IDG CONNECT

15-MINUTE READ

Lattes, lunch, and VPNs: securing remote workers the right way

How changing work habits are reshaping security policy

A Management Briefing by IDG Connect in association with Malwarebytes

Contents

"Remote working habits, in combination with the need to enable collaboration across dispersed teams inevitably involves multiple digital tools and mobile devices, which in turn raise serious security concerns. However, a well thought-out, detailed plan provides both productivity and security."

Malwarebytes

Introduction

It will come as no surprise that, despite a constant pendulum swing in workplace trends, remote work is still booming. With climbing real estate prices in high-opportunity cities and clogged freeways from workers taking on long commutes, remote work is a trend that will only continue. Yet with that workplace flexibility comes security challenges.

"...the average number of cybersecurity incidents involving employee or contractor negligence has increased by 26 percent and by 53 percent for criminal and malicious insider incidents."

Even without remote work, cybersecurity is a growing problem for organisations. According to the Ponemon Institute, since 2016, the average number of cybersecurity incidents involving employee or contractor negligence has increased by 26 percent and by 53 percent for criminal and malicious insider incidents. Remote work has had a major impact. As a Secure Computing comment suggests, Wi-Fi is a big culprit of security breaches. Worryingly, further research reveals 77 percent of businesses do not have a cybersecurity incident response plan applied consistently across the organisation to cope with breaches.

Google recently outlined the challenges facing IT leaders who need to secure remote workers in an internal report, Working together when we're not together. Remote working habits, in combination with the need to enable collaboration across dispersed teams, demand a well thought-out, detailed plan. That plan inevitably involves multiple digital tools and mobile devices, which in turn raise serious security concerns.

The modern endpoint and changing security perimeter of organisations are mirroring this evolution in working habits. While the dangers of free Wi-Fi are well documented, the proliferation of devices, apps, and tools with remote access to networks broaden the risk.

Understanding how people want to work in the future goes a long way toward forging a security strategy. However, organisations cannot simply bolt on a remote plan because that can leave gaping holes in corporate networks.

Traditional cybersecurity measures are not keeping pace with change. As research from SANS institute found, traditional antivirus protection is failing, with only 47 percent of initial cyberattack vectors detected by antivirus tools.

Organisations need to see the modern endpoint problem with fresh eyes, redrawing the security landscape to forge an enterprise ecosystem that enables the modern worker without compromising the network.

Next:
When remote work goes wrong: a short story

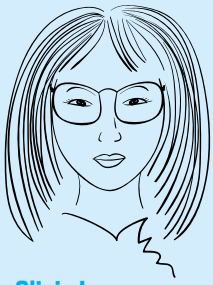
On many occasions, organisations learn this lesson the hard way. Take the case of Luciana and Olivia.

When remote work goes wrong: a short story

The characters

Luciana Gomez

Luciana is a 32-year-old manager for a midsized marketing firm. She splits her time between working onsite and remotely, and often uses public networks. She uses a company PC, as well as her personal Android phone for work, on which she has downloaded a multitude of apps. Luciana travels for work twice every quarter.



Olivia Lu

Olivia is 44 years old and the new director of IT at the same company as her friend Luciana, who referred her to the role. She works onsite, has a team of eight (six IT generalists, two security IT staff), and takes a holistic approach to security. She has been evaluating the threat landscape and IT ecosystem, and recognises that the modern security perimeter has dissolved. In her opinion, the modern endpoint should mirror the modern employee, like Luciana.

A local café

Luciana sat at a corner table at a local café, waiting for her old friend, Olivia. When she finally arrived from a nearby office building they quickly launched into shop talk.

"I want to hear all about the new job," smiled Luciana as she closed her laptop, having finished going over billing statements.

"Honestly? It's a bit of a nightmare."

"The set-up, the environment—It's an accident waiting to happen. Traditional antivirus, freeware everywhere, a firewall, and some random digital transformation projects under way, like BYOD and cloud migration. There's no clear strategy. "

Olivia outlined how the company's current practices increased IT staff workload and decreased visibility of emerging threats that could potentially result in a breach. Olivia was responsible for improving organisational resilience, but felt it was all out of control.

Luciana remembered she hadn't forwarded an invoice from the ad agency to accounts.

"I'm really sorry, Olivia. It's urgent, do you mind?" Luciana didn't wait for an answer. She opened her laptop and logged into the café Wi-Fi, not noticing Olivia's look of concern. Luciana then clicked on the invoice and let out a gasp as her files were immediately encrypted and a ransom demand popped up.

