The NETWORK Pro
Greater Response • Greater Uptime • Greater Results

Hackers Know Your Weak Spots: Do You?

Kevin Studley, President, The Network Pro, Inc.

“Never let a crisis go to waste.” That’s a time-honored saying in politics, but cybercriminals have taken it to heart, too. As the coronavirus pandemic spread earlier this year, and most people worried about safety, their jobs and finding toilet paper. At the same time, the FBI noted a significant spike in cybercrime.

But it’s not just during a pandemic that Orange County businesses need to be mindful of cybersecurity threats. They can be targeted by tactics that threaten valuable data, disrupt supply chains or bring operations to a dead stop at any time. It’s important to identify possible weak spots before the hackers do and take action so that all systems connected to vital operations are less vulnerable.

Awareness is key
Financial damage from cybercrime could exceed $6 trillion a year by 2021, according to the Department of Homeland Security. For any Orange County business, a cyberattack could produce a shredded reputation, damaged products and idled production. And it could start with something as simple as an administrative staffer clicking on an interesting link or a sales rep skipping computer updates while traveling.

As cybercrime has become more common, most companies are aware of common tactics used. They know stolen passwords can let crooks burrow into a company’s computer system and gain access to all kinds of data. They’ve heard about ransomware, through which a company’s operations are paralyzed till a huge ransom is paid. They’ve seen organizations’ credibility crumble when news of a big data breach appears on the TV news.

Smaller Orange County businesses might not offer hackers the same wealth of data they might ferret out from, say, a financial institution or a large health care provider. But as every aspect of business becomes more computerized and interconnected, no organization should underestimate the potential threats

Here are some key areas of vulnerability—including one that the COVID-19 pandemic highlighted in a big way: employees working from home.

1. Remote workers. Of course, people on an assembly line or in a tool-and-die shop can’t switch to working at home during emergency situations. But many Orange County operations are able to pack up their laptops and go home. Invariably, there will be difficulties establishing secure connections, problems with equipment that doesn’t work, concerns about privacy and lots of calls to tech support. Remote workers may miss system updates and they may be tempted to click on hackers’ fake offers of emergency information, or supplies such as sanitizer and face masks.

2. Internet of things. The internet of things, or IoT, refers to the expanding web of machines, systems and devices that interact with each other digitally and share information. Access to any of these connections could lead cybercriminals to a central database server. Many businesses that were not linked to computers years ago are very much connected now. For example, at least 35 percent of product lines in the U.S. are connected to efficiency sensors. Some organizations are tied in to third-party applications that may have their own security issues.

Other connected devices keep businesses humming along. They may include smart TVs in conference rooms, time clocks, digital sign-in systems for visitors, entrance security, alarm systems, and various devices connected to Wi-Fi. Access to any of these less obvious connected devices also could allow entry to more sensitive and critical areas of a central database.

3. Routine updates. Unfortunately, these are not always as “routine” as they should be. Regular system updates, default username updates and password changes are an important way to keep cybersecurity measures current.

As much as possible, Orange County organizations need to follow best practices in these and other areas to limit their cybersecurity hazards. A weak link anywhere in the system could result in lost data, compromised production, and costly, time-consuming down time during the restoration and cleanup process.

Risk-reduction strategies
There’s a lot Orange County businesses can do to reduce risks. It can start with an inventory of a company’s systems—computer servers, devices and software. An assessment might well turn up some devices or programs that are not really essential to keep the business running. Consider eliminating those.

Implementing best practices will include customizing and possibly upgrading procedures for things like:
• Updates of systems, passwords and usernames.
• Limiting access to the internet.
• Providing ongoing training for employees so they’ll not only appreciate the seriousness of cyberthreats, but also get better at spotting tricks such as phishing and social engineering.

Some companies opt to work with a cybersecurity firm to address their vulnerable areas. An outside consultant also can assist with plans for regular cybersecurity assessments, perhaps monthly or quarterly.

The NIST Cybersecurity Framework is one widely accepted resource for help with best practices. (The National Institute of Standards and Technology is within the U.S. Department of Commerce.) It helps companies assess risks, implement protective measures, and if necessary, recover from a cybercrime incident. The Center for Internet Security is another good resource for information about best practices, tools to enhance cybersecurity and information about current threats.

