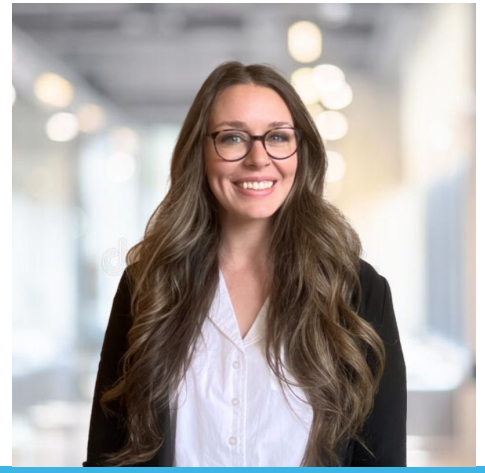
Littler Compliance HR

Data Security for Employers in the Era of AI, Remote Work, and Ransomware

Today’s Webinar Host



STEPHANIE ZIELINSKI

Marketing Director

ComplianceHR

Compliance HR

Simplify the complexity of employment law

PolicySmart™
Create and maintain an up-to-date and legally compliant employee handbook

Navigator Independent Contractor
Remove risk in determining Independent Contractor status

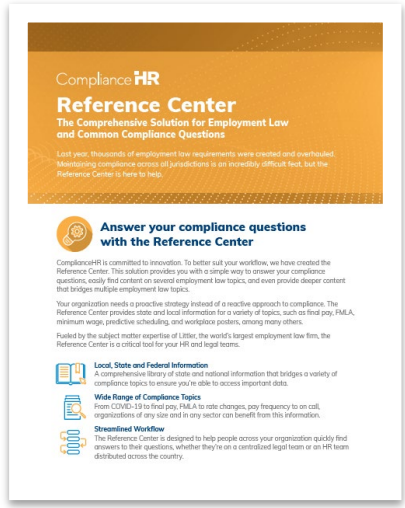
Navigator Overtime
Determine if an employee is exempt or non-exempt

The Reference Center
A Comprehensive Solution for Employment Law and Common HR Compliance Questions

The Document Center
Efficiently generate state and federal compliant documents throughout the employee lifecycle

Our Most Popular Solutions


ComplianceHR
PolicySmart™
Changing the way companies create and maintain compliant handbooks
Creating and maintaining compliant handbooks is a daunting task.
Your company's employee handbook is an invaluable tool that helps shape company culture, communicates operational policies, and minimizes the risk of employment-related legal liability. A well-written and legally compliant handbook is essential to keeping the HR process running smoothly, and most employers would agree that keeping up with federal, state, and local employment laws can seem overwhelming.
PolicySmart™ takes handbooks to the next level.
PolicySmart™ is an intuitive handbook compliance tool that provides employers with national and state specific templates, a unique compliance timeline, and so much more.
Fueled by the subject matter expertise of Littler, the world's largest employment law firm and built on Neota's AI-powered platform, PolicySmart™ allows users to easily create and maintain legally compliant handbooks that are cost effective, up-to-date, and delivered on-demand.
Federal and State Compliant Templates:
A comprehensive library of federal and state-specific templates, as well as policy templates that are fully customizable, depending on your workforce and operational needs.
Innovative Compliance Timeline:
Provides an up-to-date timeline of important legal changes that will soon take effect in your selected jurisdictions, helping to ensure that policies are updated at the right time.
Handbook Policy Checklists:
Gain access to jurisdiction-specific checklists that tell employers which policies are required by law to appear in their handbook and who is covered by each policy.
Automated Monthly Emails:
Receive a summary and analysis of relevant legal developments that impact your workplace, with guidance on how to revise policy language.


ComplianceHR
Reference Center
The Comprehensive Solution for Employment Law and Common Compliance Questions
Last year, thousands of employment law requirements were created and overhauled. Maintaining compliance across all jurisdictions is an incredibly difficult feat, but the Reference Center is here to help.
Answer your compliance questions with the Reference Center
ComplianceHR is committed to innovation. To better suit your workflow, we have created the Reference Center. This solution provides you with a simple way to answer your compliance questions, easily find content on several employment law topics, and even provide deeper content that bridges multiple employment law topics.
Your organization needs a proactive strategy instead of a reactive approach to compliance. The Reference Center provides state and local information for a variety of topics, such as final pay, FMLA, minimum wage, predictive scheduling, and workplace posters, among many others.
Fueled by the subject matter expertise of Littler, the world's largest employment law firm, the Reference Center is a critical tool for your HR and legal teams.
Local, State and Federal Information
A comprehensive library of state and national information that bridges a variety of compliance topics to ensure you're able to access important data.
Wide Range of Compliance Topics
From COVID-19 to final pay, FMLA to rate changes, pay frequency to on call, organizations of any size and in any sector can benefit from this information.
Streamlined Workflow
The Reference Center is designed to help people across your organization quickly find answers to their questions, whether they're on a centralized legal team or an HR team distributed across the country.

PolicySmart provides you with:

- Federal and state-compliant templates
- Innovative compliance timeline
- Handbook policy checklists
- Automated twice monthly legal update emails

The ComplianceHR Reference Center provides you with:

- Local, state and federal information
- Streamlined workflows
- Wide range of compliance topics
    - Leave, final pay, FMLA, minimum wage, and more

When coupled, these two solutions provide you with comprehensive compliance program support

