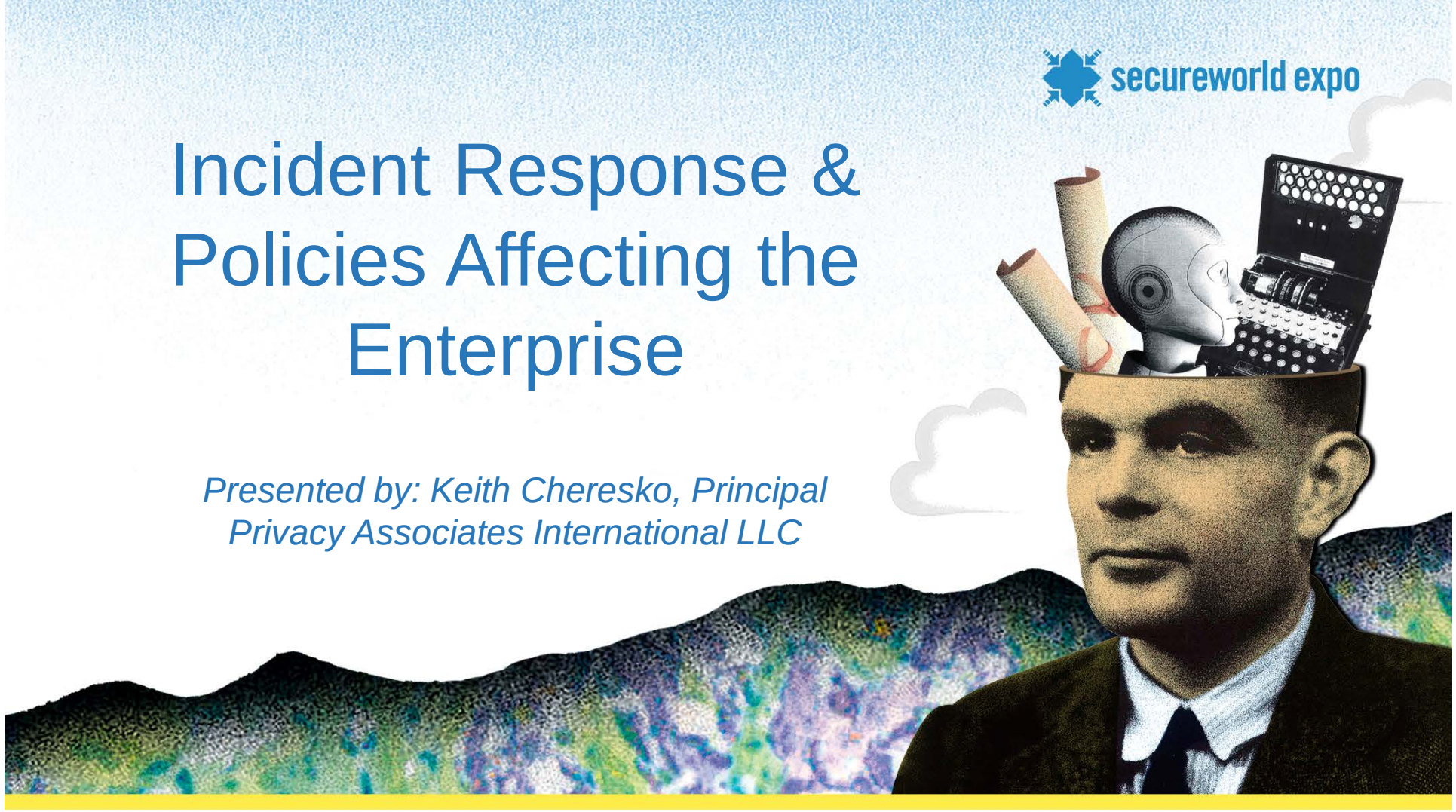
Incident Response & Policies Affecting the Enterprise

Presented by: Keith Cheresko, Principal
Privacy Associates International LLC



- After this presentation, view it again on our SecureWorld App!
- Don't forget to "check-in" to this session to use as proof of attendance for CPEs! You can also scan the QR code on the room sign outside.
- Start a discussion or ask a question about this session via the SecureWorld app. The speaker will address these at the conclusion of the conference.

