GreyCastle security

PERFORMING EFFECTIVE HIPAA RISK ASSESSMENTS

DO’s and DONT’s

500 Federal Street
Suite540
Troy, NY 12180
www.greycastlesecurity.com
(800) 403-8350

PRESENTER

MATT FARRY
SENIOR SECURITY SPECIALIST
GREYCASTLE SECURITY

Why Risk Management

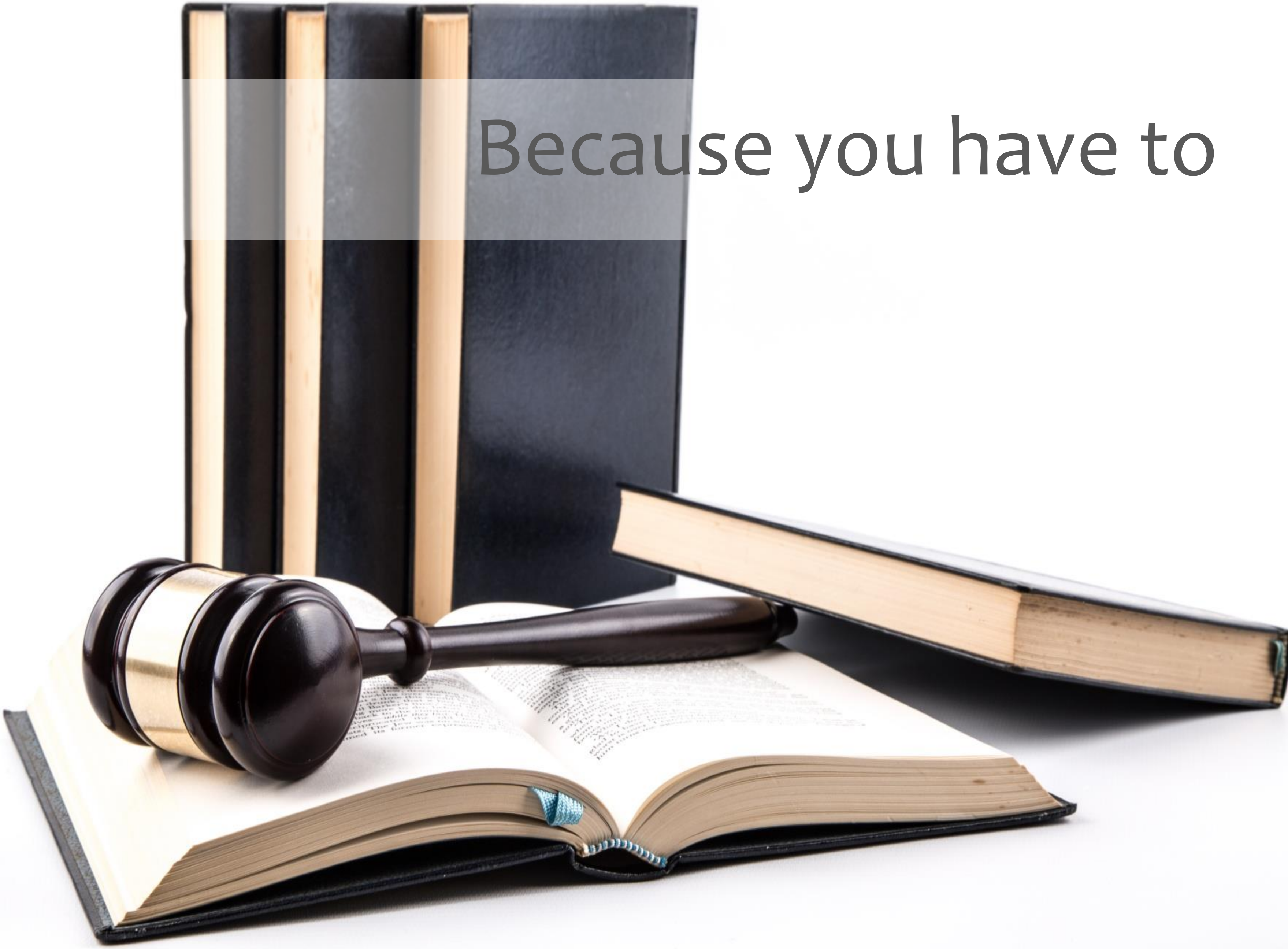
How to Determine Risk

Risk Mitigation, Not Risk Eradication

PEOPLE WHO CARE

WHY RISK MANAGEMENT

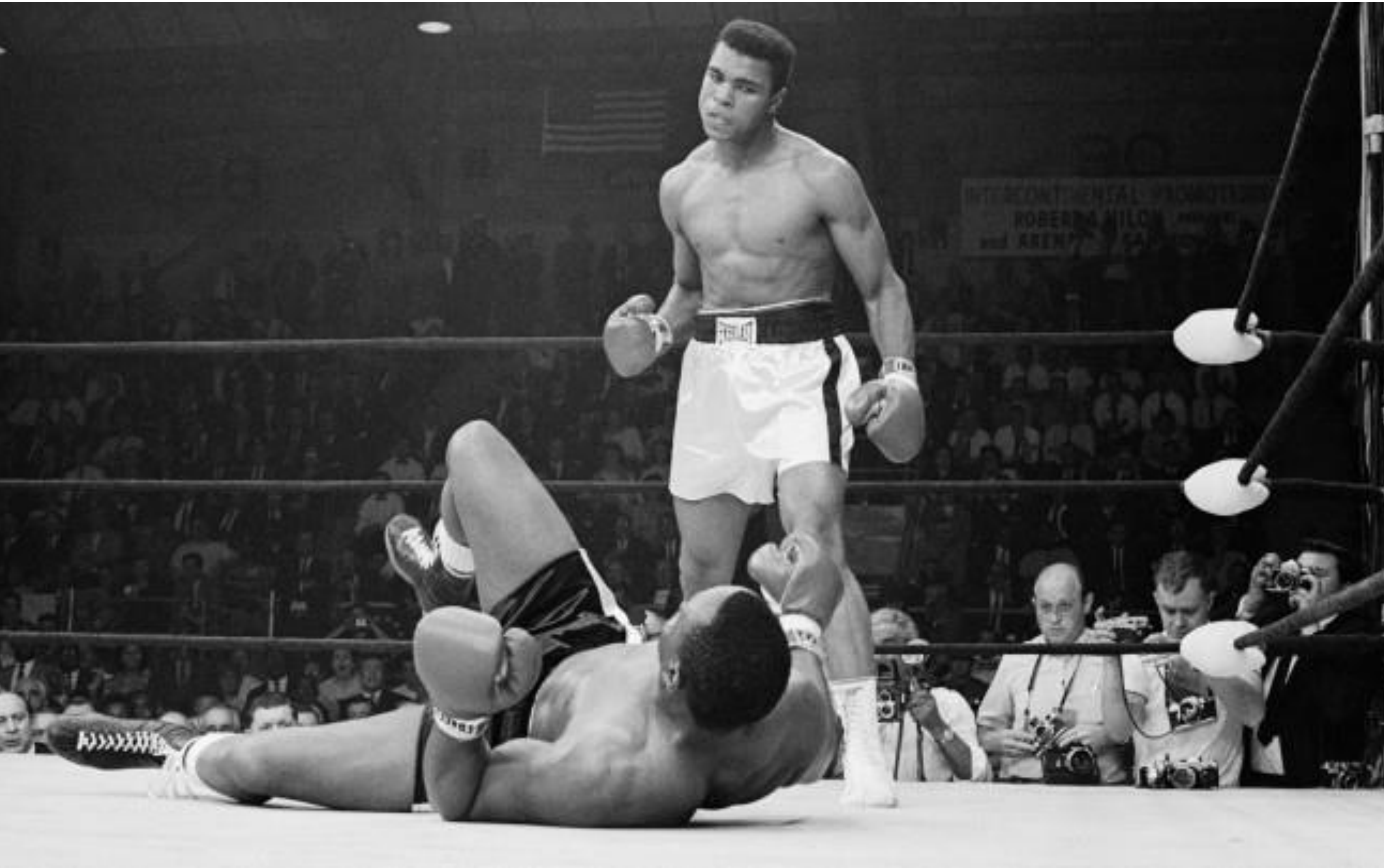
