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.

The Problem

85% of breaches involve the human element
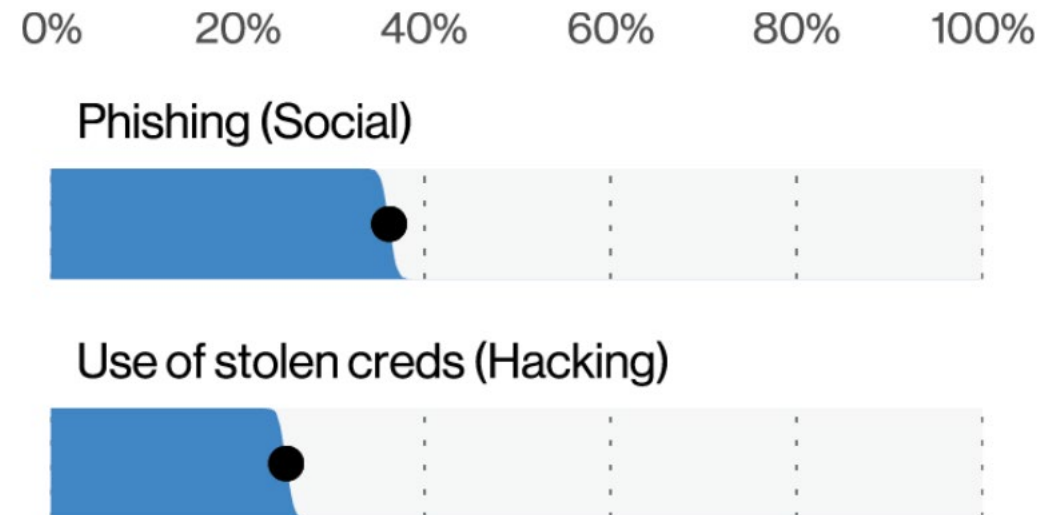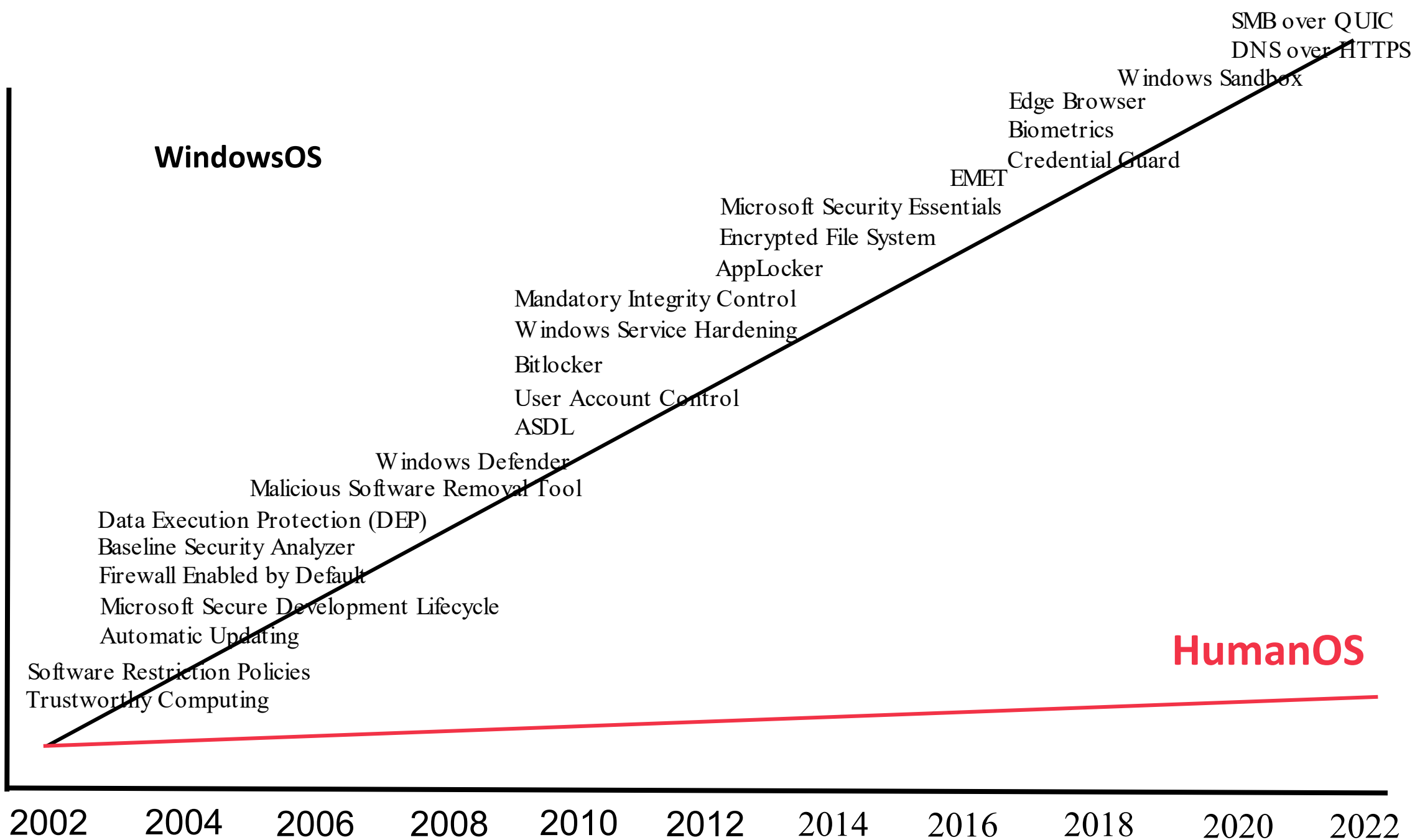
DBIR
2021 Data Breach Investigations Report