To reduce vulnerabilities in the long term, get buy-in from company leadership. Leaders need to make cybersecurity a priority and communicate this to all employees regularly. If someone breaks protocol on cybersecurity measures, there should be consequences. And while there’s always a temptation to slide back into “business as usual” when a threat or a crisis has passed, leaders must make sure that doesn’t happen.

Lessons from the pandemic
With concerns about the coronavirus expected to linger, it’s worth noting some cybersecurity lessons for organizations. While the pandemic had unique aspects, the fact is that many other calamities can disrupt business pose cybersecurity hazards.

The most crucial lesson: Have a plan. Companies that struggled and scrambled when the realities of COVID-19 hit were ones whose emergency plans were inadequate—or had not been updated in a while. Planners must think about extra equipment that would be needed in case of a crisis, including laptops and other equipment to let employees transition to working at home. Imagine a cybersecurity breach that disrupts supply chains, knocks out a key supplier or affects a third-party vendor. What’s Plan B?

Cybersecurity plans should be tested in advance, if possible. Various situations, including weather emergencies or infrastructure problems, could make it necessary for some employees to operate remotely. Before that happens, a trial run can ensure they have everything they’d need to work securely and efficiently. Orange County businesses need to take the same proactive approach to finding and fixing their cybersecurity weak spots—so they will not just survive, but thrive.

About the Author:
Kevin Studley is the president of The Network Pro, Inc. a California-based Managed IT and Security company. The Network Pro is recognized as a growth company on the Inc. 5000 fastest growing companies list, a Great Place to Work by the OCBJ, and has placed on the Top 501 Managed Services Providers list for the last seven years. Kevin Studley is an active and long-standing member of Vistage and actively participates in events that promote the business community. For more information, visit www.thenetworkpro.net or call (714) 333-9620.

