Attacks of the Industry:
A View into the Future of Cybersecurity

Paula Januszkiewicz

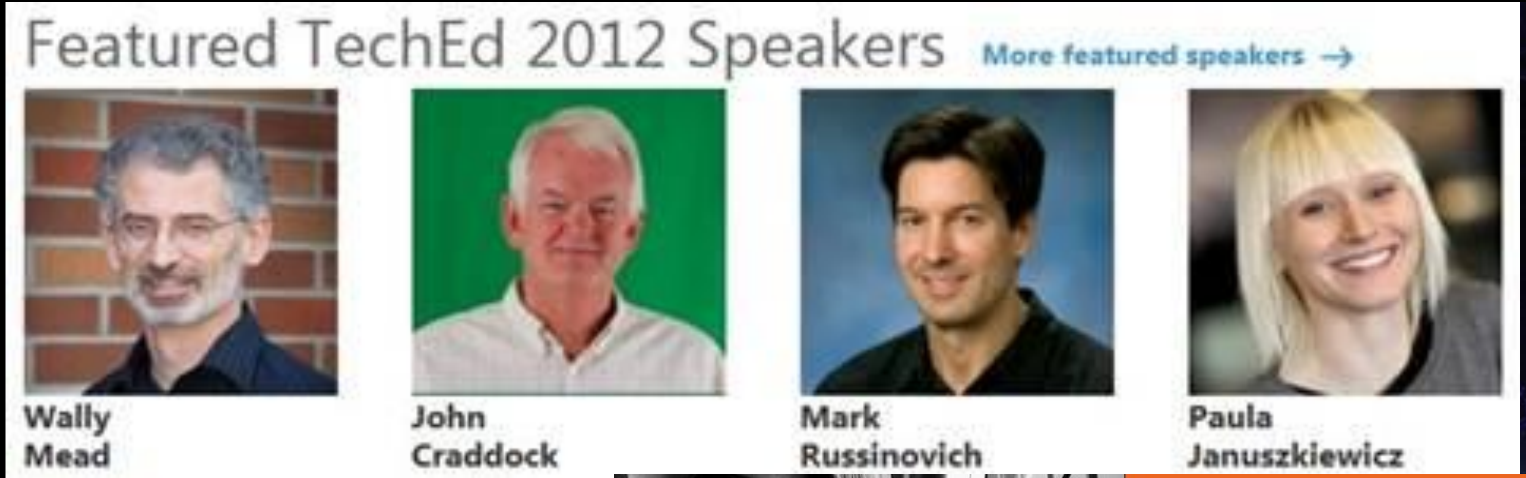
CQURE: CEO, Cybersecurity Expert, Penetration Tester
CQURE Academy: Trainer
MVP: Enterprise Security, MCT
Microsoft Regional Director

https://cqureacademy.com
https://cqure.us
paula@cqure.us

CQURE CONSULTING

CQURE ACADEMY

@paulacqure
@CQUREAcademy



Featured TechEd 2012 Speakers

More featured speakers →

Wally Mead

John Craddock

Mark Russinovich

Paula Januszkiewicz

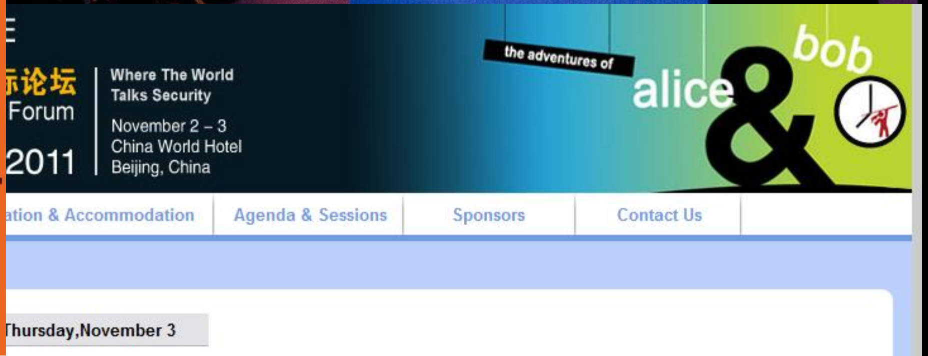
We are proud to announce that **Paula Januszkiewicz** was rated as **No 1 Speaker** at Microsoft **Ignite!!!**

May 4-8, 2015
Chicago, IL

No.1 Speaker

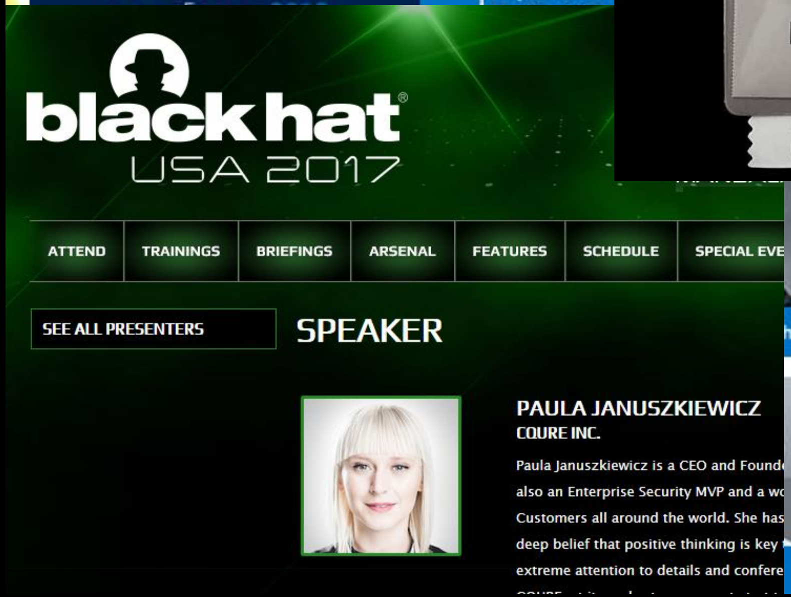
Paula Januszkiewicz
CEO CQURE

She received
a **"Best of Briefings"** award at her
"CQTools: The New Ultimate Hacking Toolkit"
Black Hat Asia 2019 briefing session



