WRITING SAMPLE

Publication: Lone Star Health News
Publish date: July 8, 2021

Lone Stars on the Medical Frontier: Marcus J. Carey is on guard against hackers

By Mary Ann Roser

The Colonial Pipeline hack in May caused gasoline supply disruptions and price hikes. It also caused more Americans to notice a sharply escalating problem that can disrupt lives in various ways: ransomware attacks.

Since this year began, the health care sector has faced more ransomware threats than any other industry—an average of 109 attack attempts a *week*, according to Check Point Software Technologies Ltd.

The September attack on Universal Health Services (UHS) shows what can happen. UHS, which operates more than 400 U.S. hospitals and care facilities, lost $67 million in the breach, and the effects were "alarming," according to a *HealthITSecurity* article. In the attack, "ambulances were rerouted, radiation treatments for cancer patients were delayed, medical records were rendered temporarily inaccessible and, in some cases, permanently lost, while hundreds of staff were furloughed as a result of the disruptions," the article says.

Cybersecurity expert Marcus J. Carey of Austin recently spoke with *Lone Star Health News* about why cyber criminals seek out health care companies and what can be done to protect patient data and minimize ransomware payouts. He became adept at coding and encryption as a Navy cryptologist, between 1993 and 2002, and has been an innovator in the field ever since. In 2014, he founded Threatcare and served as its CEO until October 2019, when the company was acquired by Tampa-based ReliaQuest. Now Carey is the enterprise architect at ReliaQuest, developing cybersecurity solutions for clients.

He also has authored books on hacking and cybersecurity, including being the creator and co-author of the *Tribe of Hackers* series. Carey's comments for this Q&A have been condensed and lightly edited.

As I understand it, ReliaQuest works with the health care sector—among others—on data security. From where you sit, what cybersecurity issues does the industry face and what should they be doing?

We have a ton of medical companies we work with, and it (hacking) is a big, big problem in health care and everywhere now. Hospitals and health care providers need to consider the insurance liability of getting breached and having data that's probably going to get compromised. There are even ransomware policies they can take out in case they get sued. So, they want to make sure they have insurance in place, and they need to understand to whom they report. It varies from state to state.

You also need an incident response (plan), and you need technical staff to mitigate the risk as well. Incident response is the best way to recover from ransomware, and the most effective thing you can do is to have your data backed up. Every hospital, every organization, needs good backups and they need to be in a place so that attackers can't get into them, too, because what we've seen is, attackers encrypt the main data and the backup data. We tell people crisis communications are very important. You want to make sure you have some kind of … statement crafted beforehand on what you are going to say when this happens. If you can't restore data from the backups, then you need to ask: Are we going to pay the ransomware?

Most organizations, especially hospitals, do pay, don't they?

Many people do because they don't have the (computer system) backups in place. So, you need people who are skilled and who understand how to negotiate ransomware. It's almost like a sales process. It could be a third party (doing the negotiating), but every organization has to consider this.

Just to digress for a moment: Given your military expertise, do you agree with those who say the next war will be a cyberwar? If so, what form will it take?

It's a component of an overall war, but there has to be a physical component to war. We call this kinetic warfare—shooting, guns. I think cyberwar is an aspect of a kinetic war, and it's going to be a part of every future war, whether it's intercepting information, like plans of the enemy, having the energy grid go down, or something like that.

Is the U.S. prepared for that?

The U.S. is very prepared for that aspect of a war. My background is from DOD (Department of Defense). The U.S. is heavily invested in cyberoperations, as are other countries, like Russia. So, the military is very prepared, but I don't think civilians are. Power grids are trying to be more secure, hospitals and supply chains are trying to be more secure. But a lot of businesses don't have good defensive capabilities and are hurting.

I would have thought the Colonial Pipeline hack would have been a huge wake-up call…

It was a big wake-up call. It showed that it (a hack) can affect the economy. Now all the people in boardrooms in every organization are talking about it and asking, what if this happened to us? In the past couple of weeks, we've had an uptick in people asking for our business.

