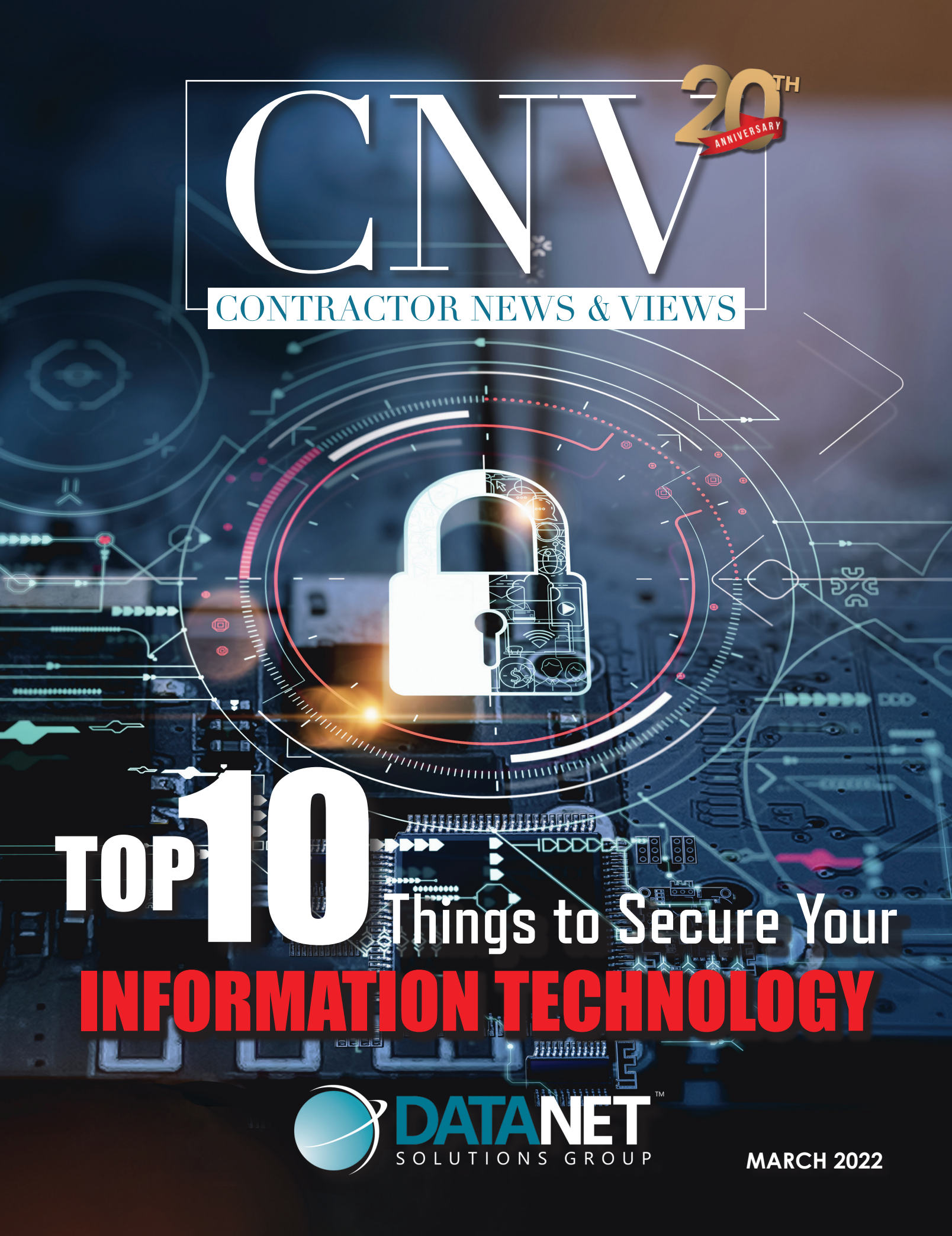
CNV
20TH ANNIVERSARY
CONTRACTOR NEWS & VIEWS



# TOP 10 Things to Secure Your INFORMATION TECHNOLOGY

DATANET™
SOLUTIONS GROUP

MARCH 2022

DATANET™
SOLUTIONS GROUP
(760) 466-1200 www.4datanet.com

**The question is not “IF you will get hacked”, but “WHEN you will get hacked”.**

# TOP 10 Things To Secure Your INFORMATION TECHNOLOGY

By Matt Slaughter, Bill Vann and Mary Montgomery

We are under attack! If your information technology infrastructure hasn’t been compromised, consider yourself fortunate. The question businesses face each day is not “IF you will get hacked”, but “WHEN you will get hacked”. Knowing and accepting that the current threat landscape is real and not just media hype or scare tactics is the first step you can take in securing your business.