Where The World Talks Security

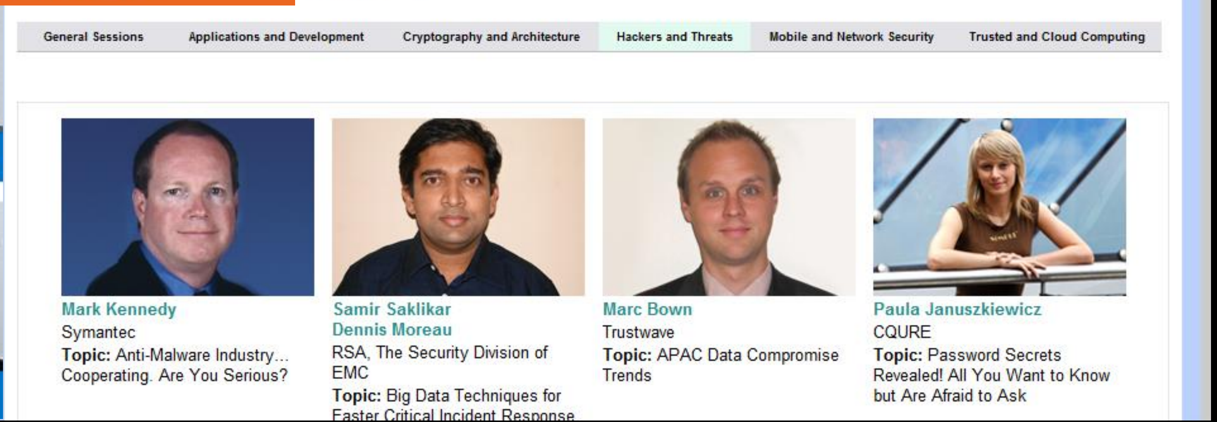
November 2 – 3
China World Hotel
Beijing, China



SPEAKER

PAULA JANUSZKIEWICZ
CQURE INC.

Paula Januszkiewicz is a CEO and Founde
also an Enterprise Security MVP and a wo
Customers all around the world. She has
deep belief that positive thinking is key
extreme attention to details and confere



Thursday,November 3

General Sessions
Applications and Development
Cryptography and Architecture
Hackers and Threats
Mobile and Network Security
Trusted and Cloud Computing

Mark Kennedy
Symantec
Topic: Anti-Malware Industry… Cooperating. Are You Serious?

Samir Saklikar
Dennis Moreau
RSA, The Security Division of EMC
Topic: Big Data Techniques for Faster Critical Incident Response

Marc Bown
Trustwave
Topic: APAC Data Compromise Trends

Paula Januszkiewicz
CQURE
Topic: Password Secrets Revealed! All You Want to Know but Are Afraid to Ask

According to the industry’s statistics, by 2019 the **market will need 6 mln security professionals.** But only 4 to 5 million of them will have the needed qualifications.

*Source: Financial Times

Awareness >> Behavior >> Culture

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

Awareness comes with experience

I know the traffic rules….

DSA®

DRIVING STANDARDS AGENCY

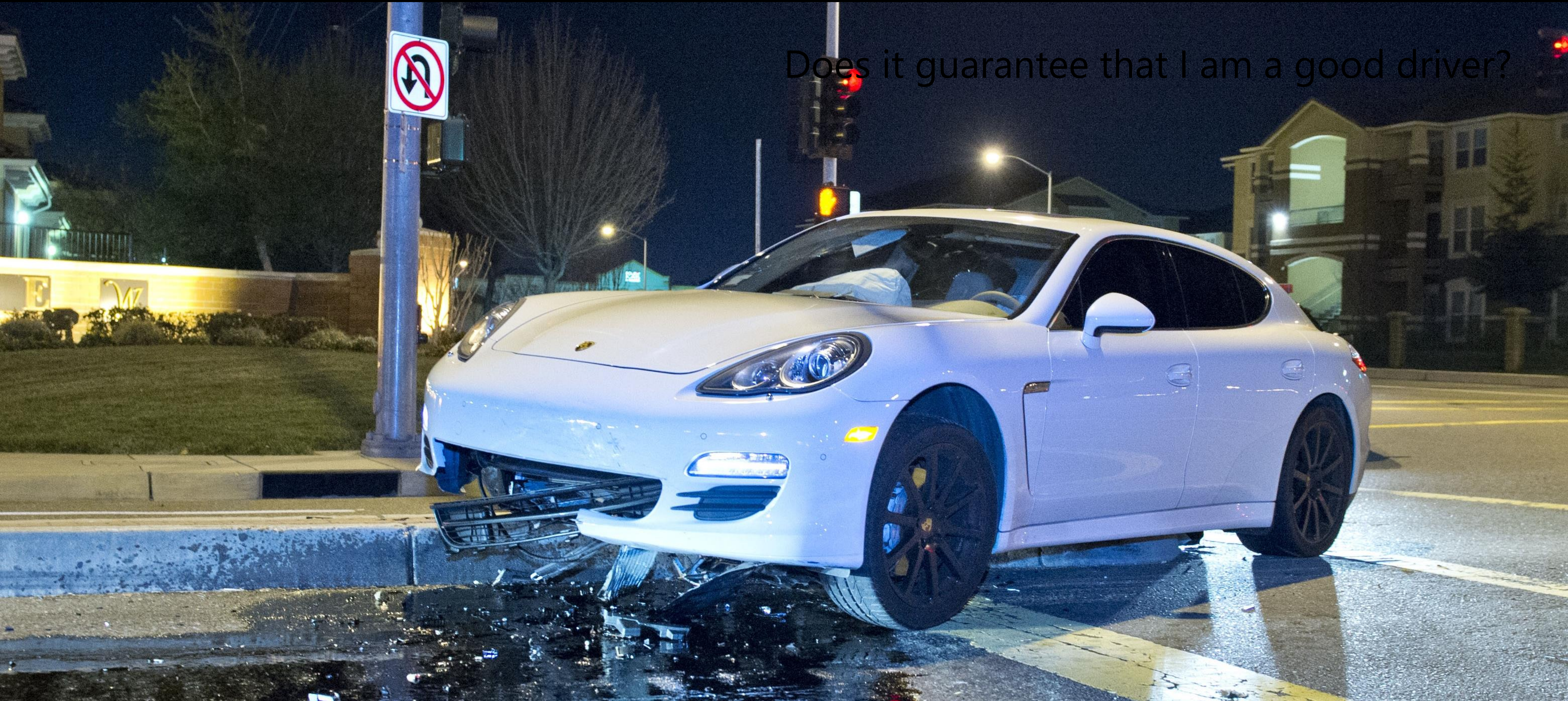
SAFE DRIVING FOR LIFE™

Issue No.	Fee	Rem Type	O/D	S/C	T/P

PRACTICAL DRIVING TEST PASS CERTIFICATE

This is to certify that:

Behavior comes with awareness

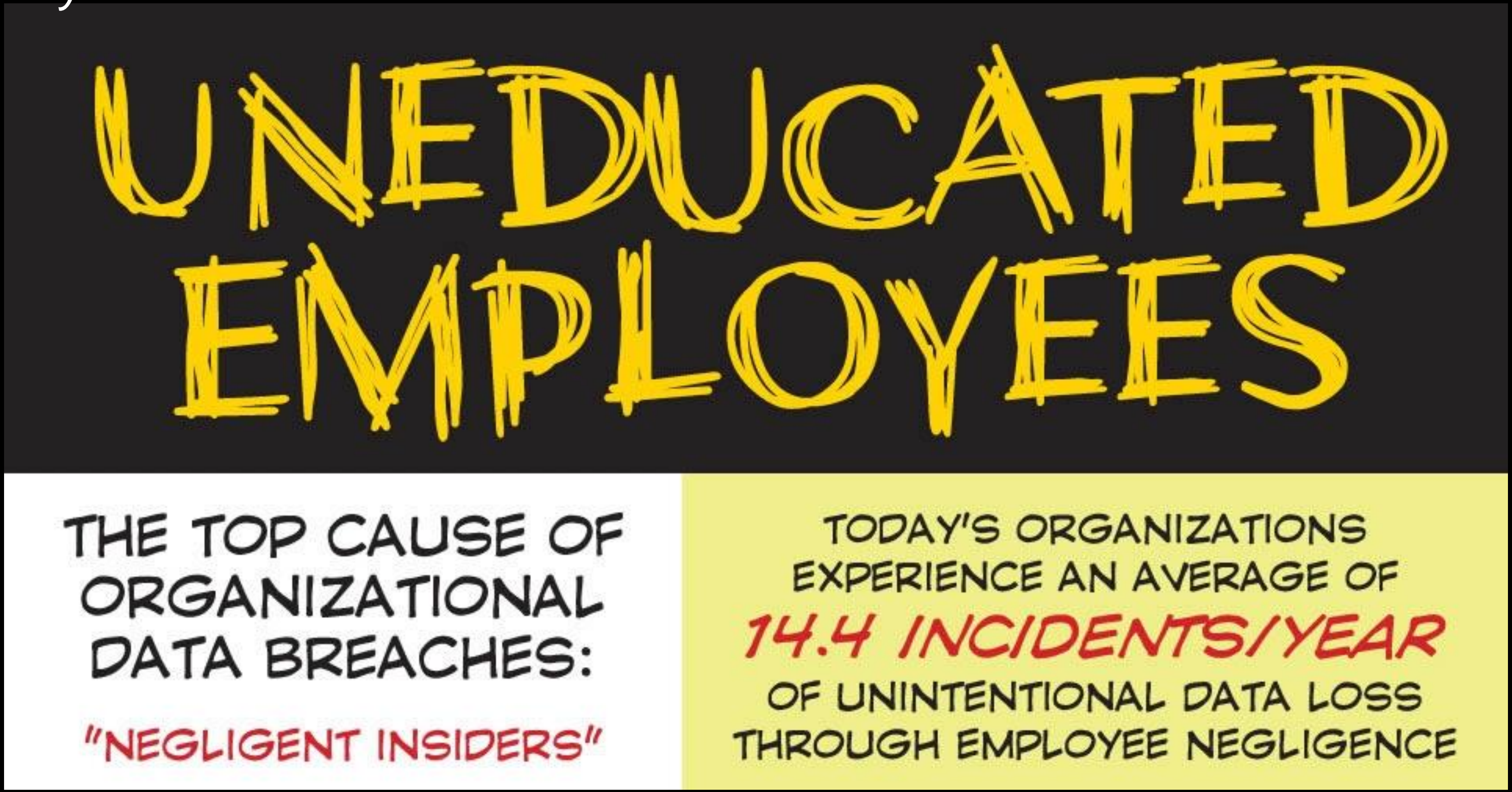


Does it guarantee that I am a good driver?

Culture comes with understanding

Culture comes with understanding

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



UNEDUCATED EMPLOYEES

THE TOP CAUSE OF ORGANIZATIONAL DATA BREACHES:

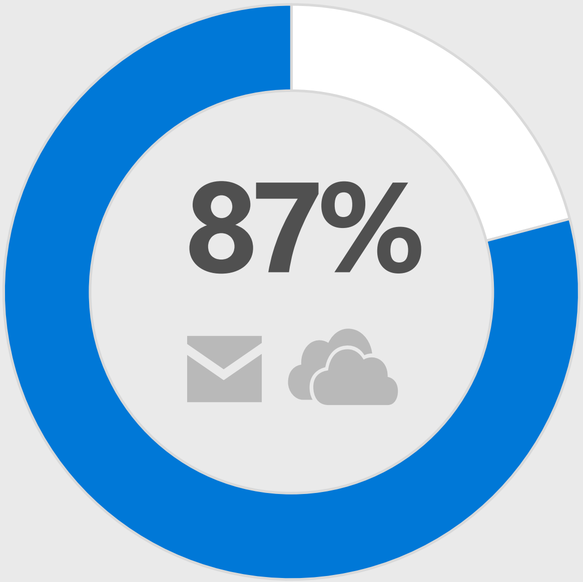
"NEGLIGENT INSIDERS"

