RSAConference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

BETTER.

SESSION ID: KEY-W06

Think and Act Like a Hacker to Protect Your Company's Assets

Paula Januszkiewicz

CQURE: CEO, Penetration Tester; Security Expert
CQURE Academy: Trainer
Microsoft MVP on Cloud and Datacenter Management
Microsoft Regional Director
www.cqureacademy.com
paula@cqure.us
@PaulaCqure

What has evolved over the years?

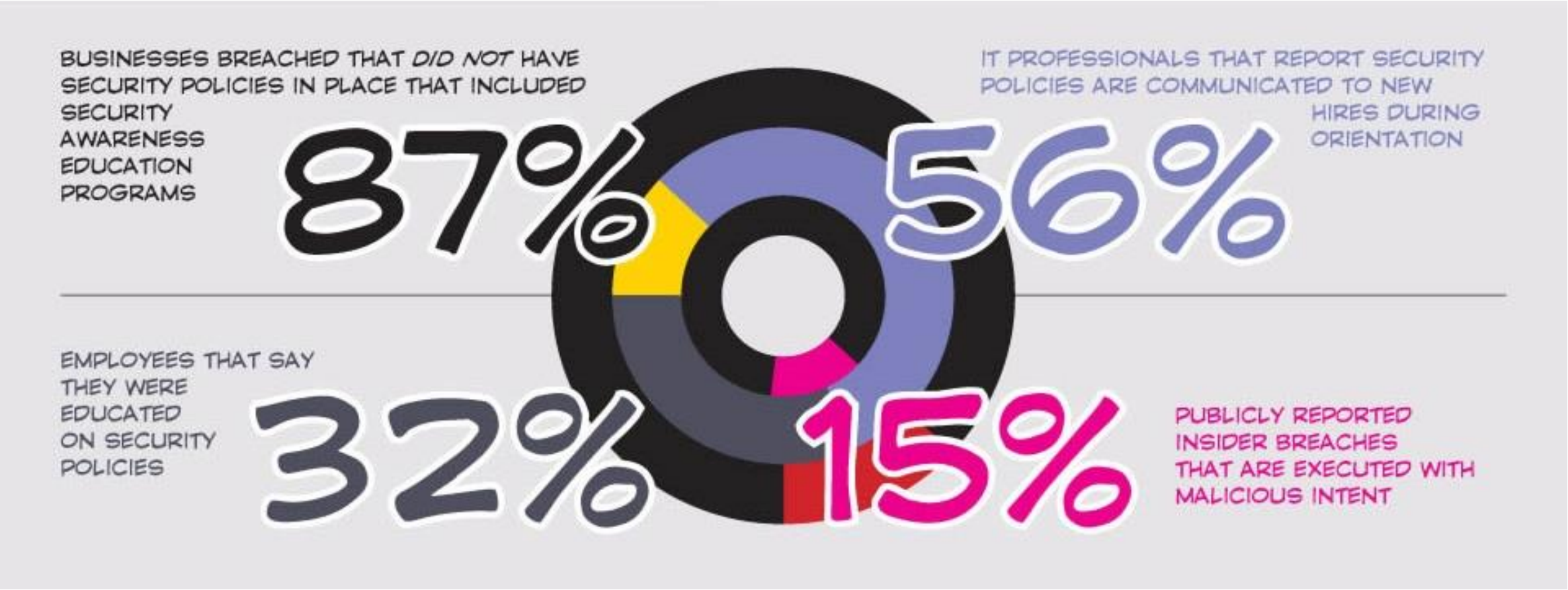
✓ Malware tries to blend in day-to-day admin operations (PowerShell scripts, LOLBINS, etc.);

✓ Machine learning may be used to identify malicious activity but also it may be used to make malware harder to analyse (e.g. hard to analyze ML model built in malware trained to check if it runs on the victim machine).