verizon✓

| | 0% | 20% | 40% | 60% | 80% | 100% |

Phishing (Social)

Use of stolen creds (Hacking)

Security Controls (y-axis) vs years 2002–2022 (x-axis)

WindowsOS

- SMB over QUIC
- DNS over HTTPS
- Windows Sandbox
- Edge Browser
- Biometrics
- Credential Guard
- EMET
- Microsoft Security Essentials
- Encrypted File System
- AppLocker
- Mandatory Integrity Control
- Windows Service Hardening
- Bitlocker
- User Account Control
- ASDL
- Windows Defender
- Malicious Software Removal Tool
- Data Execution Protection (DEP)
- Baseline Security Analyzer
- Firewall Enabled by Default
- Microsoft Secure Development Lifecycle
- Automatic Updating
- Software Restriction Policies
- Trustworthy Computing

HumanOS

People are not the weakest link - they are the primary attack vector

THE SOLUTION

Manage human risk by changing human behavior

Security Awareness Maturity Model

NON-EXISTENT

COMPLIANCE FOCUSED

PROMOTING AWARENESS & BEHAVIOR CHANGE

LONG TERM SUSTAINMENT & CULTURE CHANGE

METRICS FRAMEWORK

SANS SECURITY AWARENESS

3 Steps to Managing Human Risk

What Are My Top Human Risks & the Behaviors that Manage Those Risks?

