Presented by:
Clint Davies and Vienna Morrill

IT SECURITY RISK ASSESSMENT

A RATIONAL APPROACH TO MANAGING RISK

BerryDunn

CLINT DAVIES, MBA, CDP

Principal
BerryDunn
Management and IT
Consulting Group

VIENNA MORRILL, MSA, CISA

Manager
BerryDunn
Management and IT Consulting Group


C:\Healthcare\IT security_


C:\Healthcare\IT security
-HIPAA
-Meaningful Use
-173 breaches reported
since January_

AGENDA

1. What is risk
2. Why do an IT Security Risk Assessment
3. What does the process entail
4. What elements of this approach can you apply


Risk
Enter

STACKING UP THE RISKS

Winning PowerBall Grand Prize (1 in 175.2M)

Attacked and killed by shark (1 in 3.7M)

Getting a hole in one (1 in 12,750)

Getting struck by lightning (1 in 12,000)

Being audited by the IRS (1 in 175)

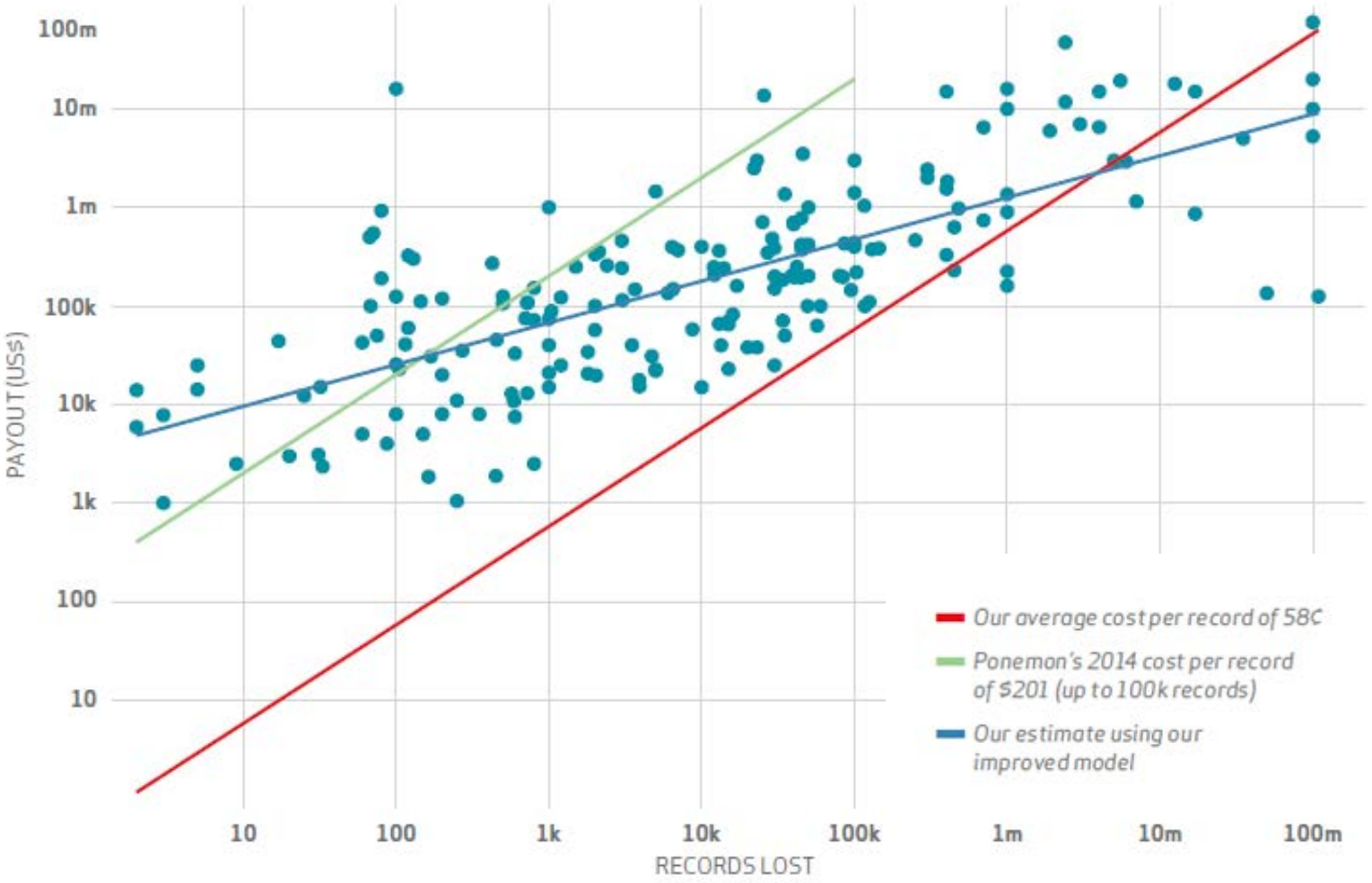
Having a security breach at your organization in the next two years (at least 1 in 5)

COST OF A DATA BREACH

Estimates range from an average of $0.58/record[1] to an average of $201/record[2]

