CISO, CISE, CISL?

A Focus on Information Security

EXECUTIVES and **LEADERS**

ABSTRACT:

Security is becoming less about tools and much more about business acumen and leadership skills. Successful CISO's are engaged executive partners who understand the core business processes of the organization as well as the safety net that must be built around it.

Presented at The ISE Southeast Executive Forum and Awards
August 11, 2010

Fernando Martinez, VP & Chief Information Officer
2009 ISE Southeast Winner

Jackson HEALTH SYSTEM
PUBLIC HEALTH TRUST

The role of the CISO is evolving in the context of Governance

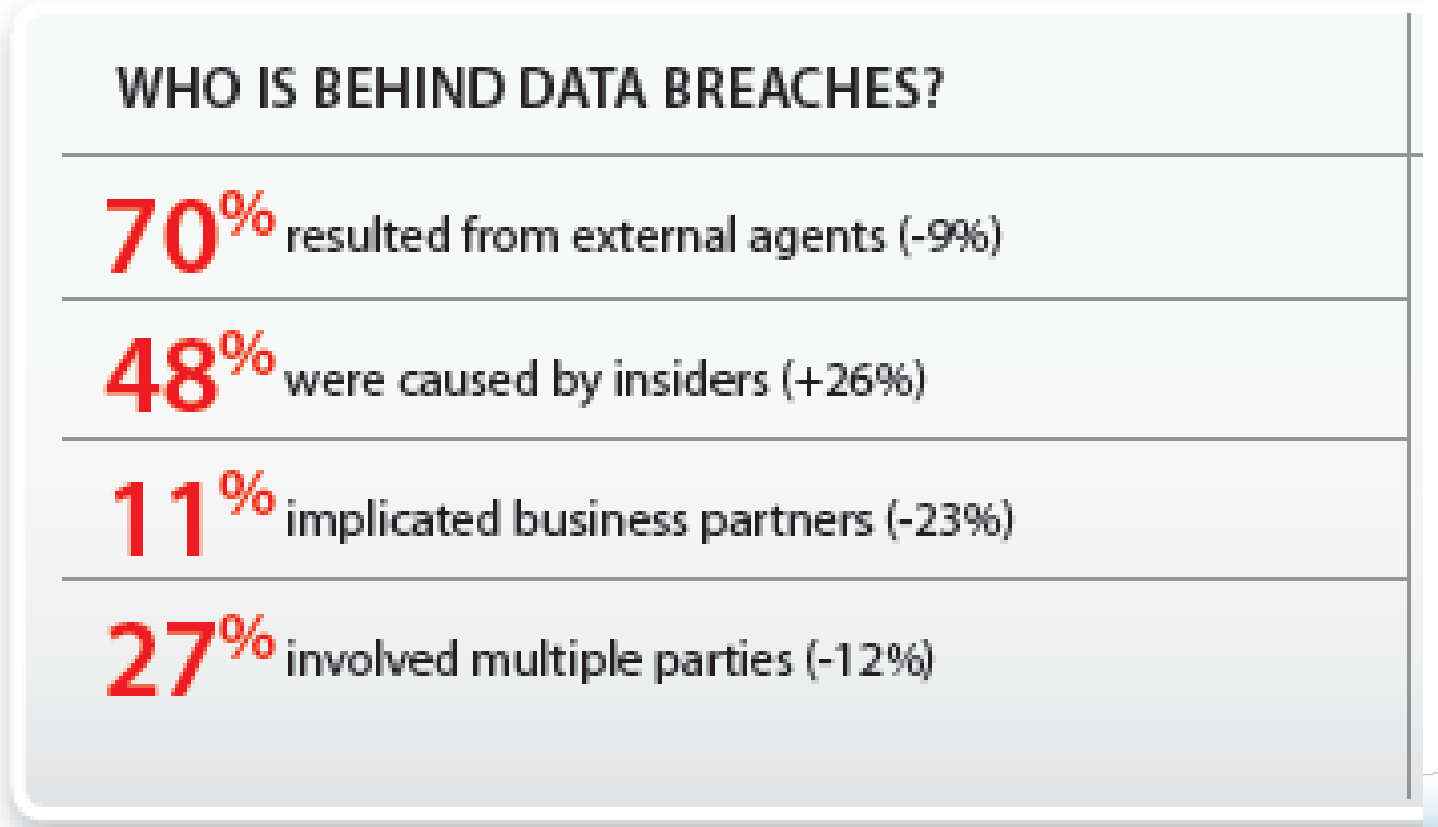
Is the title CISO the best fit?

