (as of mid-March 2021) is that the security incidents just keep coming at us faster and with more serious consequences. From a continued explosion in ransomware attacks to a record number of data breaches to pledges for much more cybersecurity support in the U.S. and abroad, global headlines proclaim that these criminals must be stopped.

In the past few weeks, we have also seen unprecedented statements from Kevin Mandia, the CEO of FireEye, on several topics. Here are two examples:

"The next conflict where the gloves come off in cyber, the American citizen will be dragged into it, whether they want to be or not. Period."

- *"Apps won't work. Appliances may not work. People don't even know all the things they depend on. All of a sudden, the supply chain starts getting disrupted because computers don't work…."*
- *"The problem is nobody knows what the rules are. There's no written document on what the rules are," he said.*
- *"And I don't know if you will get people to agree to rules on espionage because of the asymmetry where most countries can't beat us with tanks, can't beat us with airplanes. But in cyber, maybe that's where they can make investments and beat us."*

"Cyber sleuths have already blamed China for a hack that exposed tens of thousands of servers running Microsoft's Exchange email program to potential hacks. The CEO of a prominent cybersecurity firm says it now seems clear China also unleashed an indiscriminate, automated second wave of hacking that opened the way for ransomware and other cyberattacks.

The second wave, which began Feb. 26, is highly uncharacteristic of Beijing's elite cyber spies and far exceeds the norms of espionage, said Kevin Mandia of FireEye. In its massive scale it diverges radically from the highly targeted nature of the original hack, which was detected in January."

In another recent report, we learned from security researchers that at least 10 hacking groups have been using a Microsoft software flaw: "ESET's blog post said there were already signs of cyber criminal exploitation, with one group that specializes in stealing computer resources to mine cryptocurrency breaking in to previously vulnerable Exchange servers to spread its malicious software.

ESET named nine other espionage-focused groups it said were taking advantage of the flaws to break in to targeted networks — several of which other researchers have tied to China. Microsoft has blamed the hack on China. The Chinese government denies any role.

Intriguingly, several of the groups appeared to know about the vulnerability before it was announced by Microsoft on March 2. …"

Florida Water System Hit

Adding to the increased pressure is another cybersecurity incident in which a Florida hack exposed danger to water systems: "On Feb. 5, a plant operator for the city of about 15,000 on Florida's west coast saw his cursor being moved around on his computer screen, opening various software functions that control the water being treated. The intruder boosted the level of sodium hydroxide — or lye — in the water supply to 100 times higher than normal.

Sodium hydroxide, the main ingredient in liquid drain cleaners, is used to control water acidity and remove metals from drinking water in treatment plants. Lye poisoning can cause burns, vomiting, severe pain and bleeding.

After the hacker exited the computer, the operator immediately reduced the sodium hydroxide back to its normal level and then notified his supervisor, Pinellas County Sheriff Bob Gualtieri said at a news conference a few days later. Even if it hadn't been quickly reversed, the system has safeguards and the water would have been checked before it was released, so the public was never at risk, he added."

Is Wider Cyber Failure Possible?

A recent Security Magazine article asked, "Is the World Economic Forum's prediction of a global cybersecurity failure in the next 10 years avoidable?"

The article quotes an important World Economic Forum Global Risk Report:

"The situation is not forecasted to improve, unless deliberate and sustained action is taken — swiftly and broadly. Cyber crime costs are expected to reach a staggering $10.5 trillion per year by 2025 — just around the corner! According to AT&T's cybersecurity insights guide for CEOs, "50 percent of organizations haven't updated their security strategy in 3+ years." Their lack of action will be costly, especially as cyber criminals continue to iterate new strategies to keep up with evolving security innovations. The AT&T guide for CEOs recommends that enterprises identify and assess risk areas across applications, devices and people, perform threat analyses to automate responses to abnormal activity, adapt systems that allow for issues to be resolved remotely, and create action plans so that all relevant parties are empowered to respond effectively when facing a breach. …"

Leaders Warn of U.S. Cyber Vulnerabilities

One more before we wrap us this powerful case. CNBC reported this past week that CEOs worried about where this could go if these attacks get worse. At the Yale CEO conference, Ajay Banga, who is the Mastercard executive chairman, said we are not preparing for the worst case scenario with cybersecurity. "They will not only come after banks, they will do the FAA, traffic lights and the hospitals in the same day. We do not do exercises cross-sectors — we barely do exercises."

This recent heightened state is raining new red flags. While some are seeing even bigger problems coming soon, others are saying we need to remain calm and keep working the problems — and NOT say the sky is falling.

Indeed, this article from the CATO Institute has a somewhat misleading title: "The Russian 'Cyber Pearl Harbor' That Wasn't."

In reality, the article says: "For almost three decades, we have awaited a mythical 'cyber Pearl Harbor,' the harbinger of digital doom that the U.S. cybersecurity community assumes to be inevitable. Strangely enough, some believe this cyber Pearl Harbor already happened twice within the last two months. …

Hyperbole needs to stop and rational consideration of the impact of the SolarWind operation will take time and sober thought, not instant hot takes. Infiltration and extracting information is not an act of war, but evidence of the typical espionage operations that are conducted against near peer adversaries. Denying future operations will require a sober assessment of how to enable the defense when the attacker has many attack options. This will likely not come solely through government action, but collaboration between industry, the private sector and government agencies that provide for collective defense."

Final Thoughts

Taken separately, any one of these reports or recent security incidents may seem like the same, steady level of cyberattacks we have seen over the past decade. No doubt, the world has seen

numerous difficult situations (from Snowden to the OPM breach) and navigated the cyber waters without serious escalation.

But is something much worse coming? And if so, when?

As for me, I honestly don’t know, but I’m worried. Recent cyberattack patterns do seem worse than normal, and I think we need to listen closely to Kevin Mandia, who has much more information than I do.

Can someone please connect these dots before it's too late?