Life after A Data Breach – People, Processes, and Technology

Wes Withrow
Cybersecurity Expert
TraceSecurity
Agenda

- How organizations are defining data breaches
- Discuss 1st year of changes after a data breach
- How to identify and prevent “rinse and repeat” mistakes
- 5 year outlook after a data breach
Life after a Breach
Incident vs. Breach Defined

**INCIDENT**

“A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices”

* NIST SP 800-61, Computer Security Incident Handling Guide

**BREACH**

“It’s like a bad parking job. You know one when you see one.”

* Not NIST
<table>
<thead>
<tr>
<th>PEOPLE</th>
<th>An IT employee walks up to the supervisor of another department and says “I think I’ve been compromised.”</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROCESS</td>
<td>During an annual third-party audit, the audit team notices a series of discrepancies with monthly security logs.</td>
</tr>
<tr>
<td>TECHNOLOGY</td>
<td>A third-party vendor who is responsible for offsite backup lost a hard-drive with sensitive data on it. Not sure if it was stolen or not, but it was encrypted.</td>
</tr>
</tbody>
</table>
Year One – “Rack and Stack” Security
Budget and InfoSec Activity
C-Level View

“YOU sold me on THIS”

“I got a LEMON”
Employee View

• “I can’t do my job.”

• “Since you installed all the security stuff I can’t do my job.”

• “It takes forever to get IT help; I can’t do my job.”
“Baked-in” Security – Tears over Time
Hackers Aren’t Your Enemy – Instability Is

- Shift from tactical to risk-based
  - Upper and lower control limits
  - Shift from technology to process
- Measure stability over time
Five Year Roadmap

“CHEAPER IN THE CLOUD?”

“I want tactical, FOR CHEAP”
Key Takeaways

• Money isn’t your enemy, variation is

• Bouncing back is easier than expected

• You will experience a breach
  – You have to control the narrative
Thank You!

Questions?