How about CISE?

Or CISL?

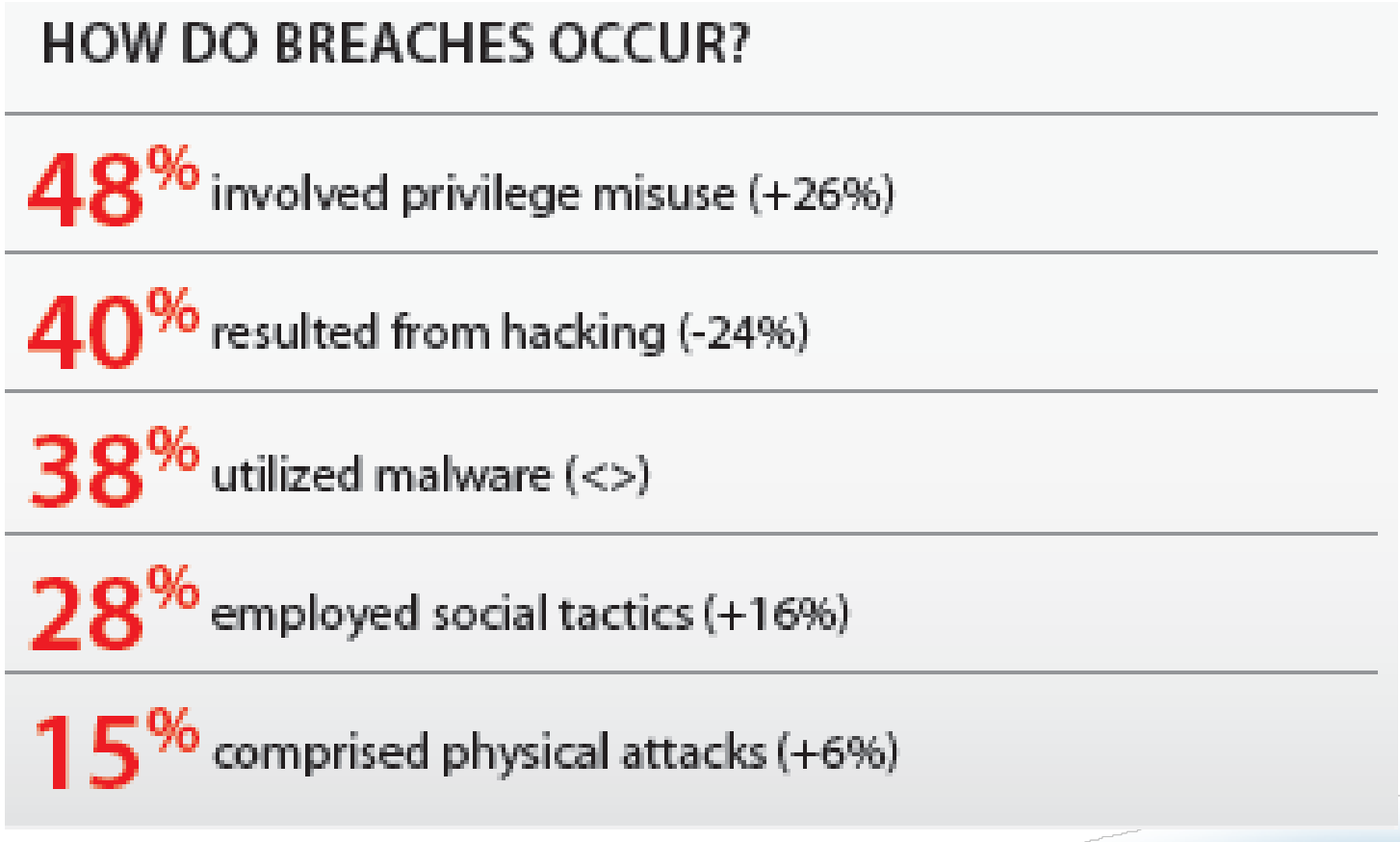
There is a growing responsibility to educate, inform and lead as a security professional.

