NO TRUCE IN CYBERWARS

FIGHTING FRAUDSTERS ONLINE

By Paul Kilby

With people increasingly living their lives online, fraudsters have never had easier access to potential victims. COVID-19 has only accelerated that trend. Indeed, business is booming for cybercriminals now focused on high-value organizations. *Fraud Magazine* talks to cyber expert Robert Herjavec and CFEs about how best to tackle this ever-evolving threat.

On July 2, around 2 p.m. U.S. Eastern Standard Time earlier this year, employees at Miami-based software company Kaseya started receiving reports of suspicious activity. Third parties, customers and Kaseya's monitoring systems were noticing "strange behavior" on their computer systems. Little did they know that this was the start of what would soon be described as the biggest single ransomware attack on record.

"We didn't know if it was an attack. We weren't quite sure what it was," recalls Kaseya CEO Fred Voccola in a YouTube video on the company's website. (See "Kaseya CEO Fred Voccola Addresses Cyberattack and Next Steps for VSA Customers," YouTube, July 6, tinyurl.com/xffnzuj2.)

As a precautionary measure, the company quickly shut down the servers that ran its remote monitoring and management software, which it sells to managed service providers (MSPs). (According to Gartner, an MSP delivers services, such as network, application, infrastructure and security, via ongoing and regular support and active administration on customers' premises, in their data centers or in third-party data centers. See tinyurl.com/byzb8nyb.)

But the damage had been done. Kaseya executives soon realized that they were the latest victims of a cybercrime spree that has spread across the globe in the wake of the COVID-19 pandemic.

And while the breach only impacted about 50 of Kaseya's 37,000 customers worldwide, according to Voccola, its reach was far wider. The company quickly solicited the help of the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, the FBI and even the White House. But a few days later, the media was reporting that the ransomware coursing through Kaseya's network had perhaps spread to around 1,500 businesses, and the hackers were demanding an eye-popping $70 million to restore all systems back to health. (See "Kaseya ransomware attack update: Hackers demand $70M, believed to be a record sum," by Stephen Melendez, *FastCompany*, July 6, tinyurl.com/2h9n2y6k.)

Victims included a pharmacy chain, a gas station chain, the state railway and public broadcaster SVT — all in Sweden — as well as IT services companies in Germany and the Netherlands. The cyberattack also brought down cash registers and self-service check-out machines at Swedish supermarket chain Coop, forcing it to close over half of its 800 stores. It even shut down a Maryland town's internet services. (See "Swedish Coop supermarkets shut due to US ransomware cyber-attack," by Joe Tidy, BBC, July 3, tinyurl.com/54y7598u, and "Maryland town knocked offline as part of massive ransomware attack," by Joseph Choi, The Hill, July 8, tinyurl.com/yve5duwz.)

The Kaseya attack may have been exceptional in its reach and the amount of ransom demanded, but it was hardly an out-of-the ordinary occurrence. Since the outbreak of the COVID-19 pandemic early last year, the world has seen surges in cybercrime and cyberfraud as the shift to remote work better enables these offenses. (See "Check Point Software's predictions for 2021: Securing the 'next normal,' " Check Point Software Technologies Ltd., tinyurl.com/mfvfs7s6.)

"We all have to take a step back and realize this is the world we live in, and it is forcing us to look at ourselves as well, recommitting ourselves to every possible consideration that is there," says Voccola in his YouTube announcement.

Fraud Magazine recently talked to Robert Herjavec, leading shark on ABC's Emmy Award-winning TV show, "Shark Tank" and Founder & CEO of Herjavec Group, a global cybersecurity firm offering comprehensive security services to enterprise organizations — as well as CFEs specializing in cyberfraud — to get their take on how fraud examiners are approaching this ever-changing threat in the post-pandemic world.

"E-commerce, digital infrastructure, cloud, the move to online, the move to remote network — we all knew this was the future," says Herjavec in an email interview. "No one knew though that the future would happen in 12 months. That's what COVID did. This movement has accelerated our business and the overall security industry. The more people online, the more security required."