TNP CYBER

Take Command and Control of Your Cybersecurity Risks with TNP Cyber

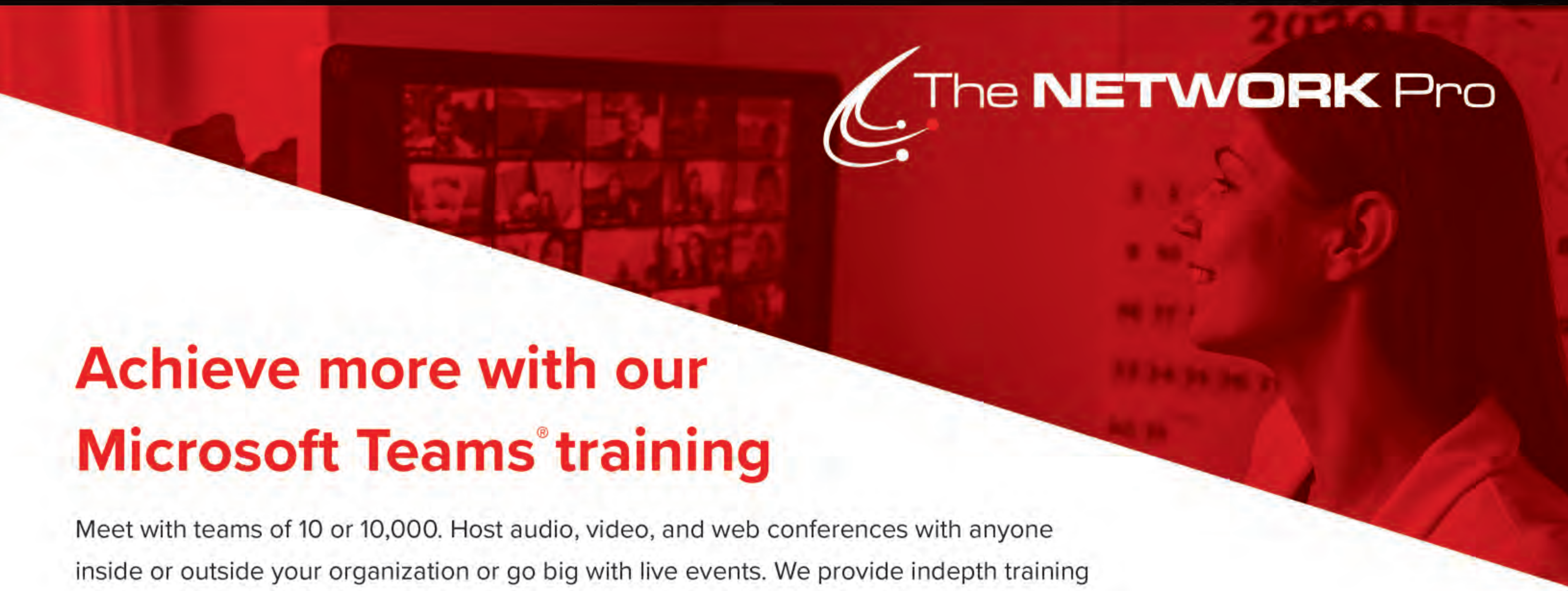
Managed Cybersecurity

IT Risk Assessment & Management

IT Compliance Solutions

We help small and medium businesses minimize their cybersecurity risk by filling in the security gaps they didn't know were there. TNP Cyber serves the California SMB market by helping our clients drastically reduce their cybersecurity risks and maintain their security standards compliance in today's perilous cybersecurity environment.

GET YOUR CYBERSECURITY ASSESSMENT AT **TNPCYBER.COM**



The NETWORK Pro

Achieve more with our Microsoft Teams® training

Meet with teams of 10 or 10,000. Host audio, video, and web conferences with anyone inside or outside your organization or go big with live events. We provide indepth training for small business to large corporations, to give you the tools for your business to thrive.

Meet with anyone, anywhere

Host online meetings—1:1, teams, live events up to 10,000 people—with consistent experiences across platforms.

