OUTLOOK

HEALTH

It's time to tackle obesity

By Gracie Cavnar

Put down that cheeseburger and wrap your brain around this: A recent report from the Robert Wood Johnson Foundation projected that half of all adults in the U.S. will be obese by 2030. To make matters worse, the RAND Corporation (which was the first to predict the collapse of the Soviet Union) just declared the collapse of the American waistline with the news that the number of morbidly obese in this country has doubled since 2010. Obesity has now replaced smoking as the No. 1 health hazard in America.

These trends aren't just alarming, provoking unprecedented rates of chronic diseases striking at early ages, and expensive, with obesity expected to cost U.S. taxpayers and businesses $370 billion by 2030. They are also a danger to our national security, as our generals report that 25 percent of American military recruits are unfit to fight.

Texas is one of the fattest states: According to the Centers for Disease Control, more than 30 percent of Texas children ages 2 to 5 are already either obese or overweight. We know that obese children tend to become obese adults, but we also know that in most cases obesity is preventable. No one would knowingly put a child's health at risk, but the sad truth is that many of us are unintentionally doing that every day. Our kids deserve better, and it's time we do something about it. And by we, I mean all of us — government, parents, educators and the private sector, working together.

Mayor Annise Parker and the Houston City Council understand the gravity of the situation all too well, which is why I was encouraged by their recent launch of the Healthy Houston Task Force. The group is charged with educating Houstonians to recognize, prevent and treat obesity; address changes in the built environment to support healthy lifestyles; make affordable, healthy food more accessible; promote worksite wellness; and teach children and their families healthy habits.

Without a doubt, a child's most influential teachers are parents, so critically important lessons about healthy living begin at home: Turn off the TV, video games, computers and smart phones to take a regular family walk and give your kids unstructured time to play outside. Add more fresh vegetables to family meals and involve your kids in grocery shopping, gardening and cooking. Like the old saying goes: The family that cooks healthy meals together avoids Type 2 diabetes together.

Our kids spend most of their day in school, which should be a centerpiece of healthy living. The Houston Independent School District and other districts deserve credit for getting school lunches in line with new federal nutrition standards. That's a step in the right direction, but more is needed. What good is a healthier menu when students can grab an ice cream sandwich for lunch instead or have unlimited access to vending machines? Let's get the junk out and the good food in. Period. No physical education? We should demand it and nutrition education to boot. But most importantly,

What good is a healthier menu when students can grab an ice cream sandwich for lunch instead or have unlimited access to vending machines?

our educators need to walk the talk. You are our children's role models.

Did I mention how much this crisis is weighing down our wallets? Health care for obese citizens costs 42 percent more than for normal weight ones. But even more breathtaking is the $190 billion the epidemic cost American businesses in 2010. Businesses focused on worksite wellness enjoy more productive employees and reduced insurance costs, so programs that support preventive measures like exercise and healthy lifestyles are win, win, win, since the benefits filter down to the entire family.

Hooray for good corporate citizens who extend their healthy lifestyle culture by encouraging employees to volunteer in school wellness efforts. Hundreds of folks from top Houston businesses like SenseCorp and PricewaterhouseCoopers have helped my foundation, Recipe for Success, build gardens and kitchen classrooms in elementary schools across the city where we have taught 20,000 children about healthy food hands-on and given them lifelong skills to make good decisions. Countless other efforts like Urban Harvest and the Food Bank benefit from corporate partnerships as well. But there is so much left to do. We all need more hands and support to effectively reach Houston's 1 million children.

We have a choice to make as a society: We can do nothing and watch as an entire generation grows from obese children to obese adults, becomes chronically ill and dies young, costing billions of dollars in health care and lost economic activity, and leaving the country without a battle-ready military. Or, we can say, "Enough is enough."

If Houstonians set their sights on a goal, anything is possible. Our mayor, City Council and the Healthy Houston Task Force are saying, "Enough already! Let's fix this problem." I'm ready to do anything I can to make a difference, and I hope you are too.

So, what are you serving the kids for dinner tonight?

Cavnar is founder, president & CEO of the Recipe for Success Foundation, author of "Eat It! Food Adventures with Marco Polo," and a member of the Healthy Houston Task Force.