Hardly a month has gone by this year without news of a major cyberattack. In June, the FBI said that REvil, the same group whose affiliate was responsible for Kaseya's breach, carried out a ransomware assault on Brazilian meatpacker JBS. And in May, bad actors unleashed ransomware at Colonial Pipeline, the largest fuel pipeline in the U.S., causing widespread gas shortages and long lines at gas stations. (See "Largest meat producer getting back online after cyberattack," by Dee-Ann Durbin and Frank Bajak, AP, June 2, tinyurl.com/39hypx6j.)

And those are just the high-profile incidents. A whole range of companies and organizations have reported similar cases this year from brewing company Molson Coors to fast-food chain McDonald's to a string of universities. (See "2021 Ransomware attacks and alerts," Cloudian, tinyurl.com/zukcrj39, and "McDonald's becomes latest company to be hit by data breach," by Michelle Chapman, AP, June 11, tinyurl.com/y3ay56tu.)

"This cybercrime world is now impacting the everyday world," says Patrick Westerhaus, CFE, CEO of Cyber Team Six. "In the past, you may have had a credit card stolen or been the victim of identity theft. Now cybercrime has matured to such a point that it impacts the general population. It is all over the media. It is no longer just isolated incidences."

Supply-chain attacks

Indeed, cybercriminals and fraudsters are becoming better at poking holes in cyber defenses and spreading malware across multiple organizations in one fell swoop through so-called supply-chain attacks.

The severity of this type of breach became clear last year when hackers inserted malware into the software of Texas-based SolarWinds, spreading the malicious code to its clients and leaving up to 18,000 customers vulnerable. (See SolarWinds' SEC 8K filing, Dec. 14, 2020, tinyurl.com/atketn9b.)

The Russian intelligence services that were thought to have carried out the breach used the malware to gain access to the networks of several U.S. federal agencies. (See "Hacker Lexicon: What Is a Supply Chain Attack?" by Andy Greenberg, *Wired*, May 31, tinyurl.com/wz2k7u54.)

Experts are particularly worried about the latest cyber break-in at Kaseya — not only because it was yet another destructive and widespread supply-chain attack, but this time the criminals used sophisticated hacking techniques comparable to what nation-states deploy. (See " 'Apex predators': Why the Kaseya ransomware attack has experts worried," by Kevin Collier, NBC News, July 6, tinyurl.com/kvkdm7ep.)

Kaseya VSA software was an ideal target for cybercriminals as the company sold it to MSPs, which small and medium-sized businesses pay to care for their IT needs. By infecting the VSA software, an affiliate of the cybercriminal organization REvil was able to demand ransom from a larger scope of victims. (See "What Happened in the Kaseya VSA Incident?" by Nicholas Weaver, Lawfare, July 4, tinyurl.com/4dhp9sc4, and "Kaseya ransomware attackers demand $70 million, claim they infected over a million devices," by Richard Lawler, The Verge, July 5, tinyurl.com/ytnbf865.)

No matter how strong their defenses, organizations that are part of a supply chain remain vulnerable as fraudsters seek to exploit the weakest link amid a network of companies that regularly conduct business with each other.

"Most of the large-scale corporate breaches recently have come through suppliers and third parties," says Herjavec. "As companies have bolstered their defenses, they have often overlooked the many third parties that regularly interact with them. Many of these third parties are smaller with limited security. The challenge is how do you enforce your corporate standard on a third party that may not have the same resources or policies?"

Herjavec was a keynote speaker at the *32nd Annual ACFE Global Fraud Conference*. (See "Cybercrime in the age of COVID-19," by Paul Kilby, *Fraud Conference News*, June 22, tinyurl.com/39epfam4.)

Post-COVID vulnerabilities

Cyberfraudsters and other criminals now have a bigger attack space. In the past, organizations largely kept their data and employees in one, easily defensible place. But that all changed as the spread of COVID-19 forced employees to work from home, where they labor on less-protected laptops and in multiple locations.

"The amount of fraud reported that goes through these channels is significant, especially from banks and large enterprises," says Westerhaus. "And it is only going to get worse because of the hybrid and remote work models which have expanded significantly as a result of the pandemic."

