RSAConference2022
San Francisco & Digital | February 7 – 10

TRANSFORM

SESSION ID: **HTA-M05**

Strong Story to Tell: Top 10 Mistakes by Administrators About Remote Work

Paula Januszkiewicz

CEO, Cybersecurity Expert
CQURE Inc.
@PaulaCqure

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Featured TechEd 2012 Speakers

More featured speakers →

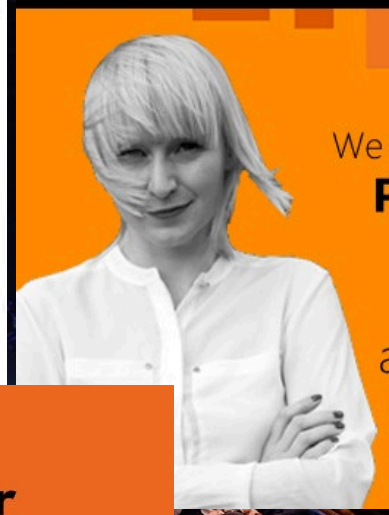
Wally Mead

John Craddock

Mark Russinovich

Paula Januszkiewicz

Microsoft CQURE ACADEMY©



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

May 4-8, 2015
Chicago, IL

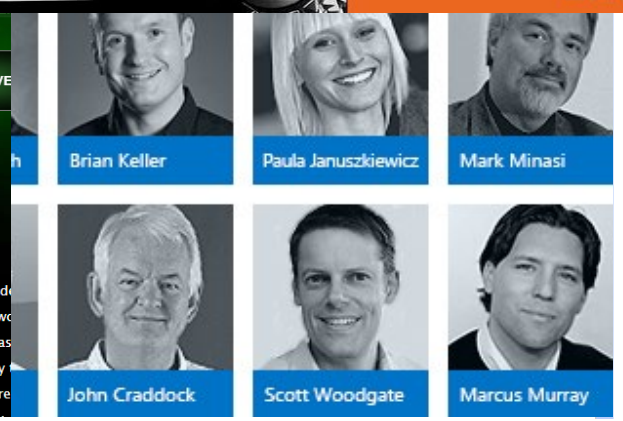
No.1 Speaker

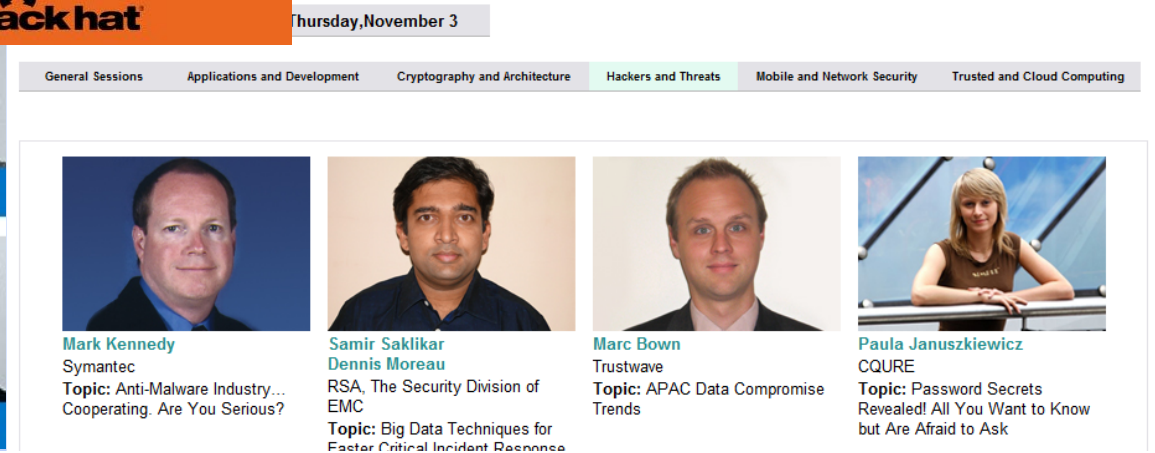
Paula Januszkiewicz
CEO CQURE

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

black hat

TechEd Learn





The power of camouflage

Source:
https://commons.wikimedia.org/wiki/File:Perfectly_Camouflaged_.jpg

RSAConference2022

The Impact of Cybercrime

Impactful Hacking Stats for 2021

1318%

year-on-year increase in ransomware attacks in the first half of 2021

54%

of malicious apps impersonated TikTok, in total 164 malicious apps related to COVID-19 scams were detected

