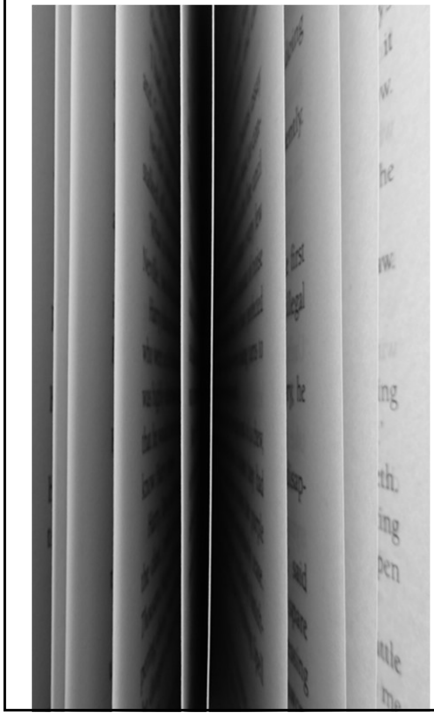


Privacy and Security Risk Assessment Best Practices

Orlando Regional Healthcare Compliance Conference

January 31, 2020

Connie Barrera
Chief Information Security Officer
Jackson Health System

Blaine Kerr
Chief Privacy Officer
Jackson Health System

1

Session Objectives

- Understanding cross-section between security and privacy-deconstructing a robust security/privacy risk assessment program.
- Analyzing the anatomy of a breach.
- Operationalizing system-wide security and privacy program, including key measures of success.

2

"Terms of Importance"

- Data…A representation of information including digital and non-digital formats
- Data Action…A system/product/service data life cycle operation, including but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission and disposal.
- Data Processing…The collective set of data actions (the complete data life cycle, including but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission and disposal).
- Privacy Risk…The likelihood that individuals will experience problems resulting from Data Processing and the impact should they occur.

3

Relationship Between Security and Privacy Risk

- Security Risks associated with loss of confidentiality, integrity or availability of data
- Privacy Risks associated with the unintended consequences of data processing
- A privacy breach occurs at the intersection of these two risks

4

Privacy Risk and Organizational Risk

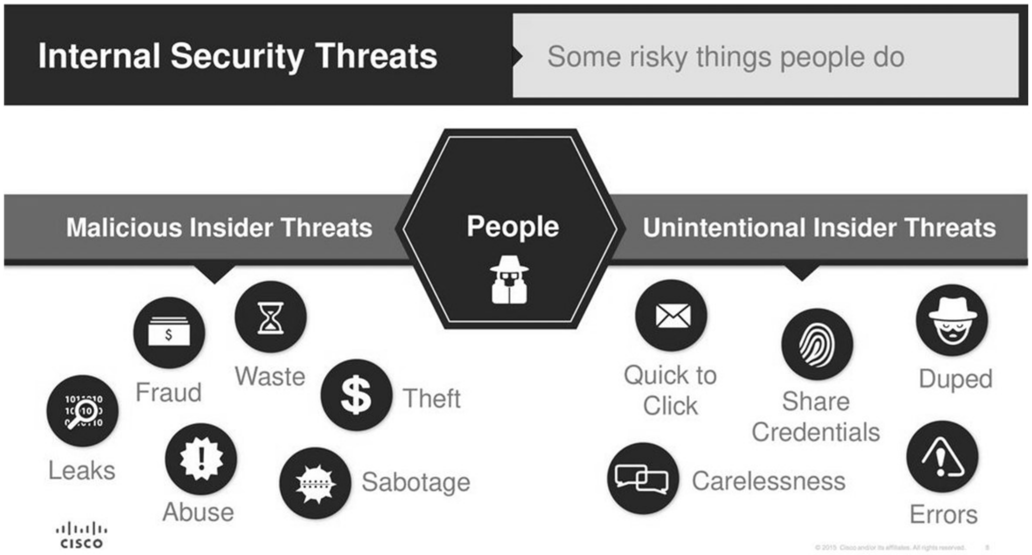
- Problem…arises from Data Processing

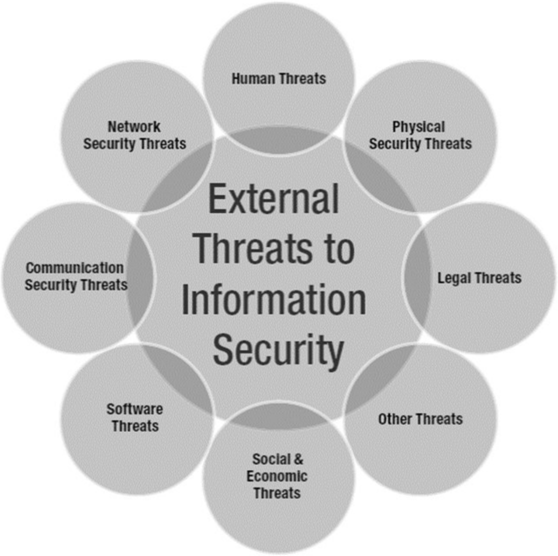
⇩

- Individual…experiences direct impact (embarrassment, discrimination, economic loss)