"Oh my God, were you on the company network? We need to tell them right now," Olivia had already pulled her phone from her pocket.

"No...I copied the files I needed to my laptop."

"Really? Is that normal?"

"Everyone does it," replied Luciana, nodding in the direction of other tables where company staff were working on laptops and talking on phones.

Olivia sprang into action. She'd seen enough.

"Close it down and bring it in," she said, while standing up. "Time to make some changes."

Next:
Back at the office

Back at the office

Olivia dashed into the IT department.

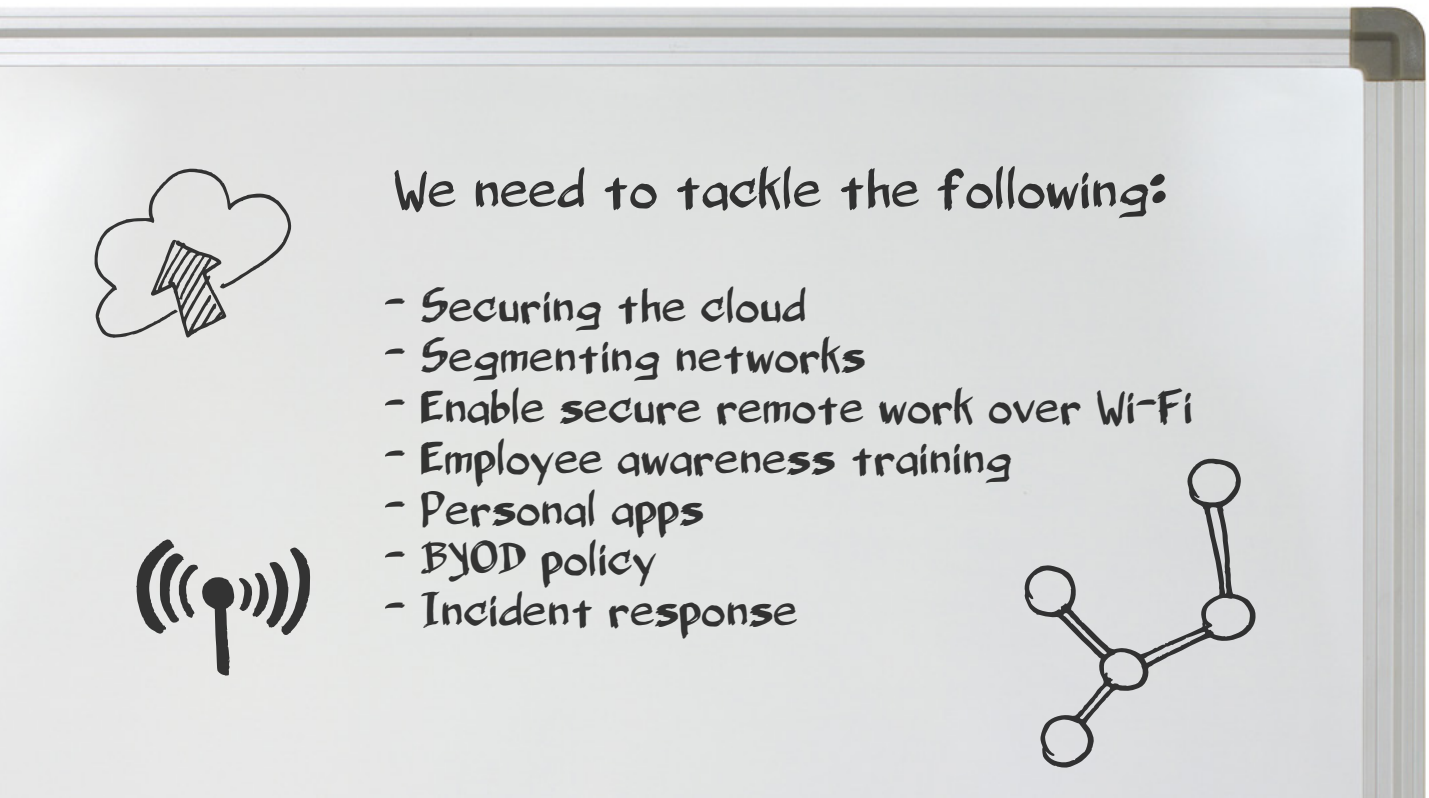
She headed straight to meeting room and gestured to the team to come in.