TODAY'S ORGANIZATIONS EXPERIENCE AN AVERAGE OF

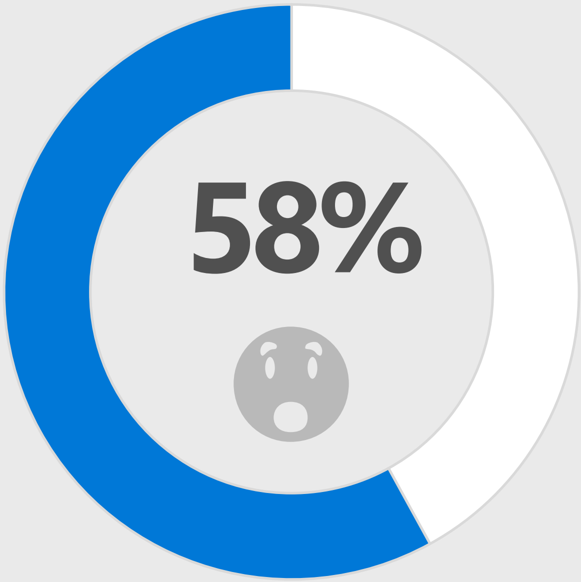
14.4 INCIDENTS/YEAR

OF UNINTENTIONAL DATA LOSS THROUGH EMPLOYEE NEGLIGENCE

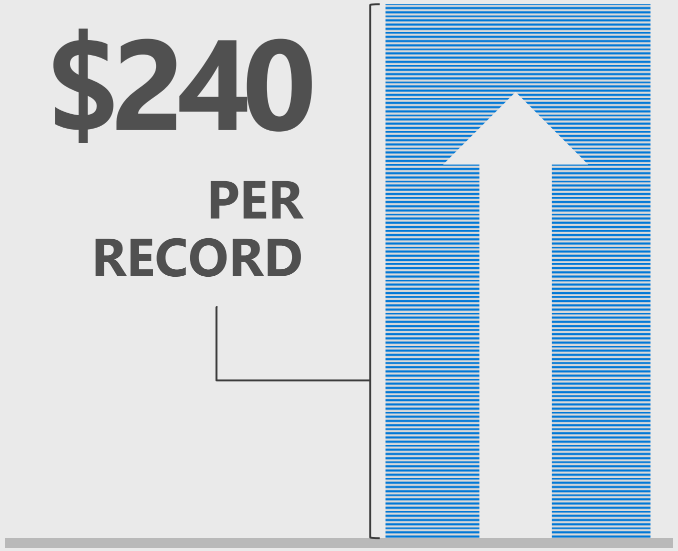
Data Leakage



...of senior managers admit to **regularly** uploading work files to a personal email or cloud account[1]



Have accidentally sent sensitive information to the **wrong person**[1]



Average per record **cost of a data breach** across all industries[2]

[1] Stroz Friedberg, “On The Pulse: Information Security In American Business,” 2013

[2] HIPPA Secure Now, “A look at the cost of healthcare data breaches,” Art Gross, March 30, 2012

We have the best security solutions...

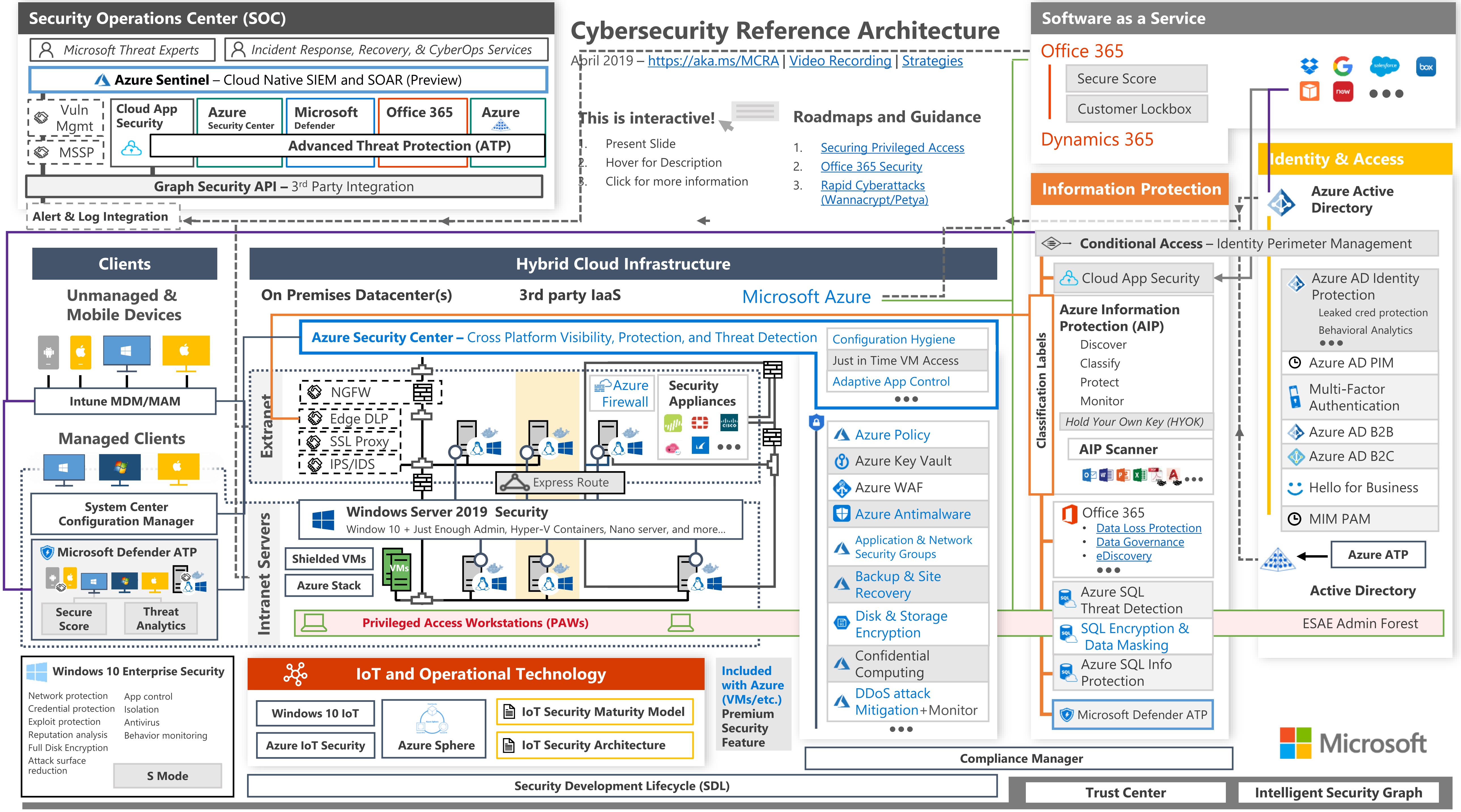
...but the security landscape has changed.