The move toward a more fragmented workplace has also gone hand in hand with increased inter-connectivity — the so-called internet of things. Everything from fridges to home security systems and other devices in the house are increasingly linked to the internet and each other, which expands possible entry points for fraudsters.

Amy Chang is head of business development at cyber insurance and security company Resilience and former executive director, global cybersecurity at JPMorgan Chase. She says, "[the internet of things] introduces all these additional layers of vulnerability and if you don't have a full understanding and awareness of your technological environment, it can make it very easy for threat actors to come in."

Convenience trumps security

Companies try to please customers by typically prioritizing the convenience of technology over what can be bothersome security protections. "This is tremendously risky, but no one thought along those lines because convenience always trumped security," says Walt Manning, CFE, CEO of Techno-Crime Institute, a future investigations research and consulting firm.

However, commercial enterprises are likely to start rethinking those priorities as they come to realize that it's not a question of if but when cyberfraudsters will try to storm their defenses. "From an enterprise perspective, I don't think you can any longer dissociate business from the security aspect of the customer," says Westerhaus.

"Organizations, to some extent, have taken it seriously to protect employees and companies, but protecting customers is not viewed as a competitive advantage," he says. "It has always been an afterthought. That can no longer be the case."

Indeed, organizations are gearing up for yet another jump in fraudulent activity, particularly in cyberspace, and appear to be taking some defensive measures, according to the ACFE's latest benchmarking report. (See *The Next Normal: Preparing for a Post-Pandemic Fraud Landscape*, ACFE.com/covidreport, and "Organizations brace for another uptick in fraud," in ACFE News on page 67.)

While survey respondents expect to see growth in fraud risks in most categories, cyberfraud and social engineering are the risk categories most expected to increase, with more than 80% of survey respondents anticipating growth in these two areas.

And perhaps reflecting increased cyberfraud risks, 38% of the organizations surveyed increased their budgets for anti-fraud technology in fiscal year 2021 compared to pre-pandemic years. (See the ACFE news article on page 67 in this issue.)

"Your cybersecurity resilience is key because you are going to be a target no matter what, especially the financial industry," says Carmi Moser, a senior principal risk specialist with financial industry regulator FINRA. "We should really be mindful of response resiliency and data protection aspects."

Business of cyberfraud

The business of cyberfraud has grown in size and sophistication over the years and even more so during the COVID-19 pandemic. The lone hooded hacker wearing a Guy Fawkes mask in a dark room may be a favorite stereotype, but it's a far cry from the reality of today's cybercriminal enterprises.

A whole ecosystem is now available to fraudsters seeking opportunities in cyberspace. "Ransomware-as-a-Service" or "Malware-as-a Service" (better known as RaaS and MaaS) are new names for businesses selling malicious software, passwords and other services on darknet marketplaces.

And in some ways, this has only made it easier for fraudsters to ply their trade. "In the old days, it took an effort to be a white-collar criminal; it really did," says Westerhaus, who previously worked as a senior manager in the FBI's Cyber Crime

CYBER CONTROLS AND PREPARING FOR BREACHES

Despite the increasing sophistication of cybercriminals, some commonsense measures go a long way to protecting organizations and individual households from cyberfraud, say experts.

"In some ways the more things change, the more they stay the same," says Robert Herjavec, CEO of cybersecurity firm Herjavec Group. "Most ransomware still comes from email. Traditional security [firewalls, multifactor authentication] is as important as ever."

Even so, implementing such controls in a large company with a lot of employees, who these days are often working remotely, is easier said than done. It just takes one employee clicking on the wrong email to open a brief window for a hacker to insert ransomware — no matter how much an organization invests in IT. JBS, for example, spends more than $200 million annually on IT and employs more than 850 IT professionals globally, yet it failed to prevent criminals breaching its system.

"Nothing is bulletproof," says David Utzke, Sr., Ph.D., CFE, associate professor at the University of Advancing Technology. "We live in a fallible world. It doesn't make any difference how well you educate employees; someone is always clicking on something they shouldn't just because of personal curiosity, or they don't pay attention to the red flags and allow malware to get into the system."

