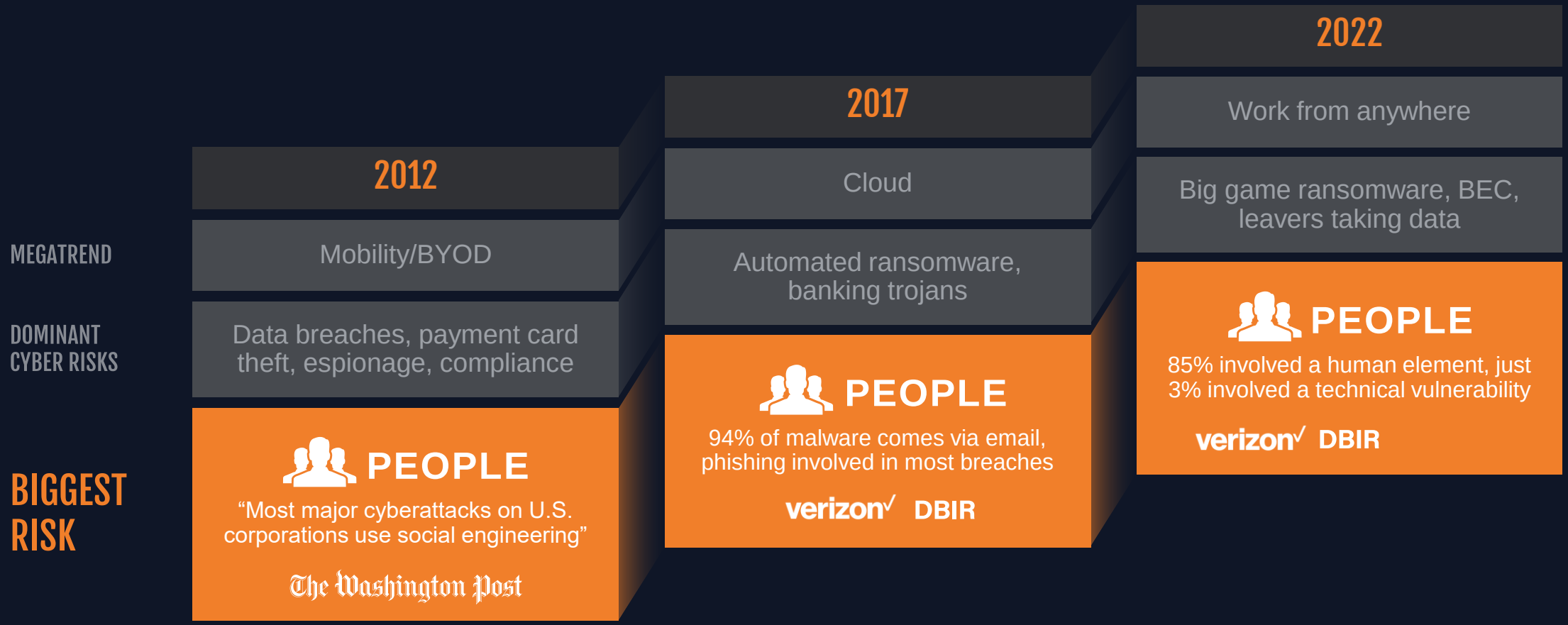
proofpoint®

Defend Data, Investigate Insiders

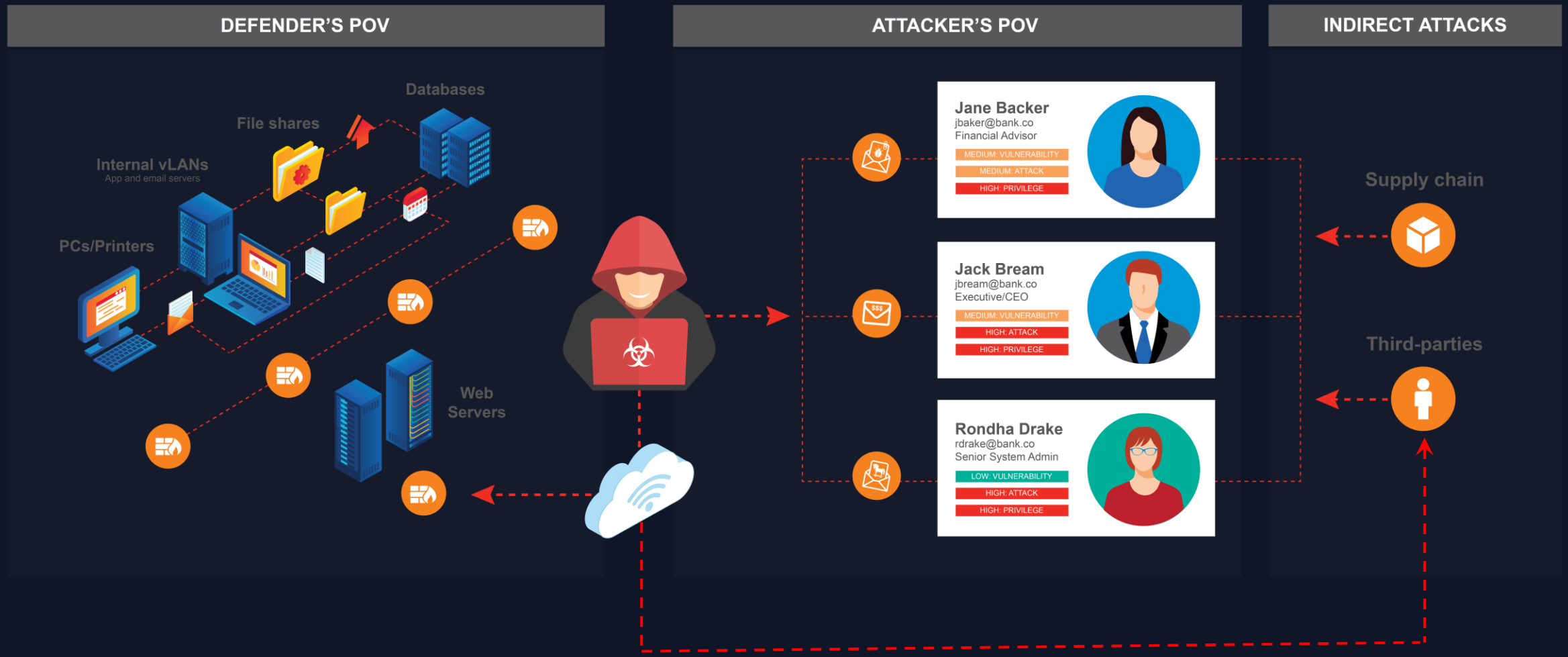
A People-Centric Approach to Information Security

Oktober 2022, Rudolf K. Jatschka

DESPITE ALL THE CHANGE, ONE CONSTANT IN CYBERSECURITY



ATTACKER HAVE CHANGED FOCUS – *HAVE WE?*



proofpoint.

Our Mission: Protect People \ Defend Data

Protect People:

Email Security and Fraud Defense
Cloud Security
Security Awareness

Defend Data:

