TECH & CYBER

CUSTOM CONTENT • February 28, 2022

How Cyberattacks Have Affected 2022—CRTG Can Help

Russell Poucher is CEO of Creative Resources Technology Group. Before starting CRTG, he partnered with Apple, Adobe, and Dell to help with several initiatives and projects. As a national speaker, he has had the pleasure of sharing the stage with some of the top speakers in cybersecurity and information technology such as Kevin Mitnick and Steve Jobs.

For over 25 years, CRTG has been the leading Apple Consultant for businesses in Southern California. Their services include:

- Cybersecurity
- Managed IT Services
- Remote IT Services
- Network Security
- IT Consulting
- Disaster Recovery/Business Continuity Planning
- Hardware as a Service

Russell Poucher

"We have witnessed a significant increase in cyberattacks in 2022 and this trend will continue. The pandemic has forced individuals to work from home, which puts businesses in a vulnerable state with cybersecurity."

-Russell Poucher

A recent attack on the NFL team, San Francisco 49ers, proves the vulnerability of businesses of all sizes. A small ransomware gang called BlackByte encrypted files on the team's IT corporate network. The attack was confirmed on Feb. 13th, after BlackByte listed them as one of their victims on the dark web. This attack could have had a larger impact if the 49ers had made the Super Bowl. This would have put Levi's Stadium and ticket holders at risk.

Ransomware attacks are notably increasing, targeting small and medium-sized companies as well. The main concern for businesses is that infrastructure and supply chains security weaknesses are the main targets of these attacks. The most targeted sectors worldwide by hackers are education, healthcare, communications, and government. These types of attacks are at an all-time high and businesses must be made aware of this.

The goal of CRTG is to engage and educate the public with the information they need to stay safer online and to enhance cybersecurity at home and in the workplace. Their focus is on key areas including ransomware, citizen privacy, consumer devices, and e-commerce security. They also cover phishing, important security updates, WIFI safety, password protocol, best practices for businesses, and so much more!

Automate ID Verification in the Post-COVID Digital Age

By Greg Brown, VP Global Marketing at Melissa

The COVID-19 pandemic forced a shift in the way people consume. As a result, internet traffic surged by 60% and money spent by online shoppers nearly doubled. And that is unlikely to change anytime soon in the environment of COVID uncertainty that remains. According to eMarketer, this year, worldwide ecommerce sales will exceed $5 trillion for the first time, accounting for more than a fifth of overall retail sales, and total spending will surpass $7 trillion by 2025.

As more consumers shop online, there has been a corresponding rise in fraudulent activity. A Juniper research report found ecommerce retailers lost over $20 billion in 2021, an 18% increase over the prior year, due to fraud threats such as identity theft, chargeback fraud, 'silent' fraud, account takeovers, and 'pharming'. It's estimated that retailers operating online could lose almost $130 billion in revenue to fraud worldwide by 2023.

Automate ID verification

Automation is the answer for those looking for the fastest, most accurate and cost-effective way to deliver ID verification online and help reduce fraudulent activity. This means adopting electronic ID verification (eIDV). Such an approach will help to prevent fraud in real time at the point of customer access online, by ensuring retailers are dealing with the person they think they are. This automated service is something that also ensures good governance by aiding compliance with know your customer (KYC) regulations.

With eIDV, when someone provides their contact and delivery details for a product on the payment page, cross-checks are made against the data they have provided in real time to ensure a smooth customer experience. This can be achieved with real-time access to a dataset of billions of consumer records from reputable data streams, including government agency, credit agency and utility records.

In fact, ensuring a seamless customer journey at the payment stage, driven by the automation embedded in eIDV, will help provide a standout experience. This is vital with so much similarity in the quality and price of products offered online.

eIDV is not something for those only operating at the high value end of ecommerce to embrace, but all merchants - particularly with fraud on the up and the cost of integrating ID verification solutions into systems coming down.

In tandem with eIDV, it's also important for retailers to use an automated address verification system (AVS). This is a service provided by major credit card processors and banks that enables merchants to authenticate ownership of a credit or debit card used by a customer. The credit card company or issuing bank automatically checks the billing address provided by the customer to the retailer against the billing address in its records and reports back to the merchant. Using this information, in real time, the merchant can block purchases made by unauthorized users.

