Cisco appoints David Meads Vice President for Middle East, Africa

DUBAI: Cisco yesterday announced the appointment of David Meads as Vice President for its Middle East and Africa operations. In the current era of digital disruption, Meads, in this newly created role, will oversee the execution of Cisco's strategy in these two regions, ensuring the technology leader maintains its momentum at the forefront of digital transformation efforts. As digital adoption gathers pace in the Middle East and Africa, the new geographical setup under Meads will allow for greater synergies, relevancy and sharing of best practices across the two regions.

"David Meads' appointment to lead Cisco's business in the Middle East and Africa comes at a time of tremendous potential for the region to reap the benefits of digital transformation, supported by the prioritization of digitization in both government and business agendas," said Edwin Paalvast, President, Cisco EMEAR. With more than 30 years' experience in the IT industry, Meads joined Cisco in 1996 and was most recently Cisco's Vice President for Africa, where he was responsible for partnering with organizations across the continent to help them implement strategies to unlock the full potential of the digital era.

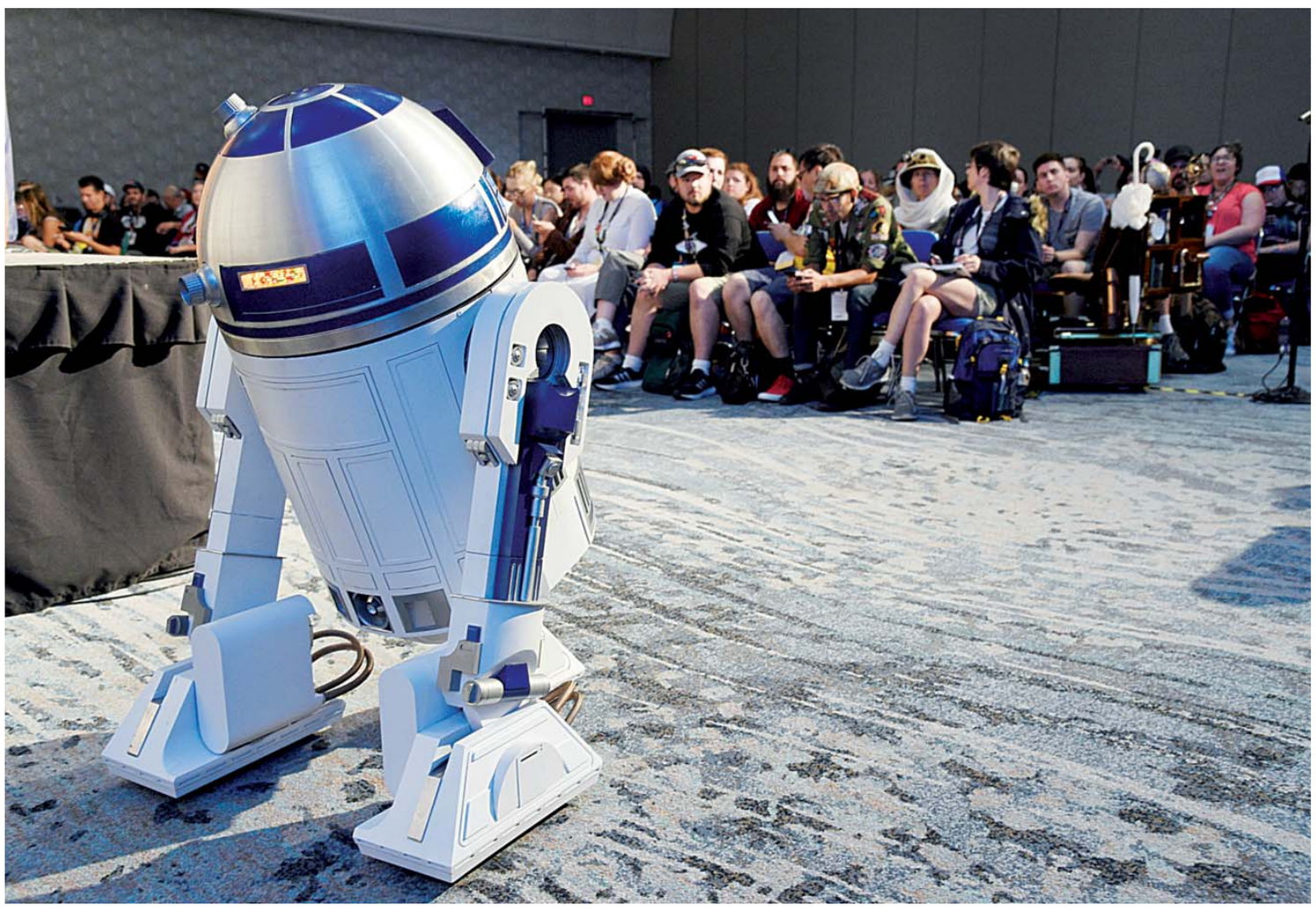
Over the years he has developed a reputation as a trusted advisor to enterprises and governments, partnering with them to deliver competitive advantages and efficiencies gained by adopting digital technologies. Meads will