⇩

- Organization…resulting impact (customer abandonment, non-compliance costs, harm to reputation or internal culture


Internal Security Threats
Some risky things people do
Malicious Insider Threats
People
Unintentional Insider Threats
Fraud
Waste
Theft
Leaks
Abuse
Sabotage
Quick to Click
Share Credentials
Duped
Carelessness
Errors
cisco



External Threats to Information Security

Human Threats

Physical Security Threats

Legal Threats

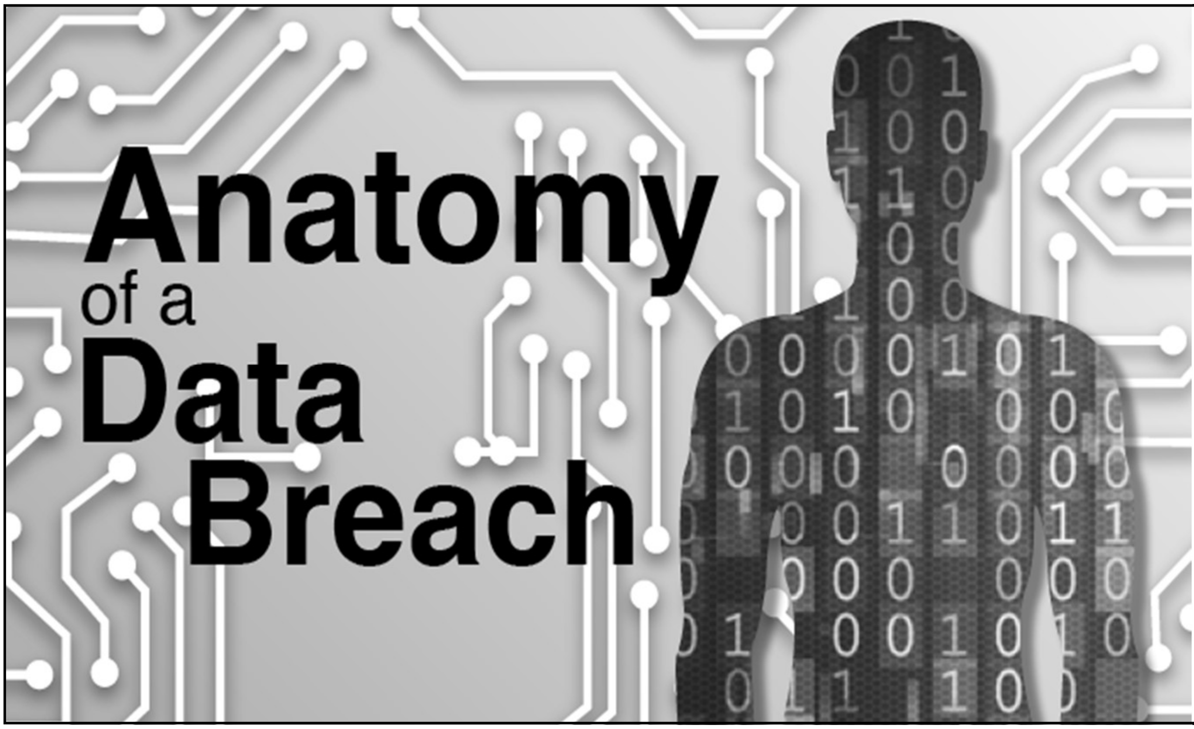
Other Threats

Social & Economic Threats

Software Threats

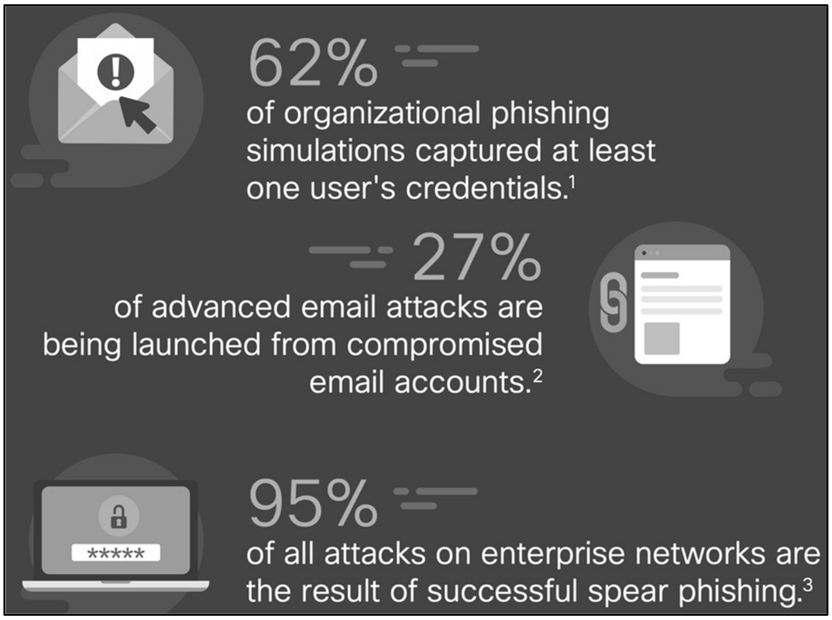
Communication Security Threats

Network Security Threats



Anatomy of a Data Breach

