Freedman Consulting, Inc.
CHANGE . . . RESULTS . . . SUCCESS

CYBERWARFARE: WILL YOU BECOME COLLATERAL DAMAGE?

Ellen Freedman, CLM

According to Wikipedia, Cyberwarfare is "*the use of digital attacks against an enemy state, causing comparable harm to actual warfare and/or disrupting the vital computer systems…. While there is debate over how to define and use 'cyberwarfare' as a term, many countries including the United States, United Kingdom, Russia, China, Israel, Iran, and North Korea, have active cyber capabilities for offensive and defensive operations.*"

Much debate rages about the appropriateness of the term. It has been suggested by scholars, political pundits, and security experts that more appropriate terms are cyberterrorism, unpeace, cyberwar, and militarization of cyberspace, to name but a few. From a pragmatic standpoint, to paraphrase a famous bard, a rose is a rose, no matter what you call it. And right now, our world reeks of rose.

I grew up on science fiction. I have lived long enough to witness how far-fetched ideas hatched in the minds of authors have played out years, often decades later, in reality. Every morning when I put on my "Dick Tracy" watch, (the Apple Watch), I am reminded of this fact.

In our country, we have seen an increasing number of successful and highly disruptive attacks. While most acts were perpetrated by cyberterrorists or cybercriminals, there is no doubt that foreign powers have directed or supported many of these attacks. Nor that there have been retaliations, both in similar kind and in true military action. For example:

- In June 2019, the United States launched a cyberattack against Iranian weapons systems in retaliation to the shooting down of a U.S. drone in the Strait of Hormuz.

- In 2018, the cyberattack on the Marriott hotel chain that collected personal details of roughly 500 million guests is now known to be a part of a Chinese intelligence-gathering effort that also hacked health insurers and the security clearance files of millions more Americans.

- In June 2015, the Office of Personnel Management data breach, in the U.S., was widely attributed to China.

- In mid-July 2010, security experts discovered a malicious software program called Stuxnet that had infiltrated factory computers and had spread to plants around the world. It is considered "the first attack on critical industrial infrastructure that sits at the foundation of modern economies," noted *The New York Times.*

- in April 2009, reports surfaced that China and Russia had infiltrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system.

Cyberwarfare is becoming a tactic of choice by many nations. It is a relatively cheap and low-risk option to weaken other countries while strengthening the user's own position. Long-term persistent attacks can cripple economies, change political views (think about the 2016 presidential election) and create unrest and conflict in targeted nations. It can reduce military readiness and efficiency. On this last point, the concern is such that all four branches of our military are actively recruiting people with "the right stuff" to fill cyberwarfare positions.

Think about the increasing volume of attacks on U.S. health care systems, energy supply systems, school systems, transportation systems, local government systems, financial institutions, telecommunications, internet service providers and so much more.

What has spurred me to write this article is the sudden increase of attacks to systems we depend on for information and communication. I'm referring specifically to email, text messaging and social media platforms such as Facebook, LinkedIn, Twitter, Instagram, TikTok and so forth. We're so used to many of these missives, that they don't rise to the level of concern. But make no mistake, you should be on red alert.

I invite you to search Google News for "cyber attack" to confirm what I say. Just one article in *Insurance Journal*, titled "10 Cyber Attacks in 2021 Cost $600M With 40,000 Businesses Put at Risk," made the hair on my neck stand up.

Russia has a long and clear history of using cyberwarfare in advance of and in conjunction with military action. When they invaded Ukraine, their cyberwar was already well underway, targeting many nations. And other terrorist groups and criminals are happily piggy-backing on those efforts for their own rewards.

Members of the Solo & Small Firm Section of PBA are sharing the sudden increase of everything from malicious emails to friend requests from Facebook people who turn out to be impersonators. Just today, someone innocently asked what possible harm it could do, that they accepted a friend request from an impersonator? Good question. One might also ask what harm there might be accepting a connection request from someone you barely know on LinkedIn. After all, isn't the whole purpose to have more connections? Another good question.

First, the increase in malicious emails and text messages are clear to all of us. We know what can happen if we click on a bad link, open an infected attachment, or even click on an infected picture or cartoon to save it to our own system. But the difference right now is that the caliber of phony communications is so good that even seasoned pros with their antennae up are being fooled.

It only takes one attorney or the attorney's staff member to click on a bad link. It takes only one distracted person who fails to look extra closely, or take the longer, safer route to open up the browser itself and put in the URL they've saved in bookmarks. It takes only one person to not first pick up the phone and say, "what is this document you sent me?" And then . . .

All the firm's information becomes vulnerable. The firm computers may be encrypted by ransomware. Sensitive client information may be sent out in bits and pieces to all those in your contacts list. Your data may be mined for information covered by Health Insurance Portability and Accountability Act (HIPAA) or personally identifiable information (PII) regulations, exposing you to huge financial penalties and bad press. Everyone in your contacts is now on the list for attack. And that includes your best clients. Your trust account and/or operating account may be plundered.

Once I accepted a friend request on Facebook from an impersonator. It opened up all my friends to exposure. Many were outright hacked. A few had profiles stolen. Many were friended successfully. Information for identity theft was obtained. Private malicious messages, and sales messages, were bombarding them. Worst, fake postings with inflammatory fake news rapidly appeared. All my fault for not taking an additional 30 seconds before hitting "Accept."

Freedman Consulting, Inc.
(215) 628-9422

For the same reasons, based on experience, I am very careful about whom I accept a connection request from on LinkedIn. To the point where I first ask, "why are you trying to connect to me?"

At a bare minimum, you should:

- Back up computers to two locations daily.
- Be sure about what you're clicking on or opening.
- Be vigilant online to ensure you're on a "real" site.
- Use two-factor authentication passwords.
- Retrain everyone at the firm in computing security.
- Change long-term passwords and ensure new ones are long and strong.
- Make sure all your software is up to date.

Folks, there's a real war happening overseas, and in cyberspace. Like it or not, you might be drawn into it. I urge you to be hypervigilant. Also, take all online news you read with a grain of salt proportionate in size to the reliability of the author. Make sure your staff members read this article, too! Don't become collateral damage.

A version of this article originally appeared in the March 21, 2022 issue of the Pennsylvania Bar News.

Freedman Consulting, Inc.
(215) 628-9422