Any online attack or compromise can have unexpected consequences, so it is wise to ensure your defenses are at full strength.

Long before Russia launched its physical invasion of Ukraine, the country was being hit by Russian cyber-attacks. Distributed Denial of Service (DDoS) attacks and wiper malware were among the cyber threats that targeted Ukrainian government ministries, banks, media, and other services. As the conflict continues, companies throughout the world have been urged to check their cybersecurity posture. Cyber-attacks do not respect geographic boundaries. Widespread cyber-attack incidents can have international consequences, intentional or not.

The Cybersecurity and Infrastructure Security Agency (CISA) is a US Government agency that leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. CISA has urged all organizations to take action to secure their networks.

San Diego based Data Net has seen major changes in the Information Technology (IT) world since it began its operations in 1983. The most significant changes seen in the last few years revolve around cybersecurity because of the massive increase in cyber-attacks. It used to be that typically only the big companies got hacked. Not anymore. Today, everyone is a target. And these attacks are not always aimed at a specific business. Attempts by hackers to gain access to sensitive information can target personal consumers as well. If you have a laptop or cell phone, you are at risk.

One way that hackers gain access to sensitive information is by sending out millions of email phishing scams, waiting for someone to open an attachment or click on a bad link. Once hackers successfully break in and get a foothold in an IT environment, they can access a company’s financials to determine the appropriate ransom amount to demand. Hacked files are then encrypted by the hackers who hold the information and access to the company’s systems hostage until the ransom is paid.

Staffed with experienced engineers and technicians, Data Net has helped many companies improve their cybersecurity posture. Data Net has even recovered entire networks that were hacked, saving clients millions of dollars in unpaid ransoms.

With the increasing threats to sensitive data in cyberspace, Data Net wants everyone to be vigilant, safe, and secure. The following steps can be taken to increase resilience against cyber-attacks.

Continues on Next Page >

## 1 Apply Patches and Security Updates

Applying patches and security updates to operating systems and software is the best way to close vulnerabilities in networks.

## 2 Use Strong Passwords

A common way for cyber attackers to breach networks is to guess usernames and passwords. Users should avoid using common, easy-to-guess passwords and instead use a password manager. Any devices on the network with default passwords should be changed.


## 3 Use Multi-Factor Authentication

Multi-factor authentication (MFA) provides an additional barrier to cyber-attacks and should be applied to all users. The benefit of multi-factor authentication is that, even if a username and password has been stolen or correctly guessed, it's still difficult for attackers to access the account. You have probably used this technology for accessing your financial information online. After entering your password, a code is sent to you that must be entered to gain access.


## 4 Teach Phishing Awareness

Many cyber-attacks start with phishing emails and staff should be trained in how to identify some of the most common techniques cyber attackers use, as well as how to report phishing emails for further investigation. Running simulated phishing campaigns in your organization helps to identify who needs more security awareness training.


## 5 Use Antivirus Software And Ensure That It Works

Antivirus software and firewalls can help to detect suspicious links, malware and other threats distributed by cyber-attacks and they should be installed on every device. It's important that antivirus software has the latest updates and that it's active and working correctly.

## 6 Know your network

You can't defend your network if you don't know what's on it, so you need to be able to identify all devices and users on the network. If a device or user account is acting unusually by accessing files they don't need for their job or moving to parts of the network that are irrelevant to them, it could be an indication that their account has been compromised. Log activity for at least a month so older activity can be traced to identify how a breach happened. Monthly network scans can help identify this activity as well.