Awareness >> Behavior >> Culture

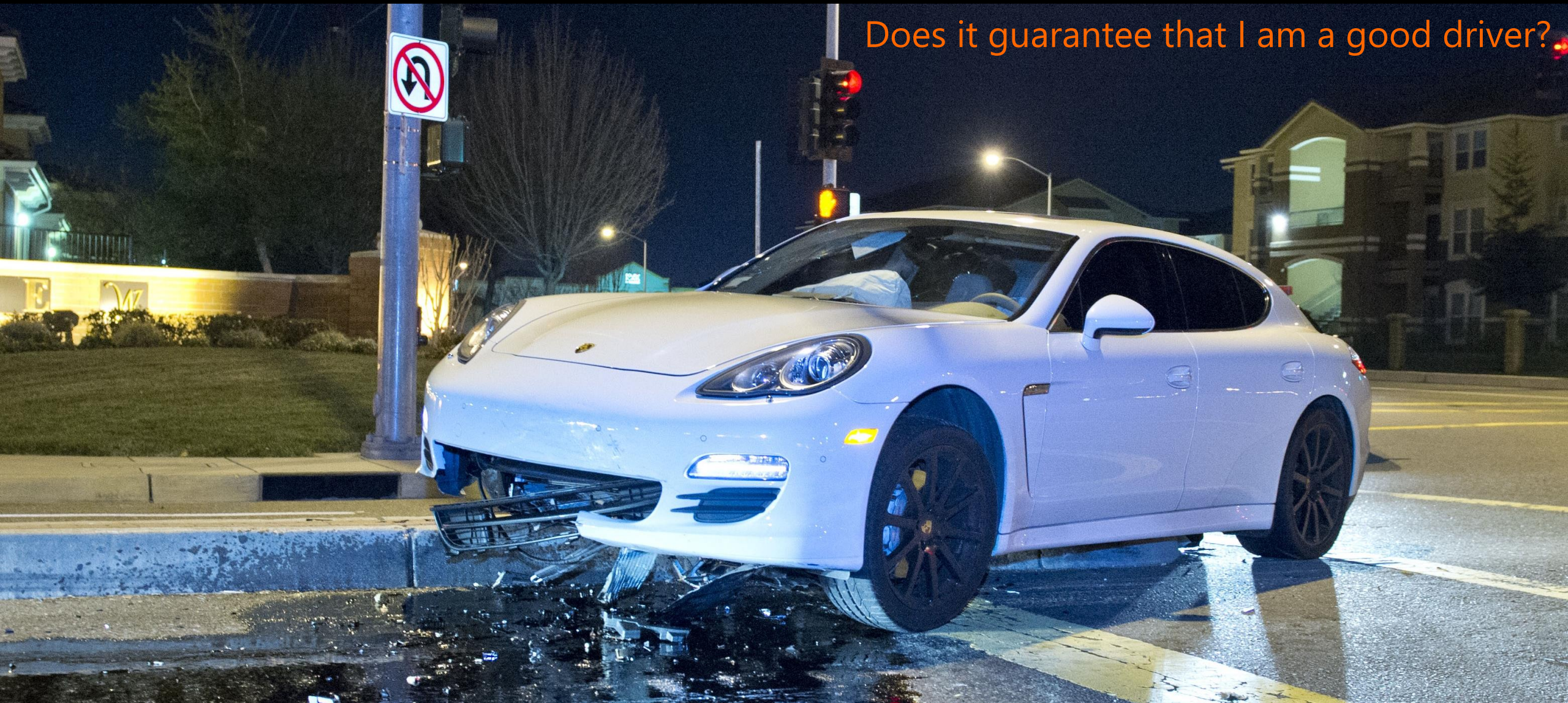
Each organization processing sensitive data **must aim for a responsible security culture.**