Presented By

ZOE ARGENTO

Shareholder | Co-Chair, Privacy and Data Security Practice Group

Denver, CO

zargento@littler.com

303.362.2876

ANDREW GRAY

Associate

Austin, TX

argray@littler.com

512.982.7267

WILLIAM SIMMONS

Shareholder | Co-Chair, Background Checks Practice Group

Philadelphia, PA

wsimmons@littler.com

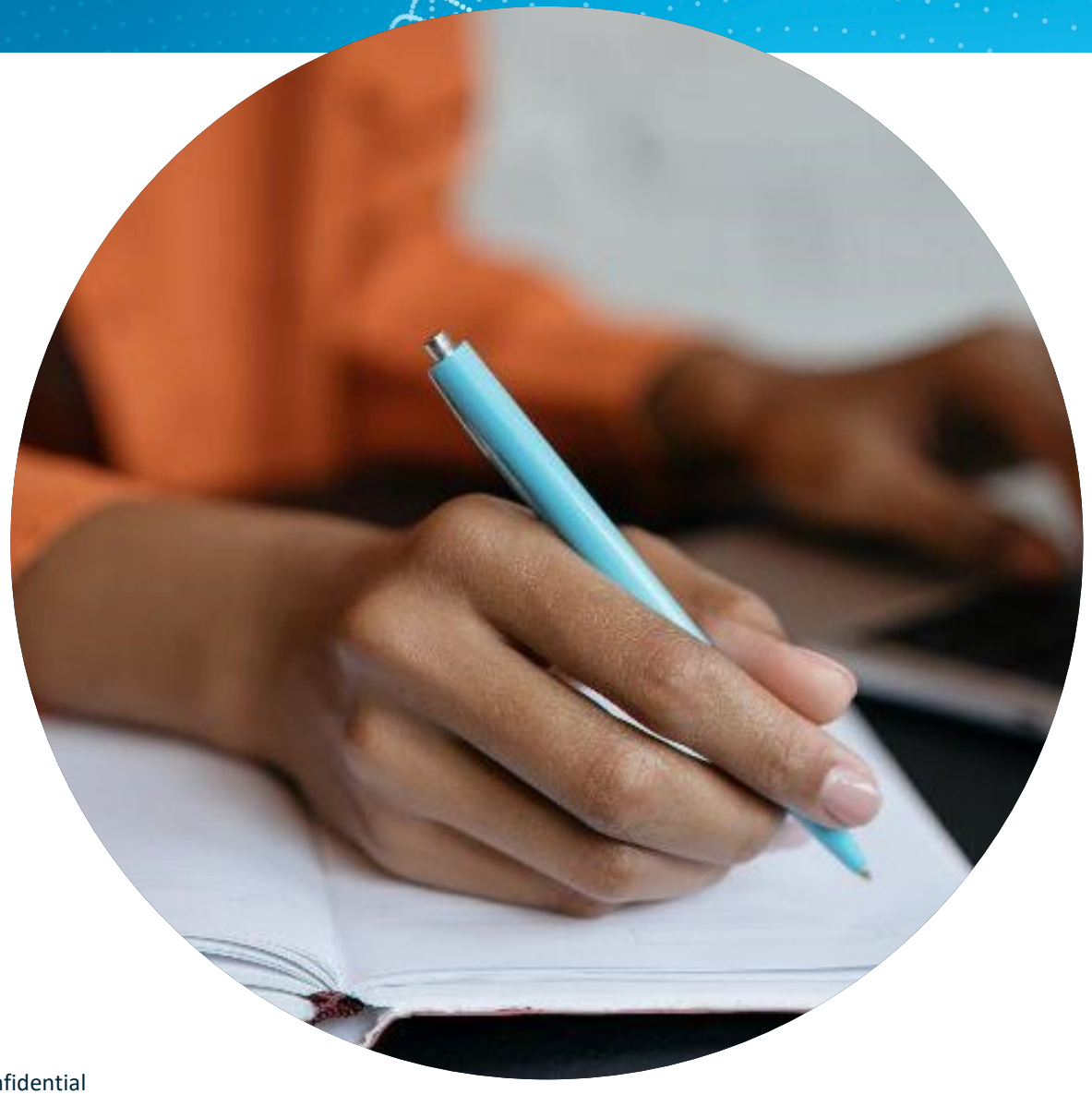
267.402.3047

JIN PARK

Senior Fellow | Stanford Cybersecurity Lab

Agenda

- Human Element of Data Security
- Getting the Right People in the Door
- Onboarding
- Access Management and Updates
- Ongoing Training
- Enhanced Monitoring
- Data Breach Preparedness
- Offboarding



- **76%** of data breaches caused at least in part by insiders
  - **90%** are mistakes
  - **10%** are malicious