Data Loss Prevention
Insider Threat
Intelligent Compliance

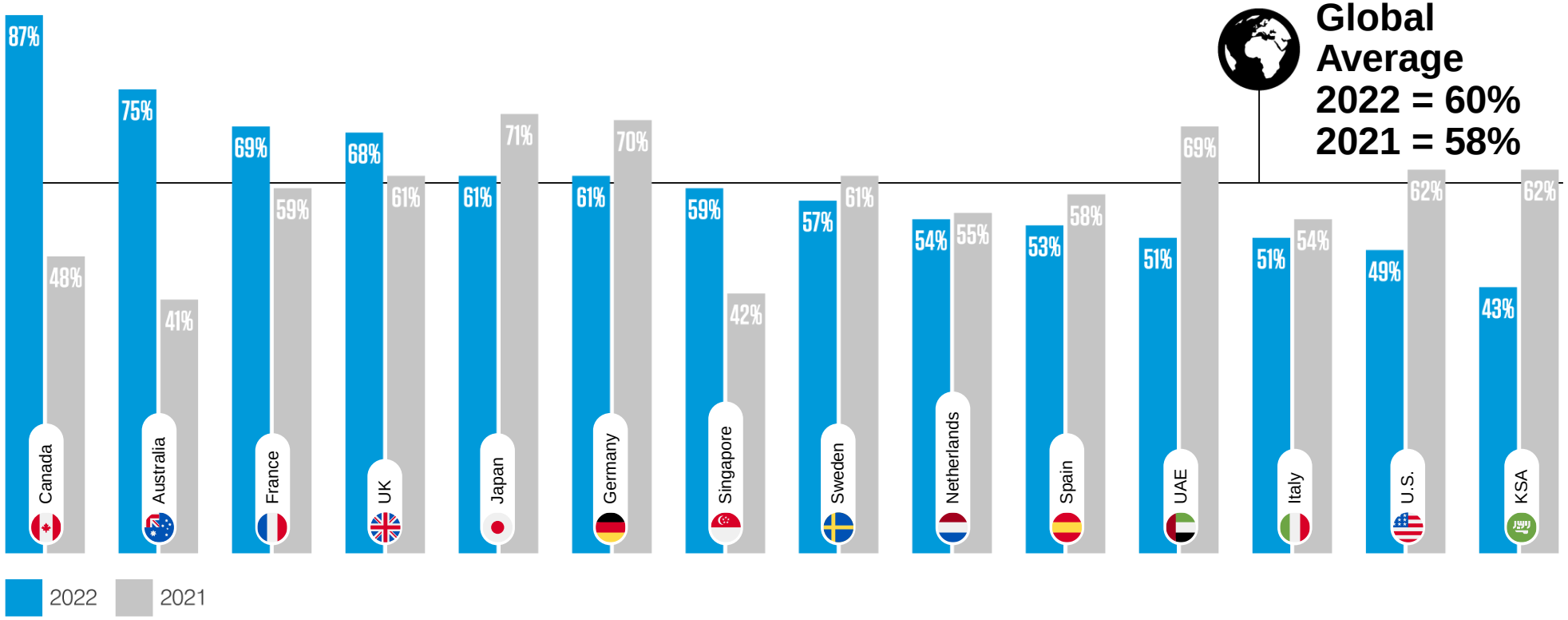
Defending Data is a natural extension of our People-Centric Security approach

proofpoint.

People As the New Perimeter

With two years of remote working under their belt, **most CISOs believe that employees understand the role they play in protecting their organizations** against cyber threats.

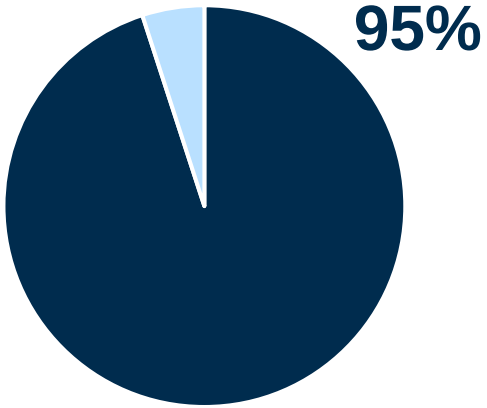
Percentage of CISOs who believe employees understand their role in protecting the organization against cyber threats



proofpoint.

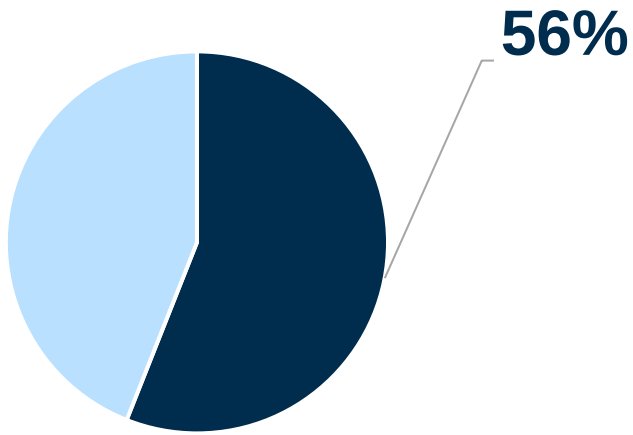
Human Factor: Perception vs. Reality Gap

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.