And here come statistics…



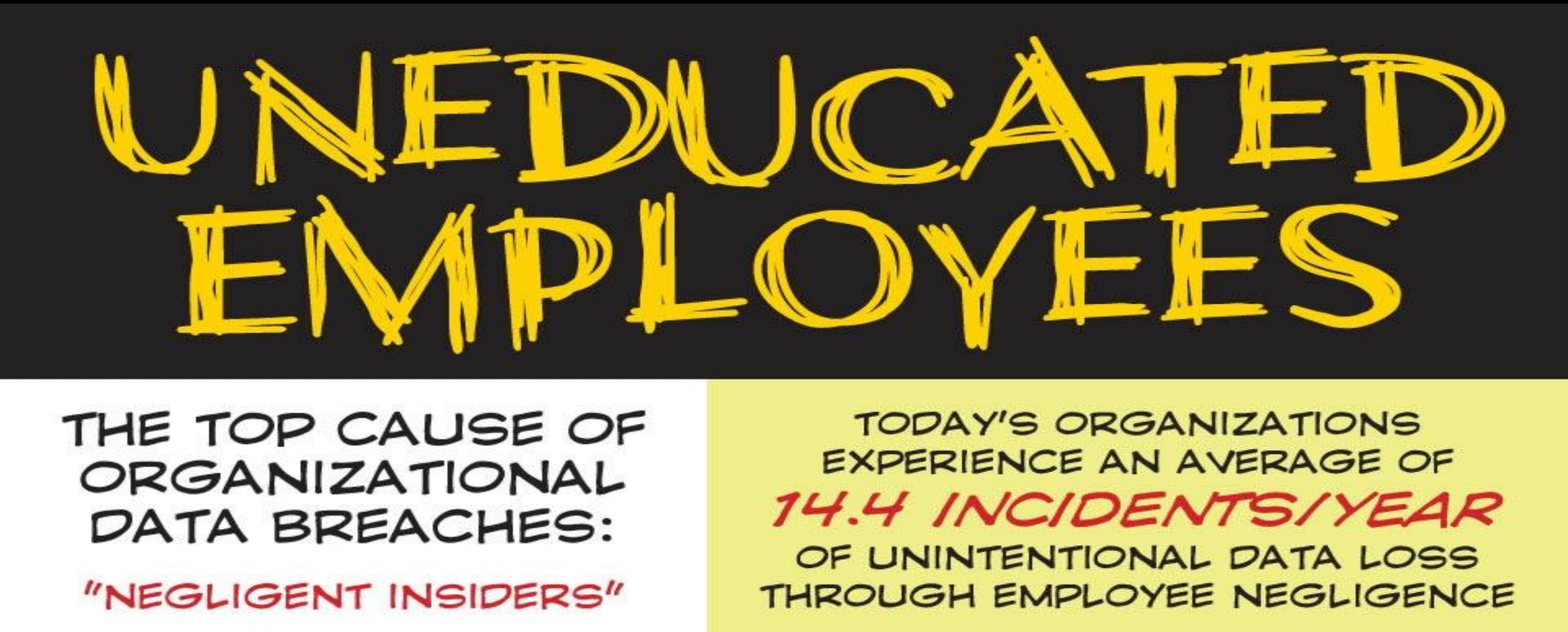
Awareness comes with experience

Behavior comes with awareness



Culture comes with understanding

Did you know that one of the main reasons for information loss are…



7 Security Issues that should not happen in 2019

RSAConference2019
Asia Pacific & Japan

Here comes the 1st issue…

#1: PATHETIC PASSWORDS

15%

IN APPROXIMATELY 15% OF PHYSICAL SECURITY TESTS PERFORMED AT CLIENT SITES WRITTEN PASSWORDS WERE FOUND ON AND AROUND USER WORKSTATIONS

THE MOST COMMON CORPORATE PASSWORD IS Password1 BECAUSE IT JUST BARELY MEETS THE MINIMUM COMPLEXITY REQUIREMENTS OF ACTIVE DIRECTORY FOR LENGTH, CAPITALIZATION AND NUMERICAL FIGURES

Solution:

Well done PKI Implementation

Solution:

Hardware-based Credentials Protection

#2: PEEPING ROM

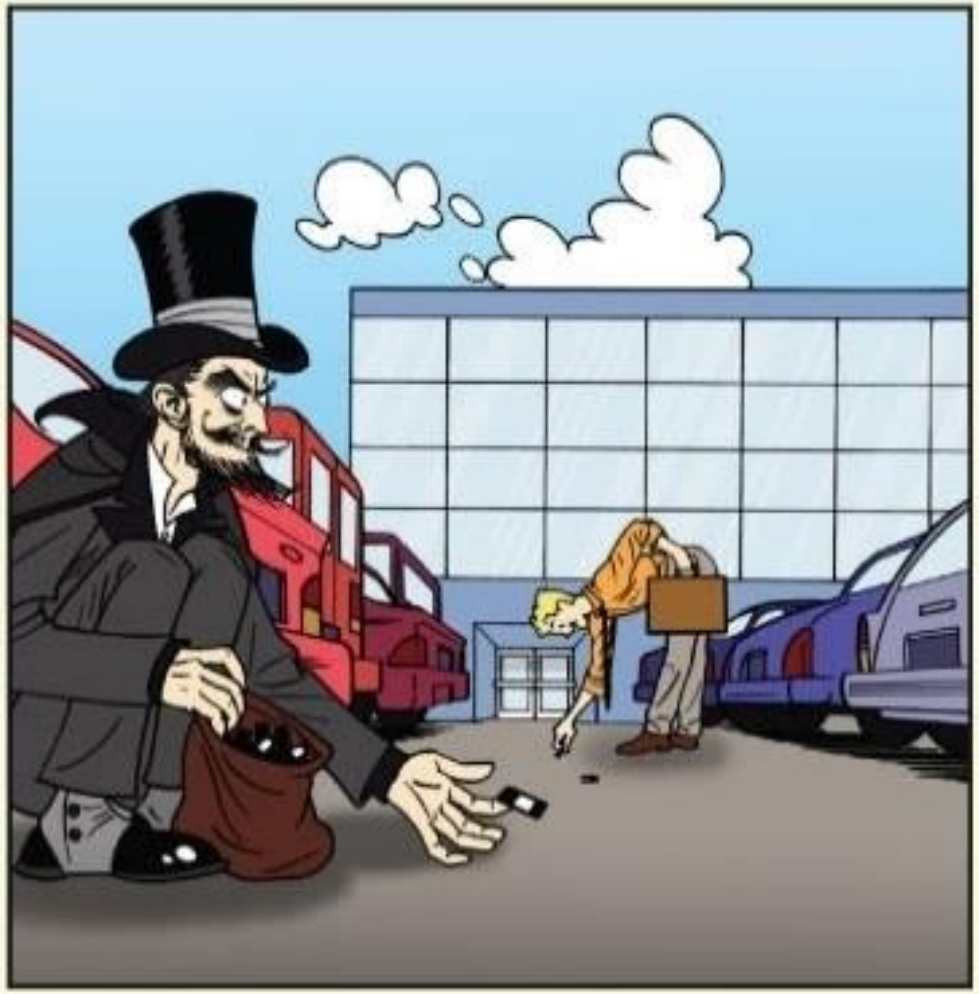
WORKERS SURVEYED THAT SAY THEY HAVE BEEN ABLE TO SNEAK A PEEK AT A CO-WORKER'S OR STRANGER'S WORK STATION IN THE WORKPLACE OR A PUBLIC PLACE

71%

ONE IN THREE WORKERS LEAVE THEIR COMPUTERS LOGGED ON TO NETWORK RESOURCES AND UNLOCKED WHEN THEY ARE AWAY FROM THEIR DESK

26.4% *OF MALWARE* IS KEY LOGGER OR APPLICATION-SPECIFIC — WHICH OFTEN REQUIRES DETAILED KNOWLEDGE OF OR PHYSICAL ACCESS TO A TARGETED SYSTEM