Human Element of Data Security

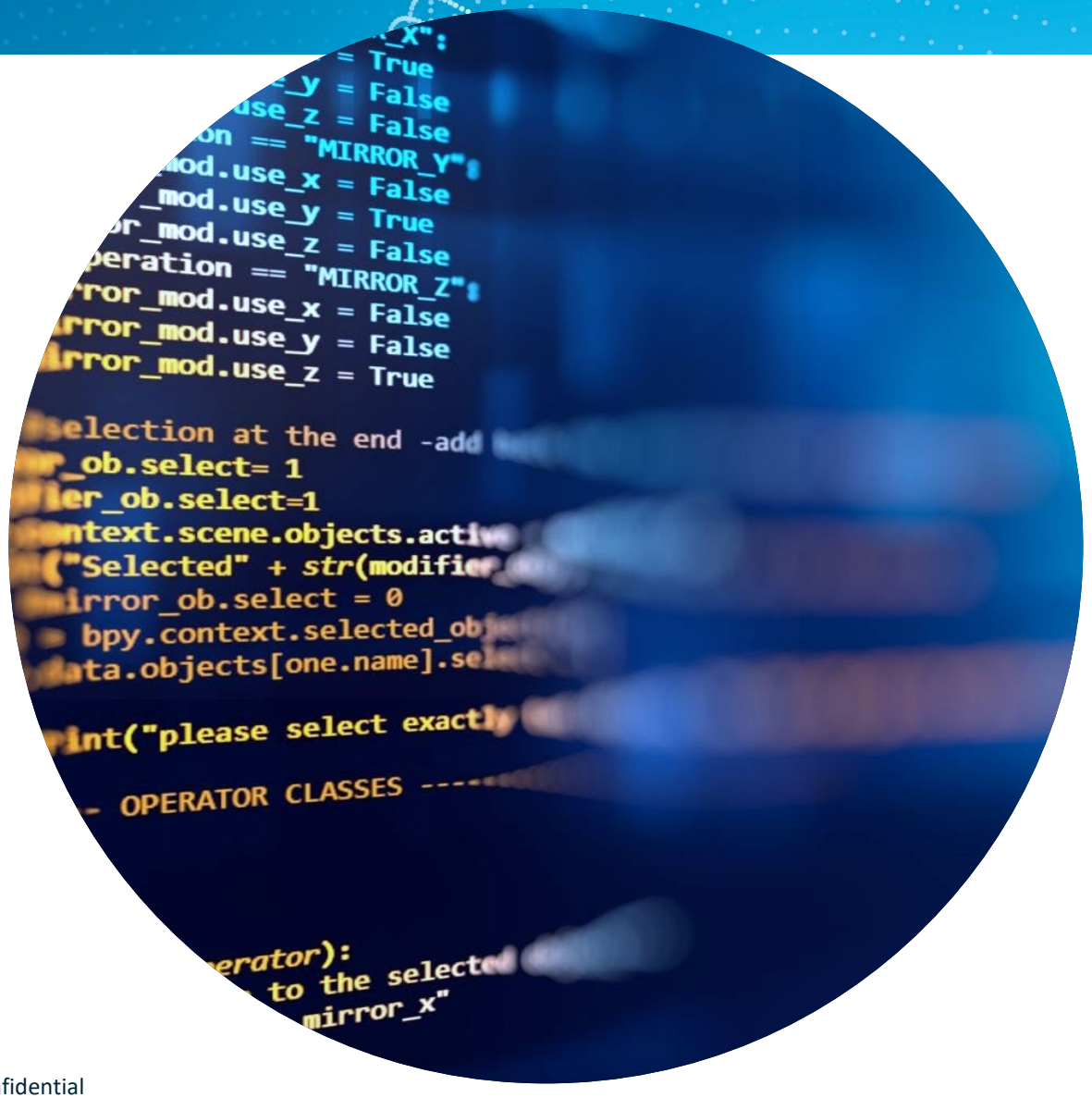
Data Security Legal Requirements and Risks

- **“Reasonable” data security a negligence standard**
  - **> Half** of states require “reasonable” data security by statute
  - **All states** require data breach notifications
- **Sectoral laws and standards**: HIPAA, finance, education, payment cards
- **2025 data breach settlements**:
  - 5 state AG settlements, averaging **$685K**
  - 10 settlements for HIPAA data breaches, averaging **$620K**
  - 4 multi-million dollar settlements, one at **$45M**

Cost of a Data Breach

- **Average cost of a data breach:**
  $4.88 million in 2024 ($9.36M in U.S.)
  - **$1.6M – detection, remediation, and investigation**
  - **$1.5M – lost business cost**
  - **$1.4M – post-breach response**
  - **$.4M – notification**
- **CEOs often lose their jobs after a major data breach**

