December 2019
VOL. XXXV, NO. 12

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 Banking and Finance

By Daniel Burrus, CEO of Burrus Research

Recently, I wrote an article reflecting on the importance of cybersecurity in healthcare due to the reality that the personal data involved in the healthcare business is extremely sensitive, not to mention the loss of trust, reputation and large amounts of money if hacked.

When a breach of cybersecurity occurs in any industry, be it retail or service industries, one of the most damaging issues at hand is the breach of trust that comes with it. A breach of trust with your doctor or other healthcare institution being my first focus in discussing this hot-button issue reflects just how dangerous cybercriminals are becoming.

If healthcare data and, ultimately, a patient's trust are as sensitive as research shows, then it should be no surprise that the banking and financial industry is even more prone to attacks, thus in serious need for advanced cybersecurity and digital data protection.

> *Socially, many customers would actually get dressed up to go to their financial institution*

Banking Evolution

Consider for a moment how banks have evolved over the history of our country. Up until at least the early eighties, transactions from a customer interface perspective at financial institutions both big and small were handwritten, calculated longhand, and done without the aid of a computer or, oftentimes, a calculator. Socially, many customers would actually get dressed up to go to their financial institution, just to make a deposit! Imagine that contrast!

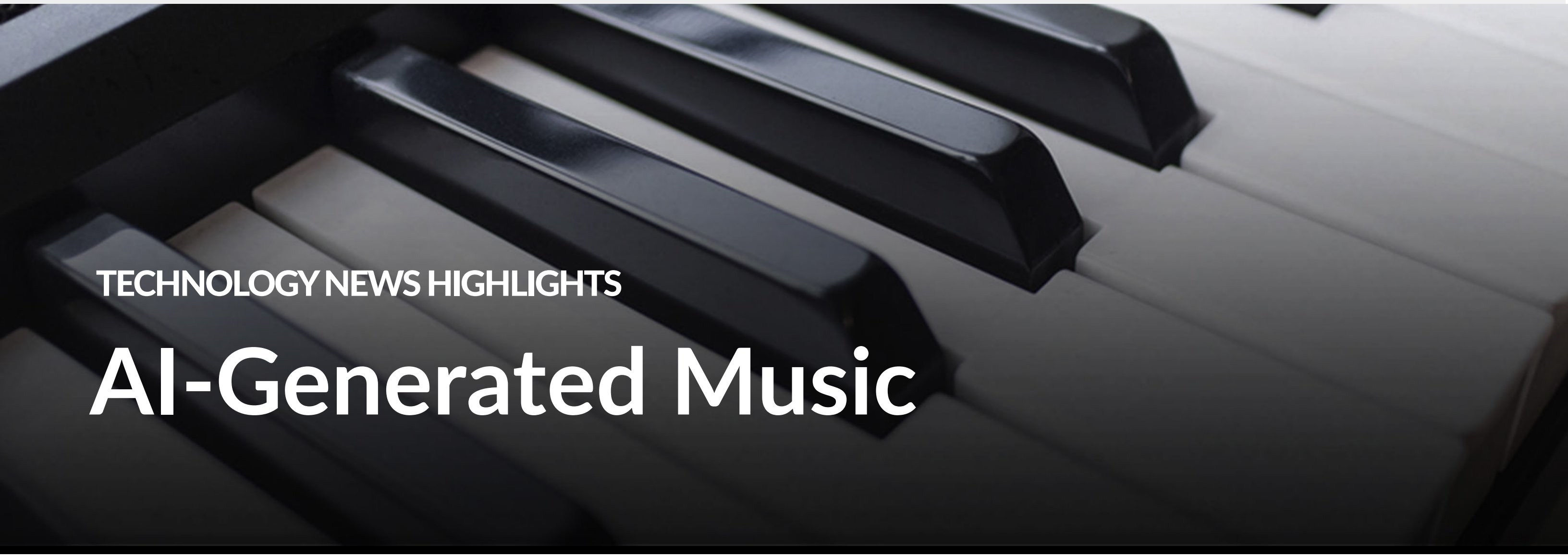
Now fast forward many years and not only can we pay all our bills, as well as deposit money, online and even automate recurring transactions without us ever logging in and pushing a button, but many employees of financial institutions are starting to have the opportunity to actually work remotely as a teller or a branch manager, as digital kiosks replace in-person tellers and redeploy them in new, strategic ways. Midsize and large companies that receive large numbers of checks or money orders from customers have the capability to lease a machine right at their facility to scan in their own checks without ever having to make a bank run on their lunch break.