Solution:
Privileged Access Management



#3: USB STICK UP

60% OF USERS WHO FIND RANDOM USB STICKS IN A PARKING LOT WILL PLUG THEM INTO THEIR COMPUTERS

ADD THE COMPANY LOGO, AND THAT NUMBER INCREASES TO 90%

35% OF USERS REPORT HAVING EXPERIENCED A VIRUS INFECTION THROUGH A USB DEVICE

Solution:
Whitelisting

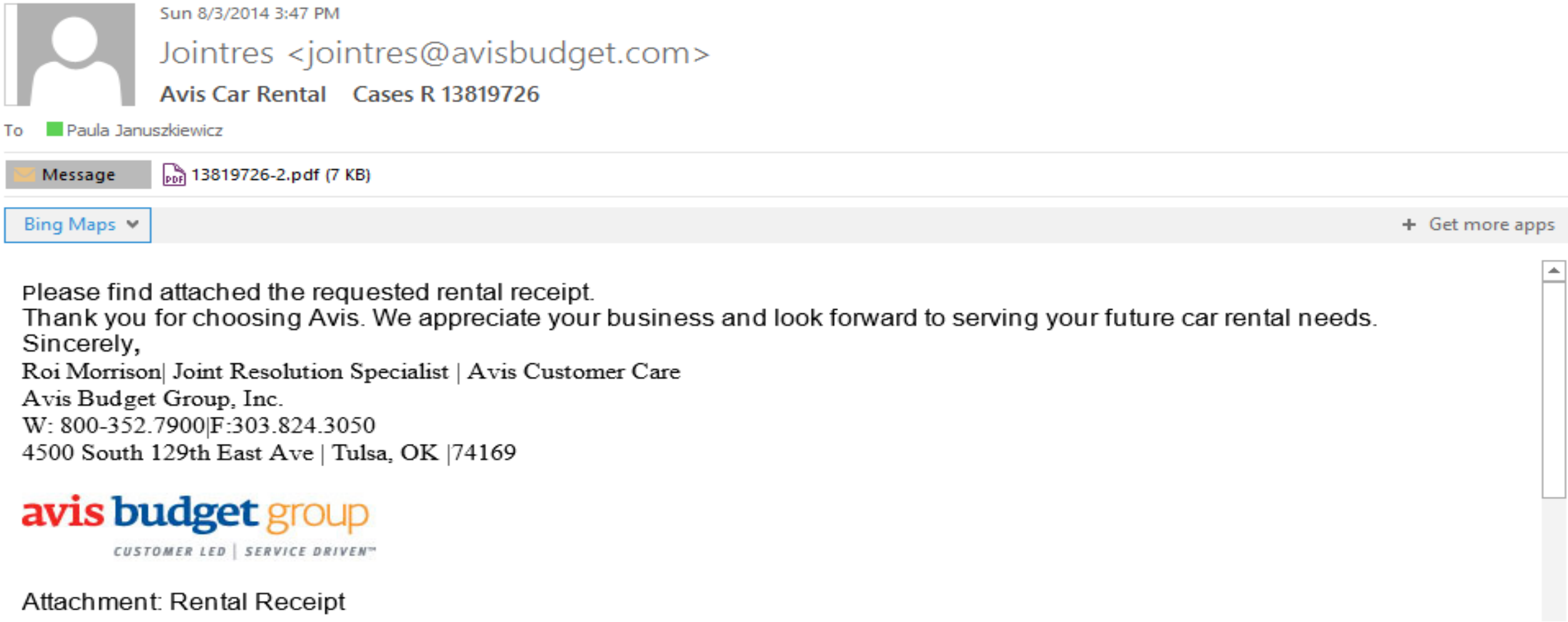
#4: PHISH BITING

69% OF IT SECURITY PROS SAY THEY COME ACROSS PHISHING MESSAGES THAT GET PAST SPAM FILTERS

27% OF IT ORGANIZATIONS HAVE TOP EXECUTIVES OR PRIVILEGED USERS WHO HAVE FALLEN FOR MALICIOUS EMAIL ATTACKS

USERS TRAINED IN AVOIDING PHISHING AND SCAM EMAILS FELL FOR THESE MALICIOUS EMAILS *42% LESS* THAN THOSE WITHOUT TRAINING

Question: Is this a phishing email?