David Meads

be based in Dubai, Cisco's hub for the Middle East. "As we deepen the commitment to the region, we're excited to have someone of David's caliber at the helm to spearhead our strategy and support customers along their digitization journey. One of David's priorities will be helping Cisco's customers and partners create value in a highly connected, digital world, while enabling greater responsiveness to emerging market and customer needs," concluded Paalvast.

Cisco has longstanding government partnerships across the Middle East and Africa, including a Country Digitization Acceleration (CDA) program with Saudi Arabia, with several other similar programs in the pipeline. In addition, Cisco is working closely with relevant government entities in the region on multiple initiatives that support IT skills training and education, as well as the development of entrepreneurship, business and innovation ecosystems. "I look forward to taking on the additional responsibility of a fast-evolving, dynamic region and to working with the phenomenal team we have in place," said David Meads, Vice President, Cisco Middle East and Africa.

He added, "Combined, the Middle East and Africa region has the world's youngest demographic and presents a significant market opportunity, where new business models and innovative technology adoption are addressing unique market needs. Cisco's expansive portfolio allows us to partner with our customers and support their digital journey." A veteran business leader, David Meads has rich sales leadership and general management credentials. He has held various leadership positions within Cisco, including a three year stint as Managing Director for South Africa, based in Johannesburg. During this time, he achieved exceptional levels of employee engagement within the organization and helped the country develop its e-skills initiative, aimed at harnessing the power of technology for inclusive socio-economic development.



CALIFORNIA: Star Wars robot character R2-D2 stands in front of the audience at the Princess Leia Star Wars Fan Club Tribute Presentation during the 2017 Comic-Con International in San Diego, California. —AP

Cybersecurity starts with training your employees

By Mohammed Basheer,
IT Security Practice Head,
ISYX Technologies

The Petya ransomware attack that hit computers around the world recently, the second in two months, is yet another reminder that computers play key roles in most enterprises, and that it does not take much to disable those computers. Irrespective of how robust your information security systems are, users are still the weakest link in your company's cybersecurity.

Mohammed Basheer

It's a business cliche that staff is a company's greatest asset and potentially its greatest risk. And while that has always been true in the area of customer relations, it's now equally applicable to data security. Users are the first line of defense against cyberattack, and also - potentially - a business's most glaring vulnerability. People are just a very large attack surface but organizations can reduce the attack surfaces by implementing an effective organization wide security awareness program.

Untrained employees are the linchpins for most data breaches. Those who attack businesses have no wish to spend a lot of time and money defeating its technology. Instead they would prefer to infect the user with ransomware, their favorite bait - "spray & pray" phishing attacks, which involves spamming with email that carries malicious content.

It has become increasingly important to embed ICT security awareness at all levels of an organization. While awareness is the key, there also needs to be a balance struck. Employees need to know the risk their online activities pose and how to manage it, without being rendered unproductive by overly complex procedures.

Computer security training isn't just a matter of giving employees information. Knowing best practices and organization policy is important, but it helps only if employees understand that they make a difference and should feel they are part of the organizations information security. The truth is that user ignorance to security make most malware attacks possible, and that employees who are aware can avoid most of the attacks.

Information Security Awareness should be part of an organization culture, business leaders need to make sure their awareness programs cover all the important aspects of cybersecurity which ensure that their employees are well trained to tackle the current security threats. At the end of an education and awareness initiative, all users should be able to understand:

How to identify security threats?

The user should be able to identify the difference between normal emails and malicious email. They should understand best practice in internet usage and understand the organizations security policies.

Response to the security incidents

The user must be aware of the security incident response procedure. Should they suspect a security incident in progress, they should be able to follow the security incident management procedure to curtail the incident from spreading across the organization. As they say people are the weakest link in the information security chain, hence employee involvement is crucial for the success of an organization's security strategy.