Automation better than manual

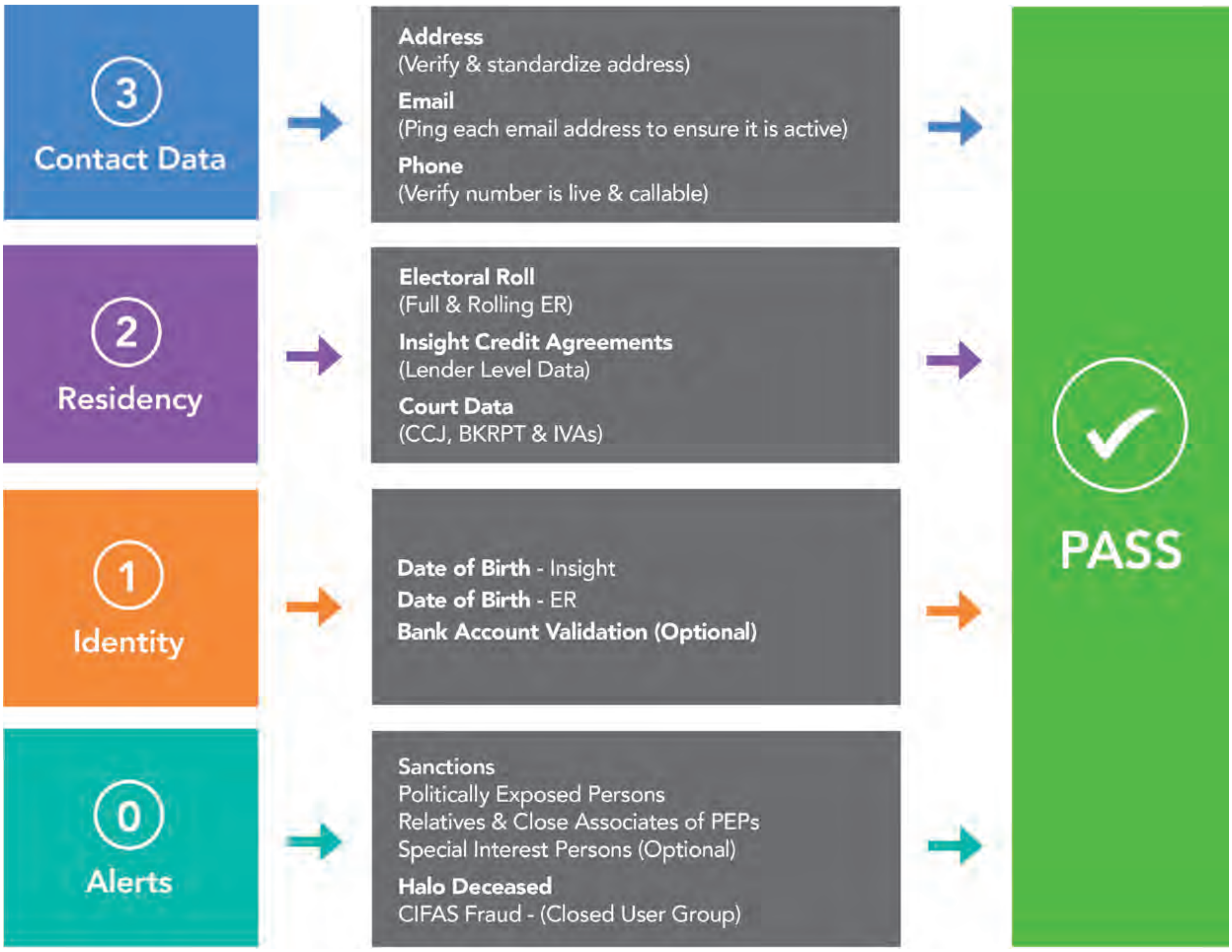
Bear in mind the automation of ID verification is far better than the physical, time consuming and more costly checks that, in lieu of automation, would need to take place behind the scenes. Also, with a manual approach you would need to employ staff with knowledge of thousands of ID document types and then there's the possibility of human error, making manual reviews less stringent than they should be.

Automate data quality processes to support ID verification

It's not just automated tools like eIDV that retailers should consider to prevent fraud, but simple data quality practices, which at their core stem from plain and simple contact data verification. A good place to start is with an automated address lookup or autocomplete service. These tools ensure only deliverable and verified addresses enter your system. They automatically reveal a suggested correct version of the address as the customer completes an online contact form, enabling them to select one that's not only accurate but easily recognized, and correctly formatted for their country location. Another benefit of a lookup tool is that as well as preventing mistakes caused by fat finger syndrome, it reduces the number of keystrokes required when typing an address by up to 70%. This speeds up checkout and reduces shopping cart abandonment, aiding the delivery of a standout customer experience.