Sun 8/3/2014 3:47 PM

Jointres <jointres@avisbudget.com>

Avis Car Rental Cases R 13819726

To Paula Januszkiewicz

Message 13819726-2.pdf (7 KB)

Bing Maps + Get more apps

Please find attached the requested rental receipt.
Thank you for choosing Avis. We appreciate your business and look forward to serving your future car rental needs.
Sincerely,
Roi Morrison| Joint Resolution Specialist | Avis Customer Care
Avis Budget Group, Inc.
W: 800-352.7900|F:303.824.3050
4500 South 129th East Ave | Tulsa, OK |74169

avis budget group
CUSTOMER LED | SERVICE DRIVEN™

Attachment: Rental Receipt

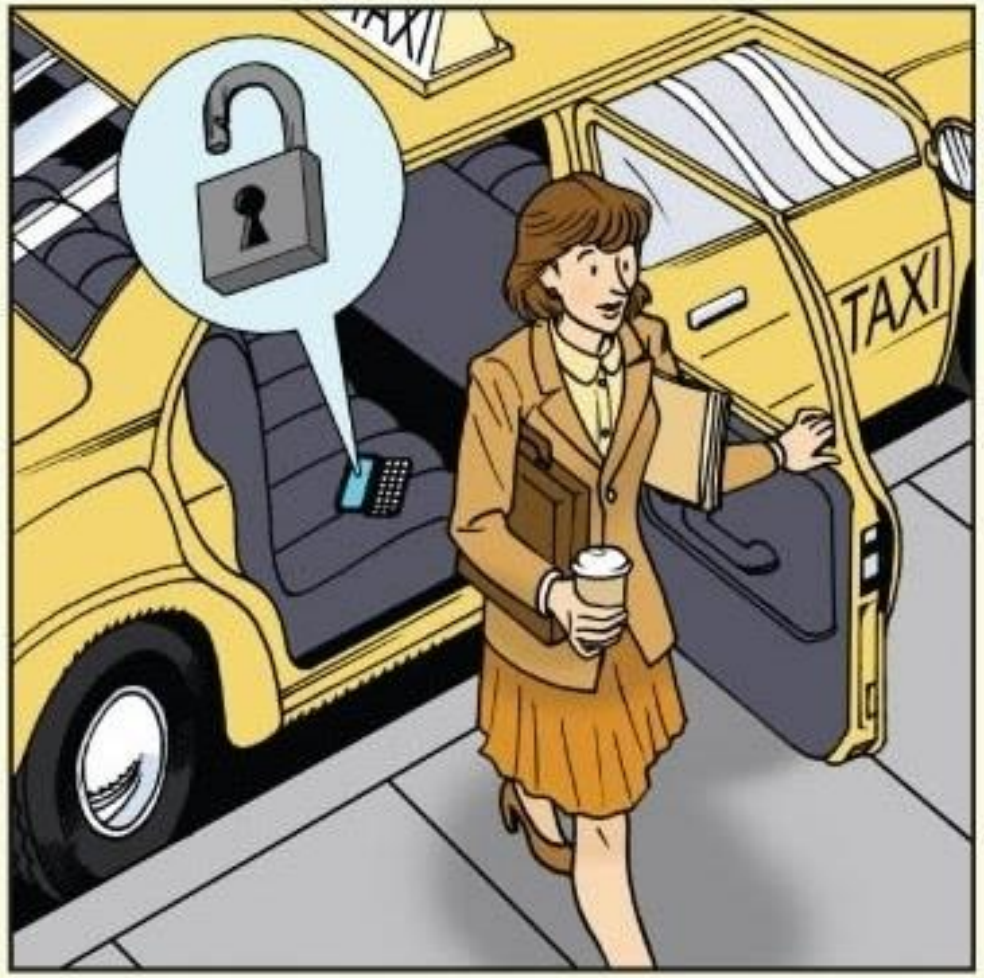
Attacks happen FAST and are HARD to stop

If an attacker sends an email to **100 people** in your company…

…**23 people** will open it…

…**11 people** will open the attachment…

…and **six** will do it in the **first hour.**



#5: RECKLESS ABANDON

70%

OF USERS DO NOT PASSWORD PROTECT THEIR SMARTPHONES

89%

OF PEOPLE WHO FIND LOST CELL PHONES RUMMAGE THROUGH THE DIGITAL CONTENTS TO LOOK AT SENSITIVE INFORMATION

"THERE ARE TWO KINDS OF BIG COMPANIES, THOSE WHO'VE BEEN HACKED, AND THOSE WHO DON'T KNOW THEY'VE BEEN HACKED."

