Analysis and Process Improvement

A data breach can hurt constituents, incur significant costs, and damage the reputation of the IT function as well as the larger institution.

However, devoting the most skilled and valuable staff to forensic analysis and verification of breach processes can sap IT's ability to move past an incident and improve future risk management. Consider how more effective preparatory steps and response processes can improve time-based metrics.

Artifact J: The Ponemon Institute's 2014 survey on cyber security issues provides a lens into industry practices (p. 29).

The Key Performance Indicators of Effective Response

Standard Model

- Did we detect the breach and understand the problem?
- Did we assign an appropriate incident response team?
- Did we fix the problem?
- Did we notify the appropriate authorities and affected parties?
- Is service restored?

Progressive Model*

- Measure Mean Time to:
  - ✓Identify: How long between breach and detection?
  - ✓Know: How long between detection and understanding of root causes?
  - ✓Fix: How long to resolve the situation and restore service?
  - ✓Verify: How long to confirm resolution with affected parties?

If You Had One Security Breach Analysis Tool…

Private industry respondents report* that storage of audit trails using a packet capture system or SIEM (security incident and event manager) tool is the most effective way to detect and analyze security breaches.

Conduct a risk assessment of the entire organization and use it as a basis for a remediation plan. Often, assessments and remediation plans are reviewed and monitored by external auditors to ensure management attention and participation. An institution's Board of Trustees may also want to be briefed on these regularly.

Breach plan language, process documents, and discussions should focus on the connections between incident response and effective risk management rather than treat breaches as isolated incidents.

Build New Threat Indicators into Future Planning

Outside Attacks and Threat Indicators

- What was the source of the attack?
- What are the key characteristics of the attacking individual or group?
- What was the vulnerability exploited (e.g., social engineering, poor security architecture)?
- How can future response processes and communications for similar incidents be improved?

Inside Theft and Accidental Exposure

- What was the source of the theft or loss?
- What vulnerabilities were exploited or exposed by the incident?
- Has the responsible employee or department caused problems before?
- Can improved awareness and trainings for local staff prevent future similar incidents?

"Cyber Security Incident Response: Are we as prepared as we think?" Ponemon Institute LLC, January 2014. http://www.lancope.com/files/documents/Industry-Reports/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf/.