That's why regular fraud training is essential at organizations that want to prevent such breaches. "Training is a big component of cyberfraud prevention, and it is something we don't see enough of," says Amy Boawn, CFE, a fraud fusion subject matter expert for the cyber defense team at consulting firm Booz Allen Hamilton.

In sectors such as the financial industry, where employees are already faced with considerable compliance training and other work responsibilities, having them focus on fraud training too can be a challenge, she says. More organizations are trying to incentivize employees with so-called "gamification," such as providing cashable points or tokens for completed training or reporting suspicious activity, Boawn says.

Communication is also key, especially within medium and small organizations, where a chief risk officer, a chief information security officer and other C-suite executives have different mandates and aren't always clear on how to come together on cybersecurity. "They all know it's important, but they don't necessarily know where to begin," says Amy Chang, head of business development at cyber insurance company Resilience.

Sometimes, she says, it's as simple as a leadership-level discussion about how cybersecurity is actually central to a company's financial and business priorities. In many cases, simple solutions can pay large dividends. For example, a companywide rollout of cyber controls, such as multifactor authentication, can prevent cybercriminals from illegitimately accessing sensitive accounts, and enabling email authentication prevents unauthorized threat actors from attempting to impersonate CEOs, an increasingly popular scam. (See "What Is CEO Fraud?" KnowBe4, tinyurl.com/u4arzn3m.)

Other controls that Chang recommends are:

- Segment your networks to protect your most sensitive data.
- Limit the ability of individuals to conduct unauthorized changes or transactions in, for example, your payment system or specific databases.
- Have and practice an incident response plan in case a supplier is impacted by cyberfraud. Be prepared to know what to do, who to call and whether you need legal counsel.
- Have a proper agreement in place with third-party suppliers and vendors that obligates them to report in a timely manner any cyberbreach that may have occurred.

James McDowell, CFE, principal intelligence specialist at the financial intelligence unit at FINRA, says the financial industry regulator recommends brokerages and other financial securities specialists to stress test a response plan well in advance and consider developing a relationship with law enforcement before any attacks occur. "The worst time to realize your response plan doesn't work is when you are undergoing an incident," he says.

division. "But if you want to be a white-collar criminal today, just be a cybercriminal. If you can download software, you can be a cybercriminal."

Sophisticated hackers, brokers and everyday fraudsters pool their skills to pull off attacks that can bring in thousands if not millions of dollars. Indeed, cyberfraud has become highly lucrative as scammers increasingly set their sights on high-value multinational firms, in what has become known as "big-game hunting," or BGH. (See "2021 Global Threat Report," CrowdStrike, tinyurl.com/c935rdwc.)

JBS Foods USA said in June that it had paid the equivalent of $11 million to what the FBI described as one of the most specialized and sophisticated cybercriminal groups in the world. (See "JBS USA Cyberattack Media Statement," June 9, tinyurl.com/6vn692n7.)

The group that infected Kaseya's software set a $70 million ransom in bitcoin to free everyone from the malware, though it also reportedly asked for up to $5 million from individual organizations. (See "Scale, details of massive Kaseya ransomware attack emerge," by Frank Bajak, AP, July 4, tinyurl.com/hucjcbn3.)

And while the FBI has clawed back some of the ransom paid, such as in the Colonial Pipeline case, the stakes are high for companies that let their guard down. (See "Feds recover millions from pipeline ransom hackers, hint at U.S. internet tactic," by Kevin Collier and Pete Williams, NBC News, June 7, tinyurl.com/se9525x8.)

"It's interesting — people are not as worried about losing money per se but they are worried about their business," says Herjavec. "The cost of a breach goes far beyond the ransom paid — it's downtime, it's brand integrity and loss, and loss of faith from consumers and partners."

The average cyber ransom paid by medium-sized companies was $170,404, but the average bill for rectifying this kind of attack was $1.85 million after accounting for opportunities lost, downtime and other costs, according to a recent survey by security software group Sophos. (See "The State of Ransomware 2021," Sophos, tinyurl.com/3pvm52fr.)

