SANS WhatWorks Summit 2008
Forensics and Incident Response

IR/Forensics Team Strategy Panel

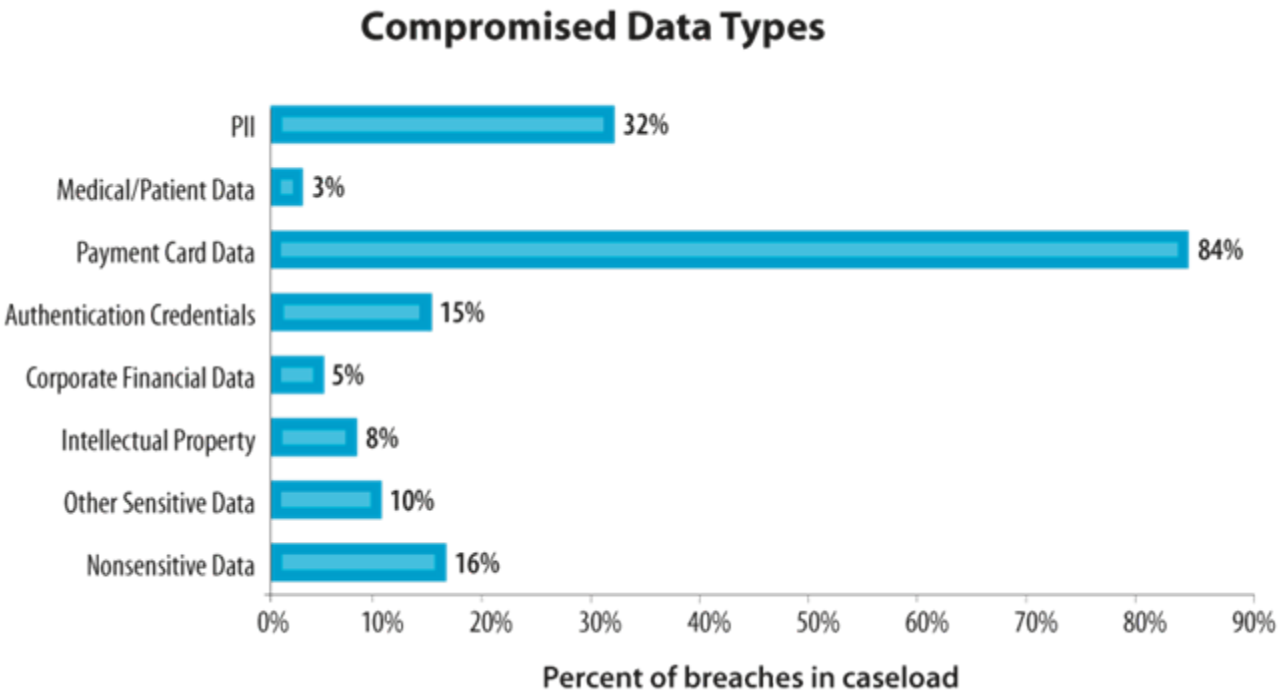
October 14, 2008
Las Vegas, NV

Christopher J Novak
chris.novak@verizonbusiness.com

Eric Gentry
eric.gentry@verizonbusiness.com

Strategic Panel Question #1a

- Q: What type of data loss should we be more concerned with: PII or PCI?
- A: They are both important, but …
  - PII compromise may have more longer term effects for victim
  - PCI may be more immediate; easily converted to cash



Strategic Panel Question #1b and 1c

Q: What should our first priority be: detailed description of the data that was stolen or detailed description of how the break-in occurred?

A: Description of how the break-in occurred.

- Must be understood in order to effectively contain and mitigate
  - STOP THE BLEEDING!
- Impacts of loss can be assessed more clearly
- May confirm whether or not a data compromise occurred

Q: If hiring an outside firm to help with IR, what 3 questions should we ask?

1: What is your response time?

2: What is your expertise with our industry, data type?

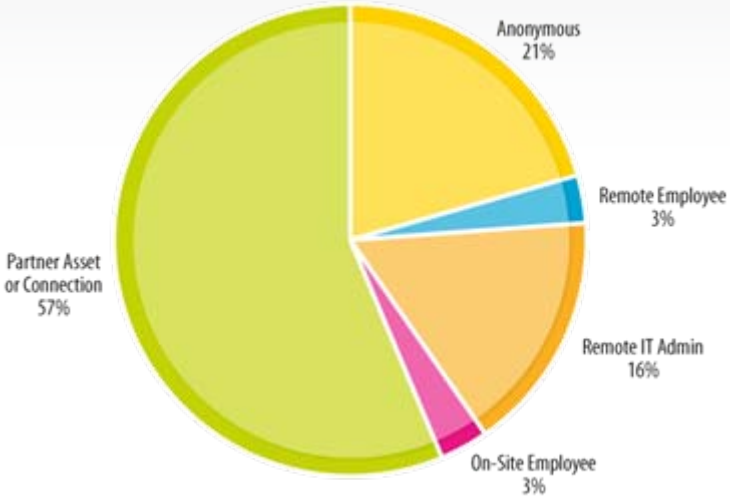
3: What kind of tools and processes do you use? Will your methodology stand up in court?

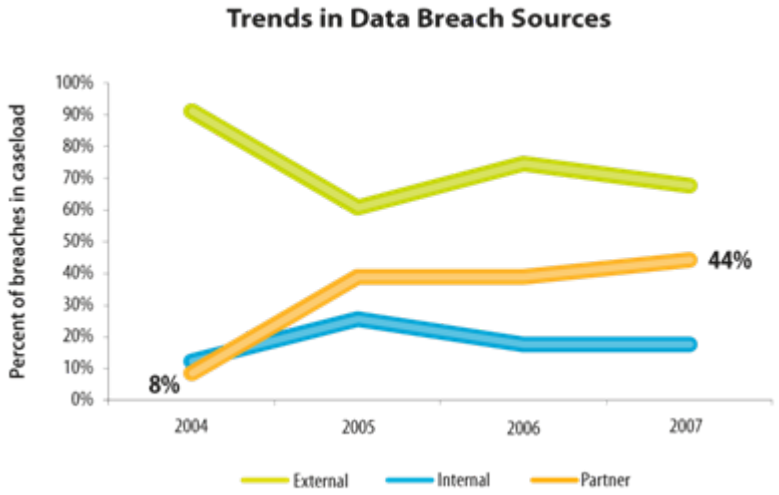
Strategic Panel Question #2a

Q: What is the number one vector of entry leading to the compromise of an organization's network and/or data?

A: Partner sources.

- 5-fold increase in the past 4 years!





Strategic Panel Question #2b

Q: What are some recommended security policies every organization should adhere to in order to prevent future attacks and outbreaks?

1. Know what/where your sensitive data resides in the environment.
2. Establish and maintain accountability for all access to that data.
3. Secure those partner connections.
4. Enable, analyze, and archive log data. (82%!)
5. Have a formal IR plan and a trained team of Incident Responders.
   - Not just an “IT” problem!
   - Should also include Management, HR, Legal, PR, etc.
6. Mock incident scenarios.