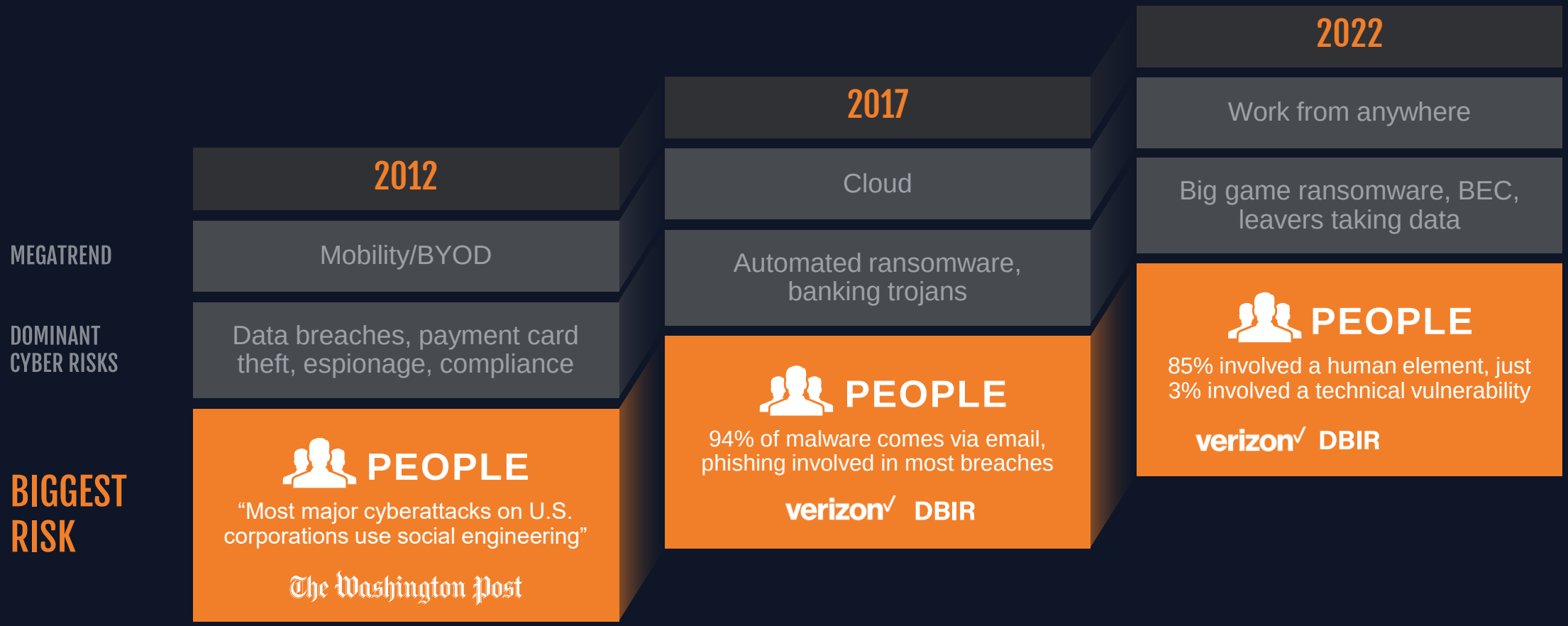
proofpoint®

PROTECTING PEOPLE

DER ÜBERFÄLLIGE WECHSEL ZU PERSONENZENTRIERTER SICHERHEIT: SCHUTZ DER AM HÄUFIGSTEN ANGEGRIFFENEN PERSONEN (VAPs) AM BEISPIEL DER ÖSTERREICHISCHEN POST

September 2022, Rudolf K. Jatschka

DESPITE ALL THE CHANGE, ONE CONSTANT IN CYBERSECURITY



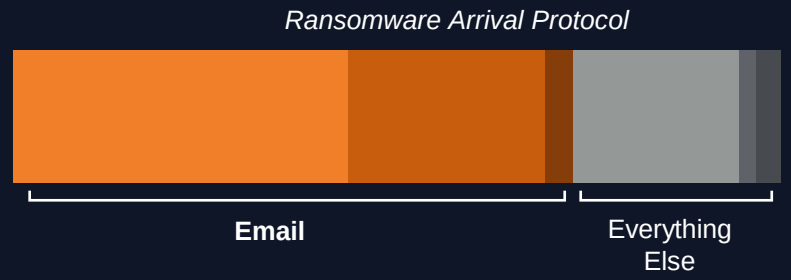
TOP 3 CYBERSECURITY RISKS: ALL PEOPLE-CENTRIC

85%

INVOLVED A HUMAN ELEMENT

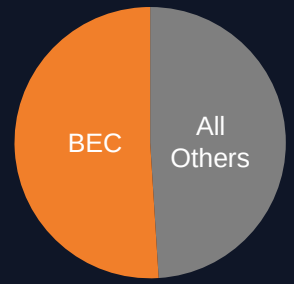
Vast majority of ransomware attacks start with email

— paloalto NETWORKS research



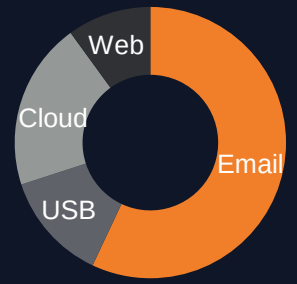
BEC losses exceed all other cybersecurity losses combined