Cybersecurity Ventures predicts there will be **additional 3.5 million cybersecurity job openings by 2021**

*Source: Cybersecurity Ventures

Cybersecurity Reference Architecture

April 2019 – https://aka.ms/MCRA | Video Recording | Strategies



This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)

Security Operations Center (SOC)

Microsoft Threat Experts

Incident Response, Recovery, & CyberOps Services

Azure Sentinel – Cloud Native SIEM and SOAR (Preview)

Vuln Mgmt

MSSP

Cloud App Security

Azure Security Center

Microsoft Defender

Office 365

Azure

Advanced Threat Protection (ATP)

Graph Security API – 3rd Party Integration

Alert & Log Integration

Software as a Service

Office 365

Secure Score

Customer Lockbox

Dynamics 365

Information Protection

Identity & Access

Azure Active Directory

Conditional Access – Identity Perimeter Management

Cloud App Security

Classification Labels

Azure Information Protection (AIP)

Discover

Classify

Protect

Monitor

Hold Your Own Key (HYOK)

AIP Scanner

Office 365

- Data Loss Protection
- Data Governance
- eDiscovery

Azure SQL Threat Detection

SQL Encryption & Data Masking

Azure SQL Info Protection

Microsoft Defender ATP

Azure AD Identity Protection

Leaked cred protection

Behavioral Analytics

Azure AD PIM

Multi-Factor Authentication

Azure AD B2B

Azure AD B2C

Hello for Business

MIM PAM

Azure ATP

Active Directory

ESAE Admin Forest

Clients

Unmanaged & Mobile Devices

Intune MDM/MAM

Managed Clients

System Center Configuration Manager

Microsoft Defender ATP

Secure Score

Threat Analytics

Windows 10 Enterprise Security

Network protection

Credential protection

Exploit protection

Reputation analysis

Full Disk Encryption

Attack surface reduction

App control

Isolation

Antivirus

Behavior monitoring

S Mode

Hybrid Cloud Infrastructure

On Premises Datacenter(s)

3rd party IaaS

Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

Configuration Hygiene

Just in Time VM Access

Adaptive App Control

Extranet

NGFW

Edge DLP

SSL Proxy

IPS/IDS

Azure Firewall

Security Appliances

Express Route

Intranet Servers

Windows Server 2019 Security

Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more…

Shielded VMs

Azure Stack

VMs

Privileged Access Workstations (PAWs)

Azure Policy

Azure Key Vault

Azure WAF

Azure Antimalware

Application & Network Security Groups

Backup & Site Recovery

Disk & Storage Encryption

Confidential Computing

DDoS attack Mitigation+Monitor

Included with Azure (VMs/etc.)

Premium Security Feature

IoT and Operational Technology

Windows 10 IoT

Azure IoT Security

Azure Sphere

IoT Security Maturity Model

IoT Security Architecture

Compliance Manager

Security Development Lifecycle (SDL)

Trust Center

Intelligent Security Graph

Microsoft

> "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+

Median number of days attackers are present on a victims network before detection

80

Days after detection to full recovery

$3Trillion

Impact of lost productivity and growth

$3.5Million

Average cost of a data breach (15% YoY increase)

7 Security Issues that just should not happen

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

#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

#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

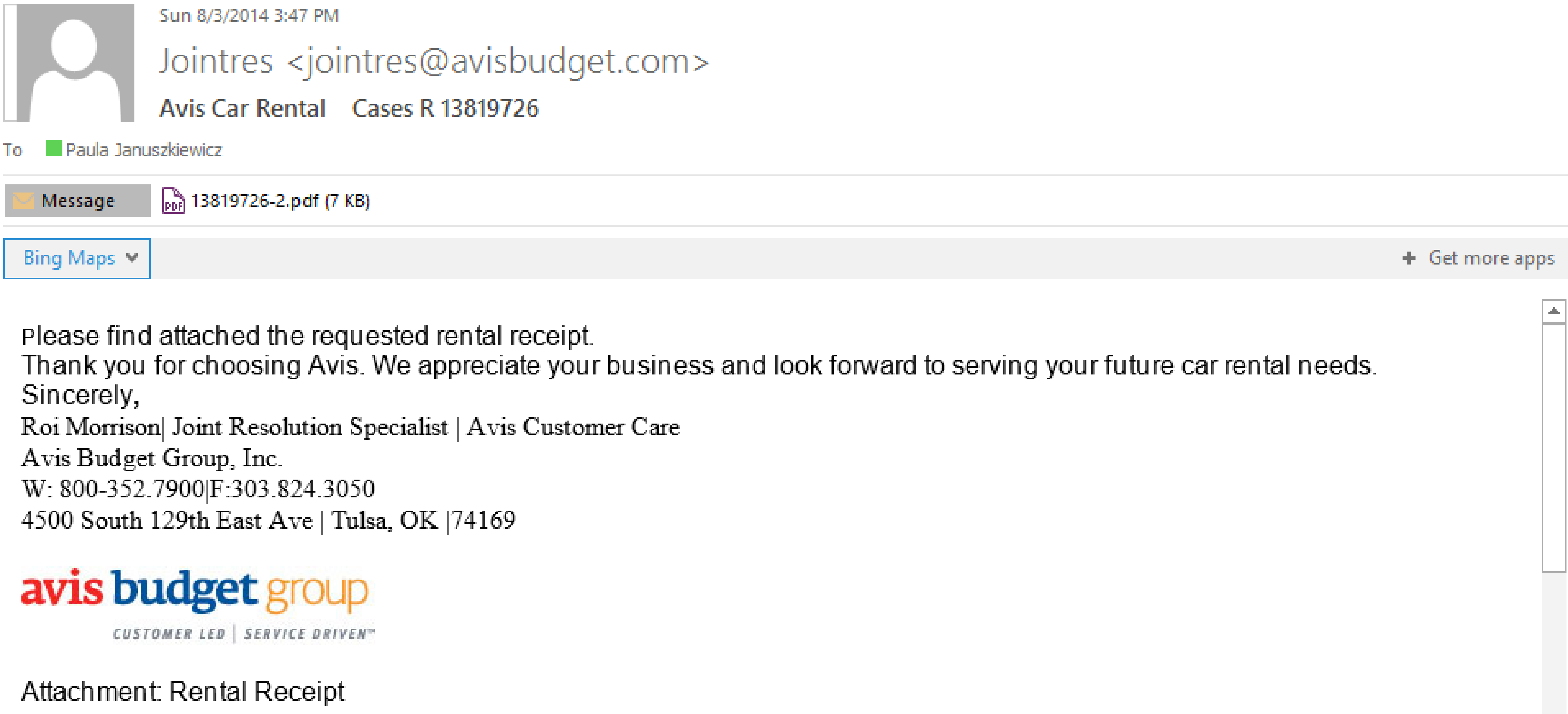
#4: PHISH BITING

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

13819726-2.pdf (7 KB)