"Listen, the way we've been doing things around here—it's not sustainable. I was just at coffee with a coworker who was viewing financial data on an unsecured network, as is common practice here, and she was hit with a ransomware attack."

Audible gasps echoed throughout the room as Olivia continued. Proactive anti-ransomware protection could have stopped this, but that data is lost now. If we put our heads down and commit to change, we can turn this around."

Next:
Securing the cloud

"At a high level, here are the top areas of concern we need to address," she stated while jotting down a few terms on the board. "Let's take a look at each of these one-at-a-time and discuss what needs to change—starting with the cloud."



Securing the cloud

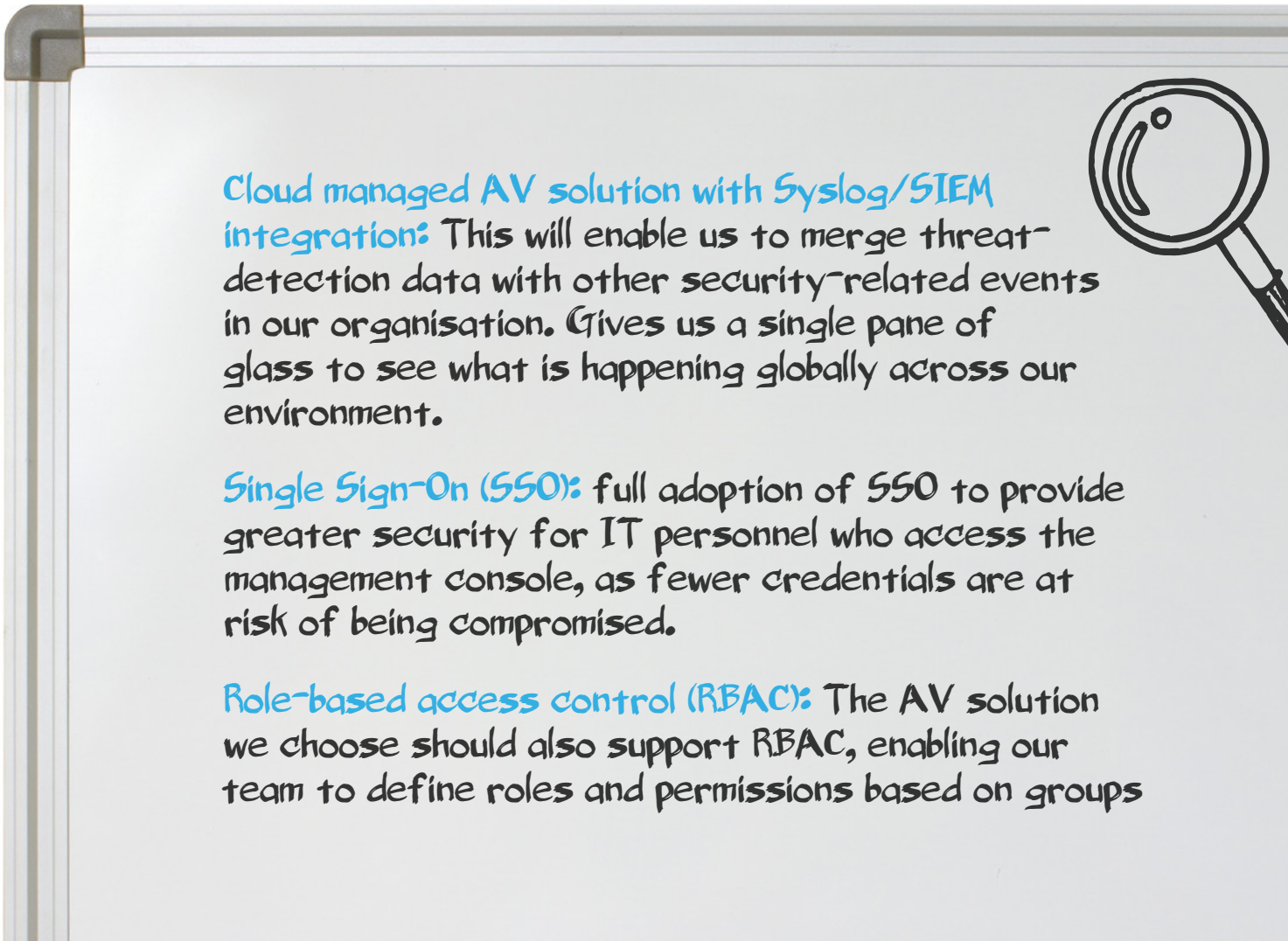
"When it comes to storing and sharing data on the cloud, we need to talk about access," Olivia began. "Right now, everyone has free reign to access and share whatever they like, and our data is wide open to the internet. Total payday for cybercriminals."

