How to Develop an Information Security Program: *The Basics*

Leslie Golden, CISSP
President, Instill Security

1. Who's in the room?
2. What can we do in 40(ish) minutes?
3. "What can I take away with me?"

Instill SECURITY

85%

WHAT'S MOST AT RISK, AND WHAT PRICE DO WE PAY?

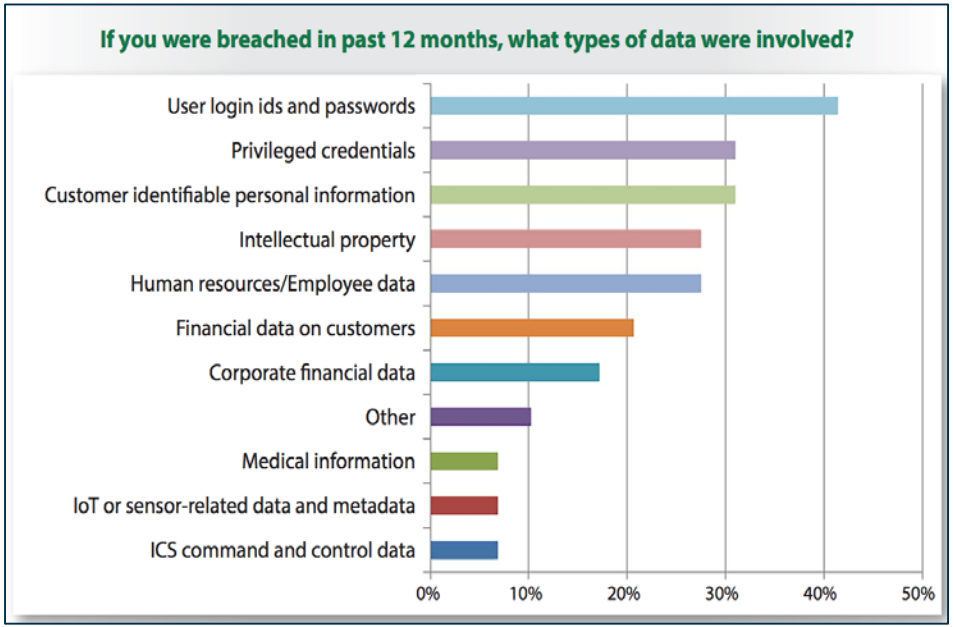


Table 1. Top Impacts from Breach

Industry	Response Percentage
Enterprise customer confidence	50.0%
Legal	46.2%
Brand reputation	42.3%
New technology costs to improve protective controls	23.1%
Direct loss of sales	19.2%
Financial losses directly from our company accounts	11.5%
Regulatory fines because not in compliance	11.5%
Other	11.5%
Valuation loss due to impact on stock/investors	7.7%

85%

WHAT INFORMATION SHOULD WE BE PROTECTING?

Start with knowing your drivers: *Information Security* or *Compliance?*

- Payment Card Information (PCI)
- Health Care Information (PHI/ePHI)
- **Personally identifiable information** (PII): Any data that could potentially identify a specific individual.

Due Diligence: Making legitimate and verifiable efforts to protect data based on your organization's understanding and accepting of **risk** (vulnerability management).

DRIVING GOALS OF INFORMATION SECURITY

85%

STARTING POINT FACTORS

DATA TYPE(S) +

GUIDANCE:

- INFORMATION SECURITY VS. COMPLIANCE
- FRAMEWORKS/STANDARDS/REQUIREMENTS
- CONTROLS
- CULTURE CHANGE

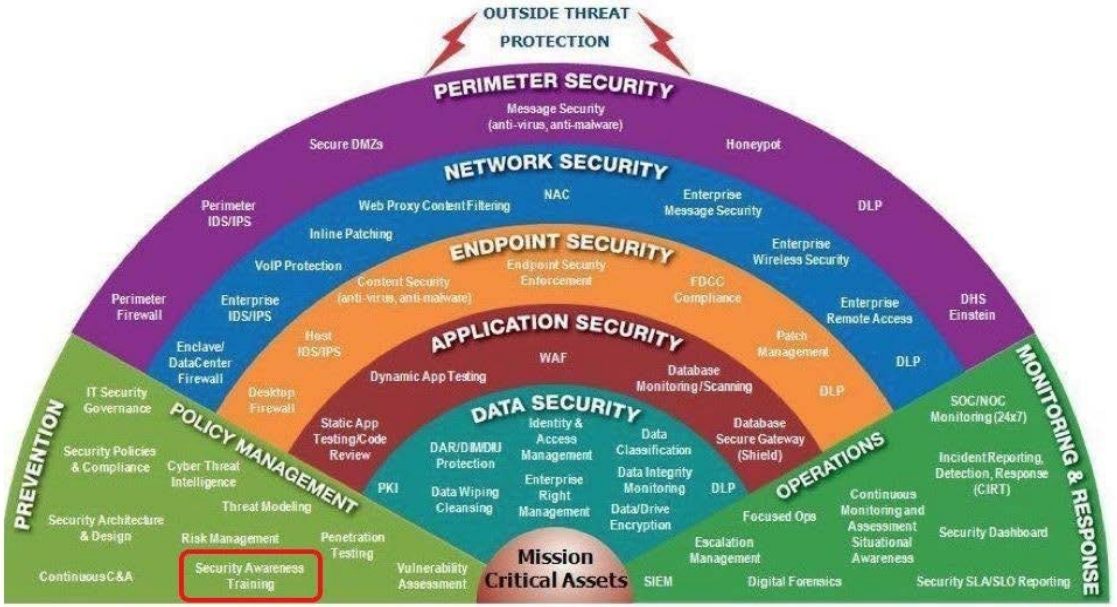
=

BUT HOW DO YOU KNOW WHERE TO FOCUS?

IT'S ALL ABOUT THE TECH, RIGHT?

85%

Charts like this is why information security is failing.



HOW DO WE START DEVELOPING AN INFOSEC PROGRAM?

INFOSEC PROGRAM OBJECTIVES

1. **Identify** and categorize sensitive data and assets
2. **Assess** vulnerabilities - *Risk Management & Tolerance*
3. **Protect** the data - ***Controls*** *based on Priorities*
4. **Continuous Improvement**

85%

BUT WHAT DO I DO NOW?

- DON’T REINVENT THE WHEEL
- DEVELOP AN IMPLEMENTATION PLAN THAT IS SLOW, STEADY, & REALISTIC
- BUILD PRACTICES THAT ARE SUSTAINABLE
- SEIZE EVERY OPPORTUNITY TO RECRUIT INTERNAL FOLKS WHO ARE INTERESTED IN DRIVING CHANGE
- NEVER STOP TELLING LEADERSHIP THAT 85% OF RISK COMES FROM PEOPLE NOT KNOWING BETTER

Instill SECURITY

QUESTIONS?

www.instillsecurity.com

THANK YOU!