

July 2021
VOL. XXXVIII, NO. 7

Daniel Burrus'

Celebrating 30+ Years of Publication

TECHNOTRENDS® NEWSLETTER

*The biggest ideas that are
changing everything*

IN THIS ISSUE

Ransomware and the
Financial Industry

Affordable Electric Pickup

Plant-Based Supercapacitors

World's Smallest Acoustic Amp

RNA Pesticides

Intelligent Tires

5G for IoT

Safer than Passwords

Fast Path to Orbit

www.DanielBurrus.com





Ransomware and the Financial Industry

By Daniel Burrus, CEO of Burrus Research

Last month, I dove deep into the Ransomware attack on the Colonial Pipeline, a topic that captured the attention of our entire nation like a sinister encore to the drama that was 2020. Gas shortages swept southern states, fueled by confusion around what exactly happened when a Russian hacker group named DarkSide brought a whole industry to its knees.

Discussing the basis of what a Ransomware attack is – software that encrypts, or locks, vital information at an organization, allowing perpetrators to demand a ransom payment to unencrypt the files or in exchange for sensitive consumer data – I explored why an Anticipatory mindset at your organization is beneficial in thwarting cyberattacks and improving organization-wide cybersecurity.

While the Colonial Pipeline attack affected the oil industry, smaller businesses suffered nearly 65,000 Ransomware attacks throughout 2020 – a staggering statistic that stands to prove not only just how easily hackers can breach a system and demolish something thought to be “unsinkable,” but, more importantly, just how imperative it is for all organizations to ensure that cybersecurity is at the forefront of their minds.

Gaping holes left in the firewalls of banks and credit unions are a glaring “welcome” sign for groups like DarkSide.

Other than healthcare, no other industry is more obviously susceptible to hacking than the banking and finance industry. With mountains of personal data about millions of Americans and their financial records, gaping holes left in the firewalls of banks and credit unions are a glaring “welcome” sign for groups like DarkSide.

I’ve written at length about the dangers of cyber threats

in banking and finance; however, it is utterly astounding to me that, to this very day, financial institutions face seemingly unforeseen information hacks and, now, Ransomware attacks that in today’s world of exponential digital acceleration, can be anticipated and, in many cases, prevented.

Ransomware Attacks Are Increasing

The Colonial Pipeline attack made headlines, but as mentioned above, was not an isolated incident. Among those 65,000 attacks that amounted to an average of an attack nearly every hour throughout 2020, the financial industry comprised several, and they’ve continued into this year like a malicious and unwanted Hard Trend.

When the oil industry buckled amid its Ransomware attack, many feared the impact the shortages caused by panic-buying would have on the stock market. But, as it turned out, that fear was only part of the equation.

The financial industry is certainly no stranger to data breaches and other forms of information leaks. Larger institutions in the industry respond by having a cybersecurity system with a power mirroring the federal government; however, hackers don’t simply throw on a ski mask, barge through the front door, and take over, robbery-style. They tend to search for the trap doors an institution is completely unaware of, with a “get-in-get-out” mindset.

Third-party vendors that large financial institutions employ, such as insurance agencies, law firms, and other consultants that lack the same level of security the institution itself boasts on the forefront.

continued on page 8

TECHNOLOGY NEWS HIGHLIGHTS

Affordable Electric Pickup

One of the biggest roadblocks to the widespread adoption of electric pickup trucks has been the purchase price, which can range from just over \$40,000 to more than \$100,000 for high-end models.

But recently, Ford announced that their new base model electric F-150 – known as the Lightning – will list for under \$40,000. With tax incentives for electric vehicle (EV) owners, that brings the purchase price down to about \$30,000, making it comparable to its conventional gas counterpart.

The range of the base model is 230 miles on a full charge, and an extended range option increases that to 300 miles. When using a 150kW fast-charging station, the extended range model takes about 40 minutes to go from 15 to 80 percent capacity, and Ford's 80 amp home charging system will fully charge the vehicle in 8 hours.