Other areas of the data quality process that support ID verification include making sure email and phone numbers are live, callable and part of a genuine host, and even determining the common language in use for the given area code. There have been too many occasions where fraudsters have used fake phone numbers and emails to bypass verification procedures when signing up and purchasing online.

The speed, accuracy and cost benefits afforded by the automation of tools like eIDV, along with wider data quality practices, are vital to retailers as more move online and fraud continues to grow. Automation also ensures a positive customer experience, with no negative impact on the customer journey, therefore enabling retailers to stand out in an increasingly competitive market.

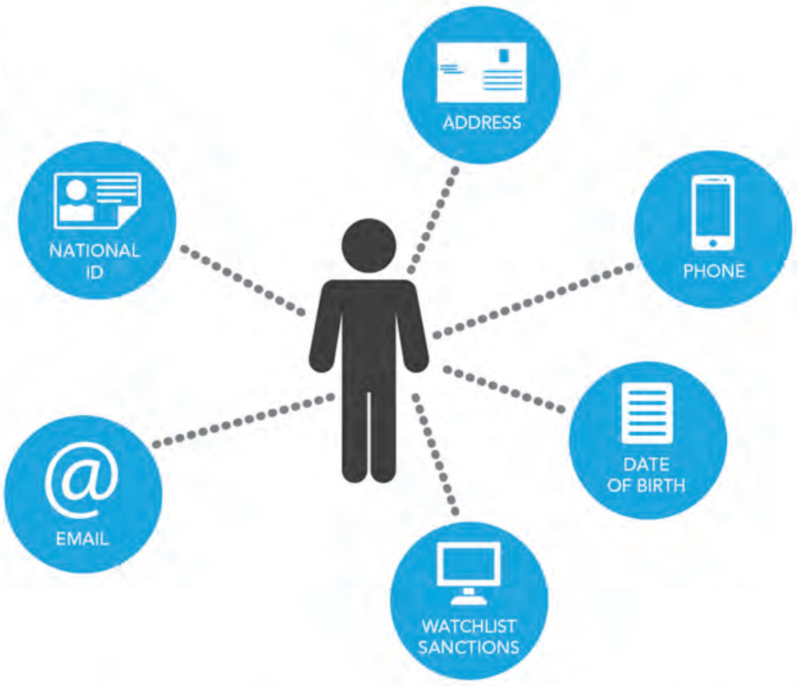

3
Contact Data
Address
(Verify & standardize address)
Email
(Ping each email address to ensure it is active)
Phone
(Verify number is live & callable)
2
Residency
Electoral Roll
(Full & Rolling ER)
Insight Credit Agreements
(Lender Level Data)
Court Data
(CCJ, BKRPT & IVAs)
1
Identity
Date of Birth - Insight
Date of Birth - ER
Bank Account Validation (Optional)
0
Alerts
Sanctions
Politically Exposed Persons
Relatives & Close Associates of PEPs
Special Interest Persons (Optional)
Halo Deceased
CIFAS Fraud - (Closed User Group)
PASS

Achieve Faster Client Onboarding & Ensure Compliance

Real-Time Global ID Verification for (KYC) Know Your Customer

In our increasingly mobile, data-driven world, your clients demand a seamless customer experience. The challenge – managing risk and compliance, while delivering faster customer onboarding. Our Personator Identity Verification solution can help you:

- Capture & validate ID documents in less than 1 minute
- Verify & standardize personal ID info & customer data
- Decide instantly whether to accept new customers
- Detect application fraud in any customer channel



We run advanced technical checks & generate a comprehensive customer due diligence report for the ultimate peace of mind.

Reduce risk, ensure compliance & keep customers happy!

i.melissa.com/compliance

1-800-MELISSA

melissa®

MARQUEE®
STAFFING
Working Wonders®

Emerging Trends in the Cybersecurity Job Market for 2022

As business increases shifts online, cybersecurity becomes even more important.

Industries that are reliant on cybersecurity expertise to keep functioning on a daily basis could be caught in a disruptive ransomware attack or data breach at any time. These industries can include all financial institutions and healthcare enterprises, and every other field from academia to manufacturing to entertainnment.

Companies who don't staff their IT and cybersecurity departments smartly could find themselves in big trouble with no warning. Proper staffing in these areas is the first line of defense against potentially disastrous cyberattacks.

As a result, cybersecurity experts are in great demand. Different fields require different areas of expertise, so people with skills in ethical hacking, app development security, risk management, cloud security, health information security, network protection and IT in general should find employers seeking their skills.

Take a look at the cybersecurity trends expected to hit the headlines in 2022, as well as the areas of expertise that should be in especially high demand.