Jose, a longtime IT technician, piped up. "What about implementing role-based access control?"

"We could restrict access to the most sensitive information to a limited number of employees on an as-needed basis—oh, and definitely include two-factor authentication," Sharon, a more recent hire, added.

"Good!" smiled Olivia as she scribbled on the board. "I also think we need a logging and alerting system to simplify and prioritise our response to security events." The team murmured in agreement, netting out the following action items:

Next:
Create separate networks



> 82 percent of cloud users have experienced security events due to confusion over Shared Responsibility Security Models, according to the Oracle and KPMG report.

Create separate networks

"We should segment the network, too," said Olivia. "Agreed?"

They all nodded.

"We can segment both for cloud and on-prem, and monitor continuously for traffic or data-flow anomalies to head off any trouble," said Jose.

"Yes, good," said Olivia, "and make sure we protect our critical assets." She took her marker and wrote three separate networks on the board:

- Corporate-owned assets network
- Critical infrastructure network
- Guest access network

Next:
Enable secure remote working

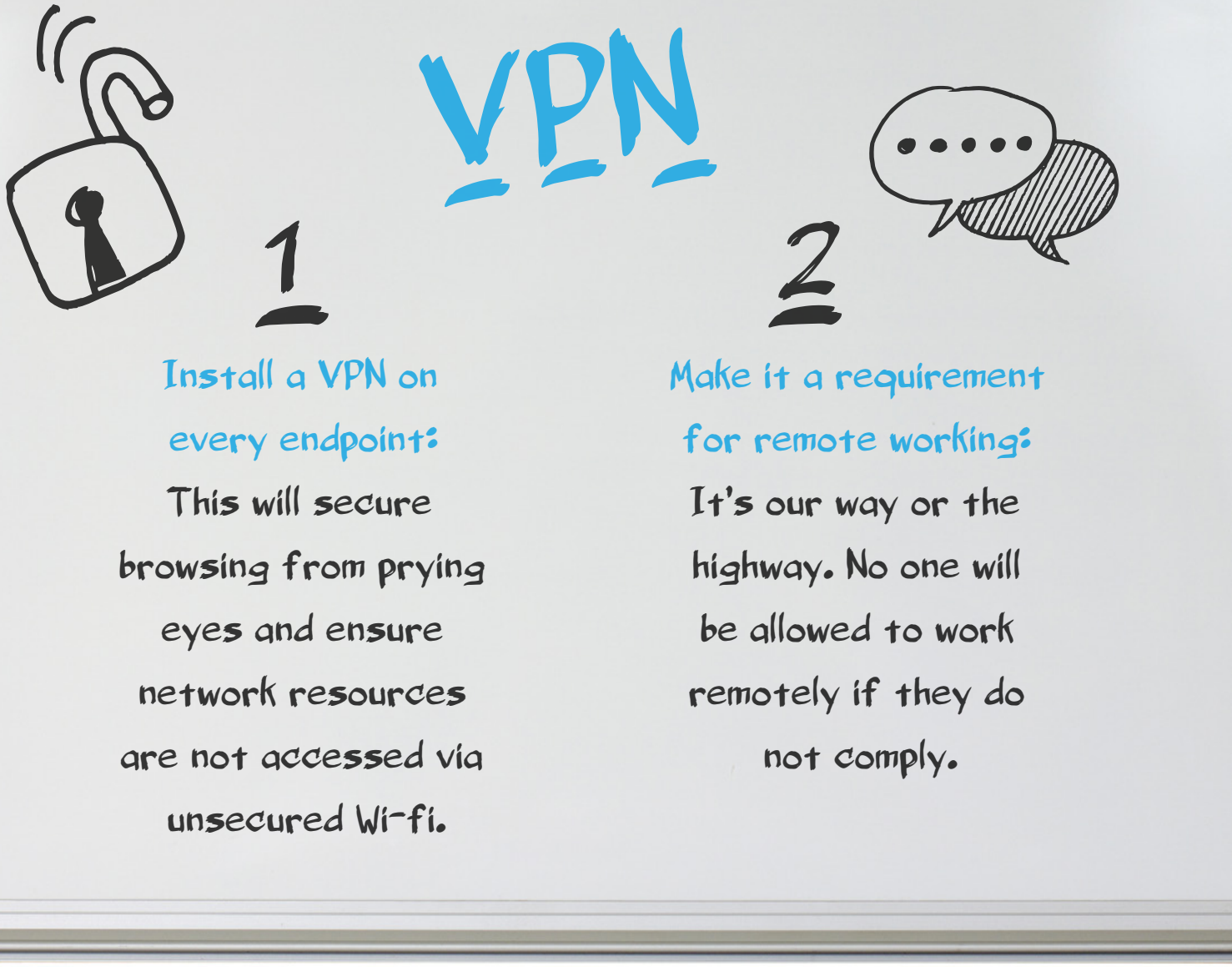
Enable secure remote working

"Okay, so how do we make sure everyone can access the network securely, whether that's at the café, a shopping mall, hotel, or airport?" asked Olivia. "Because no one should be transferring company data over unsecured public Wi-Fi. Period."

"A VPN," said Sharon.

"Yes, a VPN," replied Olivia. "Simple, isn't it?"

Next: Security awareness training



> According to Real Business, 86-year-old Alec Daniels had very little knowledge of computers prior to hacking a public Wi-Fi hotspot in 16 minutes.

Security awareness training

"We need to implement security awareness and training for all employees, especially those handling sensitive data," said Olivia. "Any ideas?"

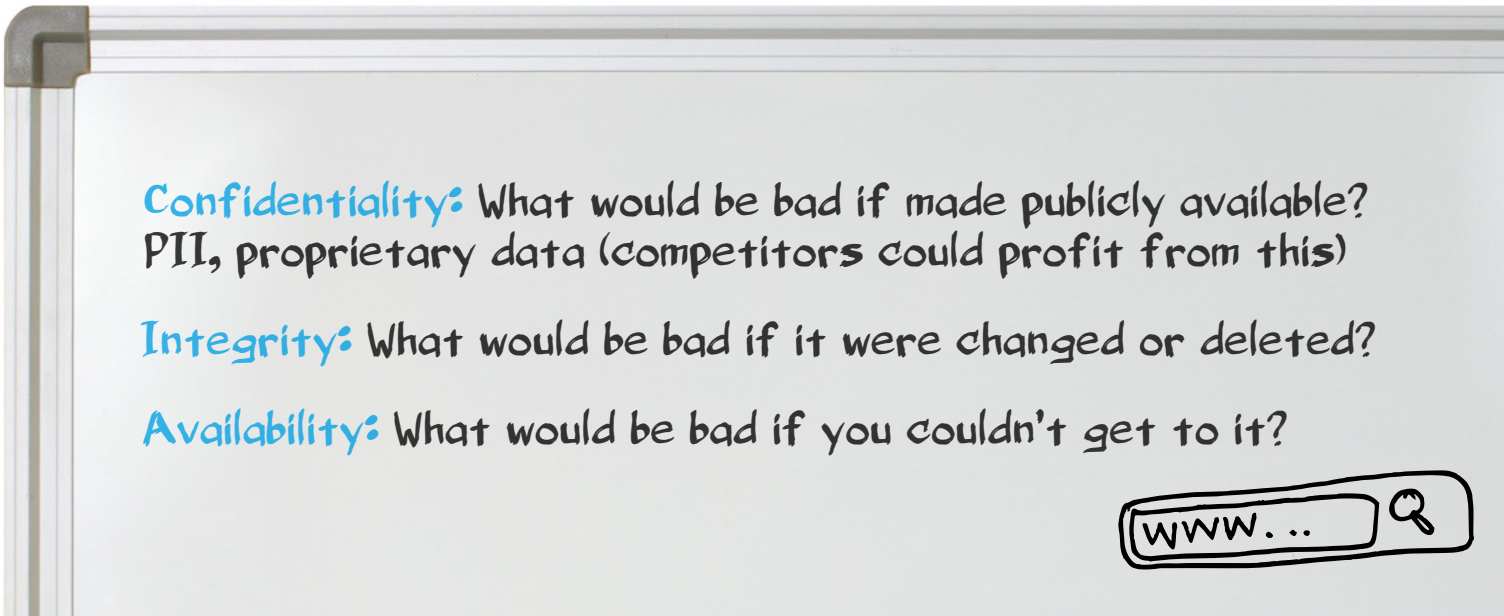
"We could push educational videos internally, implement phishing tests. New hire training on all software, platforms, and devices would result in fewer mistakes," said Chris, one of Olivia's security staff members.