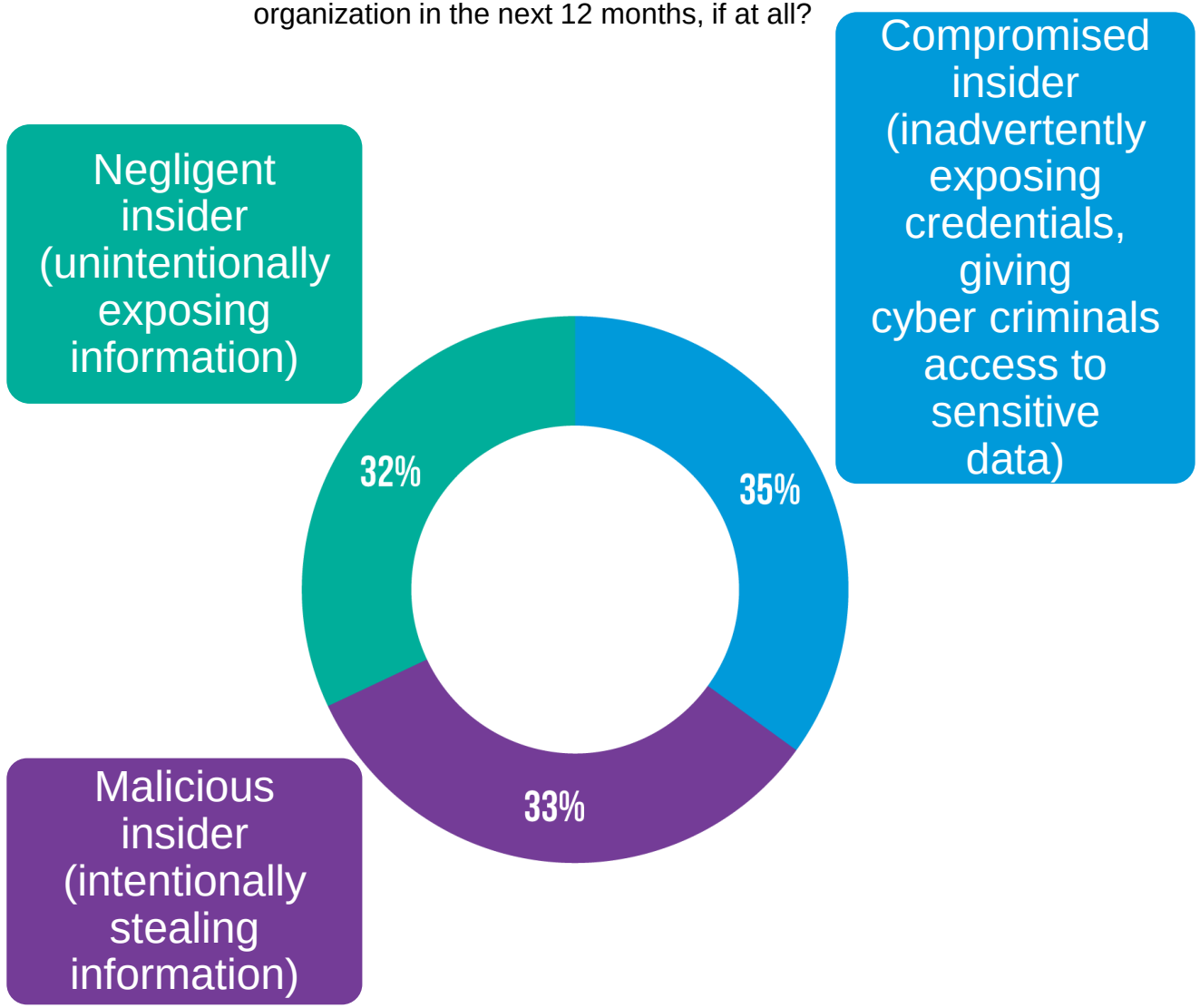
Data Doesn't Walk Away…

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).

