A LITTLER PRESENTATION

When Cyber Becomes a People Problem: A Boardroom Scenario in Oversight, Accountability, and Response

Littler®

presented by

KWABENA APPENTENG

Shareholder | Co-Chair
Privacy & Data Security
Practice Group, Littler
Mendelson, P.C.

CRISTINA DOLAN

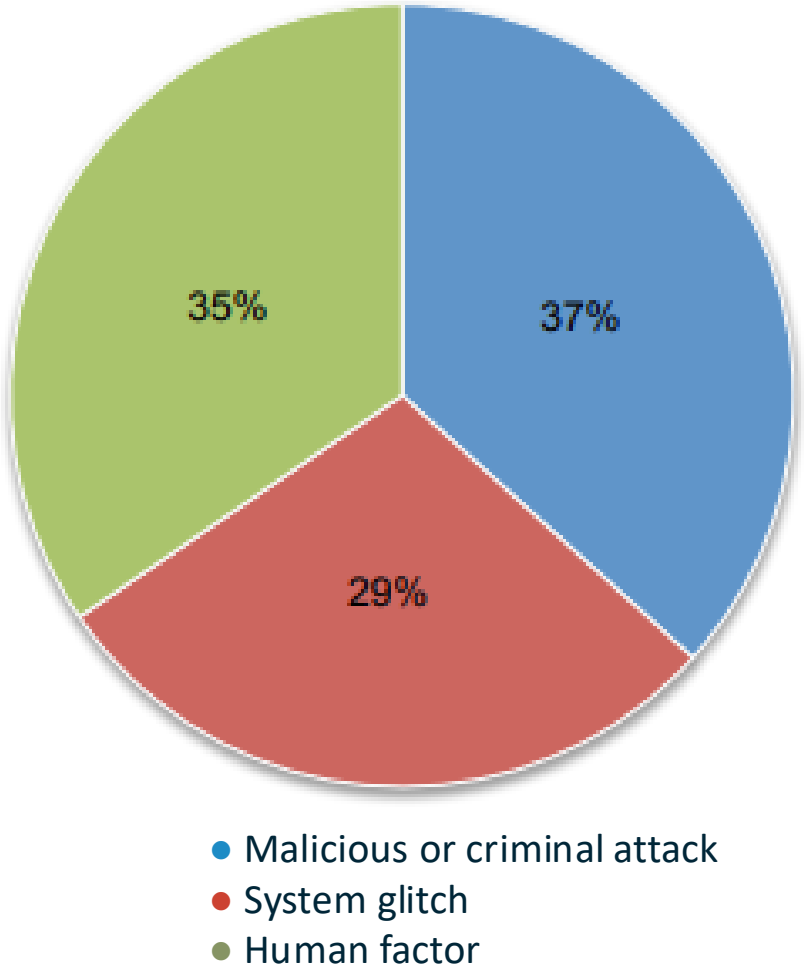
Board Member, SEALSQ;
MIT Media Lab Fellow
(Cybersecurity)

The New Threat Environment

The “Conventional” Data Breach

- In 2013, the average cost of a data breach in the U.S. was **$5.4 million**
- Only 37% were attributable to malicious or criminal attack
- **Focus of the criminal activity was the exfiltration of personal information**
  - Social Security numbers, credit card information, log-in credentials
  - Information typically sold by bad actors on the Dark Web.

(*Ponemon Institute 2013 Cost of Data Breach Study: Global Analysis*)



The Modern-Day Data Breach

- **Between 2013 and 2022** the number of data breaches **more than tripled.** (*The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase)*
- In 2025, the average cost of a data breach in the U.S. was **$10.2 million.** (*IBM Security Cost of a Data Breach Report 2025*)
- The three most expensive industries for data breaches in 2025 were healthcare, financial services, and industrial companies. (*IBM Security Cost of a Data Breach Report 2025*)
- **In 2025, 44% of all breaches involved ransomware; notably, 63% of organizations opted not to pay the ransomware demand.** *(Verizon, 2025 Data Breach Investigations Report; IBM Security Cost of a Data Breach Report 2025)*
- **Companies that had board-level oversight over a breach reduced breach costs by an average of $110,772**. (*IBM Security Cost of a Data Breach Report 2025*)
- **Focus has shifted from only data exfiltration to data encryption, data exfiltration, and extortion**

Employee Breaches Continue to Cause Problems

- **Employees remain a leading cause of data breaches.**
- In 2025, **60% of all breaches involved a human element**. *(Verizon, 2025 Data Breach Investigations Report)*
- Employee data was the second-most commonly compromised data type in 2025: 37% of all data compromised.
- What's more, employee personal information is one of the costliest types of data to have compromised: $168 per record.
  - Intellectual Property: $178 / record
  - Other Corporate Data: $154 / record

(IBM Security Cost of a Data Breach Report 2025)