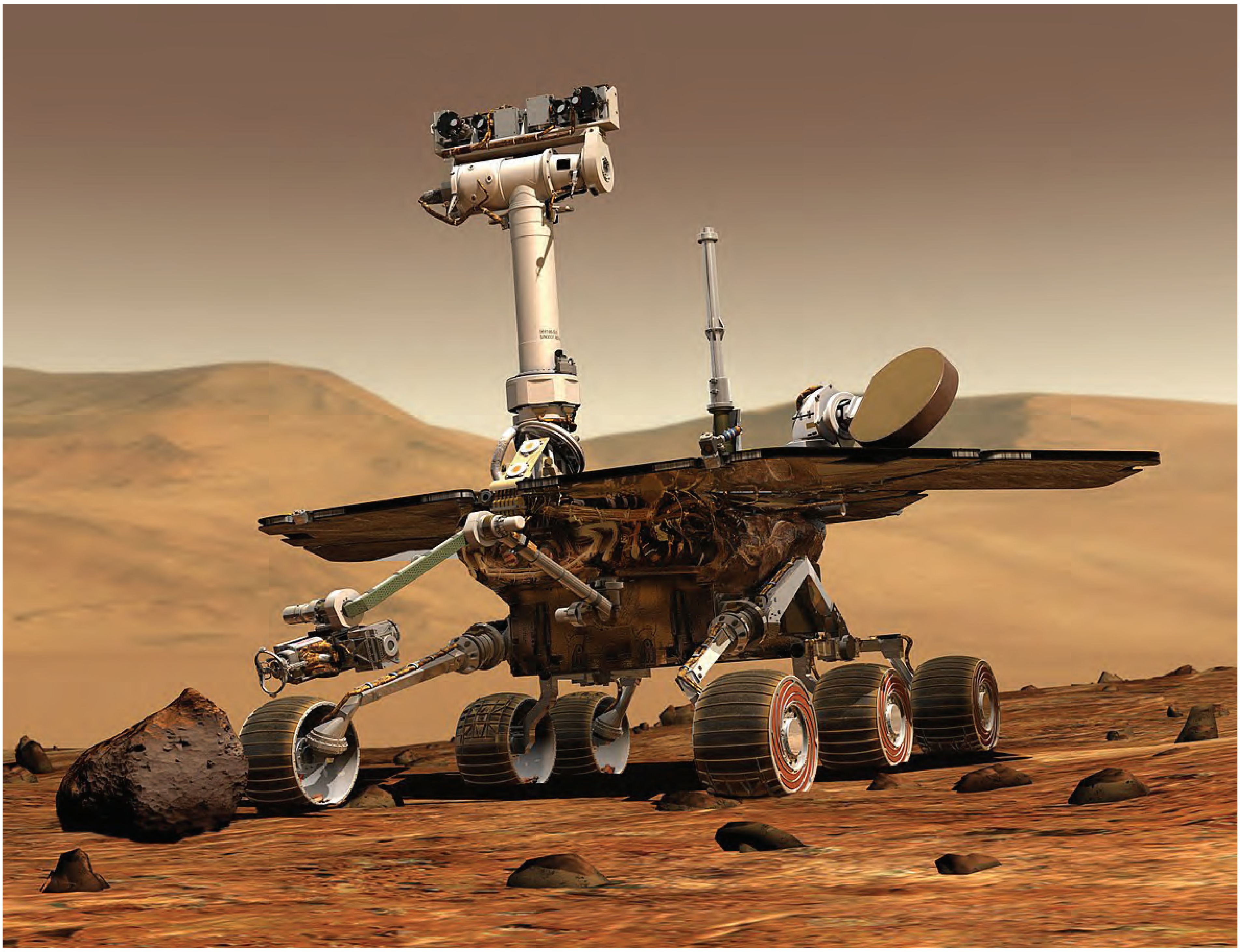
Meet with intelligence

Make online meetings more effective by sharing context and content and leveraging AI for assistance.

Meet with confidence

Get a secure meetings experience with high-quality audio, video, and screen sharing.

LEARN MORE AT **THENETWORKPRO.NET**



Tiodize Co.
Protecting Industries from Friction, Wear, & Corrosion

According to Tom Adams, Owner, Tiodize Co. the primary rule to becoming a successful entrepreneur is being honest. For Tom when you work hard and have dedication and passion, you are bound to reap rewards. “We have to ensure that alongside being honest you have to believe in yourself, enjoy what you do and have good people around you. These things matter when you are trying to navigate any industry and will also help you solve troubles in a streamlined manner.”Being ex-professional ballplayers, both Tom and his wife have travelled across the globe and met numerous people who helped Tom understand the value of communication and enhanced his capability to become a good listener.The company was founded in 1966 by Thomas Adams to fill the need for a special coating to reduce galling and its associated effects on titanium parts used in high performance aircraft. This coating and method of application, now widely known as the “Tiodize Process”, has been specified for use on practically every major space, military and commercial aircraft program since its introduction. Tiodize has over 100 different products and Tiodize process is one of them, which is the anodizing of Titanium.

Tom Adams

According to the pioneering leader, every industry has a need that involves lubrication, wear and corrosion. They all have different requirements such as temperature, use in vacuum, wear life and other problems with their engineers and run tests to verify the product meets the needs of the client, “this is very important. We have to listen to what the client’s issues are and then solve that problem in the best way possible,” adds Tom.

Today with rapid acceptance of the Tiodize Process one can see the beginning of intensified research and the development of solid firm lubricants. “Research and development have been slowed ever since Apollo was put to rest. But, today because of the Space movement research has resurfaced,” explains Tom. “The new research and development that the Moon and Mars projects will bring, will change the world as we know it.” The company has some of the most renowned clients in numerous industries which include Space X, G.E., Northrop, Boeing, Lockheed, and NASA to name a few.

However one can say that the day never ends for the steadfast leader, “I’ve heard that word unwind, but I never knew what that meant,” says Tom. “When I leave Tiodize after a days work, I go home to my wonderful wife and help her with business, which is Women’s Major League Softball International, which she is the agent for players wishing to play professional softball in Japan. When we are not doing that, we’re at the Angels, Lakers or Ducks games. Then there is the gym, when we can fit it in.”

For the days to come, Tiodize is looking towards developing new products. “When the Covid-19 hit the USA, we decided to make our own hand sanitizer to help our employees stay safe, along with giving it to our friends, fire department and polic in Huntington Beach,” says Tom. “Then we decided to make a disinfectant and degreaser to help clean the virus. Now it may become a new product line for us. This of course, is in between developing new coatings for space projects! We want to continue innovating in the best way possible for our clients.”

TIODIZE®

D99

HIGHEST QUALITY

Hand Sanitizer

DECREASES BACTERIA ON THE SKIN.

RECOMMENDED FOR REPEATED USE.

UNSCENTED FORMULA

GAL. 24 oz 3 oz

LEAVES NO RESIDUE

FDA REGISTERED

NDC: 77089-075-01, 77089-075-02 ,77089-075-03

Proudly Made in the U.S.A

Support U.S.A manufacturing.

INGREDIENTS: ISOPROPYL ALCOHOL, HYDROGEN PEROXIDE, GLYCEROL, AND PURIFIED WATER USP

ORDER # - 714-898-4377 www.tiodize.com