There is often a disconnect between what employees know they should do security-wise and what they actually do in practice. Organizations which continue to implement and reinforce effective awareness programs, have seen reduced number of security incidents, in turn maintaining better uptimes for the IT environment supporting the business processes, helping the organizations to upkeep their reputation resulting in better financial rewards.

At hacker summit, a new focus on preventing brazen attacks

LAS VEGAS: Against a backdrop of cyberattacks that amount to full-fledged sabotage, Facebook chief security officer Alex Stamos brought a sobering message to the hackers and security experts assembled at the Black Hat conference in Las Vegas. In effect, he said, it's time to grow up. Too many security researchers, he suggested, are focused on "really sexy, difficult problems" that don't address the common vulnerabilities that allow malware attacks to wreak havoc.

And too many security-minded hackers seem intent on demonstrating newly discovered hacks, such as making an ATM spit out cash or taking remote control of an internet-controlled car, rather than shoring up more mundane defenses. While part of that reflects the healthy intellectual curiosity of hackers, it's also driven by marketing and economic incentives, Stamos said. "I appreciate the showmanship, but we need a little more thoughtfulness, a little less showmanship in our field," he told reporters after his speech.

Global attacks, serious damage

Since May, the world has been rocked by two major international cyberattacks - the ransomware WannaCry and a likely state-sponsored attack called NotPetya that spread out of Ukraine. Those and other recent digital assaults have paralyzed hospitals, disrupted commerce, caused blackouts and interfered with national elections. Stamos himself was formerly the chief security officer at Yahoo, which last year disclosed breaches of more than a billion user accounts that dated back to 2013 and 2014.

Black Hat, now in its 20th year, has matured since what Stamos, a longtime attendee of the computer security conference, described as its "edgy and transgressive" early days. It has grown more professional and corporate over time. Stamos called for a culture change among hackers and more emphasis on defense - and basic digital hygiene - over the thrilling hunt for undiscovered vulnerabilities. And he called for diversifying an industry that skews white and male, and generally showing more empathy for the people whom security professionals are tasked to protect.

"It's unfair for us to say that users should be better," said Stamos, challenging his profession to find better ways to help people solve the most common vulnerabilities, such as reuse of passwords , email phishing attempts, and not updating devices to patch bugs. —AP

30 days after WannaCry, what can the Kuwaiti financial services sector learn?

By Charles Habak and Wayne Loveless

Charles Habak, Vice President at Booz Allen Hamilton MENA

Wayne Loveless, Principal at Booz Allen Hamilton MENA

WannaCry or Wcry represents the latest version of a growing threat called Ransomware - a tailored piece of malware designed to exploit specific vulnerabilities in the operating systems of its victims' computers. Malware outbreaks are not infrequent, but Wcry spread so rapidly that it revealed vulnerabilities in the business planning, employee preparation and internal procedures of organizations all over the world. A majority of affected systems were running outdated versions of software, with no access to updates because the vendor had phased out support to these legacy systems.

The financial services industry sector is no stranger to the phenomenon of outdated software. Many of today's financial systems still run on UNIX based platforms developed in the 1980s and 1990s, which often are no longer supported by vendors. What the financial sector can learn from the Wcry fallout is the importance of investing in a sound risk management framework that involves technology change management as well as updated software - all of which could have prevented Wcry.

Investing in a sound backup and continuity plan can also enable organizations to quickly rebuild and recover systems in the event of a cyber-attack or ransomware impact and eliminate any need to pay ransom. Most law enforcement agencies and cyber experts would caution against paying the ransom as it may open the victims up to further exploitation and potential identify theft.

Financial services organizations and their leadership have a duty to protect their customers' financial interests as well as their own institutions. This begins with a dedicated cyber agenda at the Board level along with the formation of a cybersecurity action committee reporting directly to the CEO. Bank-wide vulnerability assessments across all of the business units that are C-level driven and business-aligned should be prioritized.

Additionally, a dedicated cyber security business unit should be formulated with the goal of assessing and implementing new types of capabilities, processes and functions to combat growing threats. Finally, encouraging bilateral and multilateral communication mechanisms with other banks in the marketplace, and interfacing with regulators to inform of threats and share information of potential breaches as well as threat intelligence from local, regional, and international partners can provide the contextual understanding needed to proactively defend institutions from future threats.

WannaCrypt Ransomware: An action plan to improve your cyber resilience defences

By Steven Malone,
Director of Security
Product Management at Mimecast

The global reach and considerable impact of the WannaCrypt (WannaCry/Wcry) ransomware is a wake-up call for organizations and governments around the world. This on-going cyber threat will continue to adapt to take advantage of weaknesses in IT systems and procedures. New variants of this malware may cause even more damage if you do not act immediately. At Mimecast our first priority is to help protect our customers against the latest threats. Our services help protect email which has traditionally been the primary attack route for ransomware.

