Daniel Burrus'

Celebrating 30+ Years of Publication

TECHNOTRENDS®
NEWSLETTER

The biggest ideas that are changing everything

IN THIS ISSUE

www.DanielBurrus.com

The Cybersecurity of Healthcare

By Daniel Burrus, CEO of Burrus Research

Prior to 1992, the thought of cyber war, cybersecurity and hacking was predominantly constrained to Hollywood fantasy, as seen in the 1983 Matthew Broderick film WarGames, where his character unknowingly hacks into a military supercomputer while searching for new video games. Fast-forward to present times, and with the majority of humankind connected via the Internet and a mobile device of some sort, the level of data breaches and hacking has become horrifyingly real.

> "*Our data is being used or even copied, often without us knowing it*

Horrifying, indeed; the reality is it's happening every day, in some way or another. Our data is being used or even copied, often without us knowing it. Think about it, we willfully input our information on multiple websites everyday, be it Amazon to make a purchase or Uber to call for a ride at the end of the night. Yet, we seem to concern ourselves less and less with the concept of cybersecurity even as breaches become more commonplace in the news.

Trust Must Be Earned

In conjunction with us not fully considering the importance of cybersecurity as an individual, we greatly consider our trust in a company with our data.

We trust companies we use like our bank, hospital, insurance company, and our primary retailer. We also trust state organizations like the Department of Motor Vehicles (DMV), that handles our data and sensitive information they ask for.

We're quick to assume that if they need our sensitive information like our credit card number or even our Social Security number, they must have some heavy-duty security measures implemented to prevent that data from being leaked into the wrong hands.

While that is true, we can never be too sure that a company or even the whole industry they find themselves in is up to the cybersecurity standards that must be utilized in today's fast-paced, ever-changing digital world. And it's amazing how many are selling our information, including the DMV. Presently, one of the biggest, most shocking industries that suffer financially from data breaches and hacking is the healthcare industry.

On the surface, one would think that in our country, that industry and all the incredibly sensitive data involved should be buttoned up pretty tightly, given the fact that not only is the data personal to each and every patient but, in some cases, could be life threatening if altered or deleted.

Presently, the overall cost of a healthcare

TECHNOLOGY NEWS HIGHLIGHTS

Quantum Supremacy

Google recently claimed it has developed a quantum computer that can perform, in a few minutes, tasks that would require 10,000 years for even the most powerful supercomputers today.

Quantum computing is based on the fact that, at the quantum level, a single particle can hold two values. Unlike traditional computers where each bit of information is stored as either 0 or 1, quantum bits – also known as qubits – can be both, and the number of values (which correlates to computing power) grows exponentially with the number of qubits.

For example, two qubits can hold four (2^2) values; ten qubits can hold 1,024 (2^{10}) values; and fifty qubits can hold more than one quadrillion (2^{50}) values.

But qubits are extremely unstable, and creating these elusive particles is a monumental challenge that requires special metals super-cooled to temperatures near absolute zero (-460 degrees Fahrenheit or -273 degrees Celsius).

So, while this represents a huge breakthrough in quantum computing, it is still basically a proof-of-concept design, and it will likely take years to exploit its full potential.

Regardless, governments and venture capitalists are already investing millions of dollars to explore the technology, which would have broad application in many fields including security, cryptography, medicine and materials engineering.

For information: Google, LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043; Web site: https://www.google.com/contact/

Regrowing Cartilage

Wooden Cars

According to recent research, scientists are looking at salamanders and zebrafish to develop possible treatments for osteoarthritis (OA) – a leading cause of disability worldwide. The goal is to use what we already know about the ability of these animals to regenerate limbs and apply it to human tissue repair.

OA is characterized by a degradation of the cartilage in the joints. Currently, once pain levels become severe, joint replacement is the only therapy available. But it was recently discovered that, contradictory to past belief, microRNA molecules similar to those used by salamanders for re-growing lost limbs are also present in humans (albeit to a much lesser degree).

Samples of human cartilage were examined using mass spectrometry, which allowed the researchers to determine the age of the proteins present.

They noted that the proteins got progressively younger the further down the leg they went; in other words, the cartilage was renewing itself at a faster rate in the feet and ankles than in the hips.

By identifying which microRNA molecules humans are lacking, they hope someday to slow the degradation process by boosting the production of these molecules in the joints. The next step will be to conduct experiments in animals to assess the viability of microRNA injections to slow the development of OA.