In addition to simple cash-in transactions, cash-out technology is also replacing physical cash and check exchange in many ways, including but not limited to PayPal, Venmo, Zelle, Apple Pay and many more, where the exchange of money has become a social network of sorts with minimal or no fees, depositing straight into your bank account without a physical bank ever being involved as a middle person, but merely the digital repository where your money sits.

A Breach of Banking Security

Whether you're taking the time to drive to a bank to withdraw some cash, or you're doing

continued on page 8



TECHNOLOGY NEWS HIGHLIGHTS

AI-Generated Music

A musical keyboard that incorporates the latest advancements in machine learning is designed to create original music from a simple input melody. Known as AWS DeepComposer, the system uses generative artificial intelligence (AI) – a technique that "connects the dots" between creative concepts and generates something that is totally new.

In generative AI, two networks (often called generative adversarial networks, or GANs) effectively work to train each other. The first is the generator, which takes the input and creates the output. The second is known as the discriminator. Its function is to provide feedback on whether the output is good or bad, as well as suggestions for improving it. This feedback loop takes only seconds in the SoundCloud, and the result is music that has never been heard before.

The melody is input via a 32-key, 2-octave keyboard, or a virtual keyboard on a touchscreen. The user can select from a variety of musical models, including rock, pop, jazz and classical, and the system will automatically generate a finished song, complete with accompaniments including guitar, bass, synthesizer and drums. In addition, a build-your-own model allows developers to select sample songs from a variety of genres to train the generative algorithm.

DeepComposer is the third in a family of machine learning devices to enhance human-AI collaboration, which also includes DeepRacer (a cloud-based racing simulator) and DeepLens (a camera for developing deep learning-based computer vision apps).

For information: Amazon Web Services (AWS); Web site: https://aws.amazon.com/deepcomposer/

MagLev Train Hits Record Speeds

A testing prototype of a new magnetic levitation (maglev) train was recently unveiled in China that boasts a maximum speed of 600 kilometers (373 miles) per hour.

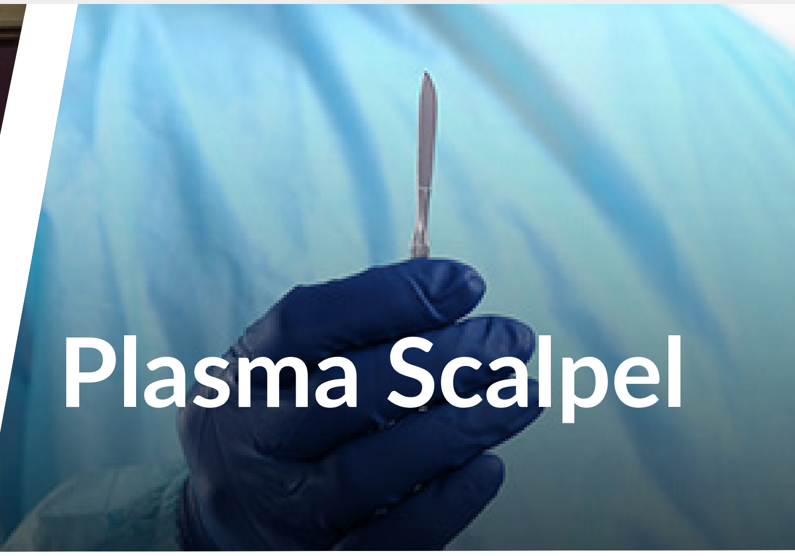
Once completed, the bullet train will be able to transport passengers between Beijing and Shanghai in about three-and-a-half hours – faster than it currently takes to travel by plane.