— data for 791,790 incidents

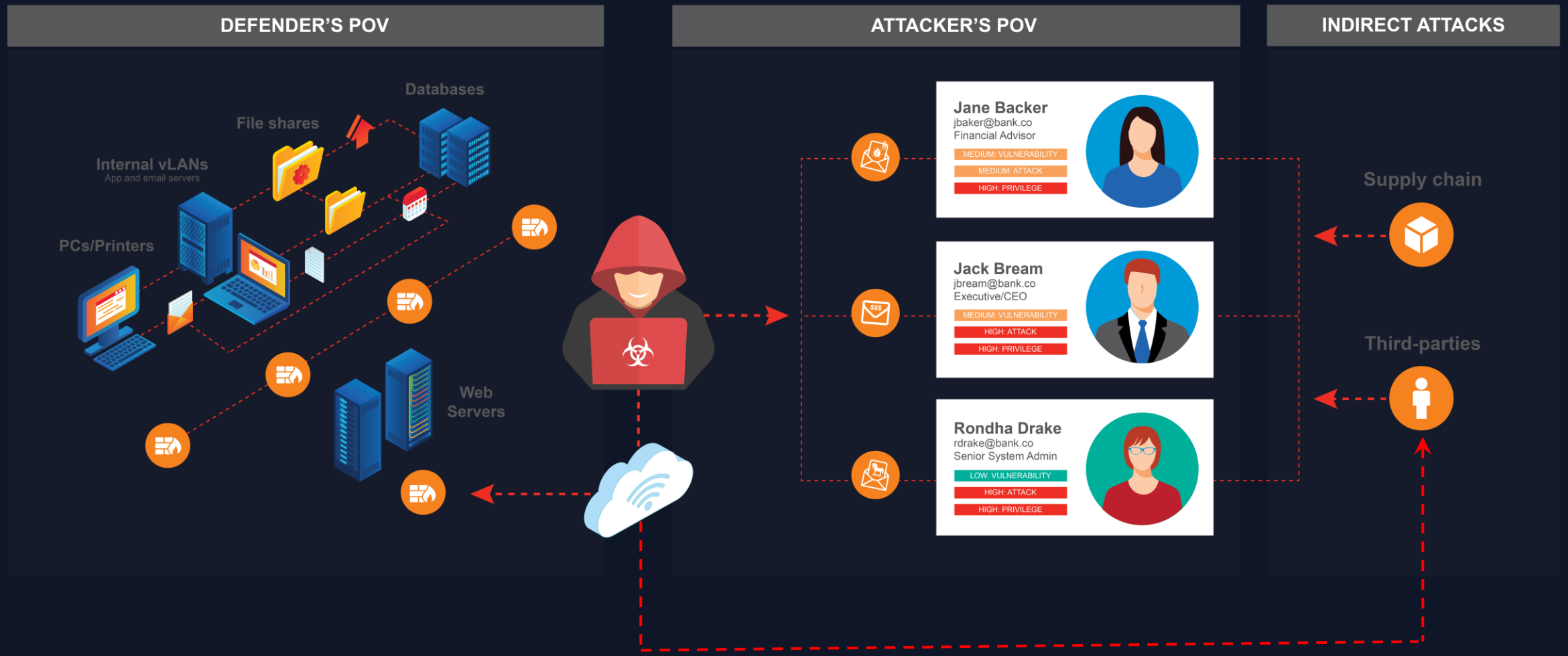


99% of data loss incidents are human-driven

— **proofpoint** data across 3,000 organizations



ATTACKER HAVE CHANGED FOCUS – *HAVE WE?*



proofpoint.

EXPLOITING FAST AND SLOW EMOTIONS

- Exploitative emails try to compel you to take an action based on emotion.
- Where an email elicits an emotional response, the chimp takes over and the chimp cannot be educated!

"Fast" emotions

- Anger and outrage
- Concern, worry and fear
- Excitement
- Confusion
- Greed
- Pride

Examples

- *Rejected expenses/ deactivation alert*
- *COVID infection alert*
- *Missed parcel*
- *Missed bank payment*
- *Nigerian prince scam*
- *Alumni speech*

"Slow" emotions

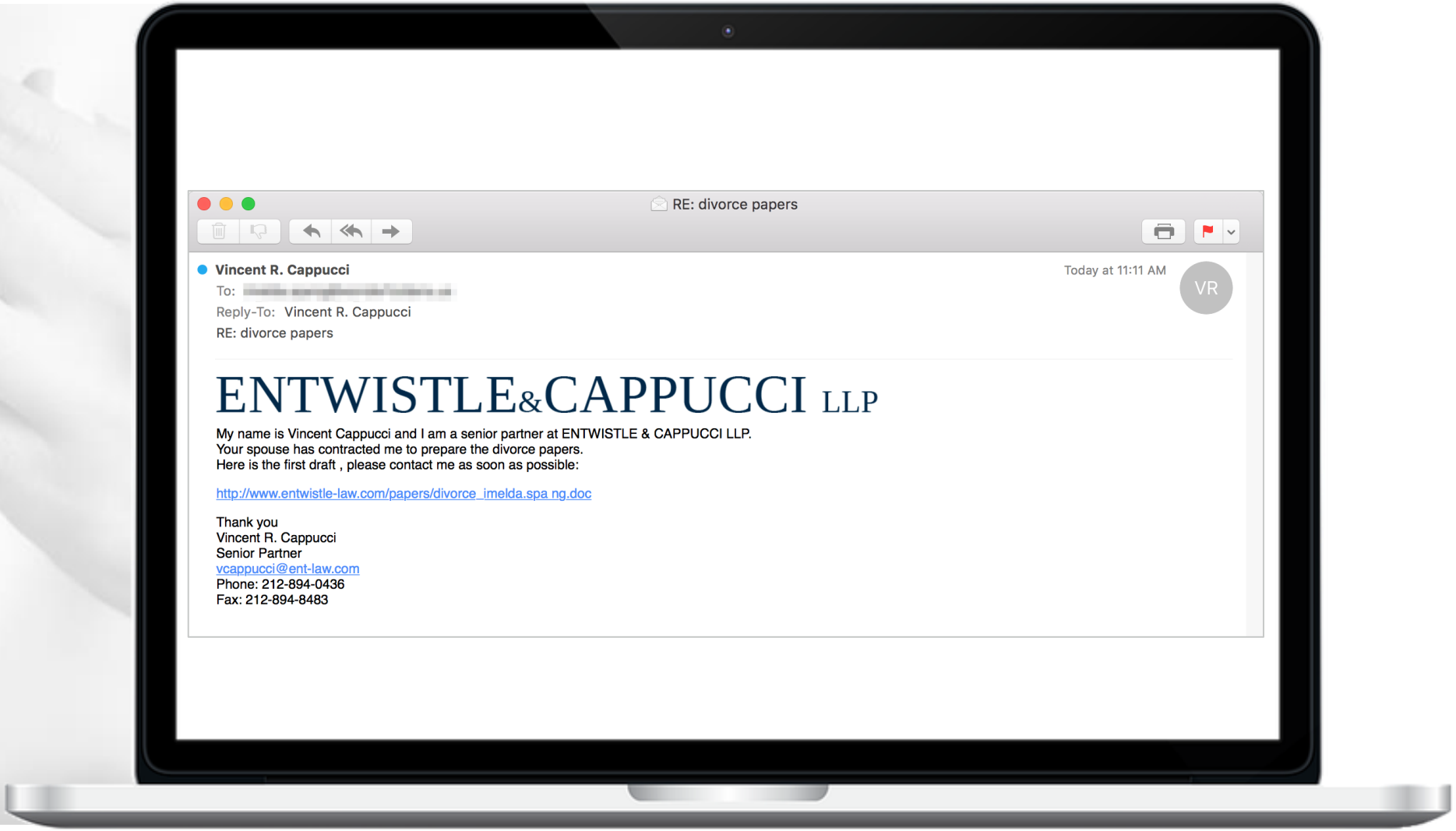
- Love
- Loneliness
- Trust
- Confidence
- Guilt and shame