94%

of malware is delivered via email

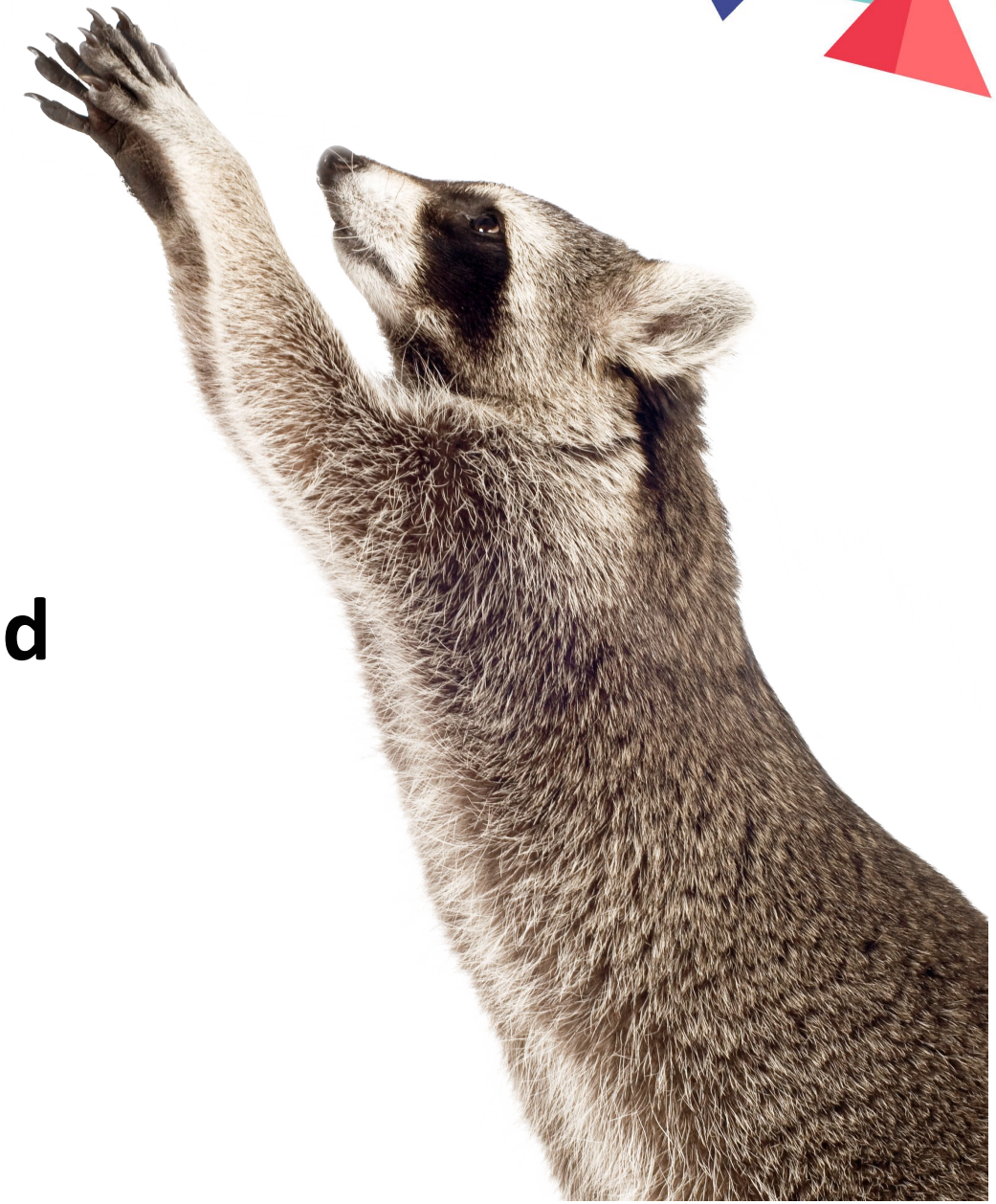
77%

of organizations do not have a cyber security incident response plan

COURE

Source: Source: Trend Micro, IBM, CSO (2021)

**Since COVID-19,
the US FBI reported
a 300% increase in reported
cybercrimes**



“THERE ARE TWO KINDS OF BIG COMPANIES, THOSE WHO’VE BEEN HACKED, AND THOSE WHO DON’T KNOW THEY’VE BEEN HACKED.”