Maglev trains have been in use in China since 2003. Using powerful magnets, they virtually "float" above the tracks, substantially reducing friction and enabling them to move at extremely high speeds.

This testing prototype will be used to optimize key technologies and system components in anticipation of an engineering prototype scheduled to be released in 2020.

Comprehensive testing and verification will continue through 2021, at which point the new trains will enter production.

For information: China Railway Rolling Stock Corporation (CRRC),Qingdao Sifang Co., Ltd., No. 88 Jinhongdong Road, Chengyang District, Qingdao, China 266111; phone: +86-532-87801188; fax: +86-532-87801688; website: https://www.crrcgc.cc/sfgfen



Plasma Scalpel

A scalpel that emits a small jet of supercharged plasma "soup" has been demonstrated to kill cancer cells that may be left behind after surgery.

While the cold plasma technique has been used in the past to treat infections, sterilize wounds and cauterize tissue, this is the first time is has been used to destroy tumors while leaving healthy tissue intact.

The pen-sized device converts helium into positive ions and electrons. The electrons, in turn, convert the oxygen and nitrogen in room air into a variety of reactive compounds including superoxide, nitric oxide and oxygen atoms.

When sprayed on a tumor site for a few minutes, the plasma interrupts the metabolic processes of the cancer cells to inhibit reproduction.

Based on more than a decade of laboratory work, the researchers have identified the chemicals generated, determined how far they penetrate the tissues, and developed a better understanding of the mechanisms by which they disrupt cancer cells.

In October, they began a clinical trial of 20 patients, all of whom have late-stage, solid cancers such as pancreatic, ovarian or breast cancer. The goal is to fine-tune the optimum dosages to kill the cancer without causing damage to healthy cells.

For information: Mounir Laroussi, Old Dominion University, 231n Kaufman Hall, Norfolk, VA 23529; phone: 757-683-6369; email: mlarouss@odu.edu; website: https://www.odu.edu/ or https://www.odu.edu/ece/news/2019/12/low_temperature_plas

Silk Bioinks

As we've reported in the past, 3D printing is being widely used to generate tissues and even organs for human implantation.

Most of these methods utilize collagen as a scaffold for cells to grow, but a new technique has been developed that uses wild silk to build the supporting structure.

Before it can be used in humans, collagen (which is extracted from animal remains) must be purified – a process that is costly and complex. On the other hand, silk can be easily removed as a liquid from silkworm glands, or fibers can be dissolved in solvents to be deposited layer by layer using a 3D printer.

Wild silk also has natural properties that enable cells to adhere to the matrix without the need for chemical binders. And once the cells grow, the silk scaffold safely reduces to amino acids.

Prototype structures of bone, heart and liver tissue have already been developed. Next the researchers hope to create a human knee meniscus and reconstruct the intricate cartilage structure at the ends of a bone.

For information: Biman Mandal, Indian Institute of Technology Guwahati, Surjyamukhi Road, North, Amingaon, Guwahati, Assam, 781039, India; phone: +91-361-258-3000; email: biman.mandal@iitg.ernet.in; website: http://www.iitg.ac.in/ or http://www.iitg.ac.in/biman.mandal/index.html

Real-Time Interpreter

Google has announced that their AI-powered interpreter tool will be available for Android and iOS devices as part of their Google Assistant.

