WHAT TO FORESEE WHEN YOU’RE FORESEEING
Navigating the threats and dangers of cyberspace

COMPANIES
As of 2017, phishing emails in the US targeted over 400 businesses every day, draining $3 billion over the last 3 years.

AGENCIES
The US Dept. of Defense experiences 41m scans, probes and attacks a month; in 2016, the NSA’s hacking tools were leaked online.

IoT (INTERNET OF THINGS)
Everything is becoming computerized. For example, in 2015, it was shown that certain cars can be remote controlled.

GOVERNMENTS
It’s been reported that the Russian government influenced the 2016 US election by, among other things, hacking into the DNC and leaking its emails.

PERSONAL DATA
Credit info is stolen but also personal data can be held ‘hostage’ by use of ransomware, where data is encrypted until the victim pays off the cyber criminal to unscramble the data.

OBJECT TRACKING
We are often the weak link. We don’t update software or strengthen our passwords accordingly. We can fall victim to email scams. And we can fail oversight as when in 2013, the US Navy’s network was compromised due to a security flaw even though Navy IT experts knew about it.

A LOT OF MOVING PARTS
With so many moving parts from multiple supply chains that help create products and systems, it can be difficult to develop a wholly secure network. For example, a car whose components come from other suppliers might each have their own code in it, and for the car company to manage and account for data security is a gargantuan task, to say the least.

CULTURE
We have yet to develop a strong security culture where we fully recognize that all aspects of our digital world must involve cybersecurity at all levels. At a time when intrusions into critical US infrastructure and corporations have manifestly increased, data back-ups and strong passwords aren’t enough anymore to thwart the rise of debilitating cyber attacks.

WHAT’S OUT THERE
DEVELOPING SOLUTIONS

BLOCK CHAIN TECHNOLOGY
This is the technology that just might upend the internet and how we move and secure data. It’s a technology where digital assets and transactions are logged into an immutable “ledger” with no single point of failure. Cryptocurrency is built on it but developers are finding other applications for it such as securing medical records and financial transactions.

REDESIGN AND OPEN SOURCE
Institutions and businesses should take the lead and require that cybersecurity be an everyday priority. Companies like Google and Amazon are re-writing their code that keeps credit-card details secure. Others provide “bounties” to anyone that can spot flaws within their systems so as to improve security.

HUMAN NATURE AND ACCOUNTABILITY
It’s not enough to develop the latest cybersecurity technology or redesign security protocols to combat cyber attacks, as cybersecurity breaches are often caused by human error. Thus, just as employees undergo work training so must we include cybersecurity standards within this framework. Cybersecurity has become a fact of digital life. And knowledge and application of it must be as foundational as one’s learning of the multiplication table.