Examples

- *Romance scams*
- *Fake calls*
- *Sextortion*
- *Look-alike websites*
- *Blackmail*

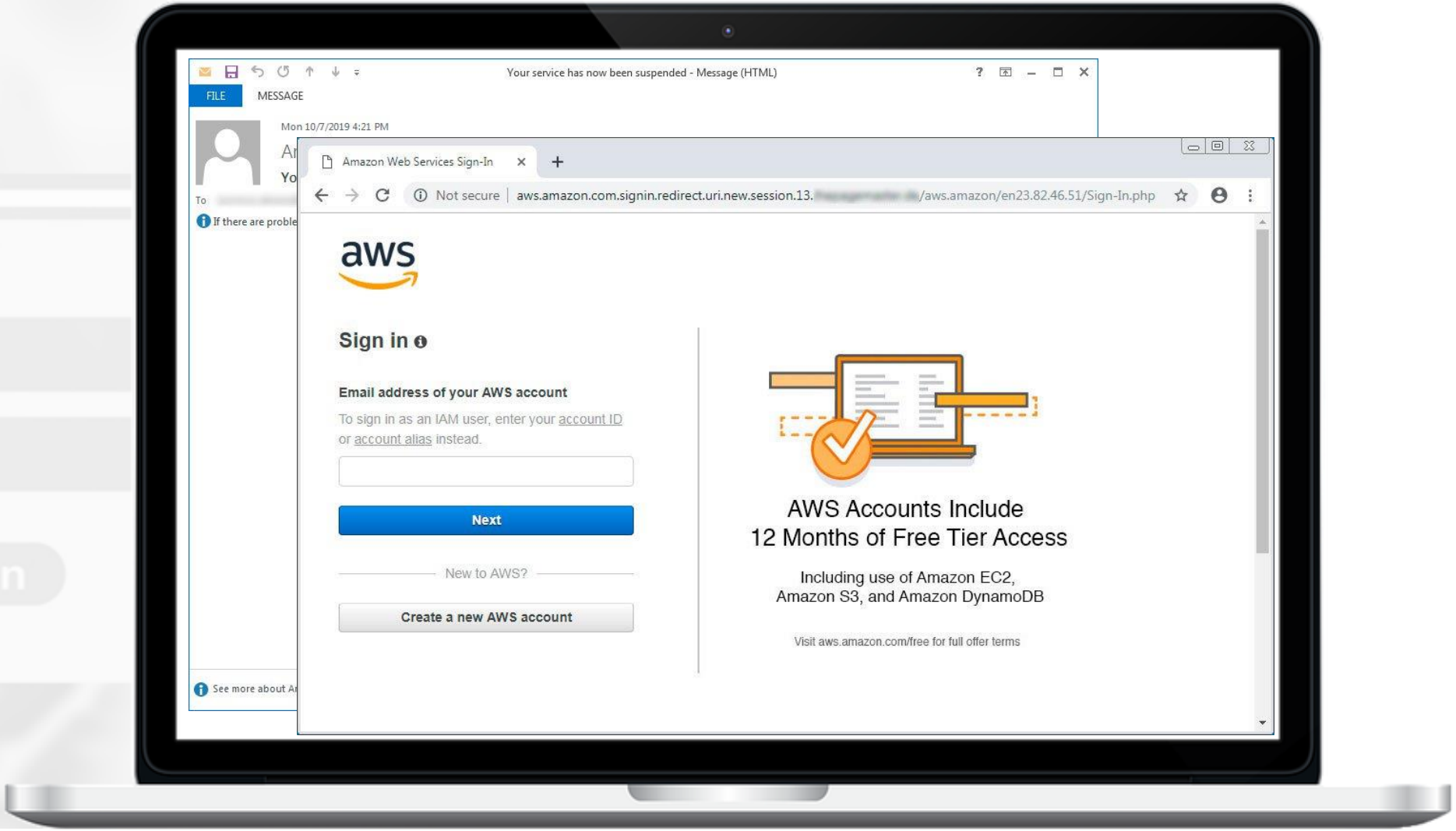
proofpoint.