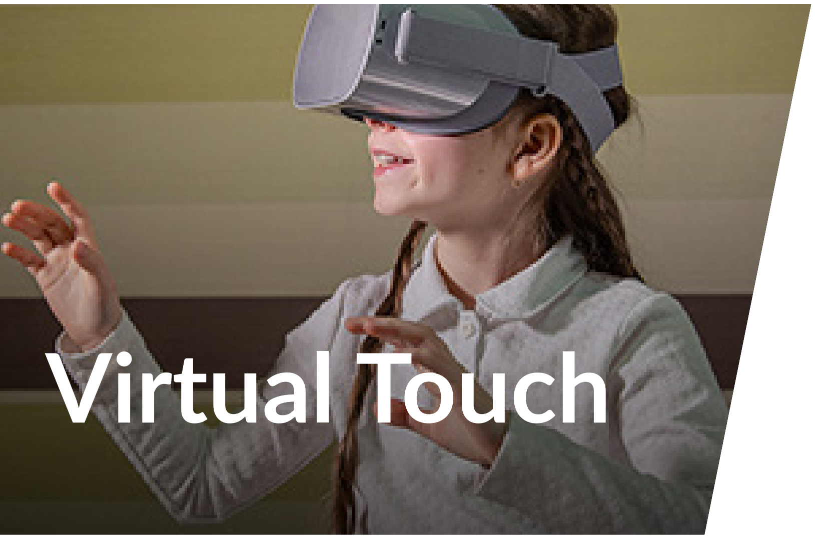
When the assistant is activated, the user simply says something like "Translate into German" and then speaks a phrase. The smartphone responds and listens for further input. The feature also works with keyboard input and can translate 44 languages, including Mandarin and Greek.

Interpreter mode is an obvious benefit

for travelers, allowing them to carry on a conversation in real-time while speaking different languages.

Although it's not the first development for translation-on-the-go, the sheer volume of users represented by Android and iOS means that it will have a huge impact in the market.

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



Virtual Touch

A soft, silicon "skin" embedded with sensors, actuators and wireless communication could someday add the sense of touch to virtual reality (VR) systems.

Known as "epidermal VR" the platform adds a whole new dimension to long-distance communication and entertainment, and could even provide sensory feedback for people who wear prosthetics.

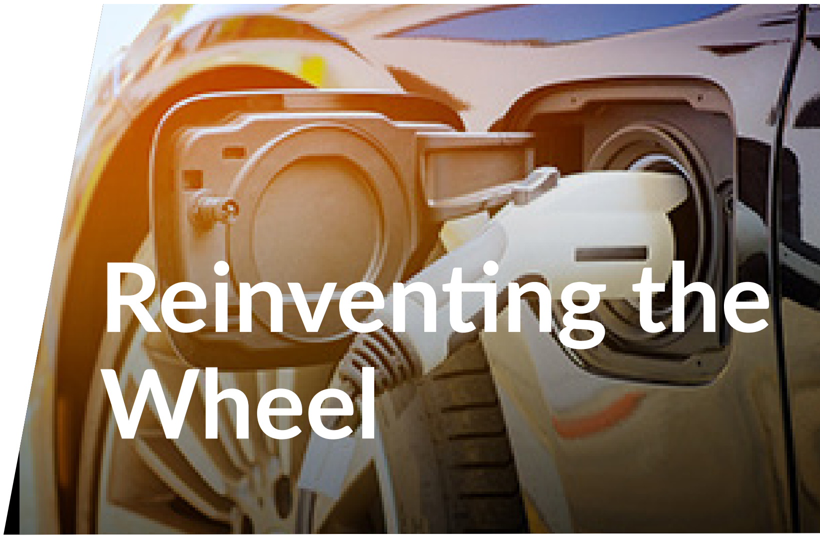
The 15-by-15-centimeter prototype sheets adhere to the skin without the need for tape or straps and conform easily to curved surfaces. Inductor charging also eliminates the need for bulky batteries or wires.

An array of 32 actuators resonate at 200 cycles per second – a level at which human skin is highly sensitive – and as they vibrate, they produce the sensation of touch for the wearer.

The technology could enable a parent to hug their child while video chatting, or allow video gamers to feel when they get hit during play.

VR users would be able to touch objects in the virtual world, and wearers of prosthetic arms could get a better sense of the shape of objects as they hold them.