The “Phish”



62%

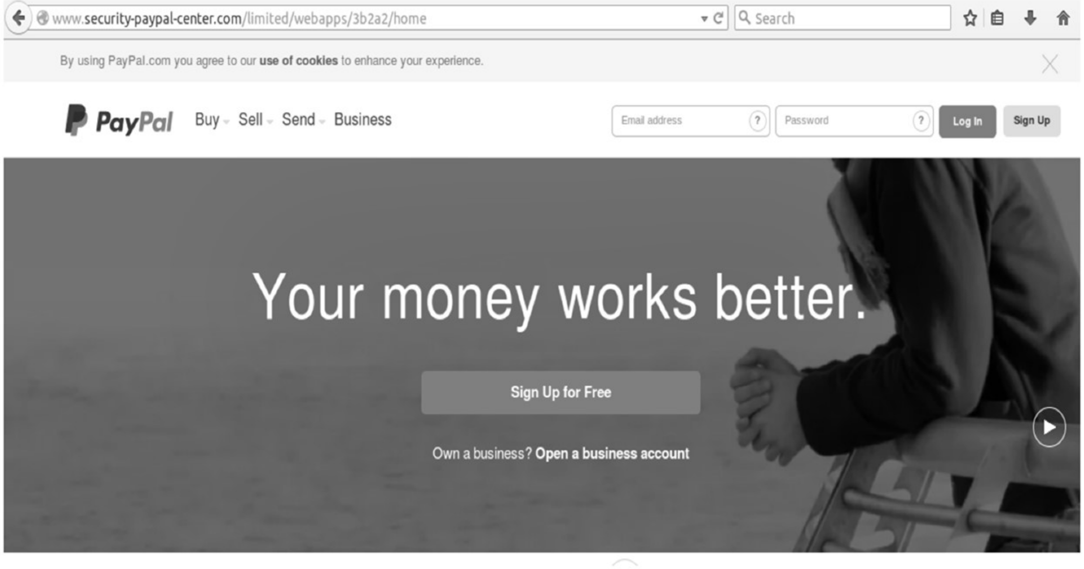
of organizational phishing simulations captured at least one user's credentials.[1]

27%

of advanced email attacks are being launched from compromised email accounts.[2]

95%

of all attacks on enterprise networks are the result of successful spear phishing.[3]



www.security-paypal-center.com/limited/webapps/3b2a2/home

By using PayPal.com you agree to our **use of cookies** to enhance your experience.

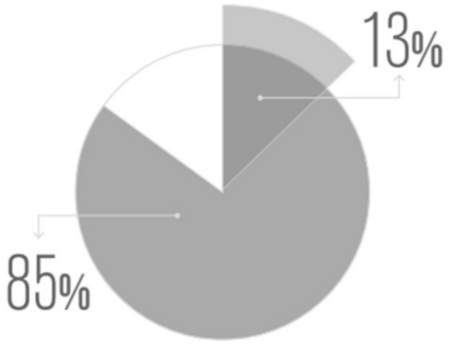
Your money works better.

Own a business? **Open a business account**

Unpatched Assets

"Cybersecurity: One in three breaches are caused by unpatched vulnerabilities"

