A Sponsored Feature of the Orange County Business Journal • February 20, 2017

MARQUEE® Workforce Solutions

Cybersecurity – More Than Just a Statistic!

Cybersecurity is amongst the hottest topics today and a growing trend for 2017. In 2016 alone, approximately 454 data breaches took place, exposing nearly 12.7 million records. Given the recent notable controversies from organizations such as Yahoo, Verizon and Well Fargo, as well as the widely publicized Russian Hack (tied to the U.S. Presidential Election Campaign), it is safe to say that cybersecurity has become vital for every government and business entity.

What Are Cyber Attacks?
There are two types of cyber attacks that organizations need to be aware of: (1) An intentional attack targeted to harm a public profile, gain publicity or obtain significant data of value from their network and (2) An opportunistic attack, derived from automatically detected vulnerabilities which can be discovered in fundamentally any resource exposed to the Internet.

In many cases, those behind cyber attacks take advantage of any weakness they may come across. Therefore, all businesses should comprehend these threats and protect themselves against both physical and digital cyber attacks.

Cybersecurity Talent Shortage
Due to the exponential growth of the cybersecurity market, cybersecurity jobs are expected to reach 1.5 million openings by 2019 – 1 million of which are estimated to be unfilled. Given this rising issue, the search for cybersecurity talent will become a crucial challenge for employers within the next couple of years. As a result, many organizations need to tailor their recruitment approach to attract and retain qualified cybersecurity professionals. Some key components to look at would include:

▶ *Selling the job:* Cybersecurity professionals get constant recruitment calls. Don't simply focus on the job posting. Instead, focus on engaging your target audience through key components such as intriguing/unique type of work, innovative new tools and flexibility such as work at home opportunities.

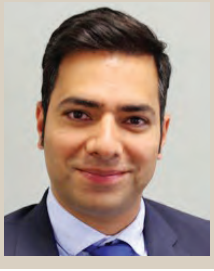
▶ *Social media use:* Blogs, tweets and posts allow organizations to enhance their company brand. Be sure to target cybersecurity communities via forums and discussion groups to spread awareness!

▶ *Stay flexible:* With the cybersecurity talent pool being so minimal, stay flexible on certain requirements such as degree requirements. Another tactic could be decreasing the years of experience required. Perhaps hiring a more junior candidate and highlighting opportunities for growth would be a tactic!

At Marquee, we make it easy for organizations to partner with us and provide our expert advice on cybersecurity trends and use of artificial intelligence to predict any threats. We provide the right resources for the right programs including software security engineers, IS security managers and Chief Information Security Officers (CISO).

Marquee Workforce Solutions is your local Technology Recruitment Solution Expert and a leading enterprise consulting and systems integration company. We offer flexible and effective engagement models and end-to end IT. Please visit us at www.marqueewfs.com for more information!

Parik Mattoo – VP Business Development & Marketing
Parik has over 12 years of experience in full cycle sales and business development. He holds an MBA in Marketing with a bachelor's degree in industrial engineering. Parik is also a certified leadership and management professional from UC Berkeley.



Emily Salanio – CEO
With over 15 years in the industry from recruitment, sales and operations, Emily strives to expand Marquee's IT division. Currently, as the CEO for Marquee Workforce Solutions, Emily stays active in streamlining processes and developing ongoing relationships with clients and candidates.

Accounting Software: What Every Small Business Should Know

by Susan Levinstein and Jay Wikum, Partners, HMWC CPAs & Business Advisors

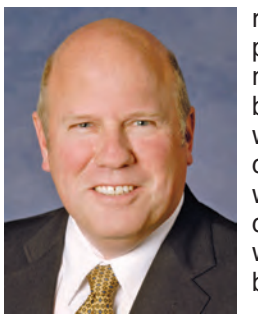
Selecting the best accounting software program for your company can be challenging. Here are some tips to consider:


Susan Levinstein

Industry impact on software selection: There are an array of small business payroll and accounting packages available, along with full-service business management programs and online applications. Some of the popular programs aren't suitable for everyone. Manufacturers will need strong software capabilities in inventory and work-in-process; hospitality companies may use a 52/53 week year; physicians need specialized billings, etc.; all of these require industry-specific software or adaptations. Regardless of which software you select, it is important to keep your versions current; the older they are, the less chance they will be supported, and if a problem arises it can virtually shut the business down.

Report generation: When management decides that new accounting software is needed, their decision is often due to their underlying frustration with reporting capabilities. The more involved and sophisticated senior management is with daily business issues, the more important ease of customization is for your specific needs. Your accounting software should help with sales forecasts, inventory control and developing budgets, among many other useful applications. You want it to help gain insights into your operations, to pinpoint problems and identify opportunities.