For information: John Rogers, Northwestern University, Center for Bio-Integrated Electronics, Technological Institute, B390, 2145 Sheridan Road, Evanston, IL 60208; phone: 847-467-2997; email: jrogers@northwestern.edu; website: https://bioelectronics.northwestern.edu/index.html or https://news.northwestern.edu/stories/2019/11/epidermal-vr-gives-technology-a-human-touch/



Reinventing the Wheel

A new electric vehicle (EV) platform featuring in-wheel motors recently debuted at the Tokyo Motor Show.

The new modular design could revolutionize EVs by reducing chassis space and weight while increasing efficiency and allowing for multiple body configurations.

All of the operational components are housed inside the wheel – motor, steering, suspension, drivetrain, brakes, sensors and electronics – to optimize internal space and allow room for a larger battery.

The wheelbase, length and width can be selected to accommodate a variety of interchangeable cabin designs.

For example, REE AIR is designed for passengers, while REE SHARE is suitable for light duty, rugged commercial applications. But the design could be adapted for just about any vehicle from a 4x4 to a sports car.

The startup is in the process of raising money based on a $580 million valuation.

For information: REE, Aharon Meskin St. 10, Tel Aviv-Yafo, Israel; email: info@ree.auto; website: https://ree.auto/

Spray-On Bandage

A new technology for applying thin layers of fiber to the skin could save lives in remote areas where immediate medical care is not available. It's based on a well-known technique called electrospinning, which is used to deposit polymer fibers on a variety of surfaces.

But because electrospinning requires very high voltages, the method is not suitable for use on biological materials.

Recently, a group of researchers combined an electrospinning device having a smaller electric field with pressurized gas in what they have dubbed the electrostatic and air driven (EStAD) device.

It works like a paint sprayer to safely deposit a fiber mat onto the surface of the skin. EStAD has been tested on a porcine skin incision and a gloved human hand.

The fibers can also be laced with antibiotics, hormones or other drugs to enhance healing. The bandage material as well as the medications can be selected as needed for the application.

For information: Jack Skinner, Montana Technological University, 1300 West Park Street, Butte, MT 59701; phone: 800-445-8324; email: jskinner@mtech.edu; website: https://www.mtech.edu/index.html

DISCOVER 25 PROVEN STRATEGIES TO ACCELERATE INNOVATION AND TRANSFORM RESULTS
THE ANTICIPATORY ORGANIZATION
Turn Disruption and Change Into Opportunity and Advantage
By The New York Times and Wall Street Journal Best-Selling Author
DANIEL BURRUS

The Cybersecurity of Banking and Finance

continued from page 1

what an increasing number are doing today and logging into your Venmo account and depositing some cash a friend sent to you to pay you back for their ticket to the movies the night before, banking in some form is a personal and very serious subject due to your hard earned money flowing through it. And let's not forget that a financial institution has every last little detail about our financial situation, and most importantly, our cash flow, whether we are self-employed, working for a company, or running a corporation of our own with multiple employees and a payroll.

Historically, security in banking was having a guard prevent a robbery. Robberies of physical banks are now paling in comparison to cybercrimes committed against financial institutions for more than just your cash: for sensitive information and even your very identity.

Much like I discussed at large with the healthcare cybersecurity industry, financial institutions of all sizes are faced with hundreds of thousands of cyberattacks every single day, and in comparison to a robbery of a physical bank, cybercriminals are not risking their lives or facing jail time, and the financial reward for their crime is far greater.

One example of a big bank that suffered a massive attack was Capital One. A breach in cybersecurity allowed for cybercriminals to capture the personal information of over 100 million people and leak it to the world, with a single weak spot being all these savvy hackers needed.

In the past year, there have been over 3,000 known successful cyberattacks against financial institutions, according to the Treasury Department's Financial Crimes Enforcement Network. In the case of the Capital One hack, what was discovered by once Amazon software engineer Paige Thompson was that Capital One's computer network described their system flaw as a "configuration vulnerability" in its security software, leaving vulnerable customer social security numbers and account information.

