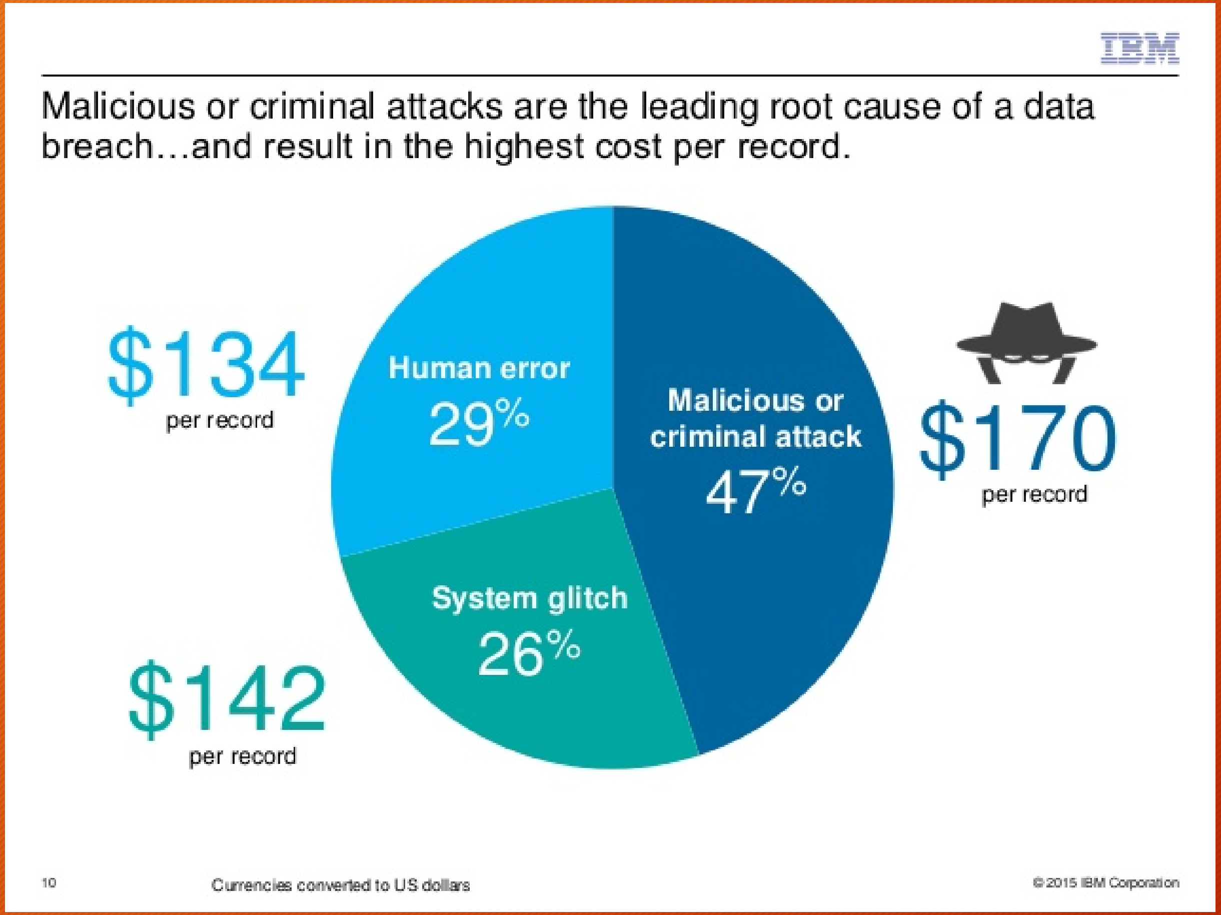
Data Protection in a Connected World

Wynn J. Salisch
CCM, ETA CPP, MBKS

Chairman & Founder
Casablanca Ventures LLC

Partner
Electronic Crimes Task Force
U.S. Secret Service

Data Compromise Risk to Your Cinema: High Cost Due to High Transaction Counts



IBM

Malicious or criminal attacks are the leading root cause of a data breach…and result in the highest cost per record.