## 7 Backup your network and regularly test

Backups are a vital component to ensuring cyber resilience and minimizing disruption in the event of a cyber-attack. Backups should be made at regular intervals and follow Best Practice of "3-2-1" (3 copies of data, on 2 different Media types, with 1 copy offsite). Backups should be regularly tested to ensure they work.

## 8 Be aware of third-party access to your network and supply chains

Managing IT networks can be complex and sometime require outside help, providing non-regular users with high-level access. You should have a comprehensive grasp on what access outside users have and be mindful of removing security controls.

Any access that's no longer required should be removed. You should try to understand the security practices of businesses in your supply chain. If one of these organizations is breached, their network could be used as a gateway to target you.

## 9 Have an incident response plan

Draw up a plan of how to react in the event of a cyber-attack. For example, if the network is down, how will you communicate a response? Thinking about different scenarios, planning, and running training exercises can reduce the impact of a cyber-attack.

## 10 Brief the wider organization about cyber threats

It's the information security team's job to know about cyber-attacks, how to deal with them, and to ensure that staff from the boardroom to the shop floor and jobsites are aware of the importance of cybersecurity and how to report suspected security events. For a business to be secure, it's crucial that everyone does their part.

**If you and your business need help to implement any of these measures, contact the experts at Data Net Solutions group. They are more than happy to assist. For more information contact Matt Slaughter at matt.slaughter@4datanet.com (760)466-1245.**

# Meet the Data Net Security Specialists

**Data Net is an engineering focused company employing a highly qualified and experienced group of talent spanning all US time zones. Their decades of experience gives them the unique ability to support any and all IT environments from on premise secure networks to cloud networks and most importantly the secure hybrid cloud environments that many companies are adopting. While this is not the entire company, listed below are the Security Specialists at Data Net.**

### Rob Slaughter

Former US Navy and civilian nuclear systems engineer and trainer. Rob is a lead engineer focused on managing enterprise integration projects. Rob is a network systems integrations expert across multiple platforms to include Microsoft, VMware, NetApp, Citrix, and more.

### Arnold Torres

Former US Navy IT Systems Engineer with a Master's degree in IT Project Management. Arnold focuses on managing all backups for Data Net clients. Arnold holds the following additional credentials: Comp TIA-ITF+ Certified; Comp TIA Security +; Computer Info System – Network Concentration; BS-Business Info Systems; VEEAM Certified Tech Sales Professional.

### Jay Puri

Jay brings many years of experience and a diverse skillset to the Data Net team. Jay holds the following credentials: Microsoft Azure Certified; Microsoft Certified System Engineer; Microsoft Certified System Administrator; Network + Certified Professional; Server + Certified Professional; Security + Certified Professional; A + Certified Professional; Project Management Certified/PMP

### Shane Chrisman

Shane has a BA in Business Administration with a focus in Information Systems. Shane is a senior network engineer focusing on Exchange and email systems, AWS and Azure cloud environments. Shane also manages the proactive maintenance program for all clients.

### Nicolas Smith

Former US Marine Corps systems engineer for C-130s. Nicolas is part of the security team focused on network and security scans, vulnerability scanning, analysis, and remediation. Nicolas is a Microsoft Certified Azure Cloud systems engineer.

### Matt Slaughter

Matt started working with Data Net in 2017 as Director of Sales and Marketing. Matt has spent 5 years leading Data Net's compliance and security efforts. Matt's extensive experience in guiding Data Net's DoD clients through the compliance and security journey has made him very well versed in CMMC and NIST 800-171 compliance frameworks as well as other frameworks.

### Michael Leeper

Chief Operations Officer (COO); Michael takes a very hands-on approach to planning, organizing, and coordinating the security and compliance efforts for Data Net and its clients. Michael is involved in the daily planning and management of all Data Net projects and Help Desk endeavors.

### Bill Vann

As business analyst for Data Net, Bill spends countless hours researching new technology solutions, compliance and security tools, market analysis, and local business affiliate relations.

### Mike Reyes

Mike was the very first employee of Data Net. Mike is a senior Help Desk engineer with a focus on implementation and maintenance of secure client network solutions. Mike is certified in Microsoft, VMware, Proofpoint, and WatchGuard.