OCBJ.COM

ORANGE COUNTY BUSINESS JOURNAL

Vol. 44, No. 34 — THE COMMUNITY OF BUSINESS™ — August 23-29, 2021

# Home Offices Like 'Wild West' for Internet Security

## Experts Cite Dangers Of Gambling, Porn, Sports

■ By KEVIN COSTELLOE

Employees who work from their homes may be putting their companies' systems at risk.

"Many employees do company work from personally managed and owned systems and these machines are often the 'Wild, Wild West' in terms of how they are secured," said **Mike Gentile**, the chief executive of San Clemente-based cybersecurity company **Cisoshare**.

**Ilia Sotnikov**
**Security Strategist, VP**
**Netwrix**

"The majority of complex attacks, such as ransomware, etc., right now are still often caused by a simple phishing attack or an employee mistake like clicking on a bad link."

Cisoshare is one of several cybersecurity firms that are emerging in Orange County, which is carving a strong position in internet security due to the proliferation of hackers from **Russia**, **China** and **North Korea** who demand eye-popping sums in ransomware.

**CrowdStrike Holdings Inc.** (Nasdaq: CRWD), a Sunnyvale-based firm that now has a $55 billion market cap, started in Orange County where it still has a large local presence. Irvine's **Cylance** sold for about $1.4 billion to **BlackBerry** in 2019 and also counts a base of operations here.

In Newport Beach, the **ioXt Alliance** started by **Mobilitie** founder **Gary Jabara**, wants to make sure the interconnections among the various devices used each day—such as cellphones, smart home lighting controls and automotive technology—are also secure.

**UC Irvine**'s **Cybersecurity Policy & Research Institute** studies ways to make the internet and networks safer, including running mock attack drills.


**OC cyber experts see hazards in working from home**



**FBI targets dangerous international hackers**

See stories in this week's Cybersecurity Special Report that begins on page 21.

### Cybercriminals

Irvine-based **Netwrix Corp.** is expanding so quickly that it's made four acquisitions since January.

"Most organizations did not have time to prepare a transition plan and provide security training to the employees" when they started working from home last year, said **Ilia Sotnikov**, security strategist and vice president at Netwrix.

"Hence the increase in reported incidents that included data loss or oversharing."

Attackers know that ransomware is arguably the quickest way to get money from a company without breaking into its system, he said.

"The cybercriminals took advantage of the global pandemic and highly divisive political scene in the U.S. last year," Sotnikov said. "We've seen considerable changes in how the threat landscape evolved over the last couple years with ransomware as a service, more specialized groups."

### The Coronavirus Chaos

"There was so much chaos during the first few months of the lockdown that every CISO will need to go back and review all of the access and changes that happened," said **Bil Harmer**, who is the chief information security officer (CISO) and chief evangelist at computer identity security software maker **SecureAuth**.

"When there is chaos and change, the threat actors will be there looking for ways

OCBJ.COM

ORANGE COUNTY BUSINESS JOURNAL

Vol. 44, No. 34 — THE COMMUNITY OF BUSINESS™ — August 23-29, 2021

in."

He predicted that companies "will begin putting more and more focus on digital identities and a continuous authentication methodology that will allow them to adjust access on the fly as the landscape or the user behavior changes."

Cisoshare, founded by Gentile, placed No. 21 on this year's Business Journal list of Best Places to Work in Orange County and No. 2 on last year's list of fastest-growing companies, both in the small-firm category.

Companies who let employees work from their homes face an increasing threat level similar to that of an apartment owner who adds more apartments to a portfolio: the more units there are, the greater the business risks, Gentile said.

"When employees are working from home, it expands the digital footprint and perimeter of the organization," Gentile said during a recent interview.

Providing security also requires using precious resources and talent—both of which are in short supply at plenty of companies, Gentile said.

"The majority of security risk lives in the cracks when people don't effectively collaborate and 'cover all the bases' when building something," he said.

Training on workstations from which a network is accessed can reduce the risks when employees work from home in a decentralized environment, Gentile said.

## The Hybrid

Companies that opt for a "hybrid" model combining both work-from-home and the office should be wary.

"Hybrid can be risky due to any time rules change, there is a higher likelihood of mistakes," **Kevin McDonald**, the chief operating officer and chief information security officer of **Alvaka Networks** in Irvine lists 16 points of vulnerability. They include use of bootlegged software, browsing illicit sites, opening infected files that would otherwise be blocked, communicating with unverified individuals and illegal sharing of various contraband such as movies, images, and games.

"Gambling, pornography, sports, gaming sites, alternative bulletin boards, messengers, even terrorism and extremist sites lead to infections of the host that then connects to the company," he said.

"We all suffer from a bit of that-won't-happen-to-me syndrome. We're not a target, we don't have anything they want, we're not that rich of a company."

He says ransomware attackers are well aware of the potential payoffs: "One hit and you can retire."

Companies are starting to nudge employees into coming to their offices though the daily back-and-forth from the COVID-19 Delta variant makes it difficult to set firm guidelines.