Bald Tire Scenario



Because you have to

Because you can’t always be completely secure

Security VS. Compliance



HIPAA & RISK MANAGEMENT

GreyCastle security

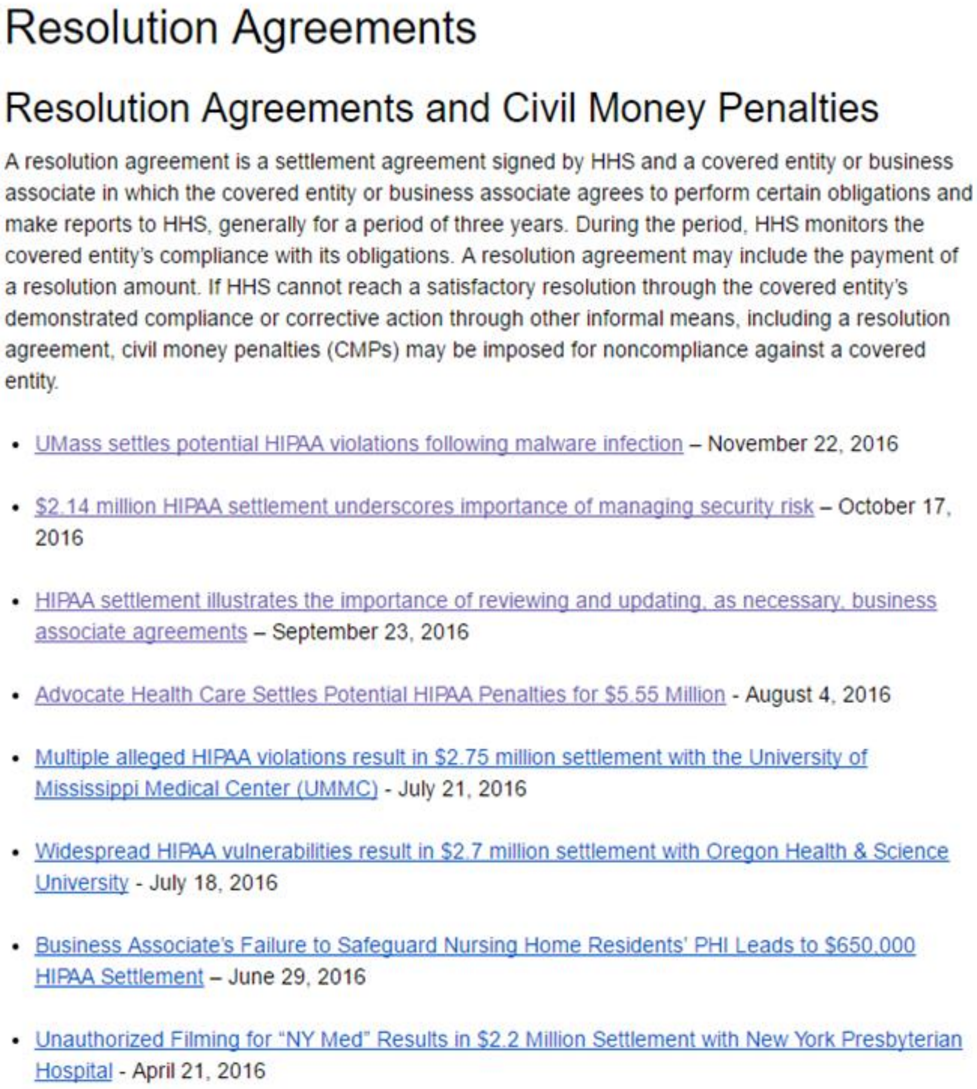
WHAT DOES HIPAA SAY?