  IBM Cost of a Data Breach Report, 2024



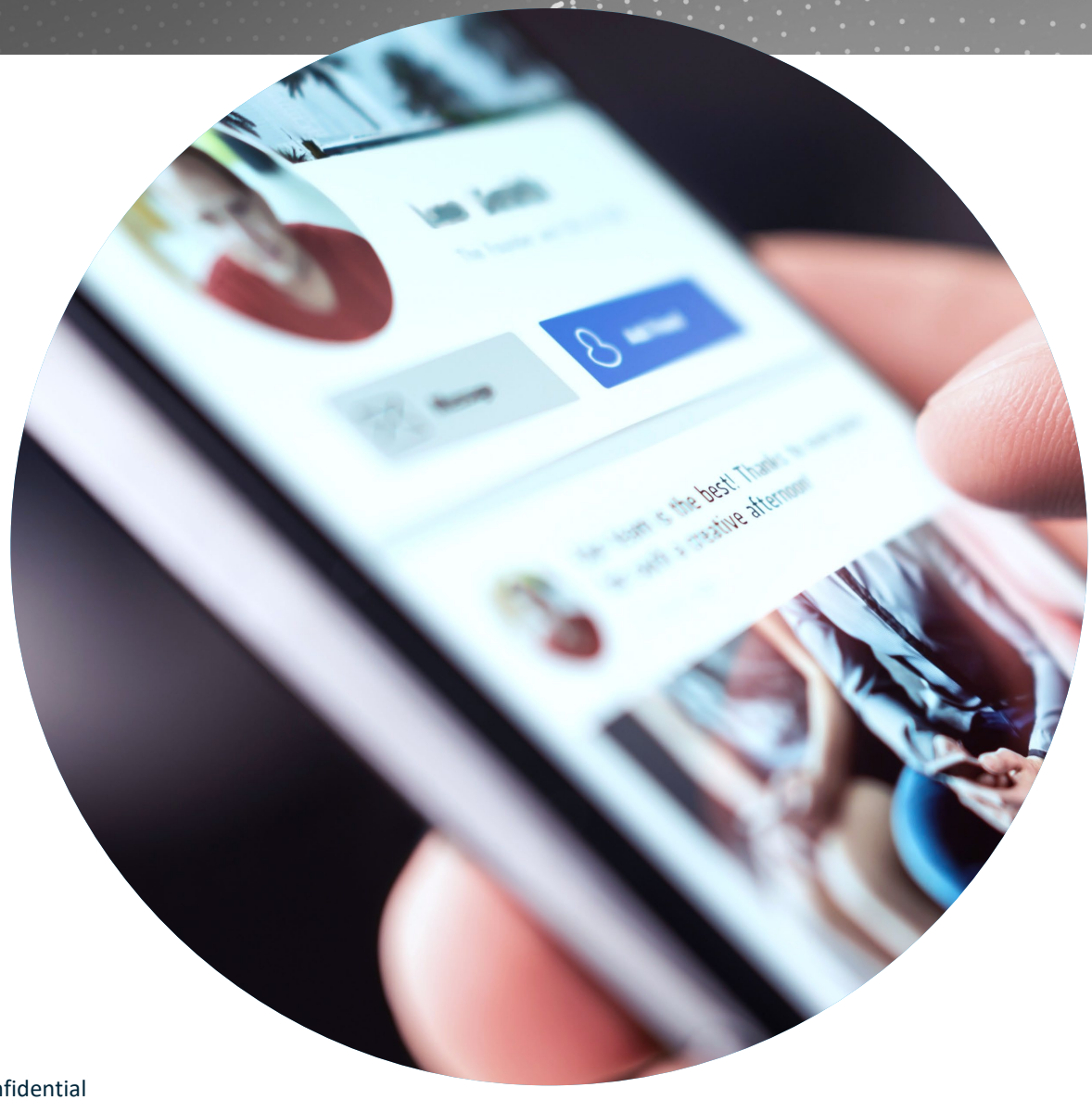
Getting the Right People in the Door

Background Screening

- **Imposters/Bad Actors:** changes in hiring practices over time may have created opportunities for imposters/bad actors
- **“Old School” vs. “New School”**
- **Balance:** consider balance that works for business

Background Screening (Cont'd)

- **Formal Social Media/"Adverse Media" Screening**
  - Typically search common media platforms for categories identified by the employer
  - May have other attendant risks (e.g., disparate treatment claims)
  - May find things "traditional" background checks may not
- **Newer "Identity Verification" Products**
  - Many variations, investigate offerings/ promised functionality



Background Screening (Cont'd)

- **Common "Misses"**
  - Not having a federal criminal records search
    - "Federal Criminal" vs. "National Criminal Database"
  - Missing that employee used different PII for screening than during hiring or onboarding process

Onboarding

Concrete and Actionable

- **Confidentiality Agreements:**
  Legal recourse to regain sensitive data
- **Training:**
  - What exactly are the risks?
  - What data exactly should they protect?
  - How exactly to protect that data?
- **Encompass the Full Workforce:**
  - Temps, interns, vendor workers, etc.,
  - Bear in mind misclassification risks

Access Management and Updates

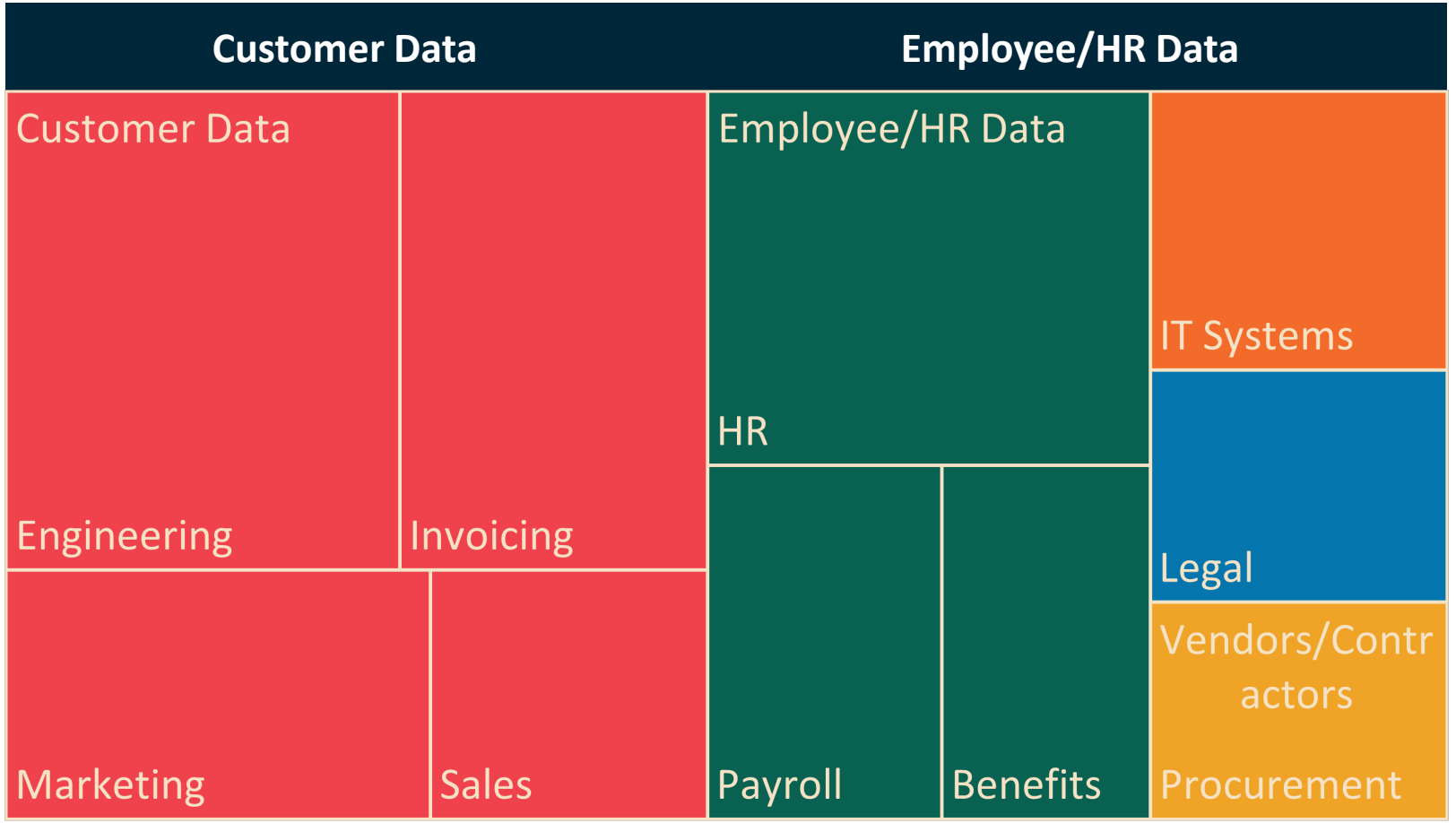
Access Rights

- **Establishing access rights at the outset**
  - Setting access by team/role vs. job function vs. per-employee
  - Differences for internal databases vs. vendors
- **Updating rights and role changes/termination**
  - Managing proper timing for changes
- **Is this a job for IT, HR, or someone else?**