Social Engineering: Divorce Papers

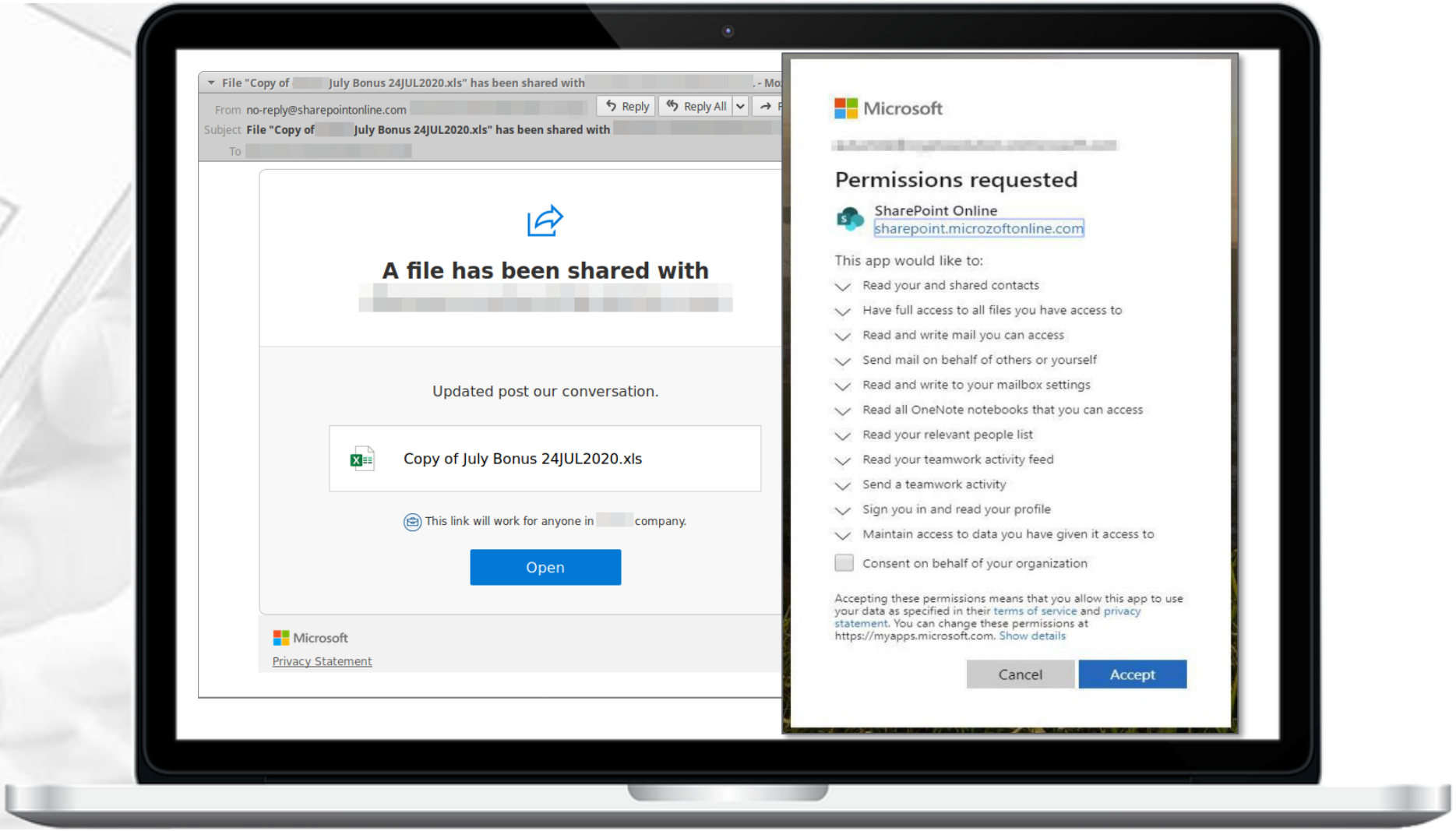


proofpoint.

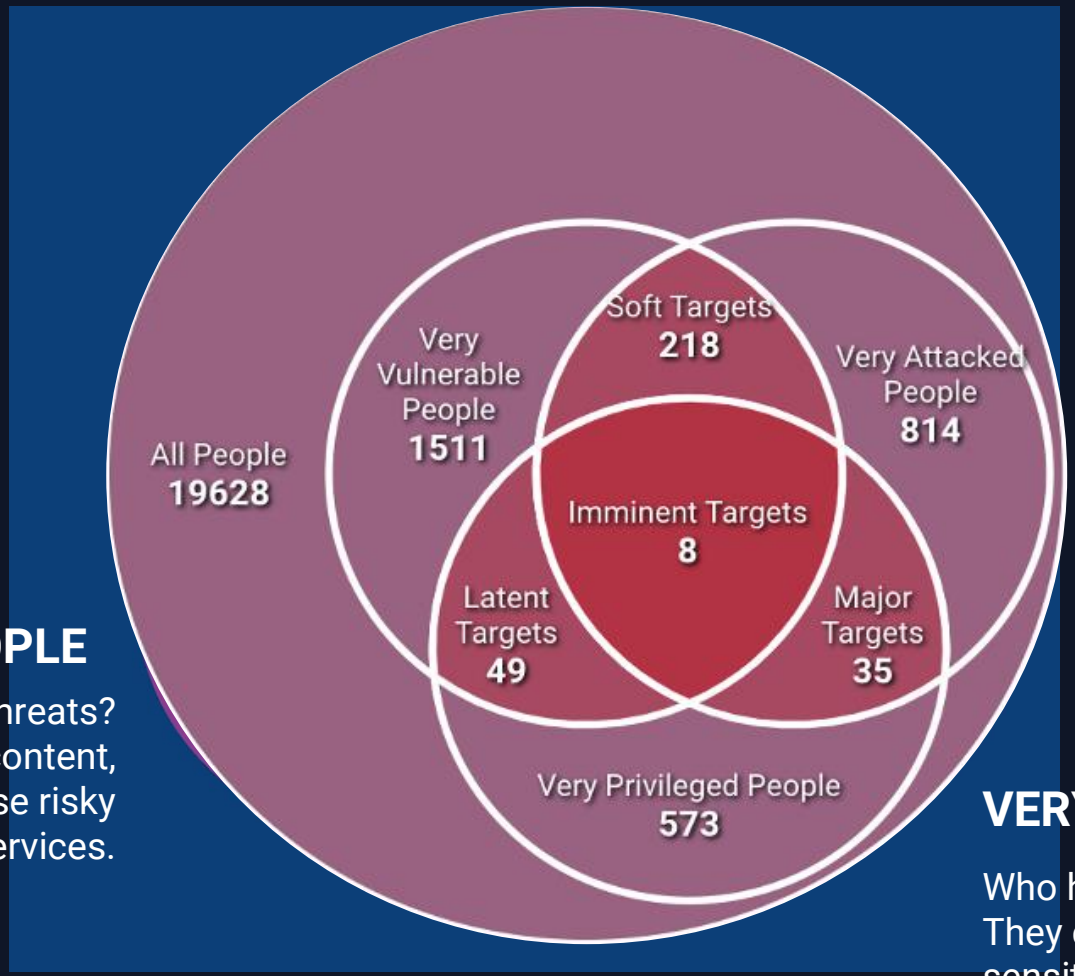
Social Engineering: AWS Cred Theft



Social Engineering: MFA Bypass



ASSESS THE HUMAN ATTACK SURFACE. *WHO* IS YOUR RISK?