Why are health care companies vulnerable to ransomware attacks?

They have volatile systems (memory is lost when the computer is turned off), and the more volatile the systems are, the less you can actually patch them and upgrade them. Certain machines at a hospital always have to be on and always have to be available. Systems at hospitals have to be certified, so sometimes you can't patch them or it would break the certification, or accreditation. You can upgrade it, but it's a laborious process.

Sometimes the software won't work with anything else, so hospitals can't upgrade to the latest version of Windows because it would break the software. Some hospital systems are old, and that's the biggest problem. The culture of hospitals also is an issue. It's a more open culture when they're university hospitals, so basically people don't take security seriously. A cultural shift is needed, and I think we'll get there.

Do the cyberthieves want to use patient data for some nefarious purpose or do they just want the hospital to pay ransomware?

It's 100% percent about the money. They don't care about anything else.

Would they sell my health data if the hospital doesn't pay up?

They'll start leaking the data if they don't pay. They'll say to the hospital, you have until midnight Friday or I'll start leaking your data. So, many pay the ransom.

What alternative do they have? These criminals are hard to catch.

The alternative is to have an amazing backup. If they don't, they have to know how (the criminals) got in before they pay and make sure they can't come in again.

This could take a few weeks, right?

It could take months.

Meanwhile, the computers are not accessible.

Some systems could be inaccessible, and the organization tries to do without them so they can get the situation fixed.

Why is it so hard to find the criminals?

They're overseas and in different Eastern Bloc countries that the U.S. doesn't have a good relationship with. If they're in Russia, it would be hard to extradite them. They've got a free-for-all in some cases.

Do we know who they are? Or are they unknown because they require victims to pay with cybercurrency (like Bitcoin)?

Sometimes we know who they are, and sometimes we don't. It's really hard to track them because they're taking cryptocurrencies. But in some cases, they're openly flashing their stuff on Instagram. They're loud and proud.

Are the criminals a step ahead of companies trying to protect their data?

The vendors who make software, they're building modern systems to be more secure. Back in the day, the systems weren't built that securely. Over time, we've been seeing more software companies, like Microsoft, understand the security implications. It's actually getting harder and harder to hack the systems themselves, However, what's easy to hack is humans. If they want to break into a system, they'll send a doctor or a salesperson a phishing email. That's the main way somebody gets hit. Spear phishing means targeting a particular person. Then if the person clicks on the link, there might be a spear phishing attachment. All those rely on the user doing something they know they shouldn't do, but they get tricked into doing it. We call it social engineering: I'm going to convince you that you need to open this email and download this. No matter how good the systems are that you put in place, it all falls down if someone gets tricked. Ninety percent of the time, it's because somebody clicked on something.

What innovations are used to stop people before they do that? Is there a way to protect people from themselves?

We used to think if you have an antivirus firewall, no one could hack you. We're past thinking that now. The new buzzword is *zero trust*, which is validating that people are who they say they are. The zero-trust model and identity management will continue to be used for identification, authentication and authorization. That's the future.

How does it work?

Most people are using two-factor authentication. So, I log in and have to use a code on my phone to validate it's really me.

Are we getting to a place where we can out-think the attackers?

The attackers are using the same thing they were using 10 years ago. With the advent of cryptocurrencies and ransomware, it's an official business enterprise with untraceable funds. Cryptocurrencies have emboldened people to do crimes and get paid. That's where we are. That is the big change. A lot of this has been around forever, and the criminals are not so far

ahead of anybody. What they do is prey upon people who are vulnerable … and get paid with untraceable funds.

What advice do you have, including for individuals?

It's not about if it's going to happen, it's about when it's going to happen. You've got to be prepared, you've got to patch early and often. Avoid using the same password. That's the easiest way hackers get into your bank account. Use a password manager. Let the password manager decide your passwords. I don't even know my passwords. I'll save my passwords to Google Chrome and use the Chrome password manager. We have come a long way, but there's still a long way to go.