- JAMES COMEY, FORMER FBI DIRECTOR

200+

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

80

Days after detection to full recovery

$3 Trillion

Impact of lost productivity and growth

$3.9 Million

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

Remote Work: Challenges and Requirements

Remote work options require:

- A possibility to share data with other users
- An enterprise virtual private network (VPN) solution to connect employees to an organization's network
- Access to business applications
- Trusted work environment to be able to process data securely (HO vs. Shadow IT)
- Security of home computer is usually doubtful

Overview: The list of top 10 mistakes

Misconfigured Network Communication Services

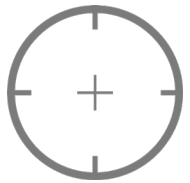
Overly simple passwords and security questions

Lack of network segmentation

Lack of Server Message Block Signing

Allowing unusual code execution

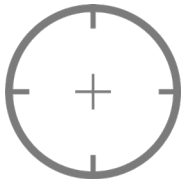
No whitelisting on board



Old protocols or their default settings

Trusting solutions without knowing how to break them

Giving Vendors and Contractors Too Much Access

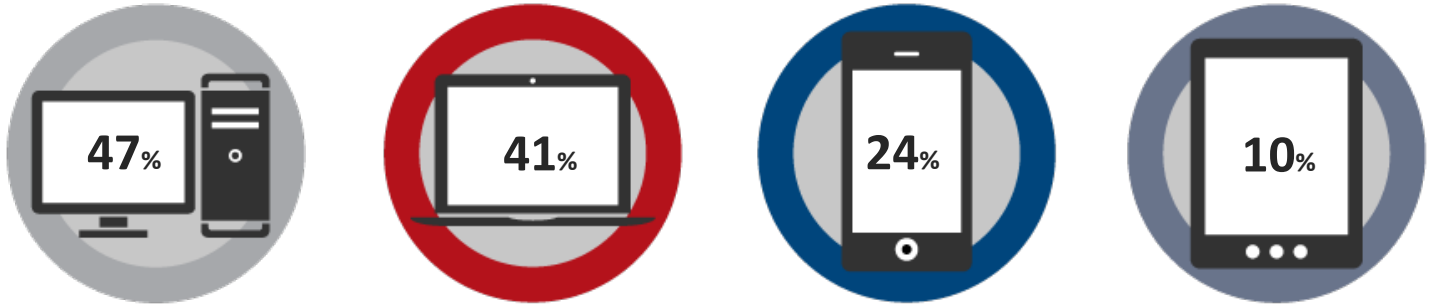


Falling for evil tools

CQURE

Remote work by the numbers

DEVICES THAT STORE AND/OR ACCESS COMPANY INFORMATION



Desktop | Laptop | Smart Phone | Tablet

But have companies provided their employees working from home with additional security awareness training? It's rarely the case…

SOURCE: ESET, Harris Interactive

Remote work by the numbers

IT PROFESSIONALS RESPOND

40%

Said they've experienced an increase in network traffic.

65%

Said they don't have the necessary tools in place to manage non-company issued mobile devices on the network.

27%

Said they are not at all confident.

44%

Said they've seen an increase in help desk requests.

SOURCE: ESET, Harris Interactive

RSAConference2022

Top 10 Mistakes by Administrators About Remote Work – Broader Picture

#1 Misconfigured Network Communication Services

Key learning points:

- Firewall is often misconfigured
- Firewall is a great segmentation tool
- You can allow only certain processes to communicate with the Internet or locally
- No need to know processes to block them, you can operate on the services list
- RDP is not a bad thing as long as it's accessed through VPN

RSAConference2022

DEMO
#1 Misconfigured Network Communication Services

Phishing Little

#2 Overly simple passwords and security questions

Key learning points:

- Passwords are almost always re-used
- There is almost always (ekhm… always) some variant of the company name with some number (year, month etc.)
- It's highly reasonable to check for obvious passwords and continuously deliver security awareness campaigns

RSAConference2022

DEMO
#2 Overly simple passwords and security questions

Bypassing MFA

#3 Lack of network segmentation

Key learning points:

- Network segmentation can be a blessing or a curse.

It also allows:

- a greater control over who has access and to what;
- the rules to be set to limit the traffic;
- limiting the exposure to security incidents;
- the Broadcast Domains to be reduced so that broadcasts do not spread on the entire network.