VERY VULNERABLE PEOPLE

Who is likely to fall for those threats? They click on malicious content, fail awareness training or use risky devices or cloud services.

VERY ATTACKED PEOPLE

Who gets targeted by serious threats? They receive highly targeted, very sophisticated or high volumes of attacks.

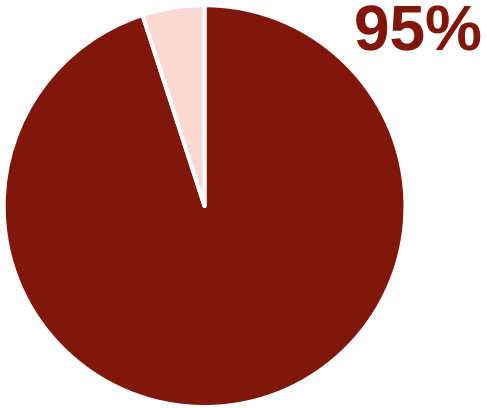
VERY PRIVILEGED PEOPLE

Who has access to sensitive information? They can access critical systems or sensitive data or can be a vector for lateral movement.

proofpoint.

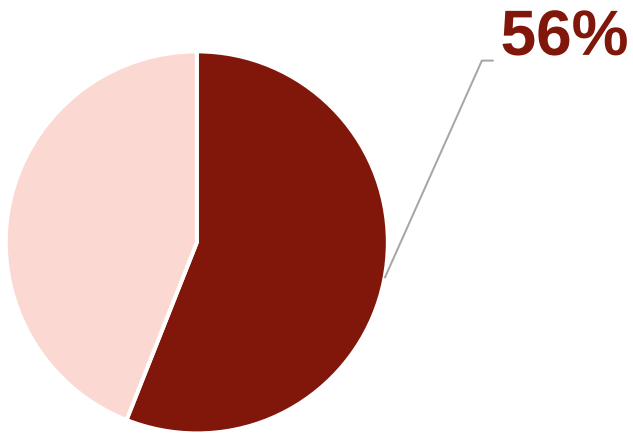
HUMAN FACTOR: PERCEPTION VS. REALITY GAP

The World Economic Forum reports that **95% of cybersecurity issues are traced to human error**…



WORLD ECONOMIC FORUM

…yet **only 56% of global CISOs consider their employees their biggest cyber vulnerability.**



REPORT

2022 Voice of the CISO

proofpoint.

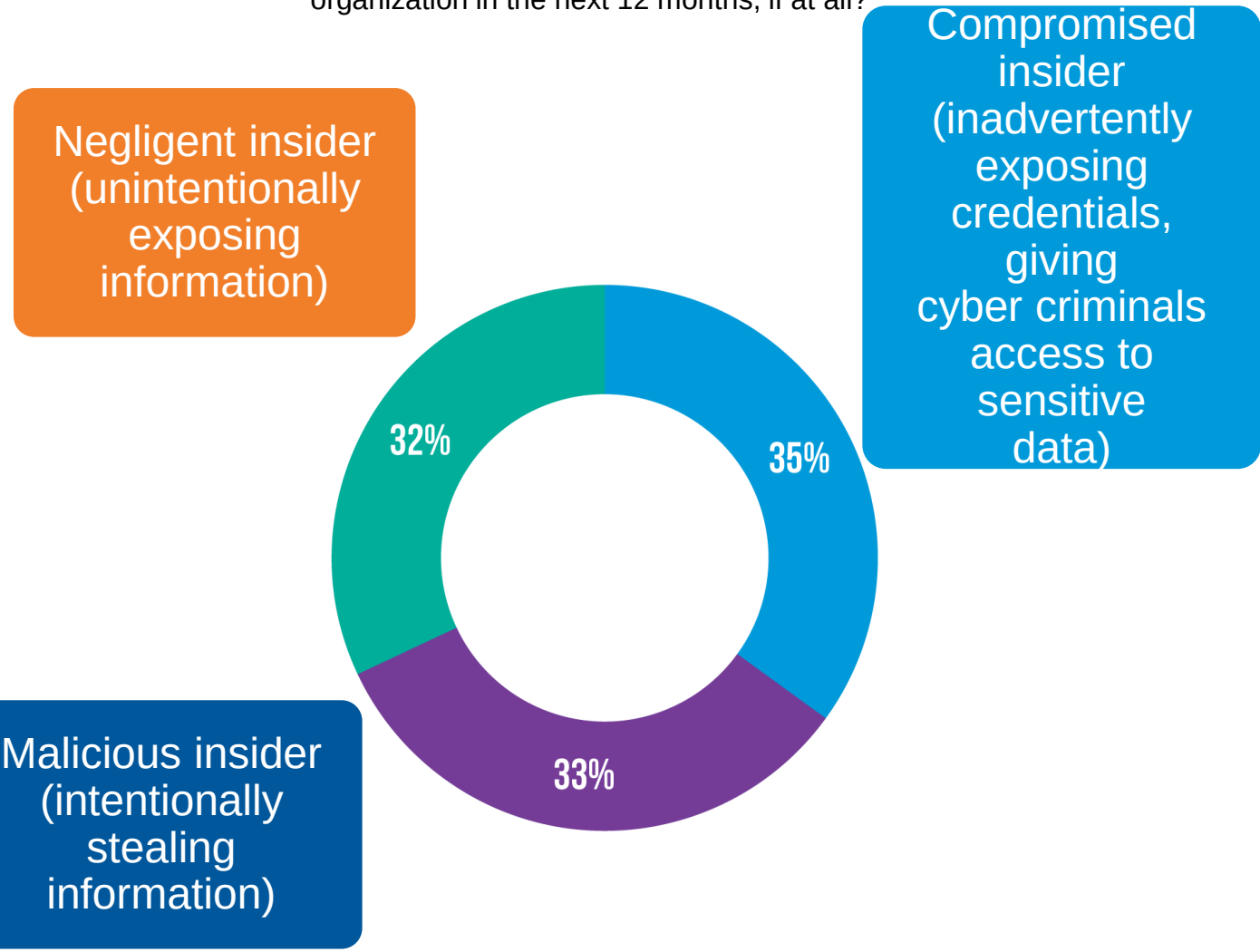
Data Doesn't Walk Away…

Employees leaving a job present another data protection problem for global CISOs.