Data Mapping

- **Breach Response:** Breaches involving unmanaged data:
  - $790,000 higher average cost
  - 64 days longer average response time
- **Other Benefits**
- **Techniques:**
  - AI, automated mapping tools, mapping via metadata
  - People-driven mapping

IBM Cost of a Data Breach Report, 2024



Ongoing Training and Awareness

New Risks, Human or Not

- Phishing and other social engineering accounted for **over 4,000** data breaches in 2024
- **Generative AI threats by bad actors…** AI-generated text in phishing emails has doubled between 2023-2025
- **…And by employees:** 15% (and rising) of employees regularly use GenAI tools on work devices — Use personal accounts over 70% of the time

Verizon Data Breach Investigations Report, 2025

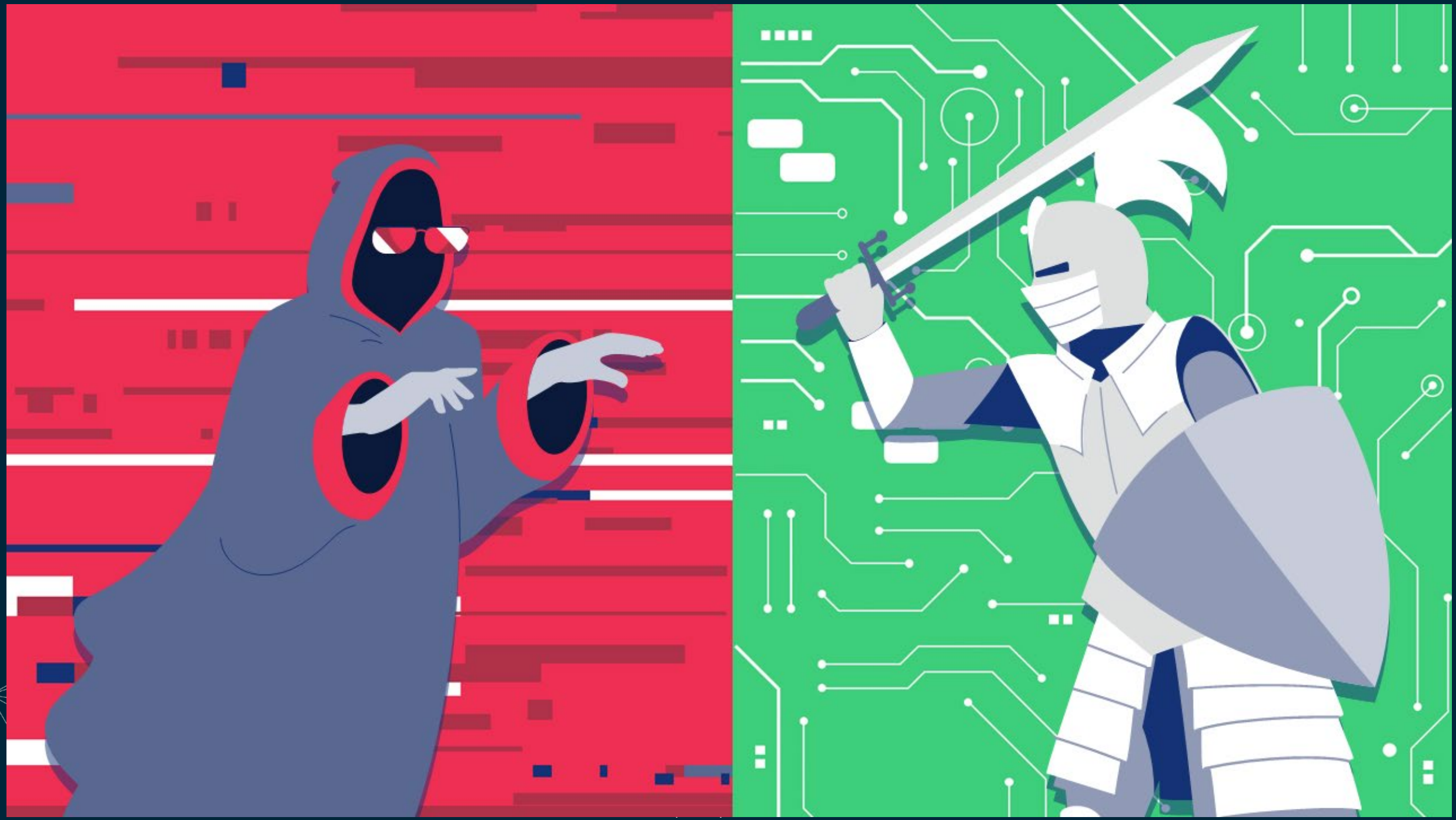
Changing (and continued) Threats

- **What do 2025's phishing scams look like?**
  - Less misspellings or awkward language, and fewer princes
  - Relationship and location-specific pretexting (*e.g.*, job offers too good to be true)
- **Other social engineering attacks:**
  - Prompt bombing for multi-factor authentication
  - Bait websites and ads
- **Misdelivery, inadvertent disclosure, and other mistakes remain an ongoing risk**

Re-Worked Training Methods

- **Recognition *and* response:** Employees spot phishing scams four times as often after training…but not often enough
- **Combined approach:**
  - Interactive Training and Engagement
  - Evaluations and Testing
  - Protocols for Transferring Data
  - Responsible AI Use