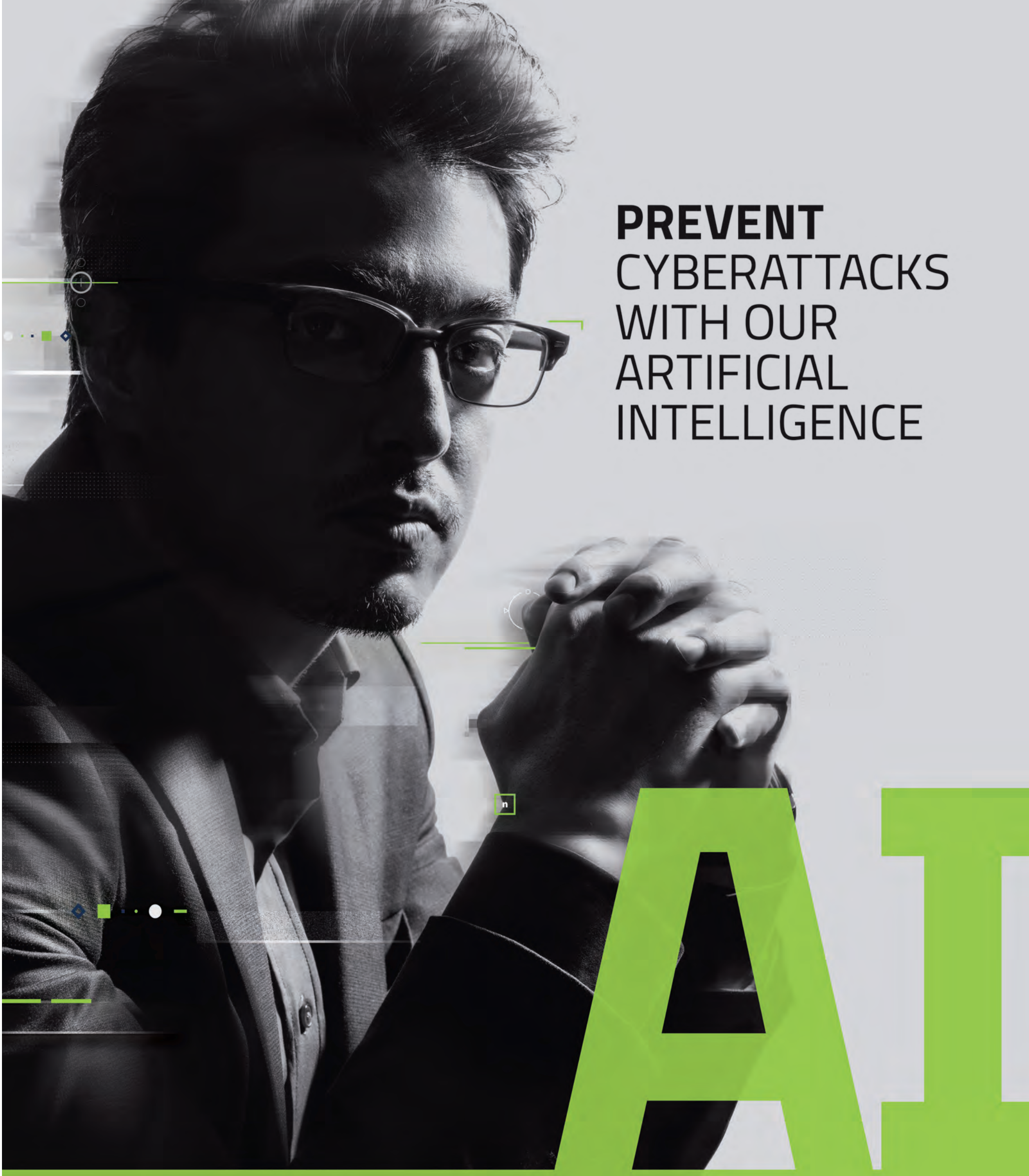
Who should help select and implement it? From the outset, it is wise to consult with your CPA, who can recommend software that has proven to be effective for similar companies and will serve your purposes. Some accounting firms will help you set up your software so that it gathers the data that they need to prepare meaningful financial statements, as well as complete tax returns. They can also help with customization and personnel training. At HMWC, we can be as involved as needed with day-to-day work, from oversight to full-cycle bookkeeping. Having your accountant involved is a surefire way to help make sure that accounting records are being completed, timely and accurately. Your CPA can also help with controls to avoid fraud. Your IT department or consulting firm should also be part of the process to help with any hardware issues, and to assure proper security and back-up procedures are in place.