Engage, Motivate & Train

Security Awareness Program

Am I Effectively Changing Those Behaviors?
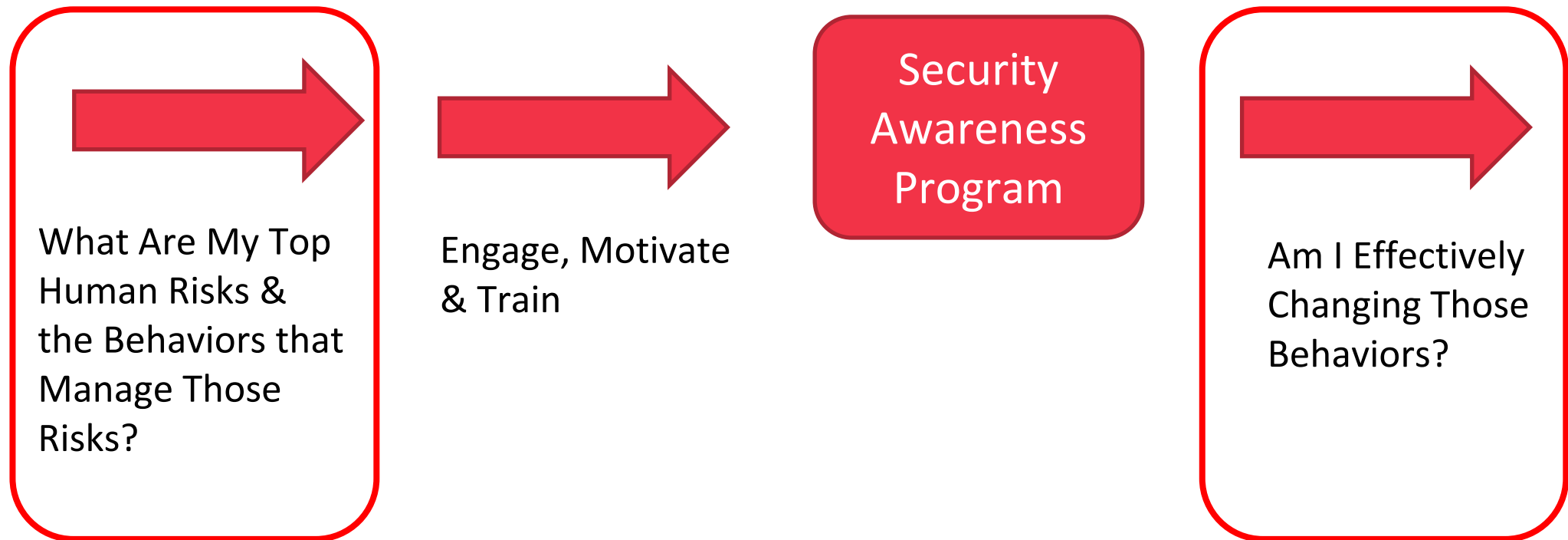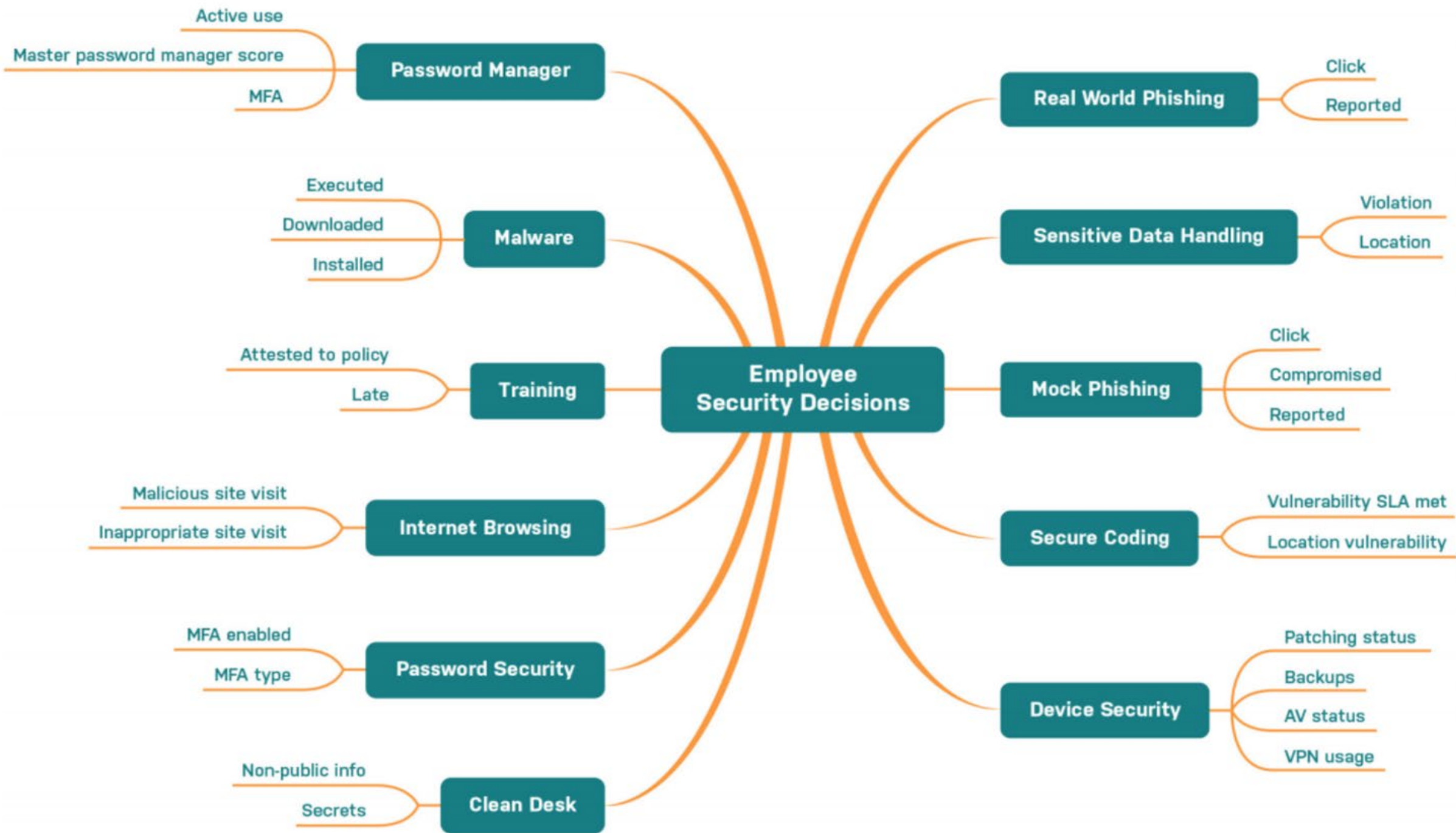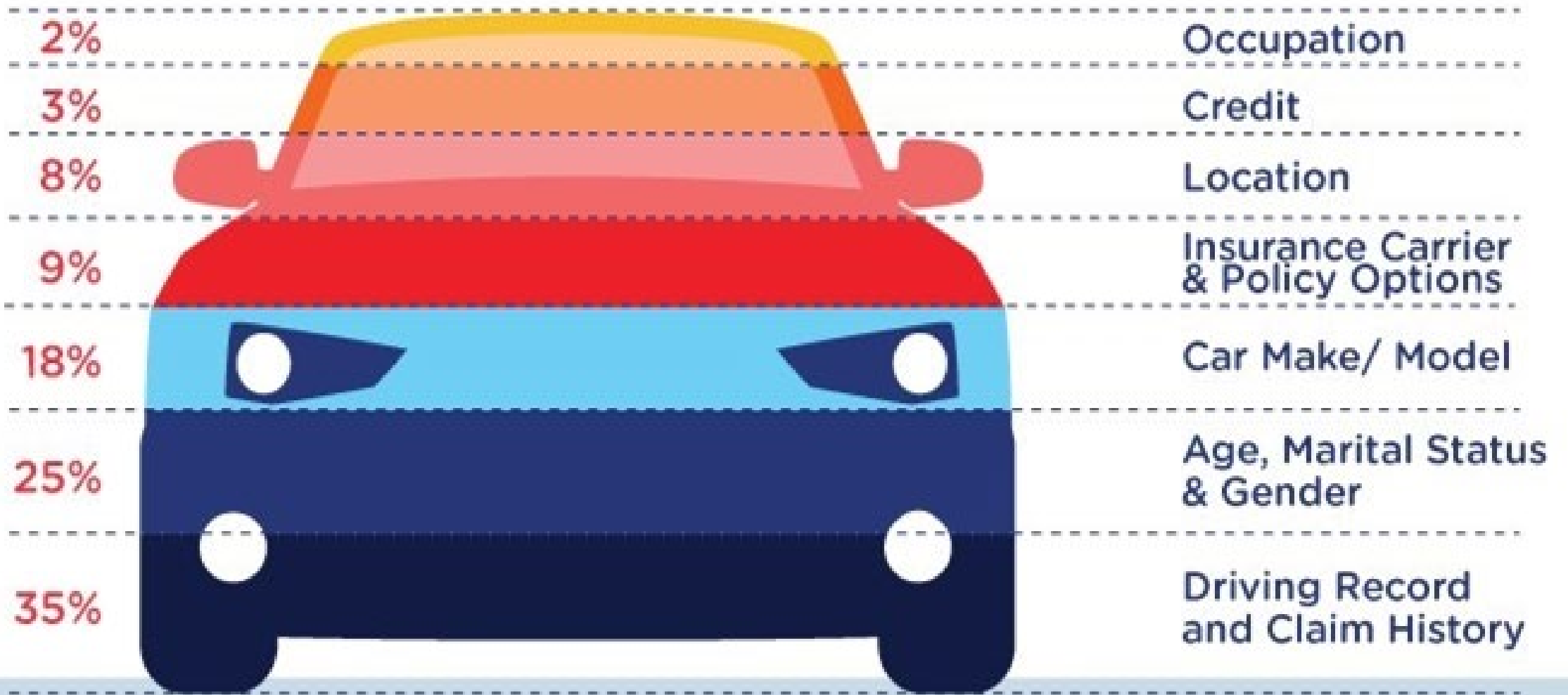
What If We Could Bring Together Seemingly Unrelated, Readily Available Data To Create **A Picture Of Human Risk?**