Considerations When Responding to a Ransomware Attack

Breach Response Strategy: Key Competing Considerations

Business Concerns	Legal Concerns
Business Continuity	Legal Compliance
Business Reputation / Public Relations Risk	Statutory Notification Deadlines
Employee Relations Risk	Litigation
[Ongoing] Data Security Risk	Regulatory Investigation Risk

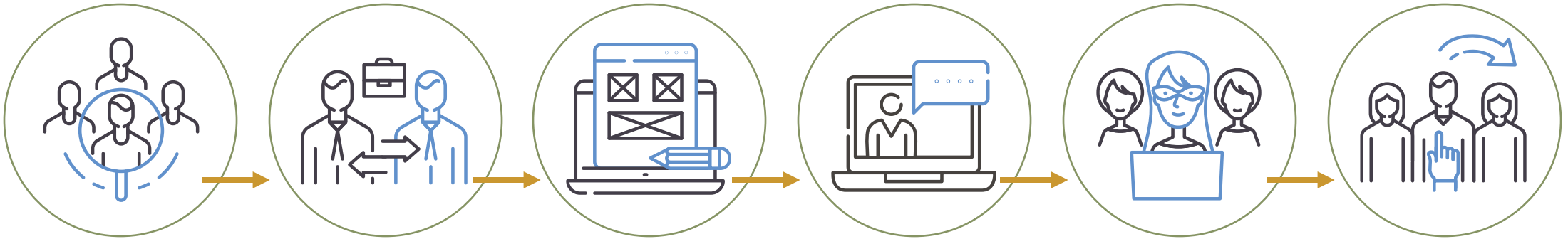
A Very Bad Day For C&K Manufacturing

Issue Spotting

1. **What should the company's response be?**
2. **What should the company consider in developing a strategy for dealing with the threat actor?**
3. **How can the company facilitate business continuity?**
4. **What should the company communicate to employees?**
5. **What are the legal considerations?**
6. **What are the post-breach considerations?**

Key Take Aways

Establish a Culture of Data Stewardship



Pre-employment screening and continuous monitoring

Robust confidentiality agreements

Policies and procedures

Information security training

Access controls & online monitoring

Exit interviews

An Organization's Security Is Only As Strong As Its Workforce

- **<u>Educate Your Workforce on Cybersecurity Risks:</u>** Cybersecurity training at onboarding, ongoing training, simulated phishing emails—ensure the workforce is trained to spot cybersecurity risk.
  - Every employee should receive **data security training at orientation**
  - Employees with access to **trade secrets or personal information** should have more **in-depth training**
  - Periodically send **reminders, updates, and notices** – not only IT-related topics
- **The average cost of a data breach at organizations that invested in employee training was $192,266 less.** *(IBM Security Cost of a Data Breach Report 2025)*

Readiness Planning Is Critical

- **Be Prepared:** The rise in ransomware attacks means an attack is a "when" not an "if".
  - Ensure that key stakeholders are familiar with the organization's overarching incident response and business continuity plans
  - Identify specific actions for the HR team and identify strategies for executing on them in the context of a "digital crisis"
  - Consider the external team (lawyers, forensic experts, negotiator, PR team) that will be utilized in the event of an attack
- **Organizations that had workflows / "playbooks" in place were able to contain ransomware attacks in 68 days vs. 80 days for organizations without a workflow or playbook.** *(IBM Security Cost of a Data Breach Report 2023)*

Understand The (Many) Legal Risks

- **Understanding the legal risks that need to be considered in the event of an attack will better inform your response strategy.**
- **Notifications & timing obligations**
  - Impacted individuals (U.S. & outside the U.S.) (***30 days in several U.S. states***)
  - Jurisdictional regulators (U.S. state regulators, DPAs) (***GDPR: 72 hours***)
  - Agency specific (SEC, HHS, credit reporting agencies) (***SEC: 4 business days***)
- **Litigation risk:**
  - Consumer and employee class action litigation
  - Securities class action litigation
  - Customer (B2B) actions
  - Regulatory action

Considerations for HR Once the Dust Settles

- **Support difficult disciplinary decisions**
  - Discipline employee(s) directly responsible for the attack (*i.e.*, should the Controller in the hypothetical be terminated?)
  - Harder decisions regarding IT personnel (*i.e.*, should the CISO be terminated?)
- **Identify team members whose access to certain systems should be restricted**
  - Employees whose actions contributed to the attack
- **Maintain talking points to respond to ongoing employee concerns about the incident**
  - Work with legal to develop this "script"
- **Post-incident review of training and policies for effectiveness**

Prepare for Vendor Breaches

- The average cost of a third-party vendor / supply chain compromise in 2025 was **$4.91M.** *(IBM Security Cost of a Data Breach Report 2025)*

- Particular areas of risk:
  - Cloud storage providers
  - Supply chain business partners
  - Software service providers

Thank You

Littler®

Fueled by ingenuity.
Inspired by you.®