Verizon Data Breach Investigations Report, 2025



Enhanced Monitoring

Growing Use of AI Security Tools

IBM Cost of a Data Breach Report 2024

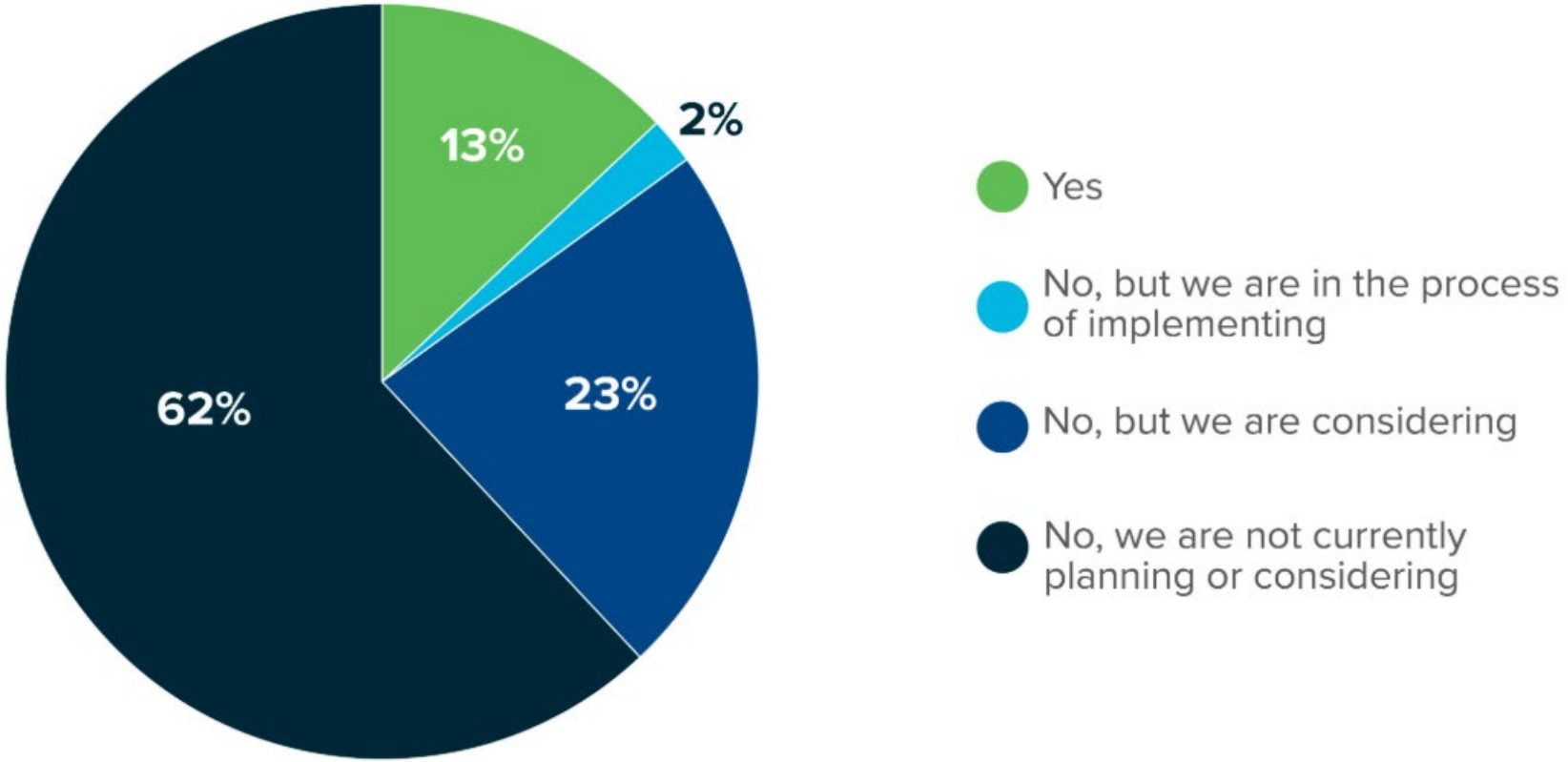
of organizations surveyed in 2024 using AI extensively for data security

increase from prior year

Amount by which extensive use of AI appeared to reduce the costs of a data breach

Littler AI Survey 2025

Does your organization use AI technology to help track or monitor employee activity and/or performance?



New AI Security Tools

- **Anomalous activity detection:** detect a baseline and alert the IT department of anomalous activity
  - **Darktrace:** identifies a “pattern of life” for every device and user in a network
  - **Vectra AI:** analyzes all network traffic, focus on privileged users
- **GenAI detection:**
  - Review sites visited

New AI Security Tools

- **Classification mismatch:** Reviews the content of folders against classification
- **Individual monitoring**:
  - *E.g.*, Zenguide: identifies individuals who take “risky actions” and intervenes with guidance
- **Phishing analysis**:
  - Detects spikes in emails from an email account
  - Proofpoint: realtime analysis of phishing risks


Be careful: possible impersonation detected
Possible impersonation: The sender's domain, "@firstcorp-mail.com", looks like "firstcorp.com", which your organization interacts with
Sense of urgency: Common technique used in email fraud
Financial request: Common technique used in email fraud
Report and Delete
Release to Inbox

Privacy Risks of AI Data Security Tools

- **Wiretap laws**: prohibit interception of communication without consent
- **Biometrics / location data**: increasing state laws
- **Common law of privacy**: provide notice
  - User-level surveillance
  - Websites visited – even when using personal internet service?
- **International data protection laws**:
  - EU/UK disfavors reviewing “personal” folders or use of resources
  - Carefully tailor risk against intrusion, even with notice

Tips on Reducing Risks

- **Understand the technology**:
  - What data, where collected, how collected, and why
- **Employee communications**: transparency, purpose, and any benefits
- **Consider what to do with findings**: education, discipline?
- **International**:
  - Documented data protection impact assessments
  - Either prohibit personal use or take care in monitoring personal use
  - Reduce intrusion: anonymization, limit access
  - Communications with labor representatives