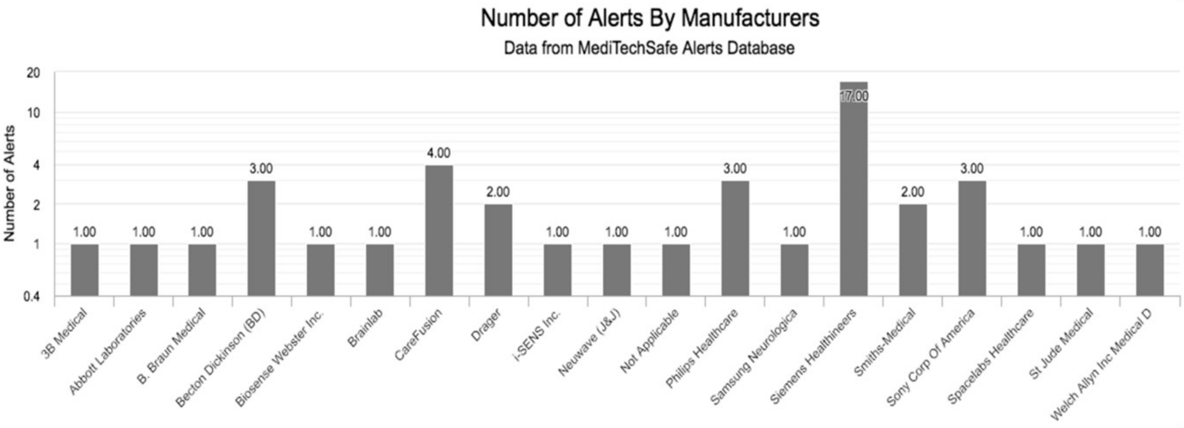
ZDNet June 4, 2019



More than 13% of all applications have at least one critical severity flaw.

More than 85% have at least one vulnerability in them.

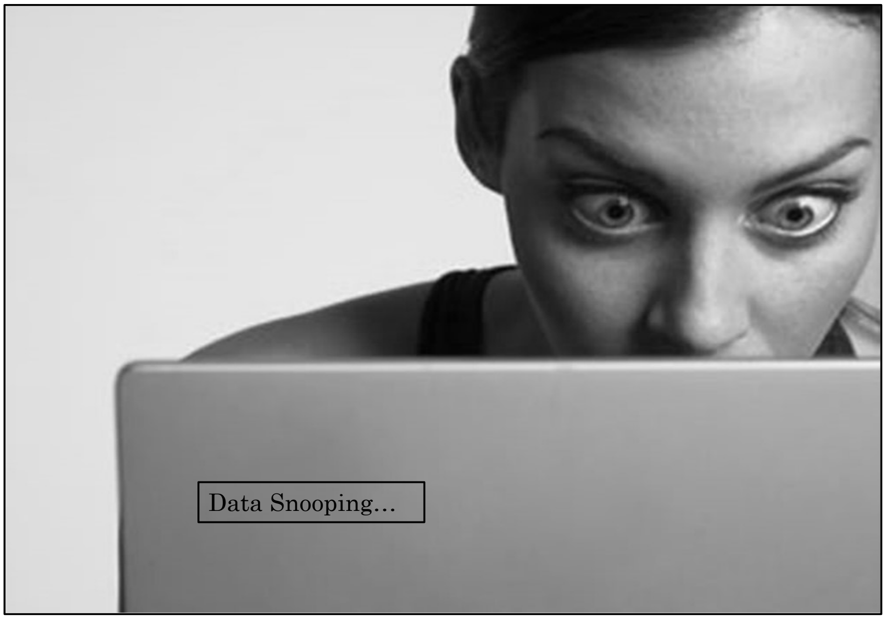
Unpatched Assets



Unauthorized Use/Disclosure

13

Unauthorized Use/Disclosure



14

Security and Privacy Framework Alignment

Information Security Risk Assessment should address:

1. Policies and Procedures
2. Identity and Access Management
3. Threat Mitigation
4. Information Protection
5. Incident Response
6. Security Management
   - Visibility
   - Tool Efficacy
   - Team Performance

Sergey Nivens/ShutterStock.com

15

15

Security and Privacy Framework Alignment

Privacy Risk Assessment component should address:

1. Identification
2. Governance
3. Control
4. Communication

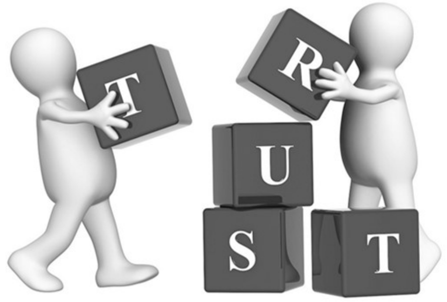
16

16

Security and Privacy Framework Alignment

Supports:

1. Building organizational trust
2. Fulfilling compliance obligations
3. Facilitating communication



"Questions of Importance"

1. What are the cybersecurity and privacy risks you need to manage as an organization?
2. Do you have sufficient resources and processes in place to manage these risks?
3. Where are you in terms of having resources and processes and where do you want to be?

Key Performance Measures

1. Security Management Visibility
2. Kill Chain Coverage
3. Incident Response Metrics
4. Quarterly Security Metrics
5. Constituent Engagement

Future Challenges

1. Emerging Technologies
2. Ever Changing Workforce
3. Information Security and Privacy Resources
4. Changing Technical Standards
5. Changing Regulatory Requirements

21

21