Internet Security Systems

# SANS Forensic Summit Strategy Panel

# Strategy Panel, Question 1 (part 1)

- **What type of data loss should we be more concerned with, PII or PCI?**
- **Which data did your customer have?**
- **Neither seem to have an appreciable customer confidence impact, and PII breaches (in general) have reporting requirements as the repercussion. PCI breaches will have financial repercussions. If I had to pick one set of data to secure it would be the one that costs money when it is breached.**

# Strategy Panel, Question 1, part 2

- **What should our first priority be? Detailed descriptions of the data that was stolen OR a detailed description of how the break-in occurred?**

**Knowing *what* data was compromised/exposed should take primary importance over the *how*. Notification requirements/legislation focus on *what* was exposed, particularly for reporting and assessing fines. However, all response activities should be directed toward answering both questions.**

**The drivers for incident response are no longer the need to protect the data/customers; current drivers are legislation and regulatory requirements.**

# Strategy Panel, Question 1, part 3

- **If we hire an outside firm to help us with IR: What are the 3 questions that we should ask?**

- **What is the background on consultants assigned to the engagement? What about other team members?**
- **What methodology do the consultants use?**
- **Are the consultants solely focused on IR, or is this one of several services (VA, pen test, etc.) they provide?**

# Strategy Panel, Question 2

**What are the top 3 incident response/forensic mistakes that organizations routinely make? Are there public examples?**

1. **Lack of senior/executive mandate for the capability; efforts focused toward those activities that generate revenue first; lack of staffing, training, etc.**
2. **Lack of understanding of the infrastructure; where data transits and is at rest, how devices interact.**
3. **Responders "stomping" on data.**

***Actions of responders may expose their organization to greater risk than the incident itself.***

# Strategy Panel, Question 2 (Example)

**First responders usually focus on containment/eradication, many times with little to no consideration of regulatory/legislative requirements.**

- **Systems (with sensitive data) infected with malware that *may* have keystroke logger component (based on a single string + Google lookup)**
- **Systems "cleaned", put back into service**
- **Legal/Compliance – was sensitive data exfiltrated??**

**How do you know? How do you determine what sensitive data, if any, was copied off of the system?**

**If you don't know, what do you report?**

# Questions?

**Harlan Carvey**

**hcarvey@us.ibm.com**