"That works for most company data, but what about our sensitive TK data?" Jose retorted. "What about a data classification and handling policy? We could set ground rules for what is critical and what is not sensitive."

"And give additional specialised training to employees."

"Good," replied Olivia, writing three considerations that should be aligned with the internal training on the board:

Next: Personal apps



Personal apps

"We need to educate on approved apps," said Olivia. "What is secure? If it's free, you are the product."

The team laughed.

"Okay okay, let's create some rules."

Next:
BYOD Policy

The Rules

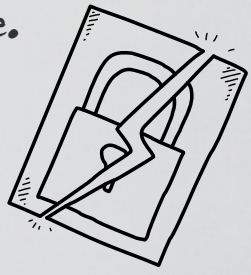
All machines should be encrypted: Create a barrier to entry for anyone who gets unauthorised access to a corporate machine. This includes BYOD.

MDM: Mobile device management, or AV on a phone; cost can be a factor. Standardise antivirus/anti-malware for corporate machines and BYOD.

Basic phishing protection: Mobile AV should have this capability on the web and warn/notify the customer if they are on a malicious site.

Mobile devices need an AV: AV needs to scan apps on devices and memory cards if in place. It should have the functionality to delete any apps that are known as malicious, as well as Potentially Unwanted Programs (PUPs) and Potentially Unwanted Modifications (PUMs).

Anti-ransomware protection: Necessary to stop screen lock or file encryption, with the ability to remediate.



More than 200 apps were found to be exposing sensitive consumer information, with close to 60 percent of the leaks coming from news, sports, and shopping apps, according to the 2017 Mobile Leak Report.

BYOD policy

"We must create and socialise a policy. This is absolutely essential," said Olivia. "But what are the device requirements?"

She nodded at Sharon who took the pen and wrote the following on the board:

- Encryption
- Passcode
- Find my phone
- No jailbreaking
- Approved device list

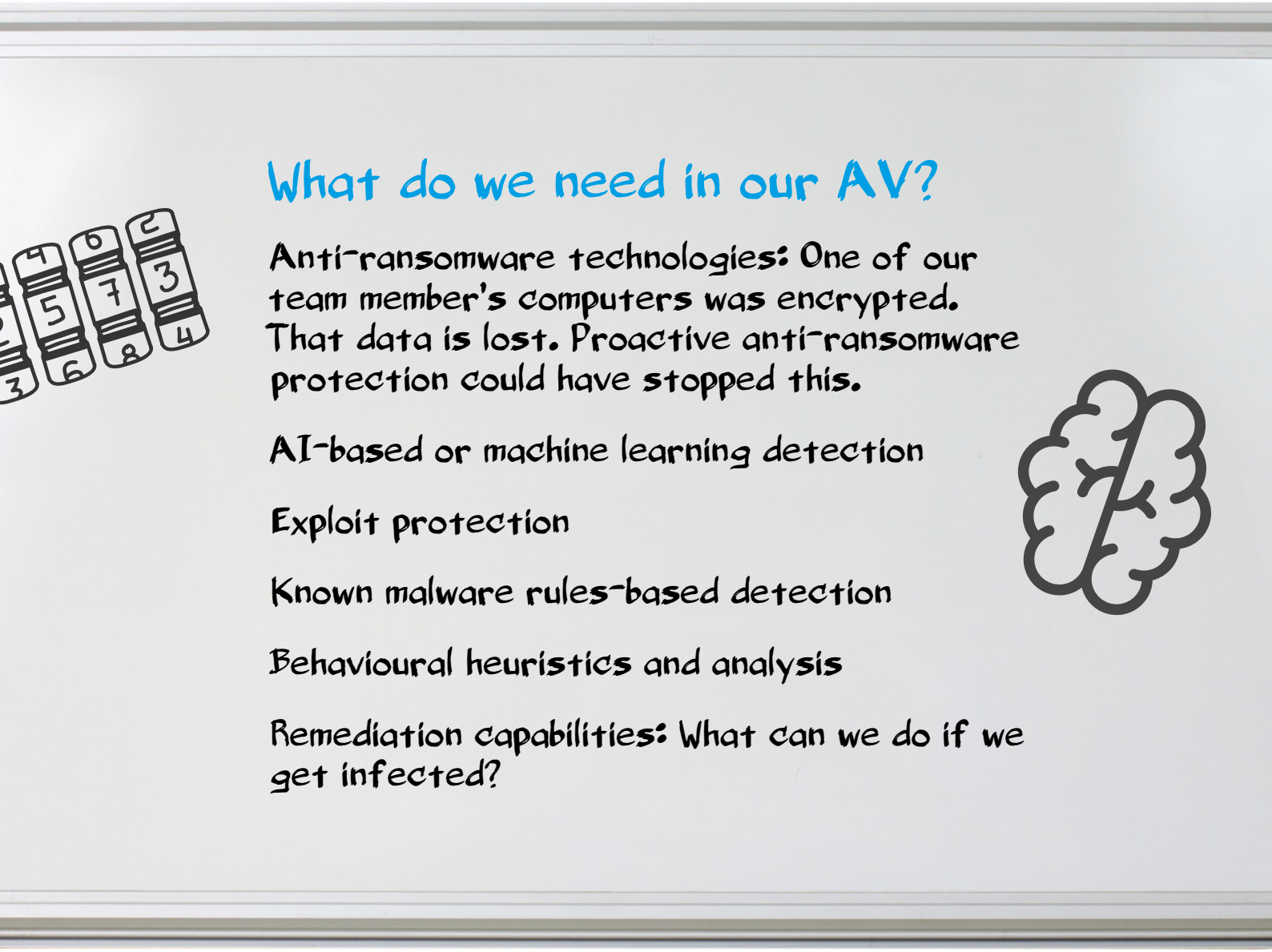
Next: Proactive protection

A BYOD infographic shows 36 percent of firms have at least half of employees on BYOD.

Proactive protection

"We need an AV solution via a cloud-based management console," said Olivia. "So, what do we need in our AV?"

This time, Olivia nodded at Jose, who took his turn at the board:



Next:
Incident response process

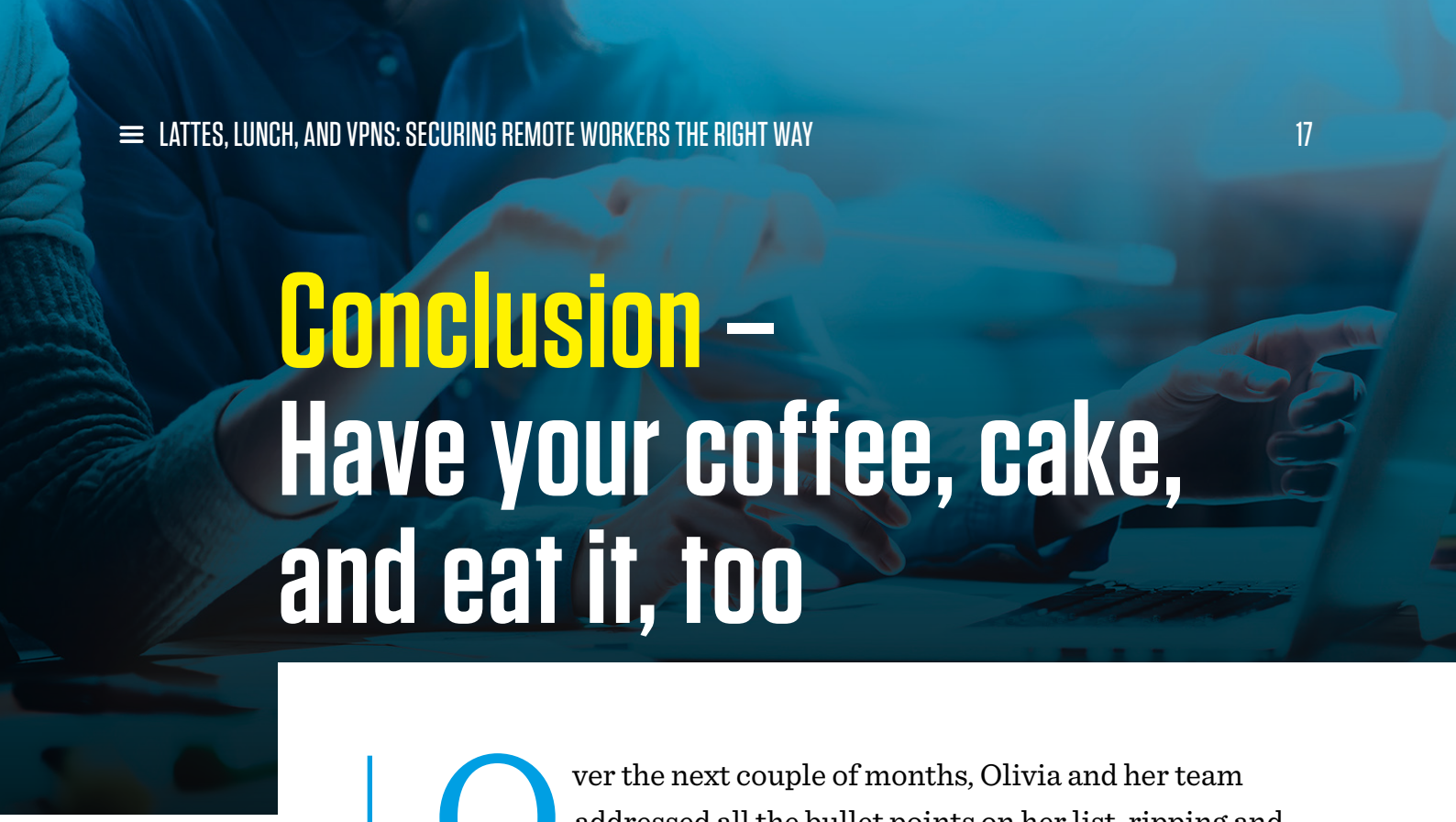
"We need all of these technologies to support workstations and servers to ensure coverage for critical infrastructure without causing a performance impact for our end users," Olivia reiterated.