- RISK ANALYSIS (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization].
- The outcome of the risk analysis process is a critical factor in assessing whether an implementation specification or an equivalent measure is reasonable and appropriate. Organizations should use the information gleaned from their risk analysis as they, for example:
  - Design appropriate personnel screening processes. (45 C.F.R. § 164.308(a)(3)(ii)(B).)
  - Identify what data to backup and how. (45 C.F.R. § 164.308(a)(7)(ii)(A).)
  - Decide whether and how to use encryption. (45 C.F.R. §§ 164.312(a)(2)(iv) and (e)(2)(ii).)
  - Address what data must be authenticated in particular situations to protect data integrity. (45 C.F.R. § 164.312(c)(2).)
  - Determine the appropriate manner of protecting health information transmissions. (45 C.F.R. § 164.312(e)(1).)

WHAT HAPPENS WHEN WE FAIL?

Three of the last four HIPAA Resolution Agreements required organizations to:

- Perform a risk analysis
- Perform risk management



Resolution Agreements

Resolution Agreements and Civil Money Penalties

A resolution agreement is a settlement agreement signed by HHS and a covered entity or business associate in which the covered entity or business associate agrees to perform certain obligations and make reports to HHS, generally for a period of three years. During the period, HHS monitors the covered entity's compliance with its obligations. A resolution agreement may include the payment of a resolution amount. If HHS cannot reach a satisfactory resolution through the covered entity's demonstrated compliance or corrective action through other informal means, including a resolution agreement, civil money penalties (CMPs) may be imposed for noncompliance against a covered entity.

- UMass settles potential HIPAA violations following malware infection – November 22, 2016
- $2.14 million HIPAA settlement underscores importance of managing security risk – October 17, 2016
- HIPAA settlement illustrates the importance of reviewing and updating, as necessary, business associate agreements – September 23, 2016
- Advocate Health Care Settles Potential HIPAA Penalties for $5.55 Million - August 4, 2016
- Multiple alleged HIPAA violations result in $2.75 million settlement with the University of Mississippi Medical Center (UMMC) - July 21, 2016
- Widespread HIPAA vulnerabilities result in $2.7 million settlement with Oregon Health & Science University - July 18, 2016
- Business Associate's Failure to Safeguard Nursing Home Residents' PHI Leads to $650,000 HIPAA Settlement – June 29, 2016
- Unauthorized Filming for "NY Med" Results in $2.2 Million Settlement with New York Presbyterian Hospital - April 21, 2016

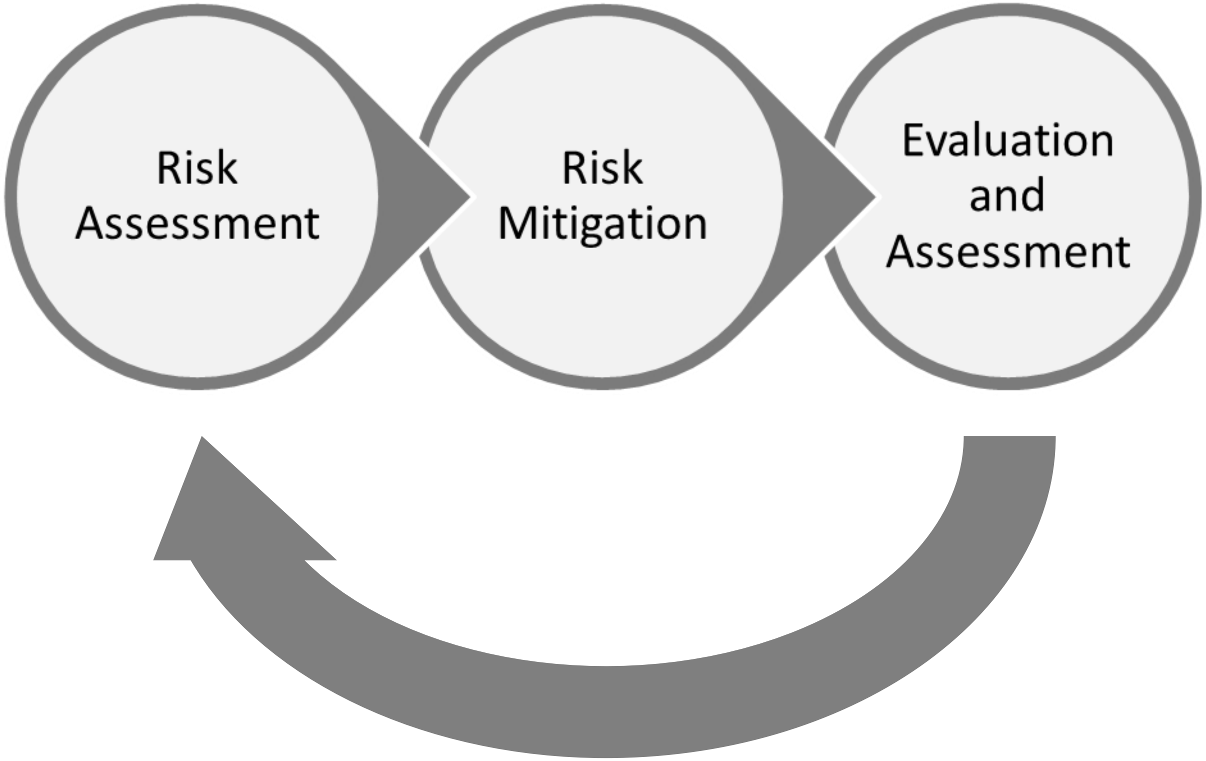
SHOW ME THIS THING YOU CALL RISK MANAGEMENT