10

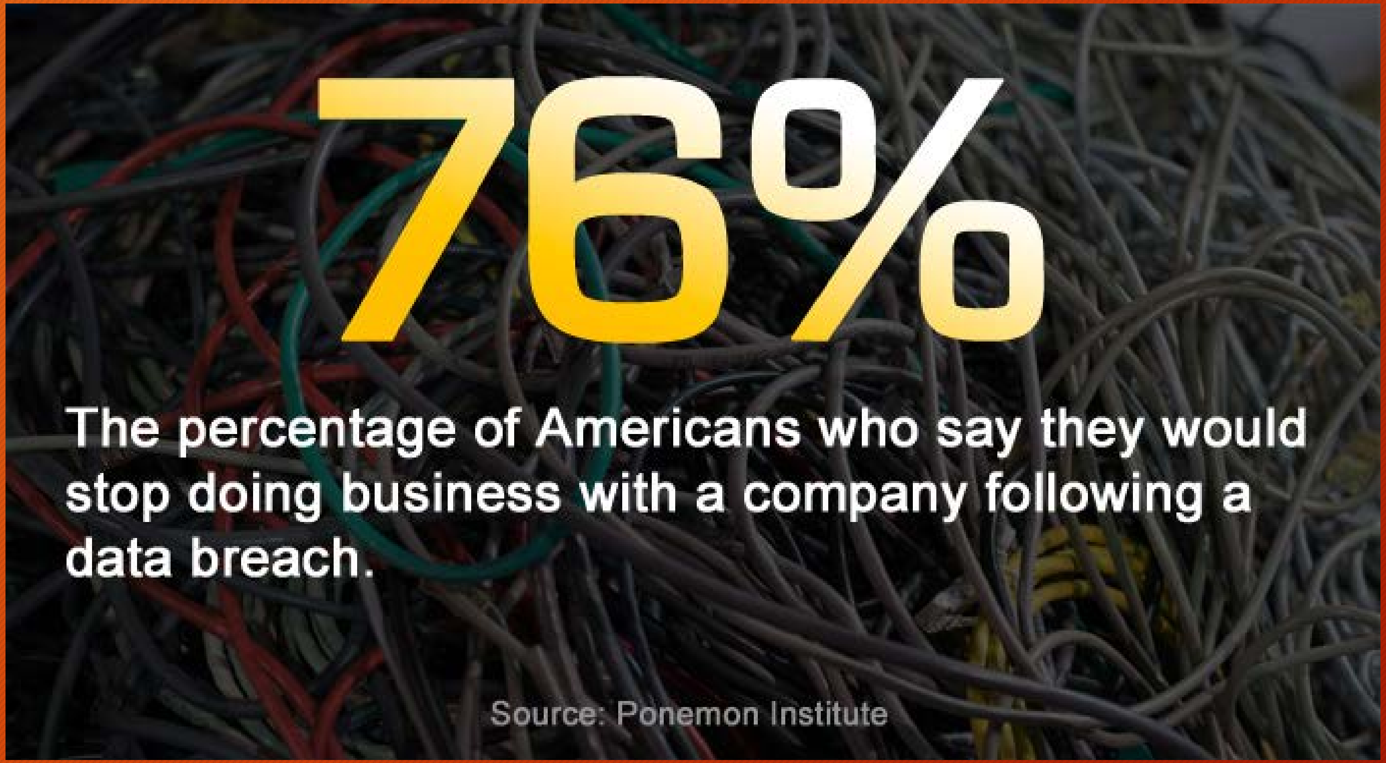
Currencies converted to US dollars

© 2015 IBM Corporation

Average time from breach to detection:

283 days

Data Compromise Risk to Your Cinema: Lost Business



76%

The percentage of Americans who say they would stop doing business with a company following a data breach.

Source: Ponemon Institute

Cinema Data Risk by the Numbers

- **4,000+** cyber attacks **daily**.
- **89%** of confirmed breaches had a financial or espionage motive.
- **80%** of card data compromises occur in small businesses of 250 employees or less

  …**60%** of which go then out of business within 6 months.
- **72%** of breaches involved firewalls not up to security standards or improperly configured.
- **63%** of breaches involved weak, default or stolen passwords.
- **61%** of breached merchants didn't have effective antivirus software.
- **60%** of hackers compromise an organization within minutes.
- **30%** of phishing messages were opened in 2015

  …12% of targets clicked on the malicious attachment or link

  …50% of those did so within an hour.

Sources: Department of Homeland Security, 2016 Verizon DBIR, PCI Security Standards Council, Digital Transactions (March 2016)

Case Study: The Target Breach

- HVAC contractor breached via malware delivered in an email.
- Thieves stole VPN (virtual private network) credentials used by the contractor to remotely connect to Target's network.
- Used that foothold to push malicious software down to all of the cash registers at more than 1,800 stores nationwide.
- 70 MILLION account numbers stolen
- ~$8.50 each on the dark web = $595,000,000.00 value to hackers
- Total Cost to Target: $291 million PLUS lost sales and profits due to reduced consumer trust

Multi-Layered Security: The Big 10

1. PCI DSS – Payment Card Industry Data Security Standard
2. Encryption – protects data in motion
3. Tokenization – protects data at rest
4. EMV – protect against counterfeit (cloned) cards; not required by any regulation, law, or PCI, so many cinemas and fast food operators are bypassing
5. Smart Passwords – no dictionary words, children or pet names, or default passwords
6. Two-Factor Authentication – complex password + cellular text code or biometric scan
7. IT Infrastructure – cinema credit card processing should be on its own separate server
8. Networked Vendor Compliance – cinema NOC, POS, HVAC and other connected suppliers
9. Awareness
10. Action