Proofpoint research shows that **56% of insider threat incidents are driven by negligence** (Proofpoint "2022 State of the Phish" report).

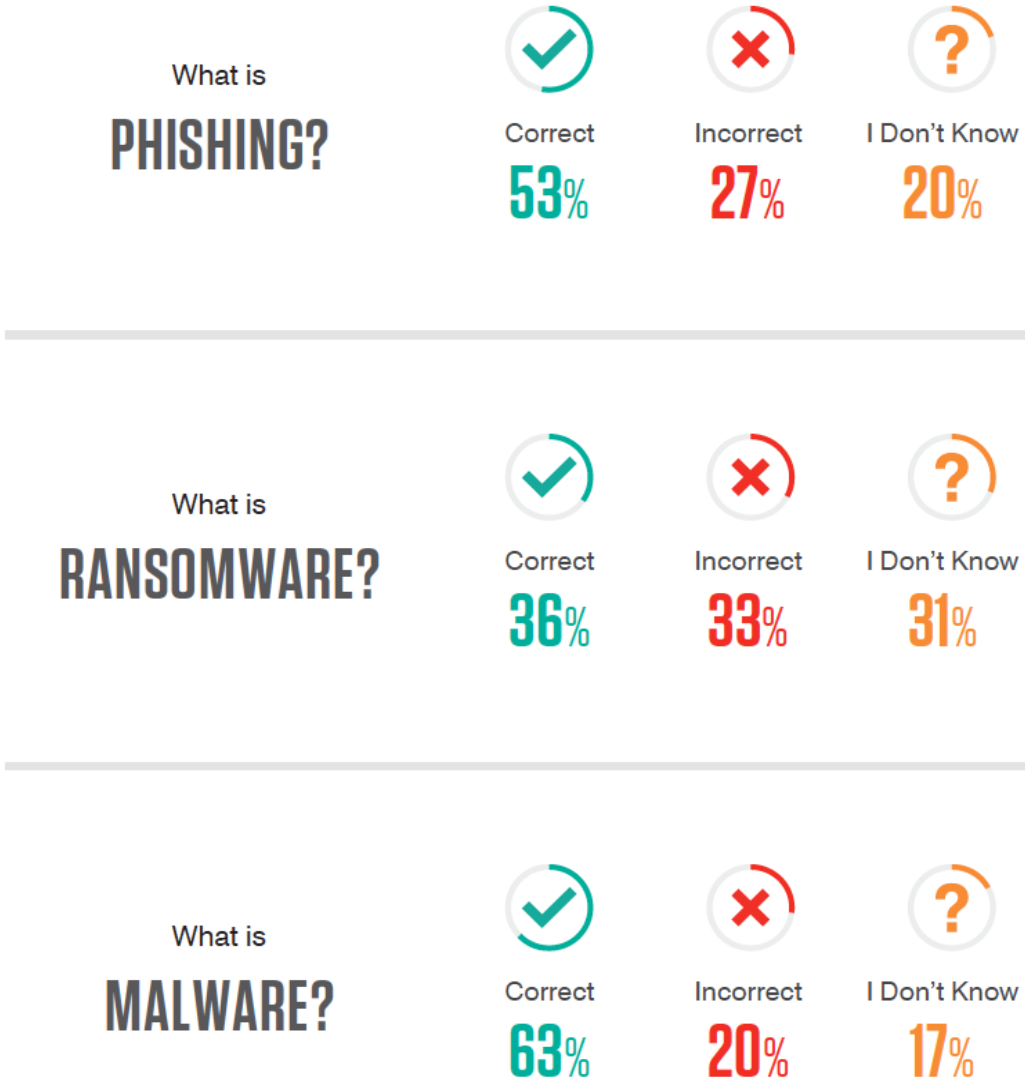
Even so, with more staff outside the office with greater autonomy over their security hygiene, **compromised, negligent and malicious insiders are of equal concern to global CISOs.**

Data loss: in what way do you think your employees are most likely to cause a data breach or exposure in your organization in the next 12 months, if at all?



proofpoint.

End User Knowledge: Prognosis Negative



CYBER COMPONENTS – ACTIVITY

DERSTANDARD

Unterstützung Abo Immosuche Jobsuche

Inland › Bundesländer › Kärnten International Wirtschaft Web Sport Panorama Kultur Etat mehr...

371 Postings

NETZPOLITIK

Grundversorgung weg, Politikerdaten im Netz: Wie Hacker Kärnten lahmlegten

Der Cyberangriff auf Kärnten ist exemplarisch dafür, wie Hacker seit Beginn der Pandemie vorgehen

Muzayen Al-Youssef, Walter Müller

13. Juni 2022, 06:00, 371 Postings

Angriff wie aus Lehrbuch

Alles begann – wie so oft – mit einer E-Mail. Ein Unternehmen habe ein Angebot, hieß es darin. Die Mail sah allen bisherigen E-Mails des vermeintlichen Absenders so ähnlich, dass jemand in der Kärntner Landesverwaltung sie ohne Bedenken öffnete. In Wahrheit handelte es sich um eine Phishing-Mail – eine Nachricht, die bewusst dem Aussehen einer E-Mail des vorgegaukelten Versenders nachempfunden wird. Tatsächlich ist sie mit einer Schadsoftware infiziert, die das Ziel hat, Zugriff auf das IT-System zu erlangen.

Für den Angriff verantwortlich zeigte sich die Hackergruppe Black Cat. Kärnten ist bei weitem nicht ihr einziges Opfer: Auf ihrer Webseite prahlt die Gruppe, die wohl aus Russland stammt, etwa mit Angriffen auf andere Lokalregierungen weltweit sowie auf Konzerne aus verschiedensten Branchen. Ihr Geschäft mit Erpressungssoftware ist während der Pandemie immer lukrativer geworden. Und mit einem unbedachten Klick der Beamten war den Hackern der erste Schritt gelungen. Sie drangen in die IT-Systeme des Landes ein, verschlüsselten sie – und kommunizierten ihre Motive: Sie wollen Geld, sonst bleibt der Landesverwaltung künftig der Zugriff verwehrt.