What's more, the large on-board batteries can power multiple electric devices, or be used as a mobile charging station for small electrics like bicycles and motorcycles.

While charging is still an issue, particularly for adventure drivers, more EVs will undoubtedly pave the way for more charging stations as infrastructure grows to meet demand. And, as one of the most popular pickups on the road, the electrified F-150 could have a huge impact on sales of EVs in general.

The new Lightning will be available in spring 2022.

For information: Ford Motor Company, P.O. Box 6248, Dearborn, MI 48126; website: <https://www.ford.com/trucks/f150/f150-lightning/2022/>



DANIEL BURRUS'

BUSINESS LEADER IMPERATIVES

How Anticipatory Leaders are turning disruption and change into opportunity and advantage.

Click here to SUBSCRIBE





Plant-Based Supercapacitors


As electric vehicles become more popular, there's a growing demand for better power storage technologies that can provide faster recharge times and longer life, while also being more environmentally friendly. Researchers may have found a low-cost, sustainable solution that uses lignin – a natural polymer found in wood fiber that is available in huge quantities as a by-product of paper manufacturing.

The lignin was used to enhance the conductivity of manganese dioxide – another low-cost material that is abundantly available. A mixture of the two was deposited on an aluminum electrode and sandwiched with a gel electrolyte to another aluminum electrode made with activated charcoal.

Unlike a battery, which can take a relatively long period of time to charge, the new device – called a supercapacitor – can charge and discharge in a much shorter period of time. Testing confirmed that the supercapacitor was electrochemically stable, even after thousands of charging cycles. In addition, the specific capacitance of the new device was up to 900 times that of other supercapacitors.

Lightweight and flexible, supercapacitors could be a game-changer for everything from mobile devices to electric vehicles, while reducing our dependence on rare earth elements and the expenses associated with mining and recycling them.

For information: Hong Liang, Texas A&M University, Department of Mechanical Engineering, 100 Mechanical Engineering Office Building, College Station, TX 77843; phone: 979-862-2623; fax: 979-845-3081; email: hliang@tamu.edu; website: <https://www.tamu.edu/> or <https://today.tamu.edu/2020/09/07/lightweight-green-supercapacitors-could-quickly-charge-devices/>



World's Smallest Acoustic Amp

Using a hypothesis that was developed nearly 50 years ago, scientists have built a device that can process radio signals using sound rather than electrons. In the future, acoustic devices like these could make cell phones, radios and other wireless devices smaller and more efficient, while improving sound performance.

Decades ago, a radio-frequency amplifier that could boost a signal 100 times measured 0.4 inches (1cm), required 2000 volts of electricity and consumed 500 milliwatts of power. In contrast, the new device measures 0.008 inches (0.2 millimeters), requires 36 volts of electricity and consumes 20 milliwatts of power. The difference? Advanced nanofabrication techniques.

Acoustic wavelengths are smaller than the diameter of a human hair, so creating components to enhance them requires layers of semiconductor materials that are extremely thin and extremely high-quality – neither of which was possible in the 1970s. The new device was constructed containing layers that are only 83 atoms thick. An intricate process known as heterogeneous integration

enabled layers of dissimilar materials to be fused together to form an acoustic-electric amplifier.

Future research will center on determining whether the technology may also be adaptable for all-optical signal processing.

For information: Matt Eichenfield, Sandia National Laboratories, 1515 Eubank SE, Albuquerque, NM 87123; website: <https://www.sandia.gov/> or https://newsreleases.sandia.gov/acoustic_amplifier/

pests for which they are designed, and do not impact other beneficial insects, animals or humans. Researchers are currently evaluating these pesticides on a virus-spreading mite that could play a role in colony collapse disorder.

Other delivery modes are also being tested, including genetically modifying crops to kill the insects that feed on them. This approach has disadvantages in that it can't be used on existing plants, and many countries have banned GMOs.