To compare this to past years in banking, it would essentially replicate a situation where the tellers and security guards all go to lunch with a lobby full of customers and potential thieves, leaving drawers unlocked and the vault wide open.

Time for a Change!

Similar to my comparison of the lucrative healthcare industry and how easy it is to hack their systems, anticipatory instead of reactive cybersecurity measures should be elevated at financial institutions. Capital One's hack is not the only example of a large-scale financial institution that succumbed to hacking, as we saw in the last several years with companies like Equifax and Morgan Stanley being attacked with various hacking methods.

Banks and financial institutions have implemented cyber protection, but are they really safe? I know of several cyber companies that test for vulnerabilities in this industry and it has never taken them more than 48 hours to gain access to everything even when the bank thought it was safe! So why do we see this same cyber issue happen time and time again? It is "assumed" that we are protected and safe. But cyber protection is both a cultural (people) and technology issue, one that is not a static "fix it once and you're done" situation. It is dynamic and needs constant testing for new vulnerabilities. From a leadership perspective, quickly implementing a new strategy that could bring in new revenue fast is usually a priority over taking the time to make sure everything in the new initiative is safe and locked down. And as I mentioned earlier, the vast majority of current cybersecurity strategy is about reacting quickly after the problem occurs, and not an anticipatory one.

A Hard Trend is: cybercriminals will always find a way to outsmart the institutions, with their customers being the real victims of the crime if institutions continue being agile fast reactors. So why not pay attention to that Hard Trend, pre-solve the problem before it becomes a nationally reported disaster, and be anticipatory in their strategies using behavior analytics and other anticipatory tools to prevent a breach of security and, as we've stated often, the breach of trust?

Once a data breach occurs, companies like Capital One tend to focus more on marketing to reassure their longtime customers, whose trust is now broken, that everything is now fixed and not enough on new dynamic protection systems.

Cyber Solutions

It's time to consider a customer, no matter how small, and their trust as actual valuable equity in a company. When hacking occurs repeatedly in an industry, a lot of times trust breaks because the customer does not feel their personal information is truly valued by the institution.

Hackers love to take advantage of weak passwords or use emails loaded with malicious computer code that lets them get inside the network. In others, hackers scan for out-of-date hardware and software missing the latest security fixes.

Given the fact that some hacks can take months, it is safe to say that at any point, with a fast reactive and an increasingly important anticipatory cybersecurity system in place, it is possible to spot a discrepancy long before it becomes a renowned attack. The fact of the matter is cybercriminals work around the clock; therefore, the IT firm or IT department of every size financial institution must be in place to do the same.

Anticipatory cyber strategies put the cyber education of employees as a priority since most cyber breaches come from poor practices on the inside of the organization. In addition, they have an outside firm or team do security scans on everything before the problem occurs, have all software scanned and updated regularly, make sure spam filters are adequate in their company's email system, and if they have an internal team as opposed to an outsourced IT firm, invest in their education as to what loopholes they should be looking for.

Free Perimeter Test

Because we see cybersecurity as a strategic imperative in protecting your future brand and reputation, we have identified best-in-class cyber testing companies that will provide a free perimeter test of your organization to check for vulnerabilities in your cybersecurity defense system, provide the results of their tests and recommend immediate actions that can be taken to stop any uncovered leaks in your system.

If you would like a free perimeter test to check for vulnerabilities in your cybersecurity defense system, please contact us.

Ask for your free perimeter test at: https://www.burrus.com/perimteter-test-request/

Burrus
Research®

Technotrends is published 12 times a year by Burrus Research, Inc., a research and consulting firm that monitors global advancements in science and technology and their direct impact on business and consumers. Mary Norby, Editor, 1860 Executive Drive, Suite E2, Oconomowoc, WI 53066. To subscribe, call 262-367-0949 or email office@burrus.com.