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

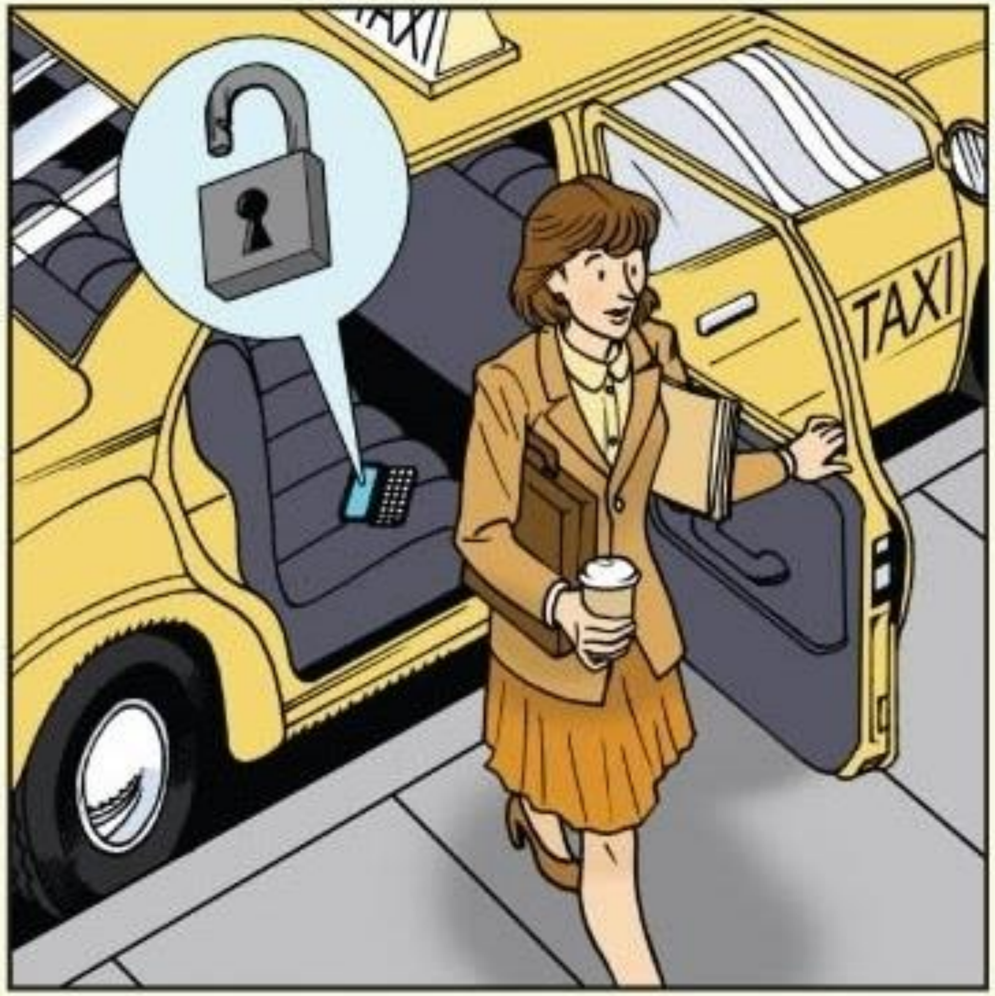
If an attacker sends an email to **100 people** in your company…

…**23 people** will open it…

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

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

Source: VerizoData Breach Investigations Report



#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

Solution: Incident Response Plan

Action list

In case of emergency situation: allows to act reasonably and according to the plan

Increases chances that evidence is gathered properly

Allows to define responsibilities for recovery

Discussions provide management with understanding of security

Recovery plan

Centralization of the event logs

BYOD management strategy

'Connect and go' approach for better efficiency

#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

Error

The super-cool video from your digital penpal failed to load due to a video codec error. Click here to download virus...err, new video codec.

#7: A LITTLE TOO SOCIAL

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

70% REGULARLY IGNORE IT POLICIES

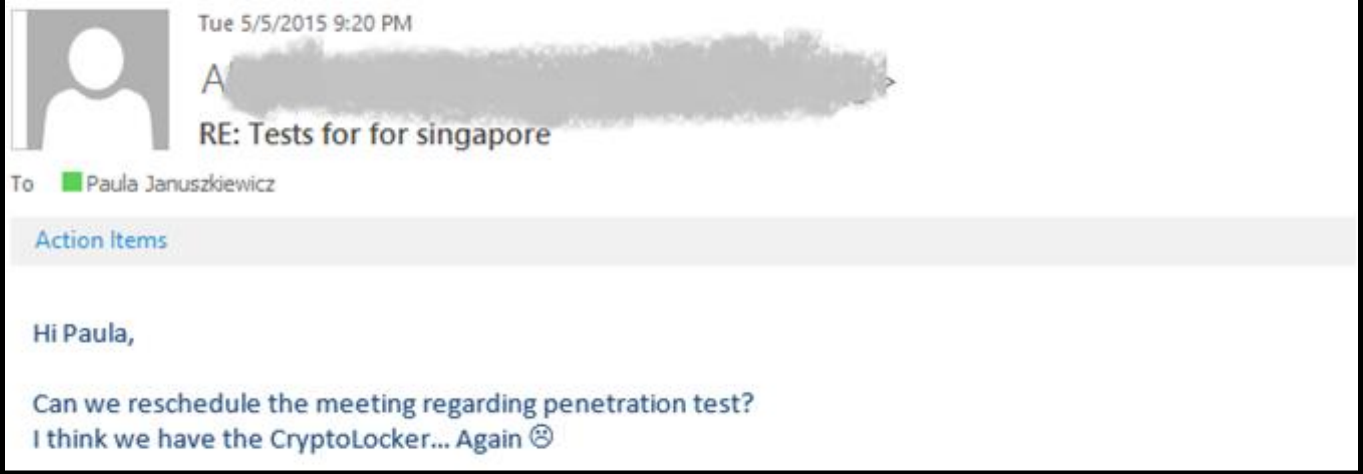
52% OF ENTERPRISES HAVE SEEN AN INCREASE OF MALWARE INFECTIONS DUE TO EMPLOYEES' USE OF SOCIAL MEDIA

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.



