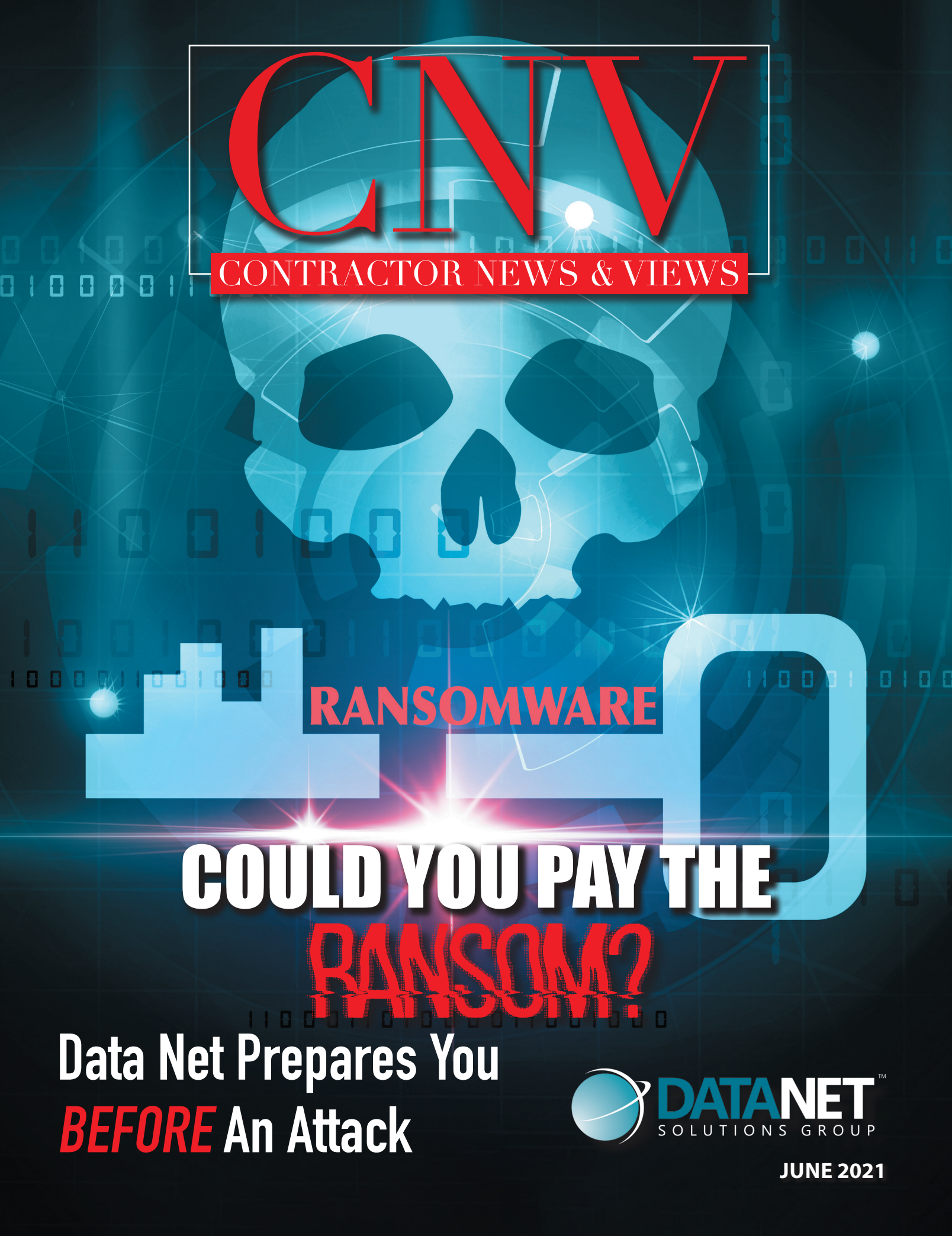
CNV
CONTRACTOR NEWS & VIEWS



RANSOMWARE

COULD YOU PAY THE RANSOM?

Data Net Prepares You *BEFORE* An Attack

DATANET™ SOLUTIONS GROUP

JUNE 2021

DATANET™
SOLUTIONS GROUP

COULD YOU PAY THE RANSOM?

Following a ransomware attack, is it better to pay the hackers the ransom to restore your data, or should this type of payment be your last resort? What are steps businesses can take to avoid being a target of cyberattack?