Online criminal forums, which have existed for many years, were first developed by fraudsters, such as Brett Johnson, who told his cybercrime story at the *32nd Annual ACFE Global Fraud Conference*. (See "Lessons From the 'Original Internet Godfather,'" by Paul Kilby, *Fraud Conference News*, June 23, tinyurl.com/3nwt5sdc.) Today those networks are thriving in part because of the unique circumstances brought on by the COVID-19 pandemic.

"It is quite a system," says David Utzke, Sr., Ph.D., CFE, associate professor at the University of Advancing Technology. "That is the real threat because they look more like a corporate network now."

Amy Boawn, CFE, is a fraud fusion subject matter expert for the cyber defense team at consulting firm Booz Allen Hamilton. She advocates a similar collaborative effort among organizations trying to prevent cyberfraud.

"The banking sector and financial services industry [for example] have forums they can go to, but by and large they don't do a good enough job in sharing information," says Boawn. "The more information that can be shared about what kind of scams are out there and the tactics being pulled, the more we can stop cyberfraud."

Rethinking investigations

Ever-evolving technology and the global reach of cyberfraud may require a rethink of how investigations are carried out, argues Manning, who helped create one of the first digital forensic teams at the Dallas Police Department in the 1980s.

> "We are fighting today's war with yesterday's tools and the hackers are constantly evolving." - Robert Herjavec

"This is a critical time for investigations," he says. "I would even call it a turning point. The old ways of doing things, by siloing investigations — particularly in law enforcement, where you have geographical, legal jurisdictions — that model on a global scale with this technology does not work anymore."

Investigative teams may need to be bigger given the number of experts required in cyberfraud cases, Manning says. He foresees cyber investigations adopting what he calls the "Hollywood" model, like how a director or a producer might hire specialists in cinematography, casting, costumes and special effects to make a single film.

"We will need a new type of investigations management philosophy and a person with the knowledge and expertise to be able to coordinate all of the different efforts from the various team members like we have never done before," he says. "[But] as the investigation becomes larger, more expensive and time-consuming, we may reach a point where a lot of organizations will say stop. The cost and the time of these investigations aren't worth the damage we suffered from the fraud."

Prevention and early detection

Those circumstance make prevention — one of the key tenets of ACFE founder and Chairman Dr. Joseph T. Wells, CFE, CPA — particularly important.

Westerhaus says the key to prevention is understanding the chain of events involved in a cybercrime and the often-lengthy time lapse between the hacking and the crime itself, whether it's theft, extortion or some other type of fraud. The whole process can take weeks, months or even years, he says.

"People think that just because someone hacks a computer or delivers malware that at that second their account is exploited," he says. "But it doesn't happen that way."

Sophisticated hackers with Ph.D.s can exploit computers and create ransomware, but they have no idea how to commit a crime, says Westerhaus. Like any marketplace, hackers then must advertise to everyday fraudsters who buy access and the malware to exploit organizations like they always have.

The trick is to stay ahead of the end user who carries out the crime. And that's done by identifying any stolen and/or vulnerable data and stopping it from being hacked or getting into the hands of fraudsters in the first place.

"The education point that needs to be made to CFEs is understanding cybercrime is an entire business, and there is an entire cycle that goes on from start to finish," says Westerhaus. "You can actually prevent a customer from having a bad experience by nullifying the work that the hacker has done before it gets to the fraudsters."

Herjavec has a similar take on how best to protect organizations struggling to keep up with new technologies and may ultimately be unable to stop cybercriminals from breaching their defenses.

"We are fighting today's war with yesterday's tools and the hackers are constantly evolving," he says. "I think one of the key goals for security leaders should be to move away from a prevention mindset and to focus on early detection."

Yet while hackers have found new and sophisticated ways to get past security measures, prevention and detection of cyberfraud often resembles fraud investigations of the past. "My philosophy is that cyber is just a tool that facilitates crimes that always existed," says Westerhaus.

"The new fraudsters are not good at creating code and hacking. They are just good at being on the internet," he says. "If you understand how people interact on the internet, then you understand the fraudster of today and tomorrow." ■ FM

Paul Kilby is editor-in-chief of *Fraud Magazine*. Contact him at pkilby@ACFE.com.