For information: RNAissance Ag, Helix Center Biotech Incubator, 1100 Corporate Square Drive, Suite 237, St. Louis, MO 63123; website: <https://www.rnaissanceag.net/> GreenLight Biosciences, 200 Boston Avenue, Suite 1000, Medford, MA 02155; Web site: <https://www.greenlightbiosciences.com/>



RNA Pesticides

All of the recent medical research on COVID-19 vaccines has dramatically reduced the cost of producing RNA, opening up new applications for this versatile molecule. One such application is developing targeted pesticides.

In addition to facilitating the formation of proteins, RNA can be used to inhibit the manufacture of specific proteins through a process known as RNA interference (RNAi). In the case of pesticides, this involves identifying a protein that is uniquely essential to the survival of a specific pest. An RNA molecule designed to inhibit production of that protein is then sprayed where the insect will ingest it. When the required protein is no longer produced, the insect is unable to regulate its internal balance of microorganisms, and it dies.

RNA pesticides effectively target only the specific



Intelligent Tires

With the explosion of business to customer (b2c) deliveries in recent years, the number of "last mile" delivery vehicles on the road has increased, and so have tire-related issues. So, tire manufacturers are putting artificial intelligence (AI) to work to help predict problems.

For example, Goodyear's SightLine combines sensors to track tire wear, inflation pressure, tire temperature, vibrations, road conditions and dozens of other parameters with a device that sends the information to the Cloud for real-time analysis. In a pilot test on 1,000 vehicles, the system was able

to detect 90 percent of issues before they became issues.

Bridgestone's technology can also predict when tires are likely to wear out, and whether or not they are suitable for retreading. Retreaded tires can reduce carbon emissions up to 24 percent by keeping used tires out of landfills longer.

Technologies like this will enable service centers to better anticipate the need for repairs or replacements. Collecting and monitoring vehicle data (also known as telematics) will also be an important feature for autonomous vehicles in the future.

For information: Goodyear; website: <https://www.goodyear-sightline.com>

Bridgestone; website: https://www.bridgestone.com/regional/north_america/united_states.html



A new 5G modem will bring Internet of Things (IoT) connectivity and speed to industrial segments like agriculture, manufacturing, construction and mining. The 315 5G IOT Modem will be able to connect everything from robots in factories to tractors in fields. The wireless processor is low-power and fits in the same size package as its 4G predecessor, making it easy for companies to update their machines quickly.

Because 5G can run between 10 and 100 times faster than a typical 4G connection, a greater number of devices can be connected to a network simultaneously. Although the types of devices typically used in these applications don't require high data rates (relatively speaking), they do require rapid response times (i.e., minimal delays in getting data back and forth).

The modem runs on global sub-6GHz bands, and can also switch to 4G if needed. It will likely begin appearing in devices later this year, starting first in Europe and China, and later in Japan.

For information: Qualcomm Technologies, Inc., 5775 Morehouse Drive, San Diego, CA 92121; website: <https://www.qualcomm.com/products/qualcomm-315-5g-iot-modem>



Apple recently announced that it is developing a new authentication platform that will be more secure than traditional passwords and easier to use. Passkeys, as they are known, are another example of the growing trend toward passwordless log-on technology.

Users will be required to set up an account by first choosing a username. They can then use Face ID or Touch ID to confirm their identity. The passkey is generated and stored in the device, and iCloud Keychain synchronizes it across all of the user's

devices. Subsequent log-ins require just a single tap.

Bad passwords are still the most common security vulnerabilities today, not to mention that people have a difficult time remembering all of them. But it's more important than ever to protect our accounts from cyberattacks and phishing scams, and the passkey approach could make servers less tempting targets for hackers by removing the need for troves of secret log-on information.

It remains to be seen whether passkeys are secure enough to reduce the need for two-factor identification (i.e., passwords and biometrics).