Japanese engineers have designed a supercar made from cellulose nanofiber (CNF), a plant-based material that is five times as strong as steel but only one-fifth the weight.

CNFs are manufactured from wood pulp that is chemically treated to remove lignin and hemi-cellulose. In addition to being lightweight and stronger than spider silk, they are highly versatile in terms of manufacturability, as they can be combined with resins and rubbers and injection molded into complex shapes.

They are also easily recycled and biodegradable. Applications for these materials range from construction materials to computer components – and now to vehicles.

Known as the Nanocellulose Vehicle (NCV) the futuristic-looking supercar uses CNFs in the bodywork as well as interior components to decrease overall weight by about ten percent.

It is estimated that this would reduce the carbon footprint of each vehicle by sustainably reducing the amount of carbon produced over its useful life by as much as 2,000 kilograms (4,400 pounds). The parts are currently undergoing rigorous testing for strength, durability and longevity.
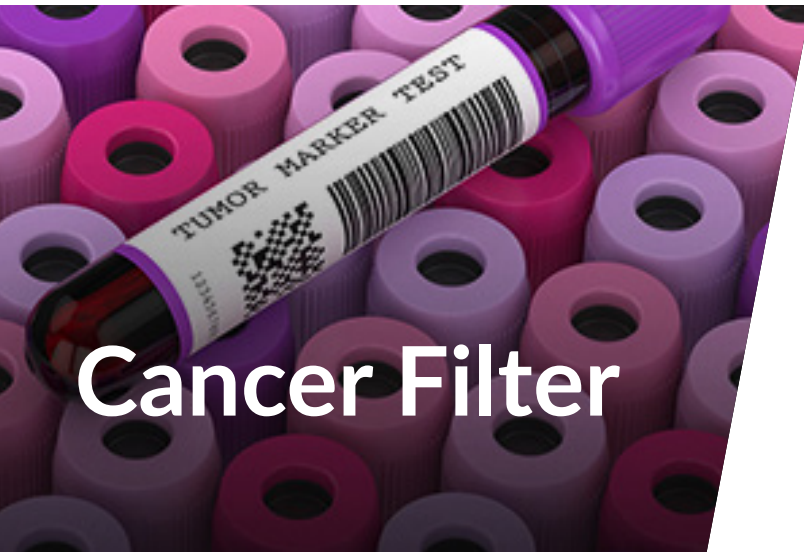
Cancer Filter

Isolating cancer by testing a blood sample is challenging. Small numbers of tumor cells are masked among billions of red blood cells (RBCs), so isolating them is literally like finding a needle in a haystack. But a filter has been developed that effectively removes the haystack and makes it easier to separate the cancer cells by trapping larger white blood cells (WBCs) along with tumor cells (which are similar in size).

The filter consists of a series of channels that are lined with antigens to trap WBCs. 3D printing maximizes the surface area available for attracting the cells by allowing channels to be printed in a zigzag pattern.

Multiple layers are supported with wax that is removed by heating the filter in a centrifuge to melt the wax and expose the channel walls, after which the antigen layers are added. Once the WBCs are removed from a sample, the smaller RBCs pass through a commercially available filter that traps any remaining WBCs and the cancer cells.

The filter was tested by adding a known number of cancer cells to a 10 ml whole blood sample. Results showed that 90 percent of the tumor cells were captured. Because it

requires minimal processing, the new filter also minimized damage to the tumor cells. Prostate, breast and ovarian cancer samples were included in the study, but the method should be applicable to a wide range of cancers.

Recycled Roads

A new process has been developed that mixes recycled plastic bottles with ground-up asphalt from existing roads to re-pave them without adding new asphalt to the mix. Best of all, the resulting pavement is actually stronger than the original hot mix.

The new method – known as G5 100% Road Replacement System – replaces bitumen (the leftover sludge from oil refining) with PET plastic to hold the paving materials together.

Using a machine dubbed a "recycling train," the top few inches of the roadway are removed and ground to a specific size. The old asphalt is then mixed with the liquid plastic before being laid back down.

According to estimates, the process reduces emissions by up to 90 percent because it eliminates hauling out old materials and hauling in new – a savings of about 84

truckloads for every single-lane mile. In addition, repairs can be made at ambient temperatures.