ERFAHRUNGEN IN DER ZUSAMMENARBEIT MIT PROOFPOINT

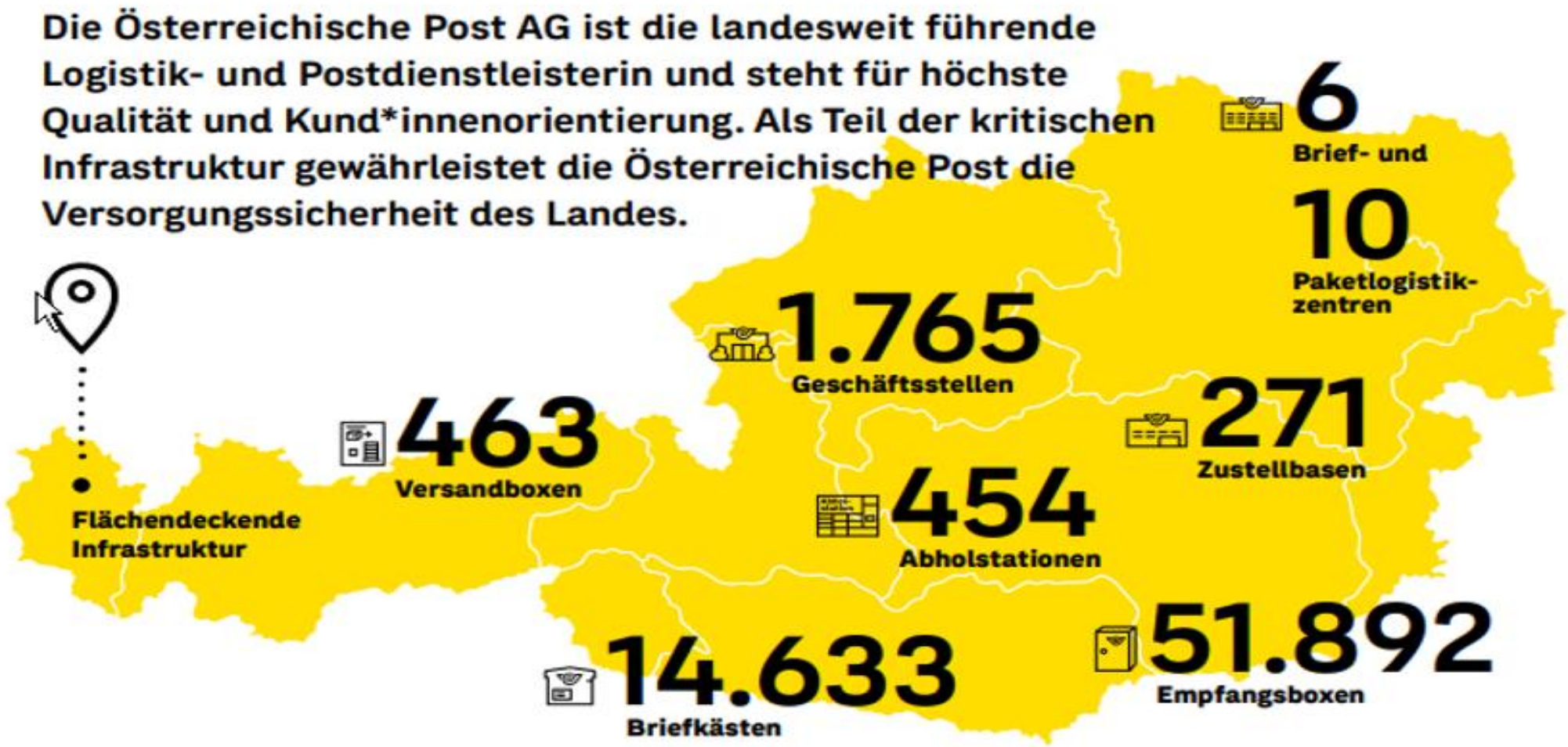
Ing. Harald Ladislav
Konzern-IT / Corporate Systems
07. September 2022

AGENDA

- Die Österreichische Post in Zahlen, Daten & Fakten
- Österreichische Post & ProofPoint