Currently, the technology works only on iOS devices; however, the company is collaborating with FIDO (Fast Identity Online) Alliance and the World Wide Web Consortium (W3C) to make it available for Windows computers and Android phones.

For information: Apple Inc.; website: <https://www.apple.com/>

Fast Path to Orbit

A new turnkey approach to satellite deployment is poised to redefine how companies, governments and other organizations collect valuable information about Earth from space.

Using off-the-shelf satellite buses, the company customizes each one with the customer's payload

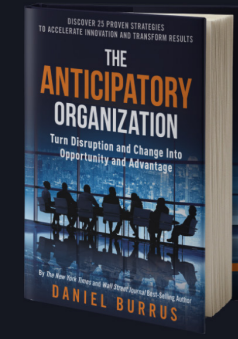
and configures the capabilities to meet their needs. The satellite is then launched via spacecraft and operated on a shared schedule by the client using an interface called Cockpit. An onboard processor receives and collects incoming data for download to a ground station at predetermined intervals.

The result is a true democratization of space. Customers pay for (and maintain control of) their specific payloads. They also pay for a portion of the launch fee, which is shared with other clients (each satellite can carry multiple payloads).

After that, customers are charged for actual usage of onboard resources such as power processing time and data transfer. The platform transforms satellite missions from a capital expenditure to an operating expense by offering satellite missions as a service. It also reduces the time to implementation from years to months.

The company currently has two satellites in orbit, carrying twelve payloads. The next flight is already booked for next year, and talks are underway to fill the fourth. By 2023, they expect to launch a mission every quarter.

For information: Loft Orbital; email: info@loftorbital.com; website: <https://www.loftorbital.com/>



Burrus Research

Become a Positive Disruptor.

You pay for shipping (\$8), we pay for the hardcover book.

Your Name Here...

Your Email Address...

Yes, I Want One!

*Outside the USA? [Click here](#) to receive our eBook version.

Ransomware and the Financial Industry

continued from page 1

Consider this anecdote: the bank locks its front door, but there is an office with an exterior door on the side of the building, where an independent insurance agent, employed through the financial institution, works after hours. The agent leaves for the night, leaving all doors to their office unlocked and unarmed. A robber simply tugs on the back door to their office and walks right in; no risk of setting off the front door alarm or navigating a way inside.

Smaller banks are even more at risk these days, in that, much like I discussed in last month's article regarding small businesses' lack of cybersecurity measures, they do not have the robust budgets that larger banking corporations have for around-the-clock IT staff and monitoring, so many simply use anti-virus software on their computers and call it a day.

Disruptions Stacking Up In Finance

Despite budget constraints, that passive "bandage" of anti-virus software does very little to ward off more advanced cyber threats, especially Ransomware.

An Anticipatory Leader in the financial industry will not only look at cyber threats as a Hard Trend that is only increasing alongside exponentially accelerated digital technology, but will also see other digital disruptions causing a stir in the many antiquated systems of the financial industry as well.

Let's look at Bitcoin and cryptocurrency; an anomaly to many. The system that cryptocurrencies are built on is called blockchain; a completely decentralized ledger system that, in short, cuts out the middleman of many legacy systems. In a recent blog about the differences between cryptocurrency and digital currency, like the Digital Yuan, I wrote that many countries have embraced blockchain technology and banks have transformed with it, finding new ways to serve their customers.

Yet, in that same blog, I outline how the United States

has been slow to jump into the "digital dollar" concept, clinging instead to legacy mindsets and, essentially, using agility to protect and defend the status quo while the disruption is right in front of their eyes. But, aside from moving physical dollars and coins into a digital wallet, the very concept of blockchain technology has far more beneficial purposes in the way of banking security than in eliminating paper money that a burglar could run off with.

Blockchain technology is in many ways unhackable, as it is a highly encrypted ledger system. Here's another anecdote to explain to those who might not understand: when you receive a new credit card to replace your old one, you have been told to shred or cut up the card so no one gets their hands on it.