Employee Security Decisions

- **Password Manager**
  - Active use
  - Master password manager score
  - MFA
- **Malware**
  - Executed
  - Downloaded
  - Installed
- **Training**
  - Attested to policy
  - Late
- **Internet Browsing**
  - Malicious site visit
  - Inappropriate site visit
- **Password Security**
  - MFA enabled
  - MFA type
- **Clean Desk**
  - Non-public info
  - Secrets
- **Real World Phishing**
  - Click
  - Reported
- **Sensitive Data Handling**
  - Violation
  - Location
- **Mock Phishing**
  - Click
  - Compromised
  - Reported
- **Secure Coding**
  - Vulnerability SLA met
  - Location vulnerability
- **Device Security**
  - Patching status
  - Backups
  - AV status
  - VPN usage

12

What Impacts Car Insurance Rates?

- 2% — Occupation
- 3% — Credit
- 8% — Location
- 9% — Insurance Carrier & Policy Options
- 18% — Car Make/ Model
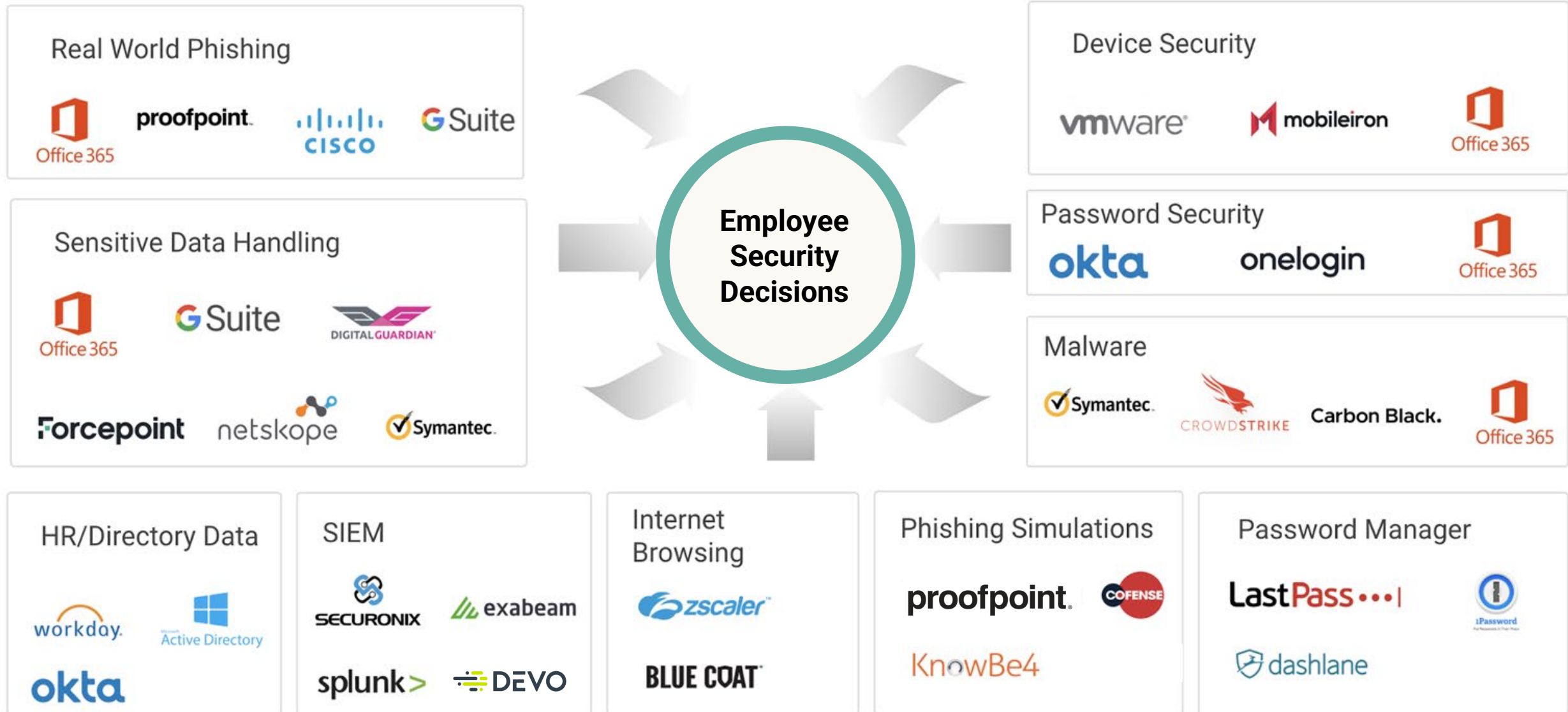- 25% — Age, Marital Status & Gender
- 35% — Driving Record and Claim History