Cybersecurity Trends for 2022
The global pandemic changed the focus of cybersecurity and opened new challenges to deal with going forward. Among the trends to expect in the cybersecurity world in the coming year are the following.

Cybersecurity for Remote Work
During the pandemic, workers flung themselves all over the globe. After all, if you're working remotely, why shouldn't you rent an apartment at the beach or in the mountains? While that may have been a good solution for employees, it added to the demands on organizations' IT teams.

Employees who can work from anywhere may be using unsecured networks to transmit business-critical data. Securing networks becomes an expanded challenge in this environment — and cybersecurity specialists who can deal with threat hunting and pen testing are in demand as a result, especially as employees often want to continue their remote work even as the pandemic dies down.

Protecting the Internet of Things (IoT)
With more than 41 billion devices from the IoT expected to go online over the next 5 years, cybersecurity specialists need to gear up to provide the needed protection. Cybercriminals are now infiltrating networks via devices as seemingly simple as baby monitors or smart plugs. Protecting against these cyberattacks requires specialized skills that are increasingly in demand.

More Multi-Factor Authentication
Passwords alone often aren't enough to protect sensitive data — especially when employees get lax about protecting their passwords. For that reason, many organizations add multi-factor authentication to guard against cyberattacks and data breaches. Cybersecurity specialists are needed to create effective authentication tech, especially because some communication channels, such as voice or SMS, don't have the necessary encryption to provide the protection needed.

High-Demand Cybersecurity Positions for 2022
To meet the cybersecurity demands of 2022 and beyond, certain IT positions are coming into the forefront. Some of these positions are new, while others are expansions and refocusing of positions that already exist. In all cases, specific skills are vital and can make employees especially valuable to their organizations. Among the cybersecurity positions expected to be in high demand in the coming year are the following.

Cloud Security Specialists
IT experts with cloud security skills can expect the largest salary boost in the coming year, thanks to the very specific expertise required. Many businesses have migrated their data and application storage to the cloud, rather than relying on physical infrastructure as was common in the past, reaping savings and increasing efficiency by doing so. However, cyberattacks are often especially vulnerable to attack, making cloud security especially important. Specialists within the cloud security field may focus on Google Cloud or Azure security, public cloud security, or cloud security architecture or infrastructure.

Cryptographers
Cryptographers are the IT personnel who are at the heart of creating the encryption needed to complete data. They create algorithms and ciphers that protect data from being stolen, copied, or deleted. In addition, these IT experts seek out security issues and test systems to protect them against vulnerabilities.

Information Security Analysts
By auditing security policies and protocols, these IT specialists find weak points in their company's networks. Security analysts must stay up to date with what's happening in cybercrime and with new developments in online security to help develop new policies and protections against cyberattack. They help the C-suite make smart decisions about how to allot security resources, based on the serious nature of various threats faced. The demand for information security analysts will continue to grow over the next 6 years or so, with an anticipated increase of 32% in the field.

Forensic Experts
These are the experts who track down what happened when a data breach or cyberattack occurs, working to find the attackers. They determine how breaches occur and work with various IT first responders. They also preserve and take care of all evidence, including hardware such as hard drives and portable drives.

Application Development Security Specialists
Look for this specialty to increase 164% in demand over the next 5 years (with a concomitant increase in their salaries). These specialists work to detect pending threats and automate security-related tasks relating to apps and software.

Risk Management Specialists
Being able to assess the risks posed by particular IT vulnerabilities is vital if companies are to spend their security resources wisely. Risk management experts include risk analysts and vulnerability assessors, both of whom analyze and probe a company's information systems and computer networks to find errors and test vulnerabilities. Analysts model various cybersecurity threats and scenarios to determine levels of IT, fraud and financial risk. Often these specialties require a fluent knowledge in the areas of artificial intelligence and machine learning.

Staffing up properly and filling your open cybersecurity positions can be tricky, given the growing demand in the marketplace for these specialists. At Marquee Staffing, we are deeply invested in the IT staffing world and are ready to help you find employees with the specialized skills you need to protect your business. Contact us today to see how we can help keep your data and your online processes safe so you can feel secure about your company's future.

Chris Kappes
Executive Vice President

With over 25 years' experience supporting Southern California technology leaders in Robotics-Automation, Aerospace, Medical Device, and Electronics-Semiconductor with industry proven Engineering-IT talent.

Kappes' strong understanding of each client's unique talent requirements for new product development, manufacturing support, quality-regulatory, operations-supply chain and his commitment to rapid response provides game changing hiring results for his customers.

STAY AHEAD OF THE COMPETITION
WITH MARQUEE.