Traditional security is like throwing those shards into the trash beside your computer desk, whereas blockchain technology is like taking separate chunks of a credit card with your number on it and discarding each one in a different area of a different state, throughout the country.

Essentially, a hacker or team of hackers will in no way be able to piece together anything of value about a customer's financial information before either being caught, or finding themselves unable to succeed whatsoever.

Cyberattacks will disrupt the banking industry in more ways than just immediate financial loss; every time a massive Ransomware attack hits the news headlines, people trust financial institutions a little bit less, and start to prefer the decentralized alternative of cryptocurrency. If blockchain is already a disruptive Hard Trend in and of itself, why not look to pre-solve other disruptive problems, such as cybercrime, by leveraging it to your institution's advantage?

Anticipatory Principles That Apply To Cybersecurity

Returning to the topic of small financial institutions and their often meager budgets in the way of IT and cybersecurity, constant surveillance of their software and systems internally is likely a no-go.

So, much like small businesses in other industries, how do both the smaller banks and even those “blind spot” affiliate businesses like insurance companies seal up cracks in their cyber foundations?

Their answer is an Anticipatory one. First, consider the Skip It Principle from my Anticipatory Leader System, where I encourage organizations and leaders to identify the actual problems plaguing them. In the way of the cybersecurity budget, maybe the problem isn't a lack of money, but a lack of ability to sustainably monitor a system that hacking groups are pinging a thousand times an hour.

Once the real problem has been identified, work to solve it. In this case, their cybersecurity team must instead be a third-party group of individuals that can work around-the-clock. Another principle I teach in my Anticipatory Leader System is to go opposite. When the masses are going left, something great might be waiting for you if you go right.

An outside-the-box example in cybersecurity is the influx of companies in the financial industry actually hiring ethical hackers for their cybersecurity. What was once a strictly Silicon Valley-type maneuver constrained to the likes of technology companies founded by hackers is now [said to be embraced by banks](#) who are leveraging the knowledge of these individuals to their advantage!

By going opposite in this way, these banks are simultaneously leveraging my Skip It Principle in a unique way – skipping the perceived problem of having to spend time and money both on hiring and training an internal IT team to watch for cyber threats, and finding a solution in hiring someone on the outside who has all the expertise needed to understand what exactly they're looking for.

An Anticipatory mindset and the principles that it consists of are vital in both positive digital disruptions and negative ones, such as cyber threats. Give your team the training they deserve by signing up for my Anticipatory Leader System to help spread good cybersecurity practices throughout your entire

organization today!

In working with many IT organizations globally each year, I have identified a best-in-class cyber testing company that will provide a perimeter test of your systems, along with results, and recommend immediate actions that can be taken to stop any uncovered leaks. If you would like a free perimeter test to check for vulnerabilities in your cybersecurity defense system, please [contact us](#).

THE ANTICIPATORY LEADER™

Live Monthly Access Cutting Edge Experience

CLICK TO JOIN TODAY

Profit From Disruptive Change Now!

The Anticipatory Leader Membership is a results-driven online experience that will quickly help you and your team master the art of anticipatory thinking.

Start Training Now

What's Included in the Membership

- THE ANTICIPATORY LEADER SYSTEM**
28 cutting-edge video lessons by Daniel Burrus. Each video is 3-5 minutes long and focuses on a single Anticipatory concept. Our Rapid Application exercises help you put each concept into action immediately!
- LIVE ACCESS TO DANIEL BURRUS EACH MONTH**
Live monthly access to Daniel Burrus as he leads a private Deep Dive training session with Anticipatory Leader members covering the latest in technology & innovation. By signing up today, you qualify for this amazing bonus!
- ANTICIPATORY LEADER CERTIFICATION**
Certification provides proof of a serious competitive advantage that even seasoned business leaders lack. This is a powerful tool for leaders, emerging leaders, managers, planners and sales teams.

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.

©2021 Burrus Research, Inc.