Pull data from tools you already have

What Impacts Credit Scores?

Five main factors that affect your credit score are:

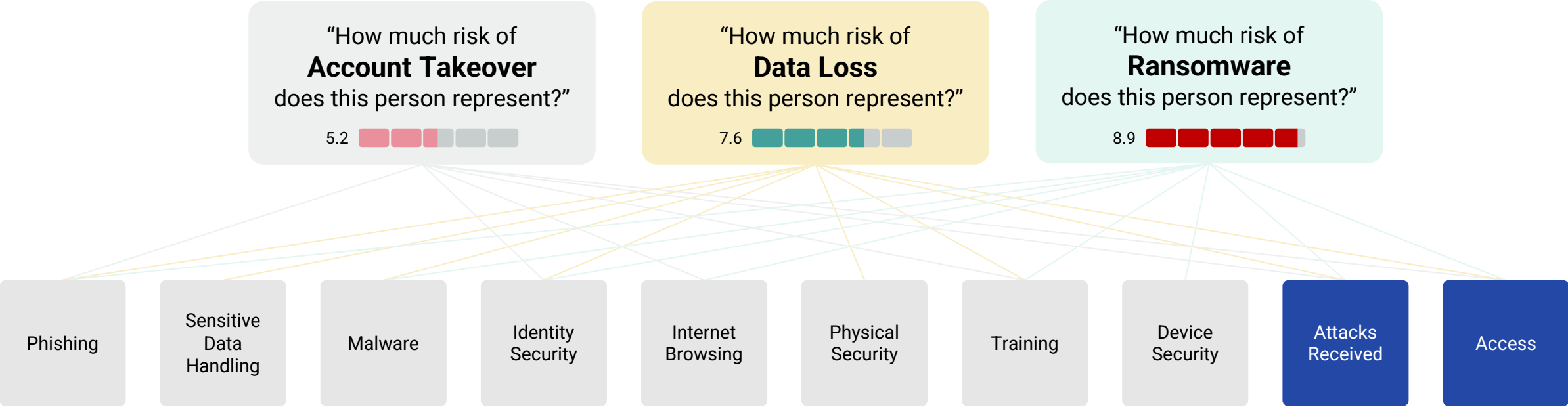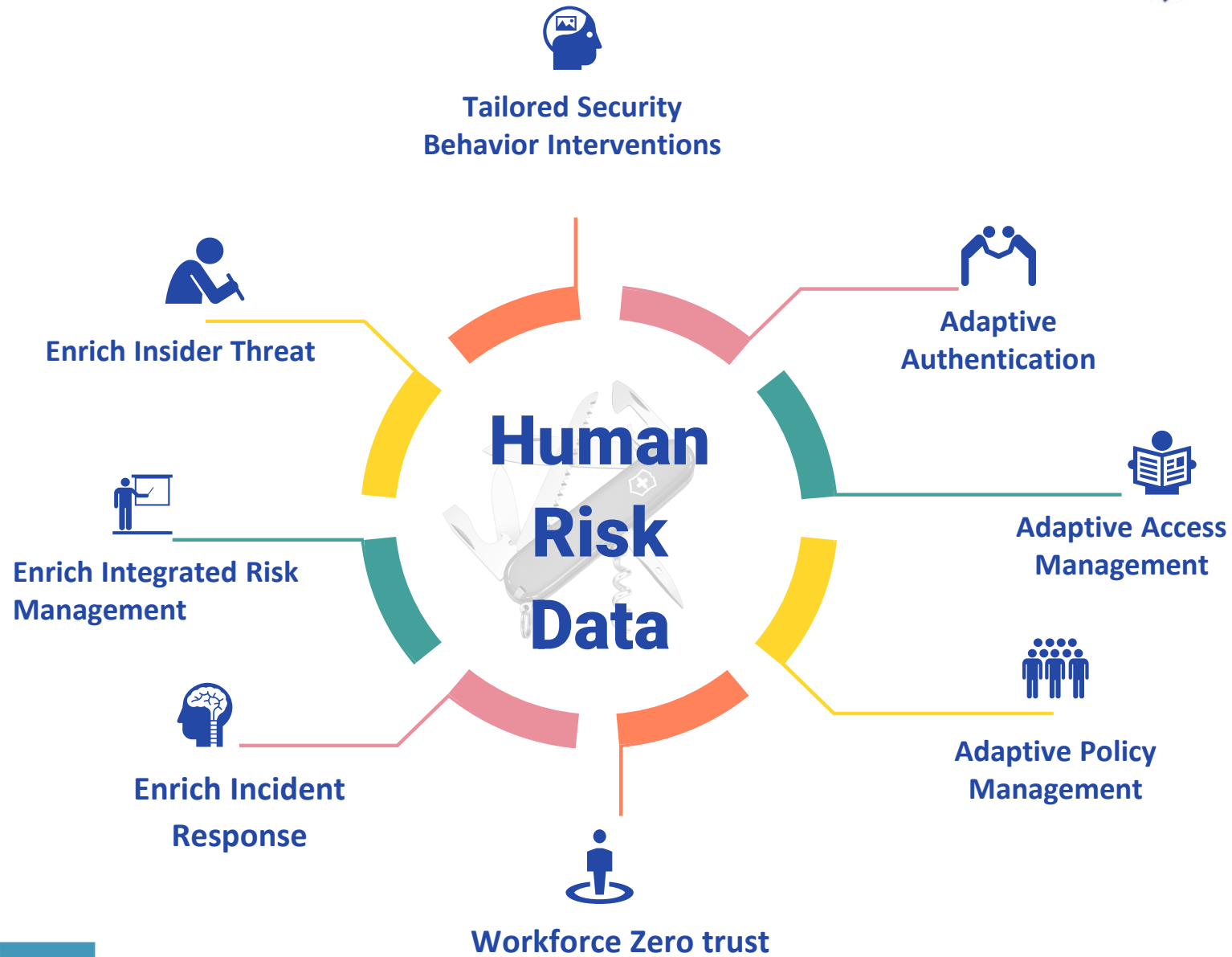Number of credit inquiries **15%**

