Two Truths and a Lie
Data Breaches
Two Truths and a Lie

- U.S. and China represent over 50% of malicious activity by source geography.
- Cost per breach is rising per incident and per record.
- Zero day vulnerabilities are rising.
Overview

- Security Snapshot: Spending Patterns
- Crisis Management
  - Manage risk
  - Lessen severity
- Crisis Communication
  - Protecting your reputation/brand
Spending Patterns

- Endpoint Security: 46%
- Encryption of Confidential Data Stored in the Cloud: 45%
- Web Application Firewall (WAF): 43%
- Advanced Anti-malware/Anti-APT: 42%
- Security Information & Event Management (SIEM) and...: 36%
- Identity Management: Authorization/Access Control and...: 35%
- Secure Configuration Management: 35%
- Vulnerability Assessment: 33%
- Data Sovereignty/Data Residency: 33%
- Endpoint or Network Data Leakage Prevention (DLP): 31%
- Computer/Network Forensics Support/Breach Response: 29%
- IT GRC – Governance, Risk, Compliance: 29%
- Anti – DDoS – Anti-Distributed Denial of Service: 29%
- Auditability capabilities – environment can be audited by...: 26%
- Liability Guarantees/Insurance in event of a breach or loss: 25%
- None: 4%

N = 1,619
Source: 451 Research
Preparation

- Identify stakeholders expectations
  - More than IT
  - Strategy
- Establish CIRT
  - Roles and Responsibilities
  - Priorities
  - Procedures
- Develop breach response plan
- Annual training including dry run
- Update your scenarios
Crisis Communication (Your Deliverables)

1. Do we have a representative set of planning scenarios?
2. Do we have a flexible set of response modules?
3. Do we have an established matching of response modules to scenarios?
4. Do we have preset signals for activating the crisis response?
5. Do we have a clear chain of command?
6. Do we have a command post and backup?
7. Do we have the right communication channels?
8. Have we put in place the right backup resources?
9. Do we conduct regular rehearsals?
10. Do we do disciplined post-crisis reviews?
Data Tips

- Keep only what you need
- Safeguard data
- Destroy before disposal
- Update procedures
- Train employees
- Control use of computers
- Secure all computers
- Keep security software up to date
- Manage use of portable media