Houston Chronicle file

Rakhi Desai with Recipe for Success helps serves pizza to a fifth-grade class at Jones Elementary School. The class planted the vegetables in the school garden and then made their own pizza from the vegetables they planted.

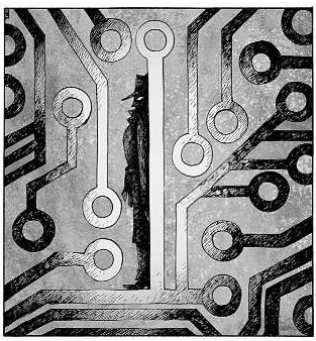
TECHNOLOGY

Let's use caution in enacting cybersecurity rules

By Chris Bronk

After failing to pass a piece of comprehensive cybersecurity legislation in the U.S. Congress this summer, the Obama administration is considering an executive order to provide powers for greater government intervention. Significant intervention will likely be directed at the oil and gas, electricity and petrochemical industries, as they are both providers of critical infrastructure needed for the operation of our economy and society. While there has been significant alarmism in consideration of cyber issues in the past, new developments illustrate how much more possible a catastrophic cyber attack against the U.S. is becoming. For operators of chemical plants the concern has shifted to the possibility of compromised industrial computing leading to environmental disaster, "the cyber Bhopal." Undoubtedly, the risk of these catastrophic scenarios is real and the Obama administration and lawmakers' efforts are critical and well-intentioned, but an executive order should not run the risk of overregulating the energy industry's ever-changing, highly-computerized technology infrastructure.

Recent developments have shown that those wishing to purloin the energy industry's proprietary information resources now regularly target the industry. These attempts include efforts to disrupt entire enterprise computer systems. This is what happened in August to Saudi Aramco. The company stated publicly it had "isolated all its electronic systems from outside access as an early precautionary measure that was taken following a sudden disruption that affected some of the sectors of its electronic network." In the days that followed, news reports speculated that perhaps as many as 30,000 computers on the company's network were compromised by a malicious piece of software, or "malware," possibly the one labeled Shamoon by the computer malware analysis community. Shortly after announcement of the disruption, an ostensibly Middle Eastern group labeling itself the Cutting Sword of Justice declared responsibility for the Aramco disruption and



Paul Lachine

that it would redouble its efforts against the company. Incidentally, I believe Aramco acted wisely in admitting to the problem, much like Google did after actors operating inside China compromised its systems several years ago.

Today, there are likely two major cyberthreats to the energy industry: (1) the vulnerability of its operations systems — computers that route electricity, open valves and operate motors; and (2) the problem of controlling access to proprietary corporate information and data, from internal email communications to long-term development plans and new technologies often carrying investments in the billions of dollars. These are not fantasy scenarios, but rather a consistent and rising set of data breaches and disruptions that have grown from a nuisance to a serious impediment to global business operations.

Though most cyber incidents involve only purloined or corrupted data, at least one case, Stuxnet, apparently damaged physical machinery in the Iranian nuclear enrichment program as well. Repeated compromises of energy company networks indicate they are exposed to a significant set of cyber threats, many produced by foreign countries, but others by more loosely connected activists. A warning sent out last month by the Canadian government to oil and gas firms involved in developing Alberta's oil sands regarding their targeting by hacker organization Anonymous indicates that the set of actors willing to steal information or disrupt operations continues to grow. This represents a potentially serious crisis and one that technology alone, despite advances in anti-virus and intrusion detection systems, has been unable to solve. Due to this failure, Congress has proposed legislation aimed at increasing cyber security in a number of business sectors falling under the heading of critical infrastructure.

But what may public policy in the form of legislation achieve in mitigating the vulnerabilities of the highly computerized and networked companies that produce and deliver energy to the U.S. consumer? Unfortunately, law alone will likely not have the desired results, despite the best intentions of lawmakers.

The nation needs a cyber security framework in which parties opt-in to working with one another without fear of negative repercussion from investors or government. Ideally, the energy industry will choose to pool its resources to solve the major problems that face it, from the construction of countermeasures to spear phishing espionage emails to the development of process control system security best practices and standards, in some form of consortium. Producing such a structure, which incorporates expertise in the measurement of technological, economic and geopolitical risk, may be a preferable alternative to regulation that is unable to adapt as quickly as those who threaten us will certainly continue to do.

Bronk is the Baker Institute fellow in information technology policy at Rice University.