Incident response process

"So, the big question," said Olivia looking around at the team. "What do we do if it all goes wrong and we get breached? It happens, even with all these great plans put into action. Remember there's no such thing as a 100 percent secure network. So what do we do?"

She started writing on the board.

Next:
Conclusion



Conclusion – Have your coffee, cake, and eat it, too

Over the next couple of months, Olivia and her team addressed all the bullet points on her list, ripping and replacing old techniques that weren't working with new solutions that were more in tune with the modern endpoint and worker. After her and her team's diligent work, the company was impacted by fewer attacks, and those that did get by the initial perimeter were squashed with swift remediation. Productivity and morale were up—and working in coffee shops is safe and permited.

Olivia achieved superhero status, securing the company's data and devices while empowering the modern endpoint and workers, such as Luciana.

"We've now got an ecosystem that can cope with remote work and a proliferation of different devices and guests on the network"

'We've now got an ecosystem that can cope with remote work and a proliferation of different devices and guests on the network," Olivia said, while sipping an almond milk latte back at the café with Luciana.

Olivia handed Luciana back her original laptop, who had been using a loaner during the IT team's transformation.

"Cleaned up and good as new," she said. "We've also taken the liberty of installing a VPN. You've got secure access to the network, so no need to copy files or use the coffee shop Wi-Fi."

> When considering whether to connect to the public Wi-Fi network at your local coffee shop, the airport, etc., I have two simple words of advice—don't and DON'T." – CSOOnline

Luciana smiled and drank her cappuccino, adding, "I noticed in your email to the company that we've just completed phase one of cleaning up our IT and security practices...so what is phase two?"

"Fine tuning and creating an ecosystem that functions as a cohesive unit, with automation and optimisation," replied Olivia with a triumphant grin. "But that's a whole other story."

For more information, visit: www.malwarebytes.com/business

About Malwarebytes

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs.
Learn more at: www.malwarebytes.com/business

Copyright © 2019, Malwarebytes. All rights reserved. Malwarebytes and the Malwarebytes logo are trademarks of Malwarebytes. Other marks and brands may be claimed as the property of others. All descriptions and specifications herein are subject to change without notice and are provided without warranty of any kind.

IDG Connect is the demand generation division of International Data Group (IDG), the world's largest technology media company. Established in 2006, it utilises access to 44 million business decision makers' details to unite technology marketers with relevant targets from any country in the world. Committed to engaging a disparate global IT audience with truly localised messaging, IDG Connect also publishes market specific thought leadership papers on behalf of its clients, and produces research for B2B marketers worldwide. For more information visit: www.idgconnect.com

Copyright © IDG Connect, 2019. All Rights Reserved.