Diversity of your credit **10%**

Age of your credit **10%**

35% Payment history

30% Level of credit utilization
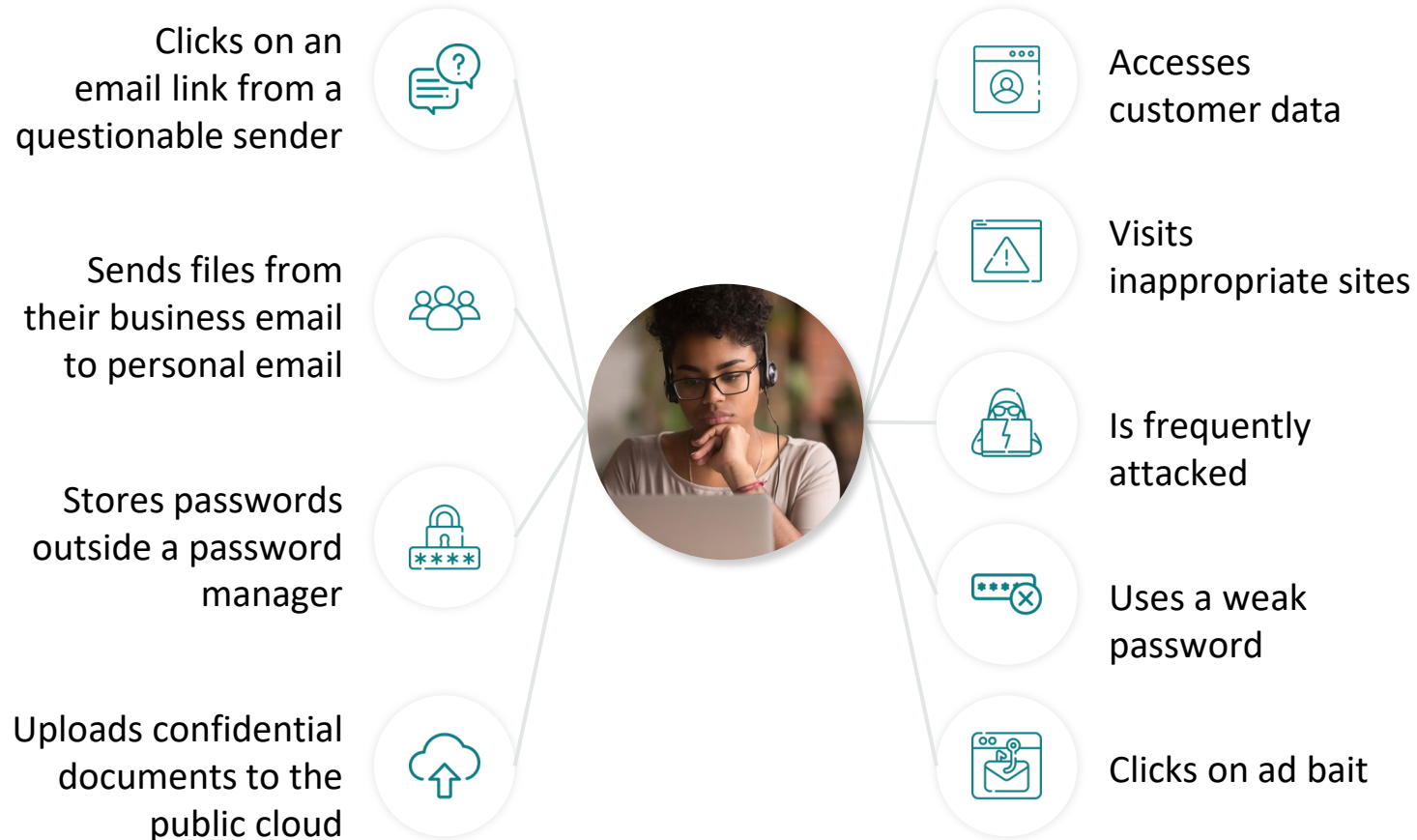
When You Get Back

- Identify who is in charge of managing your human risk

- Work with your security team to identify and prioritize your top three human risks & key behaviors that manage those risks

- Identify how you will measure those behaviors

- Focus on these top three human risks for next 12 months