Incident Response in Cybersecurity

Presenters

Bill Confer, CCSFP

» Risk Assurance Manager

With over 5 years of experience, Risk Assurance Manager, Bill Confer specializes in information security and systems auditing. He serves clients of all sizes from start-ups to Fortune 200s across an array of industries including technology, healthcare, fintech, and manufacturing.

Chris Roe

» Risk Assurance Manager

With over 7 years of experience, Risk Assurance Manager Chris Roe specializes in delivering comprehensive risk assurance services and guidance to clients. He works with organizations of all sizes and industries, providing recommendations around IT Security, SOC Audits, HIPAA Compliance, and Cybersecurity. Prior to joining SSF, Chris held positions at RSM and A-LIGN, where he served clients primarily within the technology sector.

Guest Presenter

BREACHRX

MATT HARTLEY

» Co-Founder and Chief Product Officer, BreachRx

Matt Hartley is a 20+ year innovator in cybersecurity, cyber threat intelligence, cyber warfare, and information operations. He's spearheading the development of a groundbreaking SaaS platform for global organizations of all sizes to prepare for, respond to, and recover from cybersecurity & privacy incidents. Prior to BreachRx, Matt most recently held engineering and product executive roles at FireEye and iSIGHT Partners.

SSF

Agenda

- What is SOC 2
- Incident Response and SOC 2
- Security and Compliance
- The Impact of Data Breaches
- What is Incident Response?
- Intro to Security Incident Management
- BreachRx Demo

Polling Questions

What is SOC 2?

- **SOC 2 is a compliance standard** developed by the AICPA that reports on controls at a Service Organization relevant to **Security, Availability, Processing Integrity, Confidentiality or Privacy**.
- **SOC 2 report** is an opinion intended to meet the needs of a broad range of users that need detailed information and **assurance** about the **controls at a service organization relevant to the applicable trust services criteria.**
- **Two different SOC 2 reports**:
  - **SOC 2 Type I**: Reports on the description of controls for a service organization. The audit firm will provide their attestation that the controls are suitably designed and implemented at a specific point in time.
  - **SOC 2 Type II**: Reports on the description of controls for a service organization. The audit firm will provide their attestation that the controls are suitably designed and implemented **as well as report on the operating effectiveness of the controls over a period of time**.

Incident Response and SOC 2

- **Incident response** is heavily emphasized within the SOC 2 standard. Service organizations will have to show auditors how they manage and respond to incidents, which include tracking, escalating, communicating, and remediating.
- SOC 2 has requirements for service organizations to test their incident response process and recovery procedures. **SOC 2 criteria** relevant to incident response:
  - **Security (Common Criteria)**
    - CC4.2
    - CC7.2
    - CC7.3
    - CC7.4
    - CC7.5
  - **Privacy**
    - P6.3
    - P6.6

Security & Compliance

- Typical "**Security**" refers to the systems and controls that organizations have in place to **protect data, assets, people and to protect against threats**.
- Typical "**Compliance**" refers to **meeting a standard** or framework that sets forth best practices by a third party (SOC 2, ISO 27001, HITRUST, PCI DSS, NIST).
  - Compliance plays an important role in:
  - Oversight of the organization
  - Vendor management programs
  - Internal corporate governance and risk management processes
  - Regulatory oversight
- **Auditor Advice: Work on implementing cyber security best practices and compliance will follow.**

SSF

Polling Questions

The impact of data breaches

The Facts

- The **cost of an average incident is $9.44M** in the US, while **mega-breaches** cost an average of **$250M-400M**
- Regulatory fines & directives are increasingly common on companies *and* executives
- Incidents and breaches cost businesses significant time and money
- Incidents and **breaches damage company brand reputation** and create customer churn

What is incident response?

Incident response is:

- A part of all compliance frameworks
- Identifying, containing, and resolving an incident
- A team event
- Previously prepared & regularly tested
- Coordinating with stakeholders
- Stopping the cause so it doesn't happen again

Security vs Privacy Incidents

Security

- Insider threats
- Lost or stolen credentials
- Malware infections
- Phishing
- Ransomware

Privacy & Data Loss

- Data exfilitration
- Improper disclosure
- Lost or stolen devices
- Misdirected emails

The key to incident response for SOC 2

Communication

- Incidents can easily be reported
- The appropriate personnel are notified
- Leadership is included when appropriate
- All relevant external parties are notified
- Proper channels are used

Response

- Procedures are in place
- Incidents are properly prioritized
- Impacts of incidents are assessed
- Incidents can be contained & mitigated
- Root causes are identified
- Procedures are regularly evaluated

Spreadsheets & plan documents don’t cover these requirements

SSF

What is security incident management?

Security incident management & response is:

- All about addressing and managing the effects of cybersecurity incidents and data loss
- Handling incidents that can be large or small and originate internally or externally
- Overcoming teams' struggles to keep up with threats and procedures to deal with them
- Dealing with incident response plans that are rarely used during incidents because they're too strategic and are not tailored to the type of incident or for the organization
- **Proactive** – without preparation, responses are conducted in crisis mode and end up being highly chaotic

SSF

BreachRx Demo

Questions?

Thank You!

Contact Us

For questions, contact us:

Risk Assurance Service Team | info@ssfllp.com

Matt Hartley | (703) 334-1943 | mhartley@breachrx.com

SSF SENSIBA SAN FILIPPO
CERTIFIED PUBLIC ACCOUNTANTS AND BUSINESS ADVISORS

BREACHRX