A new report from Palo Alto Networks -- which uses data from ransomware investigations, data-leak sites, and the Dark Web — found 337 victims in 56 industries, with manufacturing, healthcare, and construction companies suffering 39% of ransomware attacks in 2020. In addition, ransom demands skyrocketed during the year, doubling both the highest ransom demand — to $30 million—and the highest-known paid ransom, $10 million. The average victim paid more than $312,000, almost a third of the average demand.

Written By Matt Slaughter, Evan Etienne and Mary Montgomery

It's a beautiful Monday morning in California and you are headed in to the office as the sun is coming up. During the commute, you start going over the scheduled tasks and events for the week in your head. You arrive at the office, pour a fresh cup of coffee, turn on your computer, and start reading emails. One of the emails tells you that your files are locked and you cannot gain access to them unless you pay an exorbitant sum of money. You have seen these before, and you think it is SPAM or possibly a phishing scheme. You remember the cybersecurity training you took and say to yourself, "I will not click on any links, and I will be safe". You try to open a spreadsheet to review recent job costs, but the spreadsheet will not open. So, you go about your business and continue with other tasks. One of which is to review the new safety training policy located on the HR drive…but this file will not open either! At this point, you remember the ransom email you read earlier, and you start to panic! You immediately notify the CEO and your IT Company of the

Continues On Next Page >

"Security is not done overnight. It is a journey and commitment from the top-down or your business will be in the news."

— ROB SLAUGHTER
Data Net Owner

HOW TO AVOID A RANSOMWARE ATTACK

The best way to avoid being exposed to ransomware, or any type of malware, is to be a cautious and conscientious computer user. Malware distributors have gotten increasingly savvy, and you need to be careful about what you download and click on.

- Monitor activity on your network — Most breaches start months before the ransom is demanded. The breach could be detected when the proper tools are in place.
- Keep operating systems, software, and applications current and up to date.
- Maintain proper Access Controls based on the principles of least privilege
- Make sure anti-virus and anti-malware solutions are set to automatically update and run regular scans.
- Back up data regularly and double-check that those backups were completed.
- Secure your backups. Make sure they are not connected to the computers and networks they are backing up.
- Follow the 3-2-1 Backup Strategy — You should have THREE copies of your data (your production data and 2 backup copies) on TWO Different types of media with ONE copy off-site for disaster recovery.
- Work toward a Zero-Trust Security Architecture
- Create a continuity plan in case your business or organization is the victim of a ransomware attack.

IF YOU ARE A VICTIM OF RANSOMWARE:

- Contact your local FBI field office to request assistance or submit a tip online.
- File a report with the FBI's Internet Crime Complaint Center (IC3).

Data Net can help your business prepare for a ransomware attack so you won't have to contact the FBI and become another statistic! Cyber threats, including ransomware, can take many forms. The only solution is to maintain a robust and mature security posture.

Among cybersecurity leaders surveyed by WSJ Pro Research, 57.5% said they wouldn't pay, leaving 42.5% who said they would at least consider paying—with a wide range of responses depending on what industry a company is in. WSJ Pro Research provides data and research as part of The Wall Street Journal's professional information offerings.

situation. "What do we do? How will we access our bids and building plans to continue work on the jobsites? How are we going to access payroll to pay our staff?"

While this may sound like the plot of a Hollywood movie, the reality is that this occurs in real life more often than you would believe.

Ransomware attacks are on the rise as they are an extremely effective way to harvest monetary resources from a company. Often, unprepared companies are left with the choice to pay the ransom or suffer catastrophic data loss. Ransomware represents one of the most profitable sectors of cybercrime and is a multi-billion-dollar industry. Many of these groups operate like high-level corporations, with different departments, online support for buying bitcoins and transferring for the ransom payment, teams of specialists, and refined leadership.

Ransomware extorts victims for access to their own resources: a ransomware program encrypts everything on some level, whether it is a file, a user's workstation, or an entire network. Once the user is locked out, the responsible party offers them the key to get their data back – for a price. Users are shown instructions for how to pay a fee to get the decryption key. Costs can range from a few thousand dollars to millions, payable to cybercriminals in Bitcoin. Amplifying the pressure, these offers are often time sensitive. If the ransom is not received before the deadline passes, the attacker promises to delete everything. There is no guarantee that

Law-enforcement agencies including the Federal Bureau of Investigation have advised victims not to pay ransomware attackers, who encrypt the target's data and demand a ransom—typically in bitcoin—to unlock it. Paying creates an incentive for more cybercrime and doesn't always result in the encrypted data being restored, authorities say.

access to the files will be restored after payment and it is difficult to determine if the attackers left a back door open to maintain a presence in the victim's network.