Role of Human Resources

- **Monitoring tools are expensive:** both $ and system resources
- **HR can help to tailor the monitoring**
  - Locations of sensitive data
  - Focus on times on employee unrest
    - Lay-offs / terminations
    - Mergers / acquisitions
    - Restructuring
- **Malicious insider attacks are the most expensive and damaging**

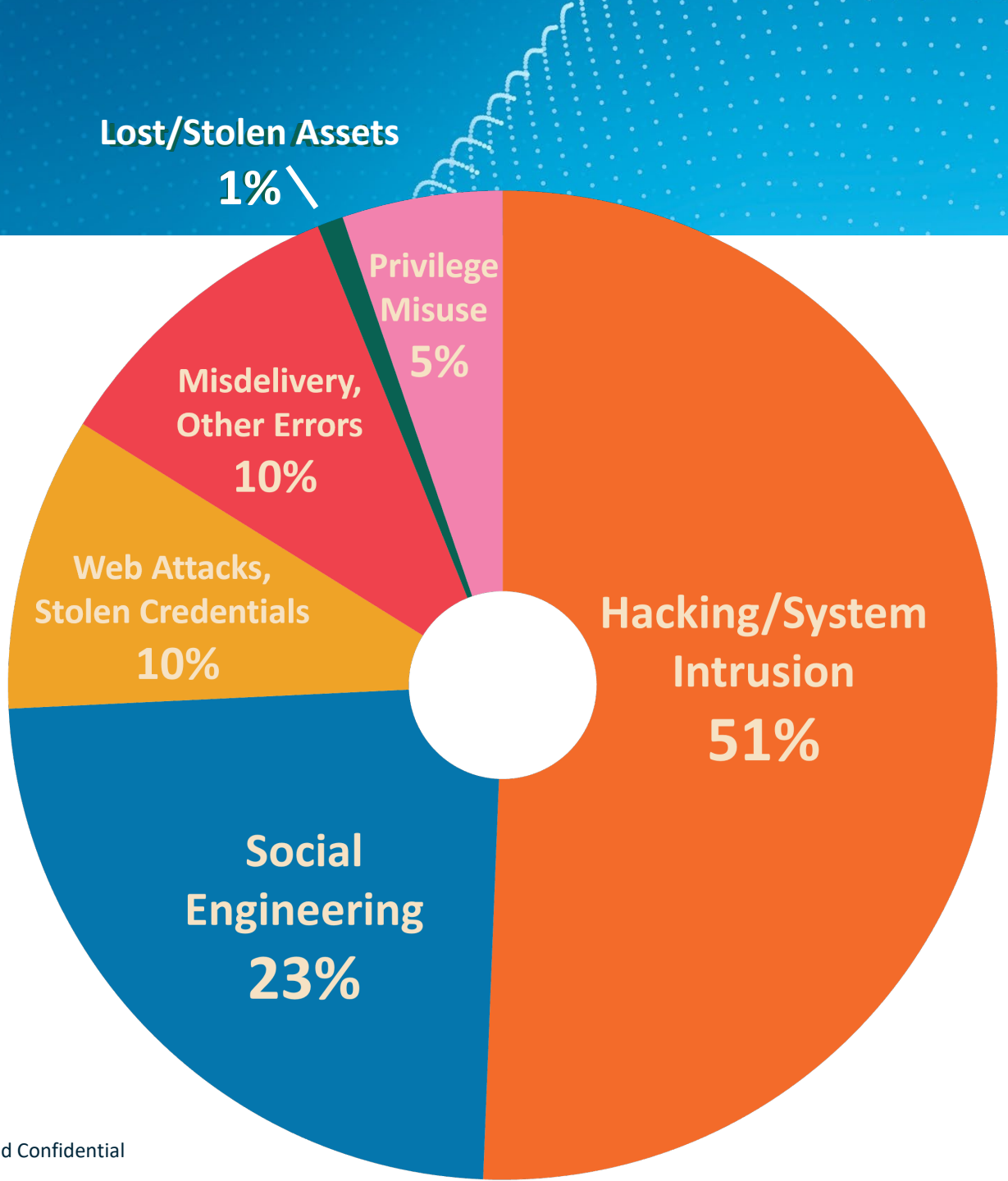
Ongoing Background Screening

- Can be useful if anything for public perception following an incident
- Generally permissible (outside of drug testing), as long as procedures followed (no need for “good cause”)
- Does not have to be “everyone”
- Some employers use annual background recurring screening, others ongoing “monitoring”
  - Monitoring sometimes used for direct employment decisions, other times through security team to take protective measures sort of employment decisions