Security Environment



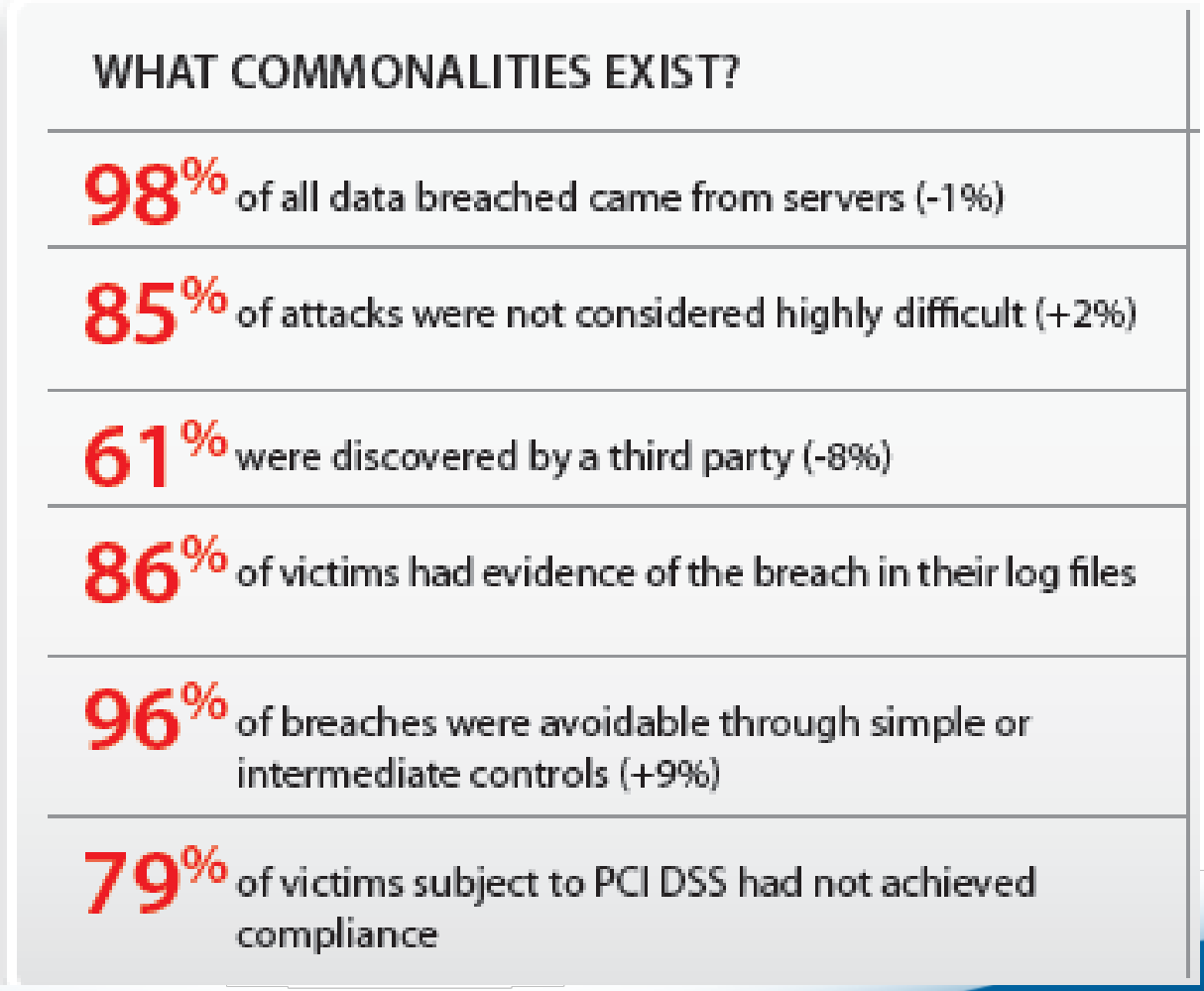
Courtesy Verizon 2010 Data Breach Investigation Report