RISK MANAGEMENT 101

“the total process of identifying, controlling and mitigating information system-related risks”*

* National Institute of Standards in Technology (NIST) SP800-30

RISK MANAGEMENT 101



GreyCastle security

RISK MANAGEMENT 101

- Focus on:
  - Confidentiality
  - Integrity
  - Availability
- Qualitative or Quantitative
- Balances risk, effort and costs

RISK ASSESSMENT

4 phase approach

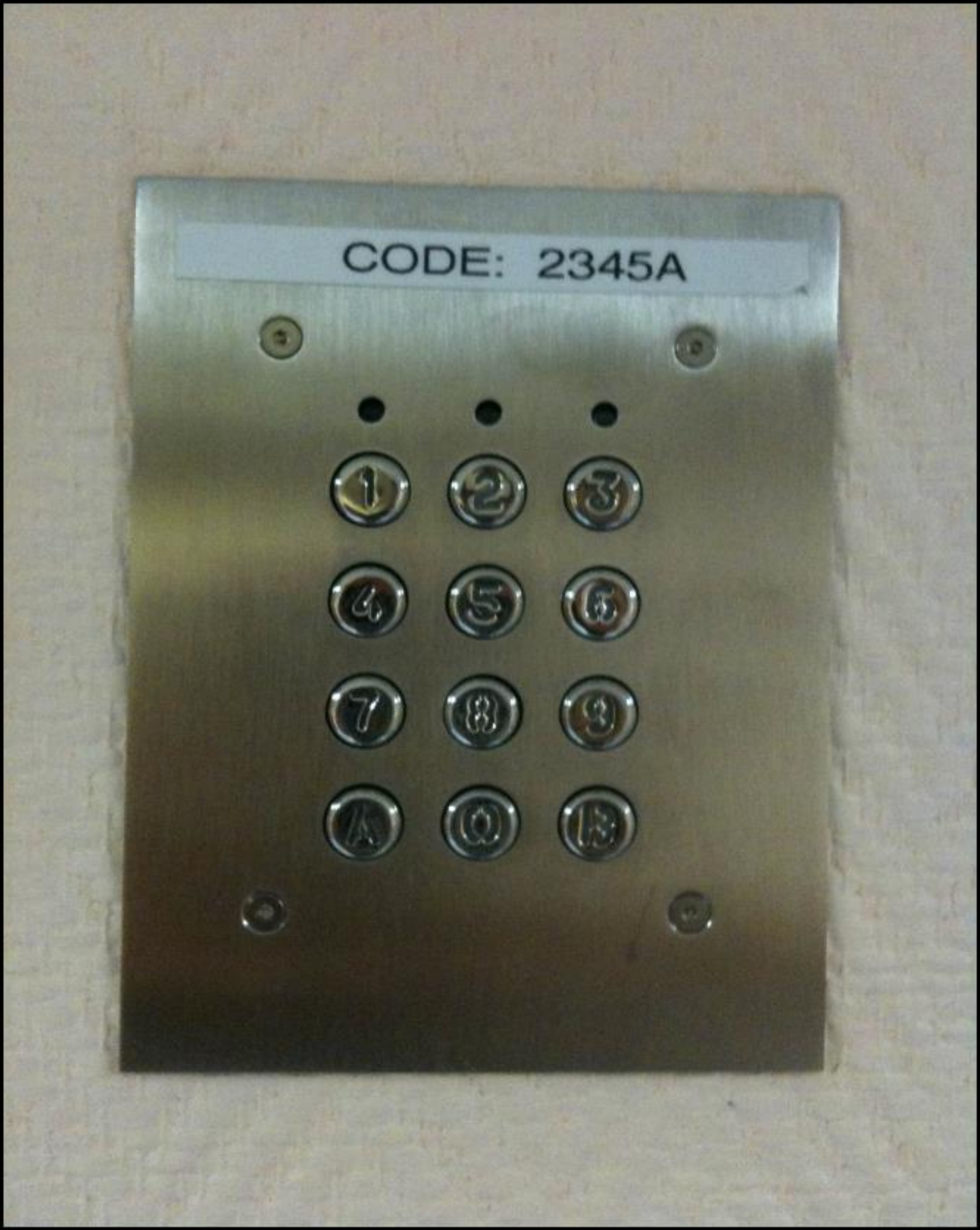
Phase 1 – System Characterization

- Characterize system boundaries, criticality and sensitivity based on:
  - Hardware
  - Software
  - Interfaces and integrations
  - People
  - Mission
  - System and data criticality
  - System and data sensitivity

Data (Asset) Inventory

Phase 2 – Gap Assessment

- Identify vulnerabilities to organizational systems based on:
  - Industry standards (NIST, ISO, CIS)
  - Security violations
  - External intel
- Identify current controls:
  - Done in practice
  - Formalized and repeatable
  - Non-existent


CODE: 2345A
1
2
3
4
5
6
7
8
9
A
0
B

Phase 3 – Risk Management

- Determine the overall likelihood that a vulnerability will be exploited, based on:
  - Threat-source motivation and capability
  - Existence and effectiveness of controls
  - All other factors
- Determine the impact if an event occurs:
  - Financial
  - Operational
  - Reputational

Phase 4 – Control Recommendations

- Recommend controls to reduce risk to an acceptable level, based on:
  - Cost-benefit analysis
  - Feasibility
  - Legislation and regulation
  - Organizational policy
  - Operational impact
  - Safety and reliability
- Produce a management-level report that helps senior management make decisions on budget, process and control recommendations

RISK vs. REWARD

Recap – Four Phases to Risk Assessment

1. Determine Scope:
    1. Characterize system boundaries, criticality and sensitivity
2. Perform Gap Assessment
    1. Identify vulnerabilities
    2. Identify threats
    3. Review existing controls
3. Conduct Risk Management
    1. Determine probability of a threat exploit
    2. Assess the impact of threat exploitation
    3. Calculate risk
4. Identify reasonable controls to mitigate risk
    1. Document the findings
    2. Document risk treatment plan