Tue 5/5/2015 9:20 PM

[redacted]

RE: Tests for for singapore

To 🟩 Paula Januszkiewicz

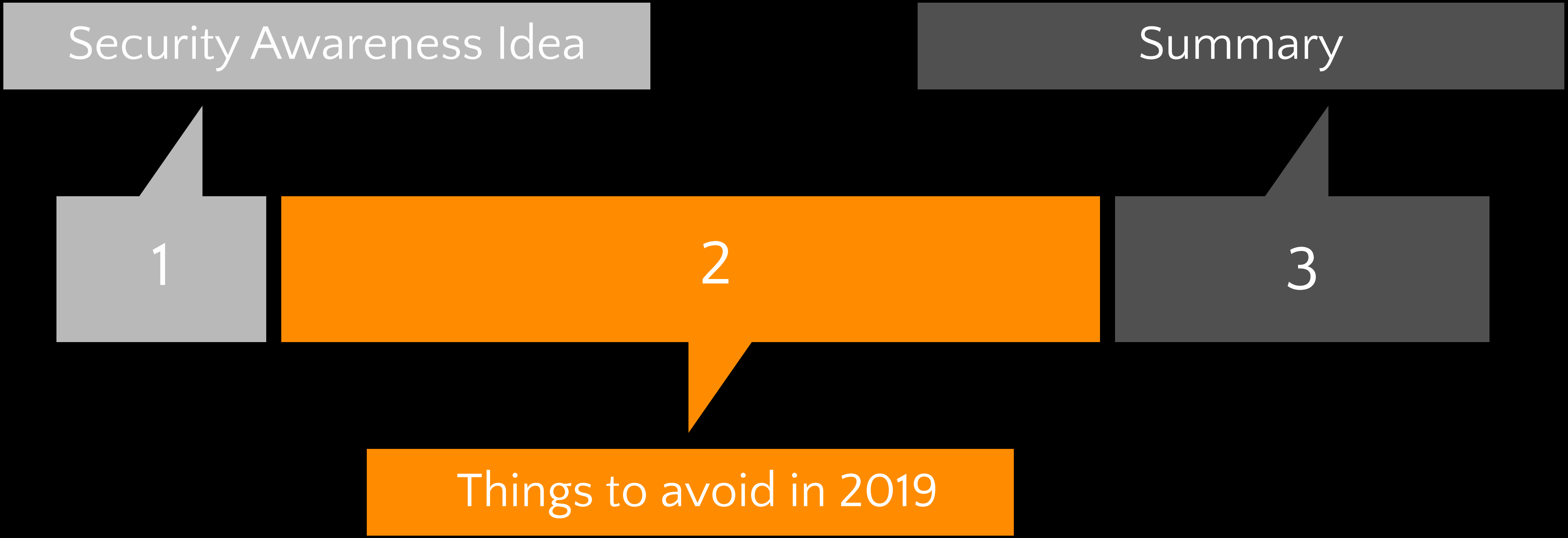
Action Items

Hi Paula,

Can we reschedule the meeting regarding penetration test?
I think we have the CryptoLocker... Again ☹

Photo: the New York Times Magazine

Agenda



1 Security Awareness Idea

2 Things to avoid in 2019

3 Summary

Why human factor is so important?

Reason 1: Security is both a Reality and Feeling

➘ For Security Practicioners

Security is a reality based on the mathematical probability of risks

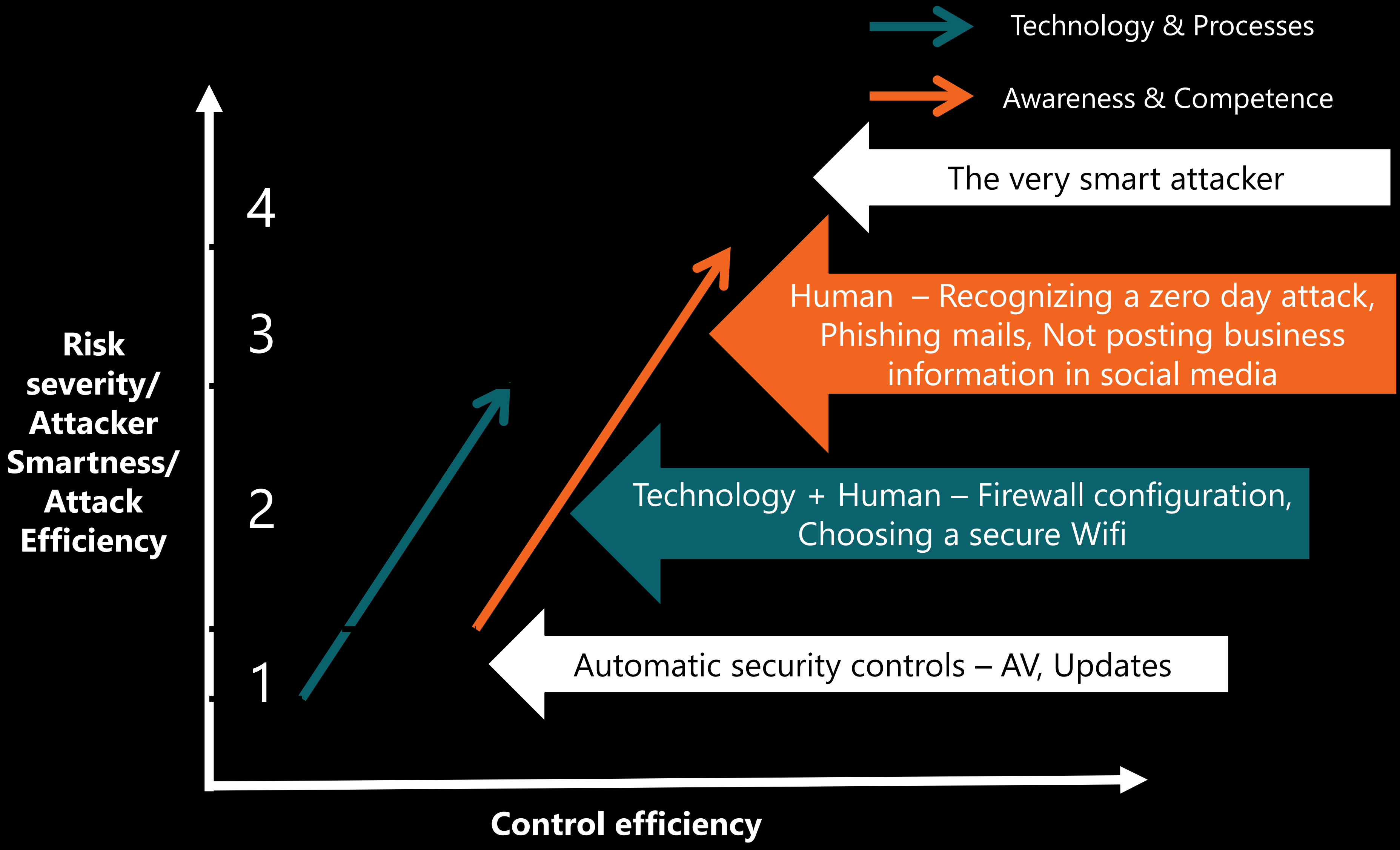
➘ For End User

Security is a feeling

Success lies in influencing the "feeling" of security

Reason 2: Not every attack(er) is that smart

People exaggerate risks that are spectacular or uncommon



The very smart attacker

Human – Recognizing a zero day attack, Phishing mails, Not posting business information in social media