Breach Incident Processing

- Assemble the team and put the IR plan in action
  - Stop the bleeding
  - Determine the injury
  - Involve those with whom prior arrangements were made -- as necessary
  - Notify as required in an appropriate manner
  - Report to authorities -- as required
  - Document actions and reasons for them
  - Fix the concern
  - Evaluate and revise as necessary

Breach Incident Processing

According to regulatory advice in the event of an incident do:

- Immediately isolate affected systems to prevent further intrusion loss of data or other damage
- Email traffic may be monitored; Use the telephone or other reasonably secure means to communicate (VOIP?)
- Notify law enforcement
- Activate all auditing software if not already activated
- Preserve pertinent system logs

Breach Incident Processing

- Make backup copies of damages or altered files and keep them securely
- Identify where affected system resides in network topology
- Identify all systems and agencies that connect to affected system
- Identify programs and processes that operate on the affected system, impact of the disruption and max allowable outage time
- If necessary make arrangements for continuity of services

Breach Incident Processing

According to the same regulatory advice in the event of an incident do not:

- Delete, move or alter files
- Contact suspected perp.
- Do forensic analysis (unless properly experienced and qualified) call expert help

Initial Diagnosis

- It is unusual to have all the correct facts immediately upon receipt of notice of an incident
- Need to collect all possible facts and based on those, preliminarily identify internal and external stakeholders
- Ask the 5 W questions – “who, what, where, when, why” + “how”

Initial Diagnosis

- Based on available facts, should further investigation be done under direction of counsel to try to obtain work product privilege rather than under direction of the IRT?
- Commence record-keeping protocol
  - Critical for possible future liability purposes to keep a contemporaneous record of what information the company had when, and what decisions were taken as a result
  - Use of standardized event logs and decision logs makes the process easier

Initial Diagnosis

Draft initial write-up of “what happened” based on knowledge to date

- Will be required to communicate to internal and external stakeholders
- Will be continually revised as facts develop/change
- A single official version mandatorily used for all purposes will help assure accuracy and avoid expensive and embarrassing inconsistencies

Initial Diagnosis

- Determine and mitigate possible adverse action by data subjects or other stakeholders
- Will notice to affected data subjects possibly be legally required? If so what are the rules, time limits, forms, etc.
- Will notice to affected data subjects possibly be required for business reasons even if not legally required? If so, is it clear who will make the decision?
- Do you require additional resources to deal with the situation? Forensic or technical experts? Outside counsel?

Containment

- The exact actions that can be taken in this phase are unique to each incident and very fact-specific
- Important to avoid group responsibilities for tasks and to be specific as to who, what, why, how and when:
  - Assignments should be included in event log and a verification of completion mechanism designed
  - Review updated template notification letters on the websites of the privacy officials in potentially affected jurisdictions
- To the extent a supplier is involved, a close working relationship coordinated by an appropriate individual should be established, if at all possible, to avoid “surprises”

Continuing Actions

Again, this phase is very fact specific

- Continue to update fact and decision logs, “What Happened” explanation
- Gage public/government reaction if news has broken
- Prepare individual and governmental notices if required
  - Note letters must be specific enough to meet sometime conflicting state law requirements
  - Letters must not be so specific as to alert the laptop thief that he has something more valuable than the laptop
  - Entire IRT should approve or suggest modifications

Continuing Actions

- Prepare to deal with the resulting communications issues
  - Customers wanting more info
  - Law enforcement
  - Media
  - FTC
  - SEC
  - Credit bureaus
  - State AGs
  - Executives, retail outlets and business partners
- Write call center scripts and do necessary training – either for holding statement or notification follow-ups

Resolution

- Send notifications as required
- Prepare constituencies to deal with the stakeholders
- Continue to update all logs under record-keeping protocol
- Identify and assign responsibility for any additional actions that have to be resolved

Closing

- Close out logs, determine if Final Report useful
- Document lessons learned and share with appropriate stakeholders
- Assign one or more members to follow-up on recommended changes