-JAMES COMEY, FBI DIRECTOR

200+	**80**	**$3 Trillion**	**$3.5 Million**
Median number of days attackers are present on a victims network before detection	Days after detection to full recovery	Impact of lost productivity and growth	Average cost of a data breach (15% YoY increase)

Solution:
Incident Response Plan

#6: HOOKING UP WITH ANOTHER MAN'S WI-FI

BY 2015, THE NUMBER OF WIFI HOTSPOT DEPLOYMENTS WILL INCREASE BY **350%**

ONLY 18 PERCENT OF USERS USE A VPN TOOL WHEN ACCESSING PUBLIC WI-FI

FBI

THE FBI RECENTLY RELEASED AN ALERT TO TRAVELERS WARNING AGAINST AN UPTICK IN MALWARE PASSED OFF AS SOFTWARE UPDATES ON HOTEL INTERNET CONNECTIONS

Solution:
Machine Learning for Threat Protection

#7: A LITTLE TOO SOCIAL

67% OF YOUNG WORKERS THINK CORPORATE SOCIAL MEDIA POLICIES ARE OUTDATED

70% REGULARLY IGNORE IT POLICIES

52% OF ENTERPRISES HAVE SEEN AN INCREASE OF MALWARE INFECTIONS DUE TO EMPLOYEES' USE OF SOCIAL MEDIA

Solution: Talk *Security* to Employees

Sad facts

Most of the companies we deal with did not have security policies in place that included security awareness education programs.

Management understands risk. IT also understands it. This can be nicely combined together when we use appropriate language.