Steven Malone

Early samples have revealed that the ransomware is spread over local networks and the internet by abusing Server Message Block (SMB) protocol weaknesses. Although no Wcry 'smoking gun' infection emails have yet been found, it is highly likely that future variants will use email. This short guide is designed to help all organizations complete a review of network security, backup and business continuity systems and processes. We are also providing additional insights into how to make easy and quick configuration changes to ensure your Targeted Threat Protection solution is optimized. As many of you already know, a comprehensive "defense in depth" strategy is the best approach to mitigation of current and future variants of Wcry and other ransomware.

Patching

Every organization must ensure its IT systems are regularly updated. Microsoft security updates are released on the second Tuesday of each month (Patch Tuesday). Microsoft released a security update back in March which addresses the vulnerability that Wcry is exploiting. For those organizations who have not yet applied the security update, you should immediately deploy Microsoft Security Bulletin MS17-010. If you are using a legacy, now unsupported version of Windows, you should consider upgrading immediately. However, if this is impossible in the short term, Microsoft has taken the unusual measure of releasing a security patch that can buy you time to upgrade. Microsoft has provided its own detailed guidance to defend against Wcry here.

Network hardening

Good security practice dictates removing or disabling unnecessary services to reduce the potential attack surface. WannaCry has spread quickly by abusing vulnerabilities in Server Message Block network protocol. Unless you have a very good reason not to, disable the SMBv1 protocol on your network, while also ensuring SMB cannot be directly accessed from the internet. Disable or block other legacy protocols on your network that you are not using.

For customers of Mimecast Targeted Threat Protection, we advise a number of activities:

URL Protect - configure a policy in line with our best practice guide in Mimecaster Central. Ensure a policy is applied to all users. Rewriting all URLs to scan for unsafe content at time-of-click is the best approach to preventing inbound URL-based phishing.

Attachment Protect - configure the "Safe Files" option for all users to ensure inbound Microsoft Office files are converted to a safe and benign format. For users who require editable documents, ensure Attachment Protect's sandboxing is configured. Refer to the best practice guide in Mimecaster Central for details.

Internal Email Protect - this service provides protection for URLs and attachments in both outbound email and also mails sent internally. Ensure policies are applied to all users and ensure remediation capabilities are enabled. Refer to our best practice guide for configuration recommendations.

Mimecast customers using Mimecast's secure email gateway, we advise using the most up to date attachment management definition as there are reports of executable files masquerading as Excel files with an administrator hold on dangerous files types. This in conjunction with the Suspected Malware policy with the ability to hold Office files containing macros provides another layer of detection, but does not provide the analysis provided by Attachment Protect. Mimecast's ARMed SMTP (Advanced Reputation Management) combines malware, reputation and anti-spam checks to reject unwanted email.

Since a very high percentage of ransomware is spread by email attachments, we urge organizations to consider using sandboxing and/or safe file conversion services. DNS authentication capabilities such as DKIM and SPF can help stop attackers from spoofing or hijacking the email domains of trusted senders, thus effectively taking away one method attackers use to fool their intended victims. DMARC, the combination of these two services adds an extra layer of defense. To learn more about Mimecast's DMARC implementation and DNS Authentication policies please check out this document in Mimecaster Central community.

Data backups and business continuity

Preventive measures alone can't keep up with the fast-evolving nature of ransomware attacks and as this attack highlights, there are many ways for an infection to enter an organization. It's vital you regularly backup critical data and ensure that ransomware cannot spread to backup files. Ransomware can take time to encrypt large volumes of files, particularly across a network share. It is imperative to ensure your back-up window is long enough to go back before any infection begins. Backup and recovery measures only work after an attack, and cost organizations in downtime and IT resources dealing with the attack and aftermath. Organizations must be able to continue to operate during the infection period and recover quickly once the infection has been removed.

Should firms ever pay a ransom?

We advise organizations never to succumb to the pressure to pay the ransom to regain access to their applications and data. There is no guarantee this will unlock files and further motivates and finances attackers to expand their ransomware campaigns. This notification provides external links as a convenience to our users. This does not constitute endorsement by Mimecast of any linked websites, or the information, products or services contained therein. Mimecast does not exercise any editorial control over the information you may find at these websites. Mimecast does not take responsibility for pages maintained by external providers.