Technology + Human – Firewall configuration, Choosing a secure Wifi

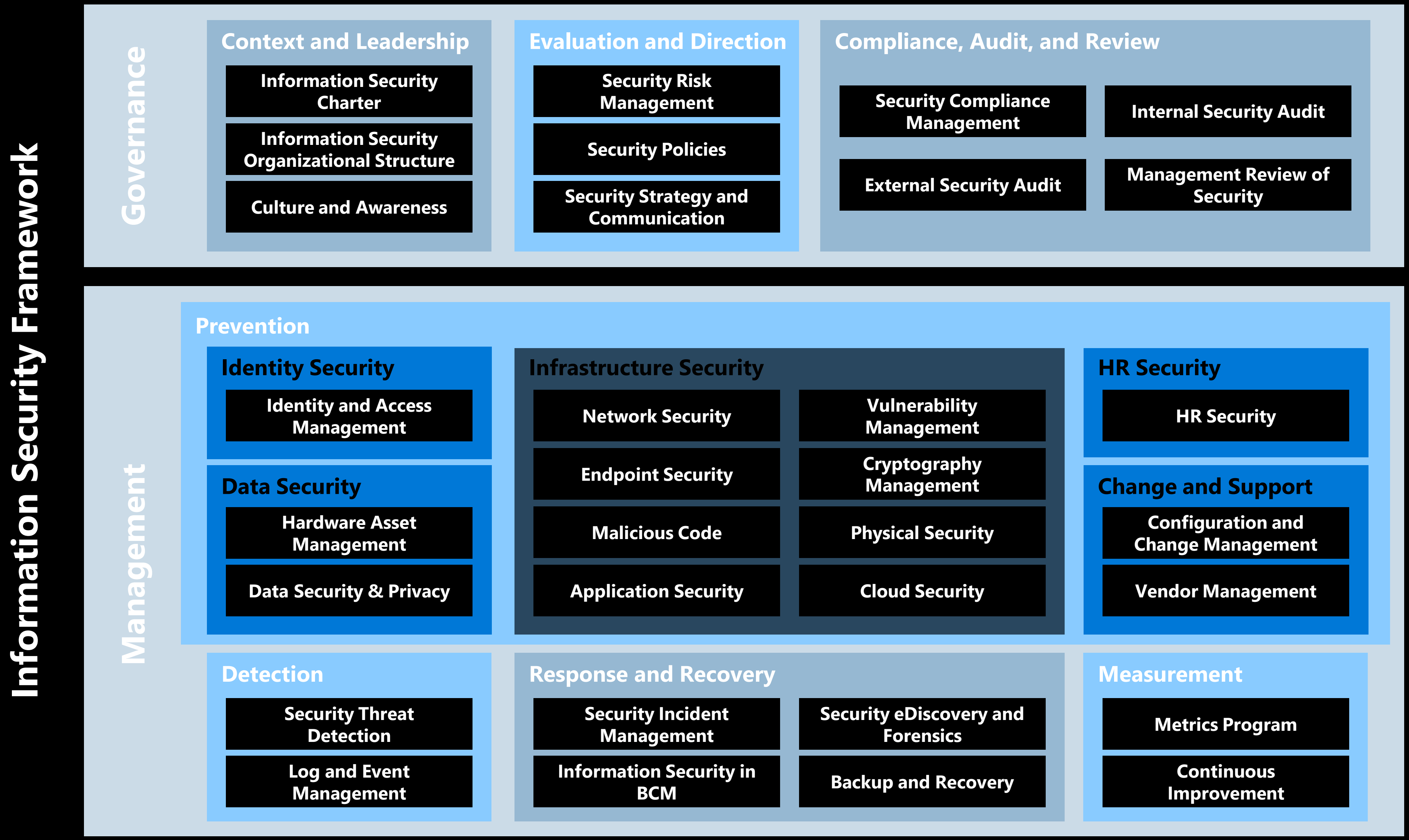
Automatic security controls – AV, Updates

Reason 3: Technology...yes, but humans... of course!

Aircrafts have become more advanced, but does it mean that pilot training requirements have reduced?

Medical technology has become more advanced, but will you choose a hospital for it's machines or the doctors?

A best-of-breed security framework



Information Security Framework

Governance

- Context and Leadership
  - Information Security Charter
  - Information Security Organizational Structure
  - Culture and Awareness
- Evaluation and Direction
  - Security Risk Management
  - Security Policies
  - Security Strategy and Communication
- Compliance, Audit, and Review
  - Security Compliance Management
  - Internal Security Audit
  - External Security Audit
  - Management Review of Security

Management

- Prevention
  - Identity Security
    - Identity and Access Management
  - Data Security
    - Hardware Asset Management
    - Data Security & Privacy
  - Infrastructure Security
    - Network Security
    - Vulnerability Management
    - Endpoint Security
    - Cryptography Management
    - Malicious Code
    - Physical Security
    - Application Security
    - Cloud Security
  - HR Security
    - HR Security
  - Change and Support
    - Configuration and Change Management
    - Vendor Management
- Detection
  - Security Threat Detection
  - Log and Event Management
- Response and Recovery
  - Security Incident Management
  - Security eDiscovery and Forensics
  - Information Security in BCM
  - Backup and Recovery
- Measurement
  - Metrics Program
  - Continuous Improvement

The 11 key cyber security questions

1. Do we treat cyber security as a business or IT responsibility?
2. Do our security goals align with business priorities?
3. Have we identified and protected our most valuable processes and information?
4. Does our business culture support a secure cyber environment?
5. Do we have the basics right? (For example, access rights, software patching, vulnerability management and data leakage prevention.)
6. Do we focus on security compliance or security capability?
7. Are we certain our third-party partners are securing our most valuable information?
8. Do we regularly evaluate the effectiveness of our security?
9. Are we vigilant and do we monitor our systems and can we prevent breaches?
10. Do we have an organized plan for responding to a security breach?
11. Are we adequately resourced and insured?

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

What was your score in our *Windows Security QUIZ 4.0*?

Share it in the comment section!

cqureacademy.com/QUIZ

Every week I'm releasing a fresh **video tutorial**
with latest hacks, vulnerabilities, and security tools

Take Paula's
HARDCORE Windows
Security Quiz

START QUIZ

How to stay tuned?

✉ Sign up for email updates:
CqureAcademy.com/newsletter

f Like CQURE Academy on Facebook:
Facebook.com/CQURE

Follow me on Twitter:
@PaulaCqure

BEST DO ALL OF THE ABOVE :)