Security Environment



Courtesy Verizon 2010 Data Breach Investigation Report

Security Environment



Courtesy Verizon 2010 Data Breach Investigation Report

Strengthening Organizational Security

Verizon Report Highlights

-> Ensure that essential controls exist

-> Audit user accounts

-> Monitor privileged activity

-> Monitor AND Mine event logs

Courtesy Verizon 2010 Data Breach Investigation Report

Jackson HEALTH SYSTEM

PUBLIC HEALTH TRUST

Get Started!

1. Identify and inventory your mission critical applications - (apply the 80/20 rule)

2. Systematically address all priority applications with the corresponding stakeholders

   - Easier said than done, but it MUST be done.

Managing access

- Requires 1X1, side-by-side interaction. Cannot be delegated or “assigned”
- Define the provisioning process and automate as much as possible
- Develop and implement a control audit program
  - First weekly, then monthly, then quarterly if compliance is at 100%
  - On backslide back to weekly

Repeat the process

- Expand this activity until all major (mission critical) applications are accounted for.
- This would be the 80 of the 80/20.
- Once this is done STOP and re-evaluate.
  - Of the remaining applications, where is the greatest risk
  - Work at addressing as many as you can

Refine and Strengthen

- Develop formal standards, but not in the conventional sense.
  - Certification standards
    - Before a server, or workstation or notebook or even a handheld device.
    - Use a checklist!
    - You are only as strong as your weakest link
- This puts the CISO in the role of enterprise advocate, it “operationalizes” the role

One more time

- Critical to know who owns the data, where it is and to what degree it is federated. This is a key step in identifying the “80”
- How “tight” is the provisioning process
  - UAR’s – can it be circumvented?
  - If it is, how do you identify it?
  - Conduct and live by control audits – proactively. Don’t wait for external audits

Control vs. Compliance audits

- Combine to augment risk management. Each strengthens the other.
- One asks if you have controls the other asks if the controls are working.
- One is annual or bi-annual, the other is ongoing.
- WORTH THE EFFORT – leadership in action, be your best critic!

Role Based Access

- Must be determined by the data owner
- Can't be delegated – there are different perspectives.
  - The data owner is thinking what is most convenient for workflow and process
  - The CISO is thinking doctrine of least privilege
  - Find a way to reconcile!
- Another example of leadership in action

Privilege escalation

- Reflects maturity in security architecture
- Must be done in real-time to be effective
- Significantly strengthens accountability and accordingly security posture
- Can be limited yet still effective
  - Reverse 80/20, or perhaps 95/5?
  - Focus on privileges with global reach

Closing thoughts

- Impact of winning ISE 2009
- Don’t be a victim of your own success
- RESIST being marginalized
- Do this by being
  - A business driver
  - A real value to your organization
  - Demonstrate true business accumen

Jackson HEALTH SYSTEM
PUBLIC HEALTH TRUST

Thank you

Fernando Martinez, VP/CIO
Jackson Health System, Miami Florida 33136

Jackson HEALTH SYSTEM
PUBLIC HEALTH TRUST