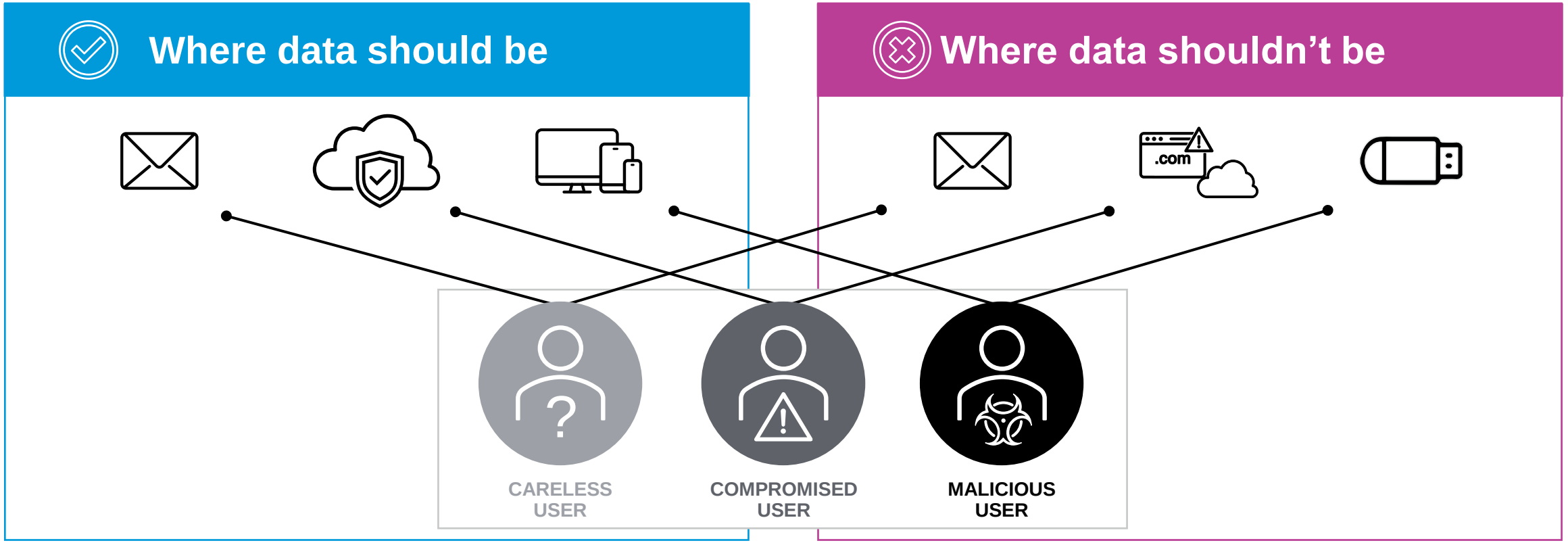
Even so, with more staff outside the office with greater autonomy over their security hygiene, **compromised, negligent and malicious insiders are of equal concern to global CISOs.**

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.

Data Doesn't Lose Itself
There's Always a Person Behind a Loss



Data is lost due to careless, **compromised,** or **malicious** users.

proofpoint.

What Is Needed In the New World to Understand People

The Old Information Protection World

*Is there **sensitive** or **regulated** data?*

The New Information Protection World

*Is there unusual user **activity**, **intent**, and **access** context?*

*Is there linkage to **compromised** accounts, **phished** users, **malware, OAuth abuse**?*

Meet Evan… She Plans to Leave the Company

- Has access to company intellectual property files
- Working remotely from home
- Going to a competitor
- Feels entitled to the intellectual property she creates

Evan has access to research data in cloud storage and decides to steal files

While working from home, downloads files to work laptop

Installs personal Google Drive on work laptop

Copies all work files to personal Google Drive

Proofpoint detects Insider Threat situation and alerts security team; triggers investigation

Evan returns fake dummy laptop to evade investigation

Security team has forensics from Proofpoint to create legal case

proofpoint.

Meet Chandler… He Is Not Careful with Company Data

- Works from anywhere
- Uses the easiest tool for the job
- Careless with the sensitive data he accesses
- Has access to PII and PHI

Chandler emails PII.xls through corporate email

Proofpoint quarantines the email based on policy

He uploads it to his company's cloud share

Sets share permission to "Public Link"

Proofpoint detects broad sharing on sensitive data; automates downgrade of sharing scope; alerts security team

He tries to send it via personal email

Proofpoint blocks the file upload due to sensitive content

proofpoint.

Meet Renda… She Is Highly Targeted by Phishing Attacks

- Remote worker, relies on cloud apps
- PII, SSNs, payroll data, intellectual property secrets
- Clicks links
- Identified as a Very Attacked Person (VAP)

Renda receives an email with a URL, which turns into a phishing page

She clicks the URL, gives her Microsoft 365 credentials

Proofpoint retracts the malicious email from her inbox

“Renda” logs into Microsoft 365

Proofpoint alerts the security team; [phished + suspicious login]

“Renda” attempts to download PII.xls from M365

Proofpoint alerts security team; blocks download for VAPs per policy

Proofpoint force password reset, revokes session

proofpoint.

One Console, One Agent, One Cloud-Native Platform

Information and Cloud Security Platform

Email DLP | Endpoint DLP | Insider Threat Management | Intelligent Classification

CASB | Browser Isolation | Web Security | Secure Access

okta SailPoint Ecosystem

splunk> servicenow Ecosystem

paloalto zscaler Ecosystem

CROWDSTRIKE SentinelOne Ecosystem

Migration Services | **Managed Services**

Alert Management and Investigations | Policy uniformity | Privacy controls | Reporting and Analytics

proofpoint.