While large-scale cyberattacks make national news, cyberattacks to small and medium size businesses can prove just as disruptive to operations. These smaller businesses typically do not have a sophisticated security posture because of out-of-date software, exposed web facing systems, and vulnerabilities susceptible to social engineering attacks like phishing. Another misconception is perimeter defense, (i.e.: The danger is behind the firewall). This has been long debunked by the security community and the concept of zero trust and defense in depth are not new. If you are a small to medium sized business, you could be fighting a losing battle and may not even be aware of the state of the battlefield.

All organizations are at risk of being targeted by ransomware and have an urgent responsibility to protect against ransomware threats. If you don't prepare now then you may get hit with a million dollar problem!

A recent ransomware attack had major consequences for a company responsible for supplying almost 45 percent of the fuel for the southeastern United States. Colonial Pipeline was targeted by a Russian-backed hacking collective called DarkSide with a ransomware attack that led to a spike in fuel prices and spotty availability that showed cracks in the nation's energy infrastructure. The ransomware attack launched on Friday, May 7th, 2021, forcing Colonial Pipeline to shut down operations to keep the attack from affecting the flow of fuel. Gas prices shot up by about six cents per gallon in a week. The pipeline runs from Texas to New York and is responsible for the transportation of an estimated 2.5 million barrels of fuel every day. The ransomware that caused the precautionary shutdown did not make it to the core system controls but had short-term effects on the supply chain.

Cleaning up ransomware is not cheap with the average cost of a forensic engagement exceeding $73,000 for enterprises and topping $40,000 for small and medium businesses.

Law-enforcement agencies including the Federal Bureau of Investigation have advised victims not to pay ransomware attackers, who encrypt the target's data and demand a ransom—typically in bitcoin—to unlock it. Paying creates an incentive for more cybercrime and doesn't always result in the encrypted data being restored, authorities say.

According to the Cybersecurity and Infrastructure Security Agency (CISA), the U.S. federal agency dedicated to advancing national security interests by reducing and eliminating threats to U.S. critical physical and cyber infrastructure, the Colonial Pipeline hack was the fourth major cyberattack in the past year. The Colonial Pipeline hack was preceded by a Solar Winds breach that allowed Russian Intelligence to hack into thousands of corporate and government servers, as well as an instance where Chinese nationals rented servers within the United States to infiltrate countless Microsoft Exchange servers. If big names like Microsoft can fall victim to these attacks, you know these threats need to be taken seriously. Whether a big enterprise or a small business, all are organizations are at risk.

About 74% of survey respondents in the construction industry said they would consider paying a ransom, making construction companies the most likely to contemplate it. Technology firms were next, with about 57% saying they would consider paying.
The sector least likely to consider paying was government, with only 18% of respondents saying they might.

> **"When we consult with a company, we review scans of the network and remediate the vulnerabilities. We are an IT company experienced in working with construction companies. We can guide and assist towards a more secure environment."**
>
> **— ROB SLAUGHTER**
> *Data Net Owner*

FROM EVAN ETIENNE – DATA NET SECURITY ENGINEER

- Ignoring your security posture may save you a dollar today, but will cost you far more in the long run.
- The number of cases is growing every day, and the adversaries are able to identify what companies are skimping on protection for their information systems. Most companies would not be able to survive without their information systems, even if their work is completely unrelated to computers and the internet. It becomes difficult when companies boil IT security down to a budget line item without accurately identifying how much of their revenue is dependent on these systems.
- There are no silver bullets. Companies need a suite of actively managed security products.
- Perimeter defense strategy is dead. Zero-Trust Architecture is the model of today and the foreseeable future.
- I can't believe I have to say this, but: You need to keep your systems, your software, everything up to date. Companies should incorporate threat intelligence into their security posture to quickly identify when new vulnerabilities are found in their systems.
- The switch isn't quick or easy- it involves a major culture shift, a ton of documentation, and a lot of time to refine. It is by no means an easy task. I recommend getting started YESTERDAY.