The new method also makes use of waste for which there is currently no use. And in laboratory tests, the manufacturer calculated that the new roads could last up to 13 times longer than traditional asphalt.

The City of Los Angeles will begin conducting tests on two sections of roadway starting in December.

For information: Sean Weaver, TechniSoil Industrial LLC; email: info@technisoilind.com; Web site: http://technisoilind.com/index.html

Thermal Solar Cells

A specially designed molecule that is capable of capturing and storing solar energy to release later as heat is the basis for some new technologies that are far more efficient than current commercial solar cells.

The molecule, which is composed of carbon, hydrogen and nitrogen, is transformed into an energy-rich isomer when exposed to sunlight. It can then be stored in a liquid form for up to 18 years, before being triggered to release the energy as heat with the help of a catalyst.

In one application of the unique molecule, a closed system forms the basis for a domestic heating system. As energy is absorbed by

collection panels, the liquid would be pumped to a storage tank until it is needed. When introduced to the catalyst, the liquid would heat up, be circulated throughout the building, and then be returned to collection panels to absorb more energy.

In another design, the molecule is incorporated into a window film. During the hottest parts of the day, it absorbs heat to keep temperatures cooler indoors.

In this way, it reduces cooling costs by reducing load during peak hours. It then releases the heat for up to eight hours after the sun sets, distributing the energy more evenly over a longer period. The film could be used for buildings or vehicles.

For information: Kasper Moth-Poulsen, Chalmers University of Technology, SE-412 96, Gothenburg, Sweden; phone: +46-(0)31-772 10 00; email: kasper.moth-poulsen@chalmers.se; Web site: https://www.chalmers.se/en/Pages/default.aspx or https://www.chalmers.se/en/departments/chem/news/Pages/Window-film-could-even-out-the-indoor-temperature-using-solar-energy.aspx or https://www.chalmers.se/en/departments/chem/news/Pages/Emissions-free-energy-system-saves-heat-from-the-summer-sun-for-winter-.aspx

CRISPR Cancer Treatment

For the first time in the U.S. doctors have employed CRISPR gene-editing to fight cancer in humans. Although the treatment appears to pose no safety issues, it is too early to tell whether it will improve outcomes.

The method – a form of immunotherapy – takes immune cells from the patient's blood and deletes three genes that have been identified as possibly hindering their ability to attack the cancer.

A fourth gene is introduced to enhance their immune function, and the cells are then re-introduced into the patient's bloodstream as a one-time therapy.

So far, three patients have received the CRISPR-edited cells; two with multiple myeloma and one with sarcoma. All of the subjects had exhausted other treatment options.

To date, one patient has remained stable, one has worsened, and the third is too early in the process to gauge progress. The researchers plan to continue the study with an additional 15 patients.

For information: University of Pennsylvania, Abramson Cancer Center, Perelman Center for Advanced Medicine, 3400 Civic Center Boulevard, Philadelphia, PA 19104; phone: 800-789-7366; Web site: https://home.www.upenn.edu/ or https://penntoday.upenn.edu/ news/positive-results-first-us-trial-crispr-edited-immune-cells

The version on display at the North American Commercial Vehicle Show runs off of four compressed hydrogen fuel tanks, giving it a range of 600-800 miles.

An additional four tanks could be added to extend that range. The current power train delivers 255 horsepower; however the company acknowledged plans to increase total power output to approximately 469 horsepower by the time Neptune reaches the market.

But performance and zero emissions are only part of the story. The futuristic concept truck boasts a sleek, sexy design with a living space that can easily accommodate two people and includes a kitchen, shower, toilet and sleeping area.

It's also fully equipped with the latest technology such as autonomous driving mode, driver monitoring cameras and a windshield that converts to a movie screen.

Production is targeted for 2023.

For information: Hyundai Motor Company, Seoul, South Korea; Web site: https://www.hyundainews.com/

Fuel Cell Semi

Hyundai recently unveiled plans for the Neptune HDC6, a hydrogen-powered semi designed to meet U.S. and European standards.

The Cybersecurity of Healthcare

continued from page 1

breach is about $408 per patient record, not including the loss of business, productivity and reputation of the entity involved.

Annually, the healthcare industry has seen a staggering $5 billion in costs to correct data breaches, hacking and all-around poor cybersecurity measures. This figure is not decreasing, by any stretch, and in addition to the cost to find a solution to these errors, healthcare entities are being fined by the Department of Health and Human Services Office for Civil Rights, sometimes as much as $28 million annually.