RSAConference2022

DEMO
#3 Lack of network segmentation

VPN Pivoting

#4 Lack of Server Message Block Signing (or alternative)

Key learning points:

- Set Service Principal Names (SPN) for services to avoid NT LAN Manager (NTLM):
- Reconsider using Kerberos authentication all over (LINK)
- Require SPN target name validation

  Microsoft network server: Server SPN target name validation level
- Reconsider turning on SMB Signing
- Reconsider port filtering
- Reconsider code execution prevention but do not forget that this attack leverages administrative accounts

RSAConference2022

DEMO
#4 Lack of Server Message Block Signing

SMB Relay Attack

#5 Allowing unusual code execution

Key learning points:

- Common file formats containing malware are:
- .exe (Executables, GUI, CUI, and all variants like SCR, CPL etc)
- .dll (Dynamic Link Libraries)
- .vbs (Script files like JS, JSE, VBS, VBE, PS1, PS2, CHM, BAT, COM, CMD etc)
- .docm, .xlsm etc. (Office Macro files)
- .other (LNK, PDF, PIF, etc.)

RSAConference2022

DEMO
#4 Allowing unusual code execution

Unusual code runs

#6 No whitelisting on board

Key learning points:

- Code execution prevention implementation is a must
- PowerShell is an ultimate hacking tool, possible solutions: block it for users, use the Just Enough Administration tool etc.
- Verify where users have write access to, for example in Windows: accesschk.exe –w .\users c:\windows
- Code execution prevention tools can run in the audit mode
- Avoid the default configuration
- Use Attack Surface Reduction Roles

RSAConference2022

DEMO:
#6 No whitelisting on board

Attack Surface Reduction Roles

#7 Old protocols or their default settings

Key learning points:

- SNMPv3 addresses: user-based system for access control, a means to properly authenticate users, and a method for encrypting SNMP traffic between agent and host
- SQL issues – Tabular Data Stream (TDS) provides by default lack of encryption
- ODBC Driver – check if it has a secure networking layer built into it

RSAConference2022

DEMO
#7 Old protocols or their default settings

Clear Text Queries

#8 Trusting solutions without knowing how to break them

Key learning points:

- The best operators won't use a component until they know how it breaks.
- Almost each solution has some ‘backdoor weakness’
- Some antivirus solutions can be stopped by SDDL modification for their services
- Configuration can be monitored by Desired State Configuration (DSC)
- DSC, if not configured properly, will not be able to spot internal service configuration changes

Example: How do I get to the password management portal?

RSAConference2022

DEMO
#8 Trusting solutions without knowing how to break them

Common PKI Pitfalls

#9 Giving Vendors and Contractors Too Much Access

Key learning points:

- gMSA can also be used for the attack
- Service accounts' passwords are in the registry, available online and offline
- A privileged user is someone who has administrative access to critical systems
- Privileged users have sometimes more access than we think (see: SeBackupRead privilege or SeDebugPrivilege)
- Privileged users have possibility to read SYSTEM and SECURITY hives from the registry
- It's important for IT security teams to follow the principle of least privilege

RSAConference2022

DEMO
#9 Giving Vendors and Contractors Too Much Access

Accounts with Issues

#10 Falling for evil tools

Key learning points:

- Even though budgets are increasing, the risk of possessing evil tools is still very high – do we know where these tools come from and what are their security practices?
- Lots of solutions were not created according to the good security practices (backup software running as Domain Admin etc.)
- Each app running in the user's context has access to secrets of other apps – Data Protection API

Summary: The list of top 10 mistakes

Misconfigured Network Communication Services

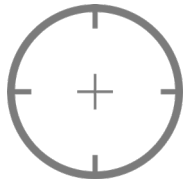
Overly simple passwords and security questions

Lack of network segmentation

Lack of Server Message Block Signing

Allowing unusual code execution

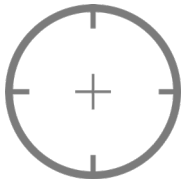
No whitelisting on board



Old protocols or their default settings

Trusting solutions without knowing how to break them

Giving Vendors and Contractors Too Much Access



Falling for evil tools

CQURE

DOWNLOAD THE TOOLS

https://resources.cqureacademy.com/tools/

Username: student

Password: CQUREAcademy#123!

RSAConference2022
San Francisco & Digital | February 7 – 10

TRANSFORM

SESSION ID: **HTA-T08**

Strong Story to Tell: Top 10 Mistakes by Administrators About Remote Work

Paula Januszkiewicz

CEO, Cybersecurity Expert
CQURE Inc.
@PaulaCqure