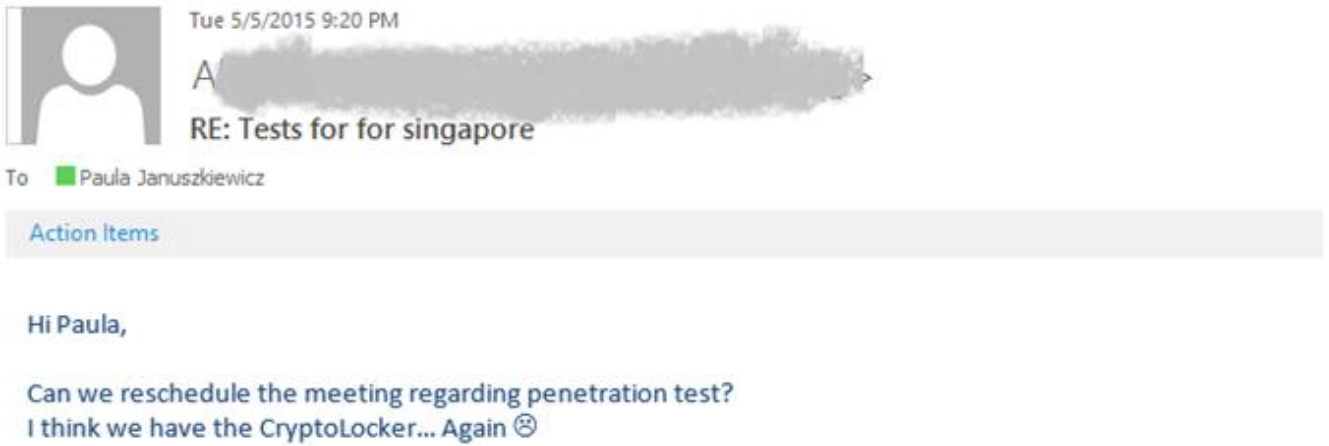



Photo: the New York Times Magazine

Summary: Best Practices

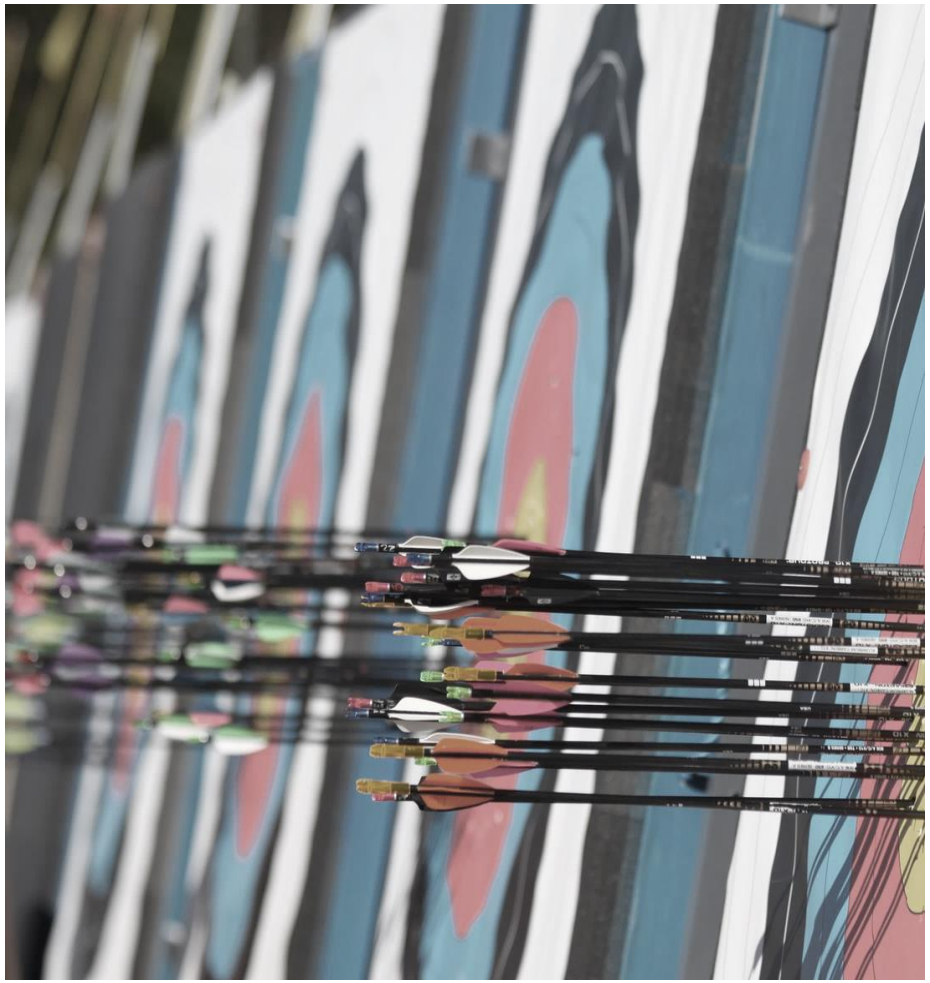
Understanding is the key to security

Continuous vulnerability discovery
Context-Aware Analysis
Prioritization
Remediation and Tracking
Configuration reviews

Put on the Hacker's Shoes

Prevention is the key to success

How can we know what to prevent if we do not know what is the threat?



Additional Resources

Websites

Ars Technica
The Register
The Hacker News
Dark Reading
Krebs on Security
Computer World
Threat Post
Beta News
Tech News World
Tech Crunch
ZDNetSecurity Affairs
Computer Weekly
Network World

SC Magazine
Wired
Schneier on Security

CQURE

To get SLIDES & TOOLS

(and not to miss out on my video tutorials):

Sign up for our Newsletter
Cqureacademy.com/newsletter

Like CQURE Academy on Facebook
Facebook.com/CQURE

Follow me on Twitter
@PaulaCqure

The best option – all of the above!
I won't think you're a stalker, promise