Why So Costly?

The cause for the steepness of these fines and losses stems from the reality that, while cybersecurity may not be perfect, and as technology gets smarter criminals do get more savvy as well, many officials feel that not enough is being done to prevent cyberattacks on personal data. Plus, the severity of a data breach in the healthcare industry is immense.

Personal information found in data records is quite valuable on the dark web, and once the damage is done, it is nearly impossible to fully correct. For example, if a credit card number is stolen, the customer can cancel their credit card. But in relation to their health records, the damage is essentially permanent.

Once an individual's medical data has been breached and even distributed on the dark web, who is responsible and what are the direct and indirect repercussions to this? As

mentioned above, the direct repercussions are astronomical annual fines and costs to correct the mangled situation; however, what about trust? How does the individual whose data has been stolen feel about their hospital or clinic, or even their doctor specifically? Once trust has been breached, much like medical data, there is in most cases permanent damage between the patient and the entity.

If a customer goes to a local store, and that store somehow gets hacked and the customer's credit card number stolen as a result, the customer will likely not trust that store any longer in a generalized way, and take their business elsewhere. We've seen large-scale breaches at chain stores, such as Target, in recent years, where customers have then lost trust and moved on from shopping there.

And that is just a store, and just an easily replaced credit card number. Now imagine going to your doctor about some medical troubles you've been having, and being contacted later in the week about how all that information you divulged to your trusted physician is now out there for the world to see. You would feel incredibly violated, and likely wonder if even your doctor was the reason it got out.

Hacking a School

Now, stepping into the hacker's shoes for a moment, they have a tendency to target industries with a lot of data and very little security. School districts have been examples of this in recent years, where ransomware has been implemented, causing delays in public schools starting the year on time, everywhere from New York to Louisiana.

The reason many hackers target school districts is due to the lack of funds and tight

budgets they have to spend on students, let alone the IT departments and cybersecurity. Many schools are too small to even consider funding any type of cybersecurity software.

In contrast to the healthcare industry, hospitals and private practices alike, these entities have much larger budgets in all capacities, therefore it is questionable as to why they seem to be behind the ball on everything.

Since increased hacking is a Hard Trend, how can a hospital better realize that Hard Trend and pre-solve future attacks before they occur? How can they anticipate what's to come, much like an organization outside of healthcare anticipates digital disruption or a competitor possibly putting them out of business?

Finding a Solution in Anticipation

The first thing that would greatly help the situation is a cyber-risk assessment. And believe it or not, many hospitals use an outside vendor to do the job. An outside vendor is a more cost-effective route to take if, given our school hacking example, budgets are often very low for internal help. Plus, preventing cybercrimes is a 24-hour-a-day venture, as software updates are always needed with criminals pinging systems thousands of times a day. It would greatly benefit a hospital or any entity in the healthcare industry to effectively outsource this responsibility to a company that has the capacity to monitor security around the clock.

As an entrepreneur, you too should consider the Hard Trend that cyberattacks on extremely sensitive data hubs such as the healthcare industry is a future fact that will not change, given how digital and paperless everything has become and will continue to be in the future. The cybersecurity market for healthcare is not only a burgeoning market, it is one with a larger, more meaningful purpose. A proverbial way to change the world, so to speak.

If the IT and cybersecurity industry is not the world you find yourself in, there is also the existence of cyber insurance, which hospitals and medical entities are purchasing.

In the case of cyber insurance, covered entities and business associates must conduct a thorough assessment of the threats and vulnerabilities, implement measures to reduce known threats and vulnerabilities to a reasonable and appropriate level, and ensure that any vendor or organization accessing or storing private health information is security compliant.

Because the rapid advancement of digital technology is a Hard Trend that will continue, cyber criminals and their tools constantly improving and disrupting things in a detrimental way is also a Hard Trend. Provided the above examples, healthcare companies and outside entrepreneurs alike should be able to pre-solve future problems before they become disastrous and use their anticipatory mindsets to help move the colossal healthcare industry safely into the future.

If you would like a free perimeter test to check for vulnerabilities in your cybersecurity defense system, please contact us. We have identified best-in-class cyber testing companies that will provide the results of their tests and recommend immediate actions that can be taken to stop any uncovered leaks in your system.

Burrus
Research®