Data Breach Preparedness

Data Breach Landscape

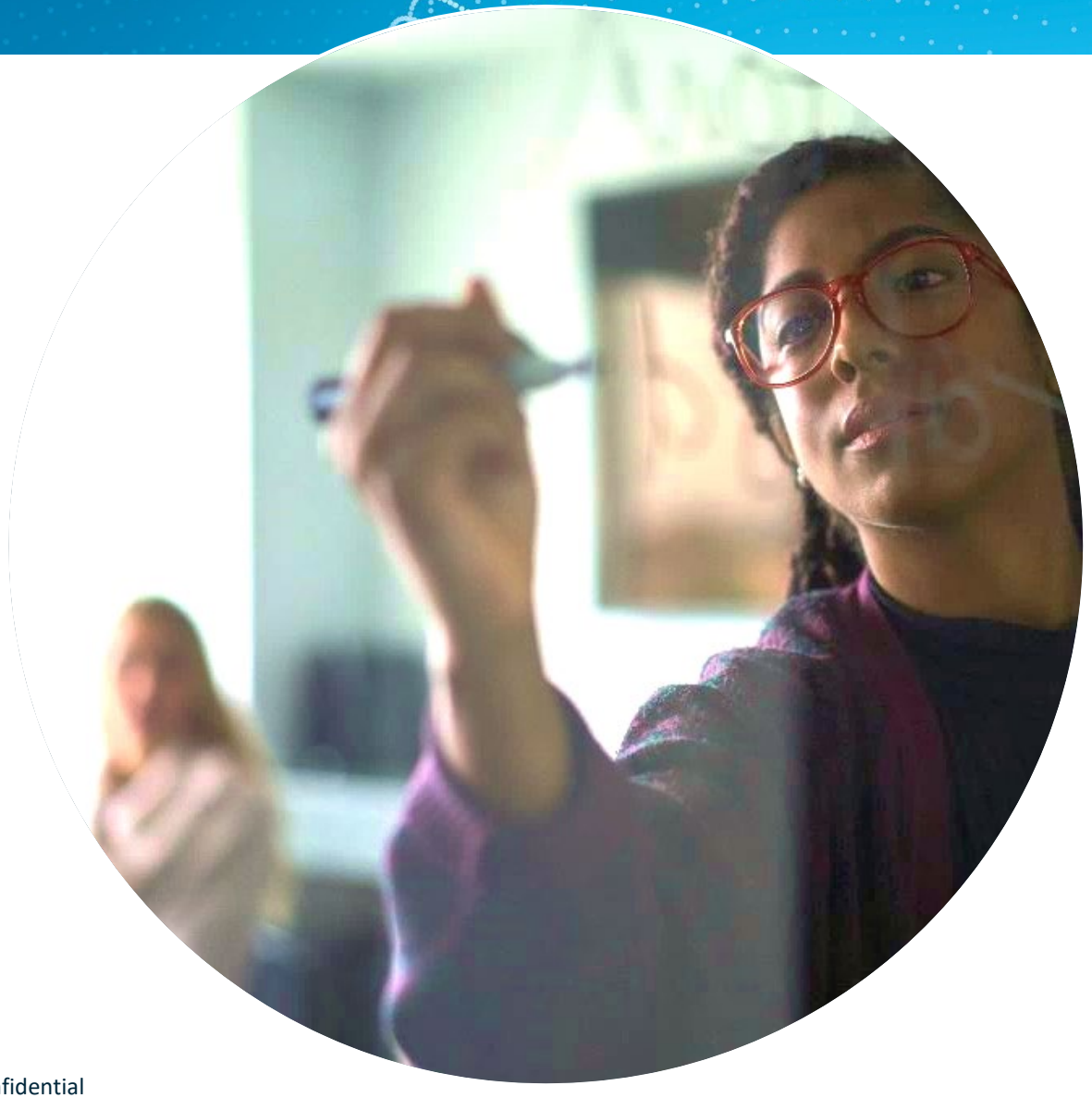
- Malicious and negligent insiders still account for the lion's share of all data breaches
- Employee/HR Data is the costliest category of data in a breach



Verizon Data Breach Investigations Report, 2025
IBM Cost of a Data Breach Report, 2024

Business-Wide Breach Preparedness

1. **Business Continuity/Incident Response Procedures**
   - Communicating with key stakeholders and the workforce
   - Backup plans for business operations
2. **Multi-Factor Authentication/ Passphrase Management**
3. **Data Retention and Purge Rules**
4. **Vendor Management and Third-Party Storage**



Offboarding

Offboarding Risks

DTEX 2023 Insider Risk Investigations Report

of employees took **sensitive IP** with them when they left an organization, including

take **non-sensitive IP** (such as presentations and templates)

Data Security and Offboarding

- **Technical Review**
  - Review for emails/downloads of company data
  - Check for suspicious activity
- **Terminate Data Access**
  - Turn off access to accounts
  - Wipe MDM contains on personal devices
- **Offboarding Meeting**
  - Confidentiality agreement reminder
  - Return equipment
  - Ask about retained company data

Sign Up for a Demo

ComplianceHR Demo & Free Trial:

https://compliancehr.com/webinar-demo/

Three ways to sign up for a demo:

1. Reply “Yes” to the on-screen poll
2. Visit our website: Compliancehr.com
3. Email our team at demo@compliancehr.com

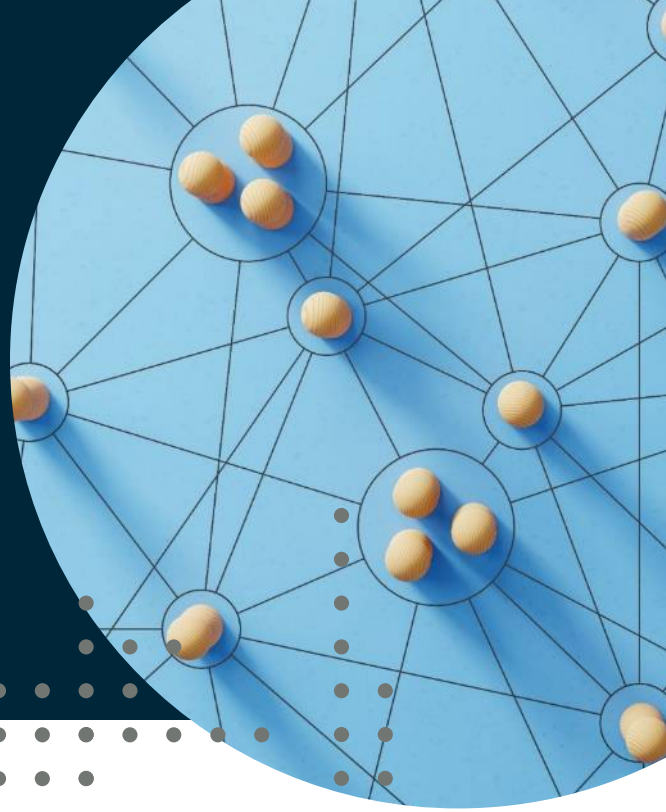
Benefits of a custom demo:

- Discuss your organization’s requirements/challenges
- Review Navigator Suite Solutions
- Share compliance methodologies

Littler® Compliance HR

Questions?

Littler Compliance HR



Thank You