DIE ÖSTERREICHISCHE POST IN ZAHLEN, DATEN & FAKTEN

DIE ÖSTERREICHISCHE POST IN ZAHLEN, DATEN & FAKTEN



ÖSTERREICHISCHE POST IM ÜBERBLICK

Brief & Werbepost

- Briefpost
- Werbesendungen
- Zeitungen und Magazine

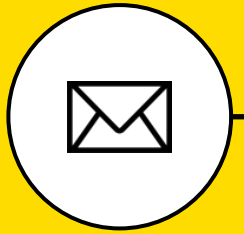
Paket & Logistik

- Pakete und Express
- Fulfillment und Werttransport
- E-Commerce Services

Filiale & Bank

- Filial- und Finanz-dienstleistungen
- Kund*innenservices

ZUSAMMENARBEIT DER ÖSTERREICHISCHEN POST & PROOFPOINT



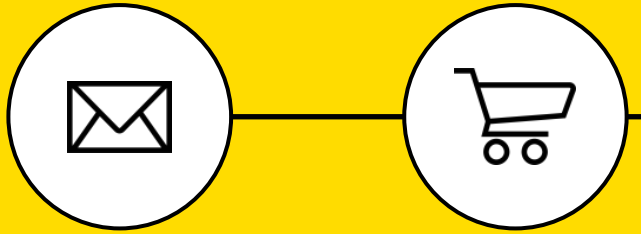
2013

Erste Ansätze zu Cloud First & Office Online

ZUSAMMENARBEIT DER ÖSTERREICHISCHEN POST & PROOFPOINT

Brightmail → Proofpoint

2016



2013

Erste Ansätze zu Cloud First & Office Online

ZUSAMMENARBEIT DER ÖSTERREICHISCHEN POST & PROOFPOINT

Brightmail → Proofpoint

2016

2013

Erste Ansätze zu Cloud First & Office Online

2017

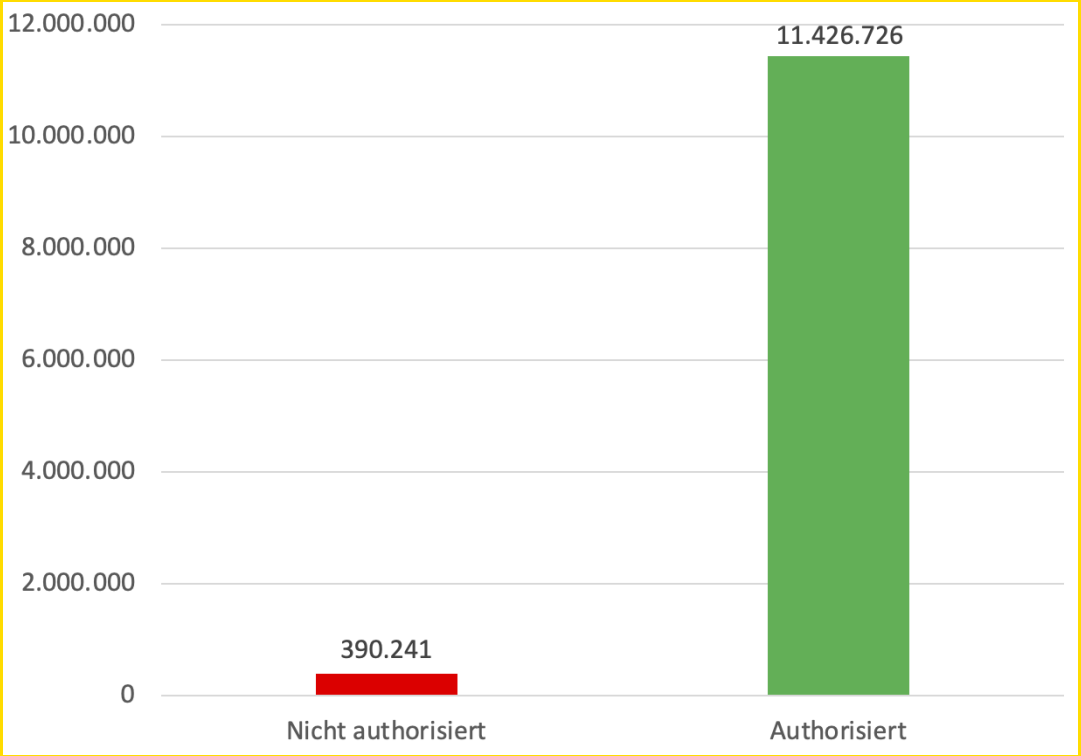
TRAP und EFD

MIT DMARC KANN DIE ECHTHEIT UND LEGITIMATION DES ABSENDERS ÜBERPRÜFT WERDEN

DMARC Prüfung:
fail

Email-Authentifizierung der Domäne:

post.at



Zeitraum: 01.01.2022 – 10.06.2022

DMARC Prüfung:
pass

ZUSAMMENARBEIT DER ÖSTERREICHISCHEN POST & PROOFPOINT

2013

Erste Ansätze zu Cloud First & Office Online

2016

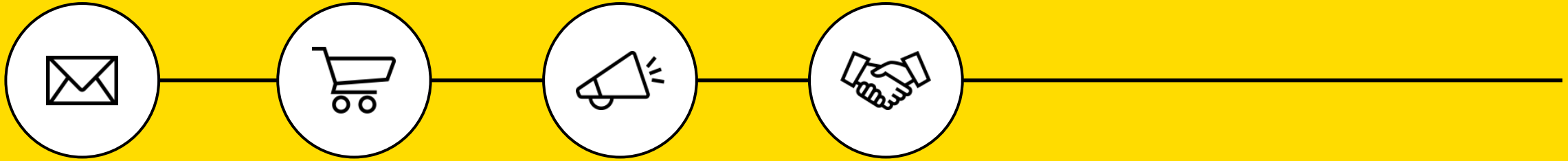
Brightmail → Proofpoint

2017

TRAP und EFD

2018 & 2019

Migration der Produkte in die Proofpoint Cloud



ZUSAMMENARBEIT DER ÖSTERREICHISCHEN POST & PROOFPOINT

2013

Erste Ansätze zu Cloud First & Office Online

2016

Brightmail → Proofpoint

2017

TRAP und EFD

2018 & 2019

Migration der Produkte in die Proofpoint Cloud

2021

IMD

ZUSAMMENARBEIT DER ÖSTERREICHISCHEN POST & PROOFPOINT

2013

Erste Ansätze zu Cloud First & Office Online

2016

Brightmail → Proofpoint

2017

TRAP und EFD

2018 & 2019

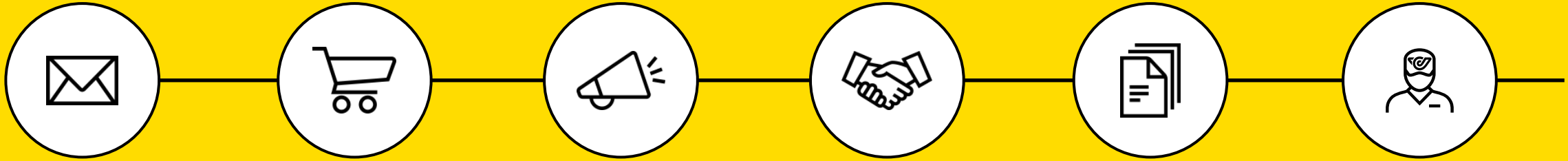
Migration der Produkte in die Proofpoint Cloud

2021

IMD

2022

TRIC, hosted SPF



ZUSAMMENARBEIT MIT PROOFPOINT

- Direkter Kontakt zum Hersteller
- Sehr hohe Kontinuität der technischen Ansprechpartner*innen bei Proofpoint
- Produkte entwickeln sich laufend weiter
- keine Punkt- oder Insellösungen, sondern ein Zusammenspiel der einzelnen Produkte zu einer integrierten Plattform

HERZLICHEN DANK.


proofpoint®
Thank you!