For example, data analytics software maker **Alteryx Inc.** has "voluntarily opened a number of our offices, including our Irvine location for those who are comfortable coming in," Chief Financial Officer **Kevin Rubin** said on Aug. 5. "There's no mandate that they do."

"We will more officially begin asking associates to start coming back no sooner than January," he added.

## Bright Spots

Sotnikov sees some bright spots.

"I think many of the WFH (work-from-home) specific dangers were mitigated over the last 12 months, as organizations had a chance to catch their breath, get new budgets in 2021, catch up on trainings for both admins and employees," he said.

The Senate included more than $1.9 billion in cybersecurity funds as part of the roughly $1 trillion bipartisan infrastructure package, The Hill website said on Aug. 10.

The funds will go toward securing critical infrastructure against attacks, helping vulnerable organizations defend themselves and providing funding for a key federal cyber office, among other initiatives.

## Russia, China

Experts point to the targeting of **Colonial Pipeline** and **JBS** meat packers earlier this year as examples of the dangers

### Cisoshare

- **FOUNDED:** 2015
- **HEADQUARTERS:** San Clemente
- **FOUNDER/CEO:** Mike Gentile
- **EMPLOYEES:** 45
- **REVENUE:** $10M (2021 projected)
- **BUSINESS:** cybersecurity, security program development, managed services

### Alvaka

- **FOUNDED:** 1982
- **CEO:** Oli Thordarson
- **HEADQUARTERS:** Irvine
- **EMPLOYEES:** 40
- **REVENUE:** $10M projected for full calendar year 2021
- **BUSINESS:** network management, monitoring, security services

### SecureAuth

- **FOUNDED:** 2005
- **HEADQUARTERS:** Irvine
- **CEO:** Ravi Khatod
- **EMPLOYEES:** 194
- **BUSINESS:** identity security to protect computers and systems

### Netwrix Corp.

- **FOUNDED:** 2006
- **HEADQUARTERS:** Irvine
- **CEO:** Steve Dickson
- **EMPLOYEES:** 500+ globally, more than 60 at HQ
- **BUSINESS:** information security, control enabling

OCBJ.COM

ORANGE COUNTY BUSINESS JOURNAL

Vol. 44, No. 34 — THE COMMUNITY OF BUSINESS™ — August 23-29, 2021

of ransomware demands.

The picture is acute on the international front, with both Sotnikov and McDonald noting President **Joe Biden**'s warning last month that a significant cyber-attack on the U.S. could lead to "a real shooting war" with a major power, highlighting the growing threats posed by Russia and China.

"That is a very aggressive and provocative statement," McDonald said. He points to China in particular as he surveys global cybersecurity threats to the U.S.

"I would far more worry about China finally deciding it's time to become the sole world power and using its understanding of our weak infrastructure to show us how much we don't really have control of the world anymore," McDonald said.

And the ultimate piece of bad news?

"Replacements are made in China," he said. ■

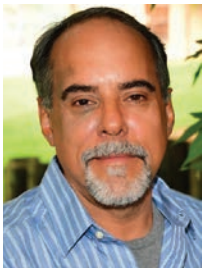
# Dangers, Positive Signs: OC Cybersecurity Experts Look at Internet Risks

## OC Cybersecurity Experts Give the Business Journal These Tips:

**KEVIN MCDONALD, chief operating officer/chief information security officer, Alvaka Networks in Irvine**

Some dangers are "removed or reduced" if the equipment is owned by the employer.

"Employee-owned computers are far less likely to be patched and kept up-to-date against vulnerability. This includes the operating systems, office applications, third party applications such as Adobe, Internet browsers, etc.



Kevin McDonald
COO, Chief Information Security Officer
Alvaka Networks

"Having a system shared with non-employees (of unknown behavior tendency, character, education, intent) means that there is a high potential for risky behaviors that can result in a compromised local computer.

"Big time execs and powerful people are targets and they're the most reticent to participate in this whole process.

"Cryptocurrency is the "primary reason" for the rise in ransomware in which hackers hijack a computer system and demand payment to release it."

**MIKE GENTILE, founder/chief executive, Cisoshare in San Clemente**

The biggest risk to work from home or hybrid for security "is that collaboration and effective small team dynamics are hindered when people can't work together in person."

Mike Gentile
Founder, CEO
Cisoshare

"The good news is that some of the strongest safeguards when a workforce is decentralized is a strong security training and awareness program, as well as a communication system so employees know how to get in touch with the security team and vice versa. Both of these items are highly effective, but also much more inexpensive than almost all technical safeguards."

**BIL HARMER, chief information security officer/chief evangelist, SecureAuth in Irvine**

"The hybrid model will not go away, there is far too much upside for companies in it. From 48 extra minutes per day per employee in productivity to reduced footprints in the office (desks, power, coffee, etc), this is a model that will continue.

Bil Harmer
CISO, Chief Evangelist
SecureAuth

"Companies will begin moving to Secure Identity as the first line of defense. They will begin putting more and more focus on digital identities and a continuous authentication methodology that will allow them to adjust access on the fly as the landscape or the user behavior changes.

"This will allow the user to move around the physical world and have their authentication and authorization adjust as they do to keep them within the acceptable risk profile." —*Kevin Costelloe*