PROTIP

Scheduling and Logistics

GreyCastle security

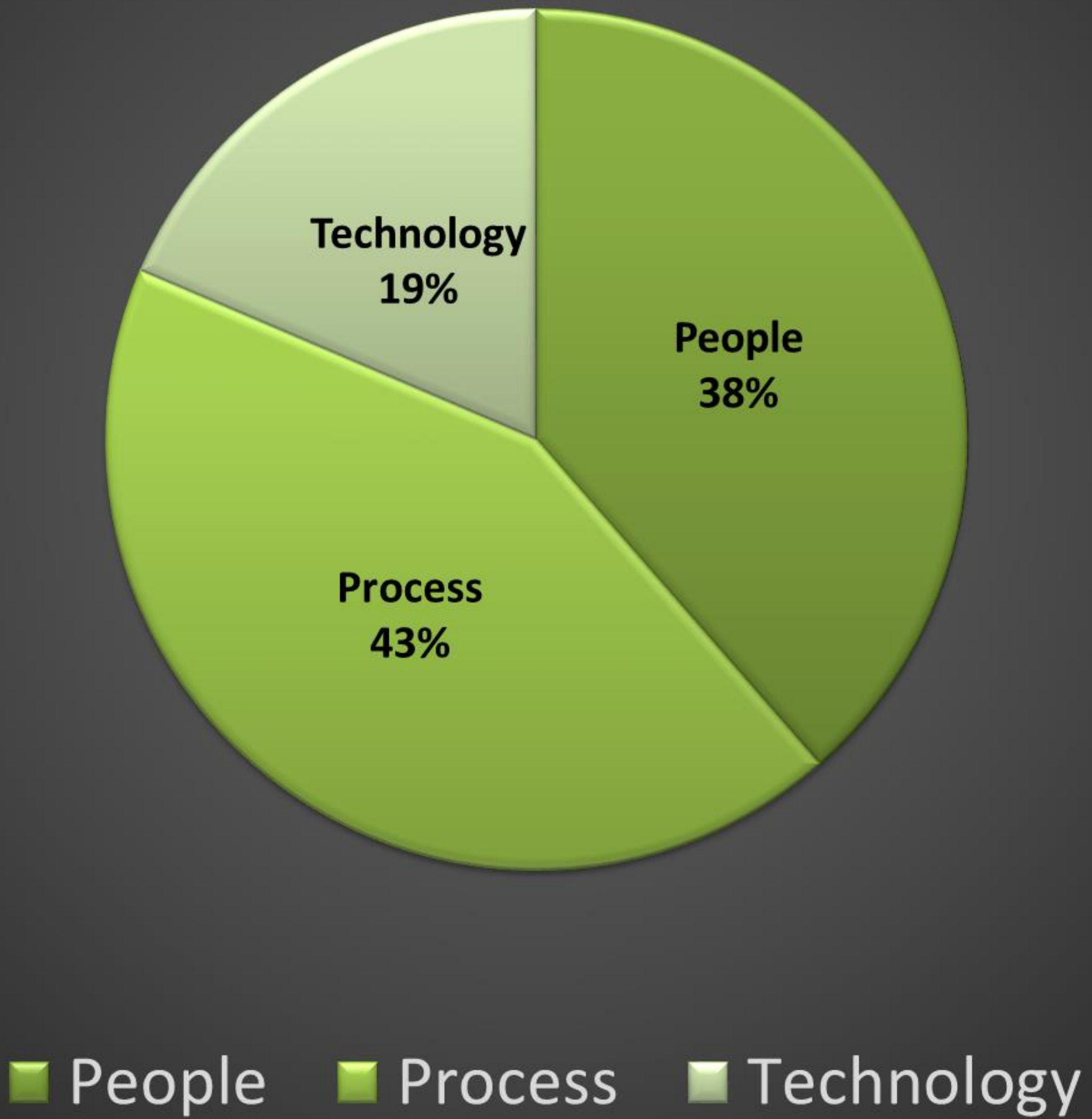
COMMON TOP RISKS AND FINDINGS

GreyCastle security

TOP 10 RISKS

1. Governance
2. Policy/Procedure/Control
3. Data Classification
4. Access Control
5. Incident Response
6. Vendor Risk Management
7. Awareness & Training
8. Secure Configuration Baselines
9. Logging & Monitoring
10. Vulnerability Management

Findings by Category



Identify Your Gaps

Prioritize

Reasonably Mitigate Risk

GreyCastle security

QUESTIONS?

@greycastlesec
(800) 403-8350
www.greycastlesecurity.com