Jay Wikum

Segregation of duties and proper training: Accounting is a field that requires education, training and experience. One solution is to have company personnel trained to do day-to-day data entry, which then are reviewed and overseen by an independent accounting professional. For those personnel, inside or outside, who will use the software, it is important to select software that is relatively easy to use and that requires minimal training.

Accessibility: If you will utilize your accounting firm with your day-to-day accounting needs, consider cloud options for ease of access. Cloud accounting software is the trend for mobility, especially for owners to have remote access, regular back-up, and to keep it current.

Susan Levinstein, CPA, and Jay Wikum, CPA, CMPE are partners at HMWC CPAs & Business Advisors in Tustin. Ph: 714.505.9000, www.hmwccpa.com.



Cybersecurity that predicts, prevents and protects. cylance.com

CYLANCE™

CYLANCE™

How to Secure Against the Rise of the Ransomware Economy

The state of cyberextortion and why artificial intelligence holds the key to prevention

The pervasiveness of ransomware has made big headlines recently, and it's a top cybersecurity concern in 2016 and beyond. Cybersecurity experts describe the proliferation of ransomware attacks in sweeping proportions, and the growing number of attacks reflect a critical threat to industries such as finance, retail, healthcare, the public sector, and more.

An opportunistic and profitable type of malware, ransomware is specifically designed to block access to data on an infected system until payment is received. Ransomware often uses a trojan to gain a foothold on a computer by targeting victims with a malicious payload disguised as a legitimate file. This digital form of extortion is motivated by financial gain and has been successful because it often costs less to pay the ransom than to restore lost data. Unfortunately, payment often leads to continued attacks.

Ransomware campaigns can be carried out by cybercriminals with little to no technical skills, or by organized crime syndicates with significantly more experience and funding. In the dark web, the unseen depth of the Internet where criminals operate, ransomware-as-a-service (RaaS) toolkits are marketed and sold, providing nearly anyone the ability to embark on a ransomware campaign. Cybercriminals not only make money through individual attacks, but they also offer their skills and services to provide ransomware to others for a fee.

Ten Things Organizations Need to Know About Ransomware

Ransomware may be damaging, but it can be prevented. Armed with the right intelligence and software, organizations can keep ransomware from holding their data hostage.

1. Ransomware was first reported in 1989
– Since then, a number of different variants have evolved
2. Ransomware doesn't discriminate when it comes to platforms and devices
– Any device that can connect to the Internet is at risk
3. Ransomware can be distributed through various channels:
– Spam email campaigns that contain malicious links or attachments
– Exploits in vulnerable software
– Internet traffic re-directs to malicious websites
– Malicious advertisements (known as 'malvertising')
– Social engineering (misleading users to break security protocols that introduce malware)
– Self-propagation (spreading from one infected computer to another)
– SMS messages
– Botnets
4. Ransomware often goes undetected
– Traditional antivirus lacks the ability to identify and remove second-generation malware
5. Organizations need to change from a reactive model to a preventative model
– Keep software up to date, including operating systems
– Avoid dangerous web locations
– Educate staff about phishing emails, infected banners, and social engineering
– Use artificial intelligence and machine learning cybersecurity tools
6. Organizations should develop a prevention and response plan
– Prepare in advance of an attack
– Find and address vulnerabilities
– Review and test your plan
7. Organizations should identify a prevention and response team
– Choose an appropriate service level agreement
– Ensure the team possesses specialized expertise
– Vet and validate the team's expertise
8. Organizations should perform a compromise assessment
– Detect current and previously compromised systems
– Collect evidence and analyze adversary tactics
– Remediate across the enterprise
9. Organizations should complete a security tools assessment
– Evaluate existing security tools
– Execute a gap analysis
– Remediate findings and outline opportunities for improvement
10. Organizations should respond and future-proof
– Contain discovered incidents immediately
– Perform complete remediation activities
– Carry out sustainable prevention

The Good News

A transformational cybersecurity approach today is changing the industry landscape and provides good news for combating ransomware. The application of artificial intelligence and machine learning provides a new level of malware and ransomware security with prevention rates as high as 99.4%.

Only Cylance® offers a pathway to prevention using its award-winning product, CylancePROTECT®, and Cylance Consulting Services, which identify, remediate, prevent, and monitor ransomware as well as other cyberthreats. Cylance's AI, coupled with its expertise, brings cybersecurity to a state of provable prevention.

To learn more about how Cylance can help you remediate, or prevent ransomware, visit www.cylance.com/ransomware.