[1] Verizon Data Breach Investigations Report
[2] Ponemon Institute Report

COST OF A DATA BREACH



Source: Verizon 2015 Data Breach Investigations Report

THE RISK ASSESSMENT PROCESS

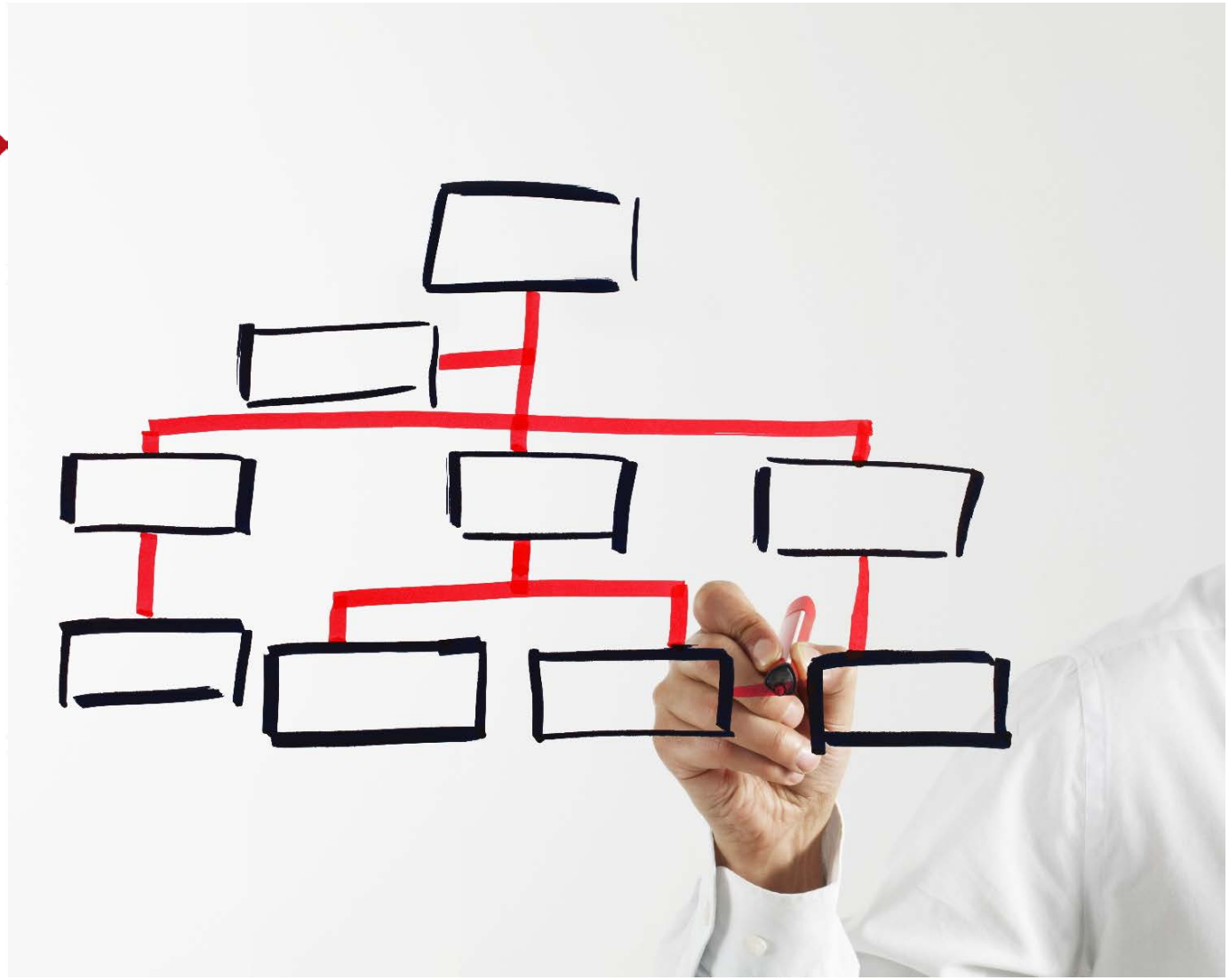
1

PLANNING

Assemble assessment team and develop work plan

Determine scope and develop IT Security Risk Assessment questionnaire

Engage and collaborate with stakeholders



THE QUESTIONNAIRE

Respondent Information			
Department			
Completed by			
Contact Information		**Date Submitted**	

Question	Response
1. **Systems and Applications.** Does your Department maintain (manage internally or license) systems or applications that store or access sensitive information including any cloud-based systems or applications? If so, please describe.	
2. **Data Storage.** Does your Department store sensitive information or data on any storage service other than IT-provided network drives? If so, please specify (e.g., departmental servers, or cloud-based storage such as Google Drive or Dropbox).	
3. **Responsibility and Oversight.** Has your Department assigned responsibility for information security to an individual or group?	
4. **Information Security Training and Awareness.** Does your department participate in regular information security training? If so, how often and what topics are covered?	

Included 20 Risk Areas:

1. Systems and Applications
2. Data Storage
3. Responsibility and Oversight
4. Information Security Training and Awareness
5. IT Security Incident Response
6. Access Controls
7. Audit Logs
8. Remote Access
9. Change Management
10. Incident Management
11. Physical Security
12. Data Transmission
13. Service Provider/ Vendor Due Diligence
14. Disaster Recovery Planning
15. Data Backups
16. Copiers and Multi-Function Devices
17. Hardware Disposal
18. Mobile Devices
19. Compliance
20. Data Protection

2

EDUCATION + FACT FINDING

Educate stakeholders about process, expectations, and objectives

Meet with participants to walk through Questionnaire

Participants complete and submit Questionnaire

3

ANALYSIS

Analyze Questionnaire responses

Conduct follow-up as needed

Develop overall Risk Assessment Report and department specific reports

ALL ABOUT RESIDUAL RISK

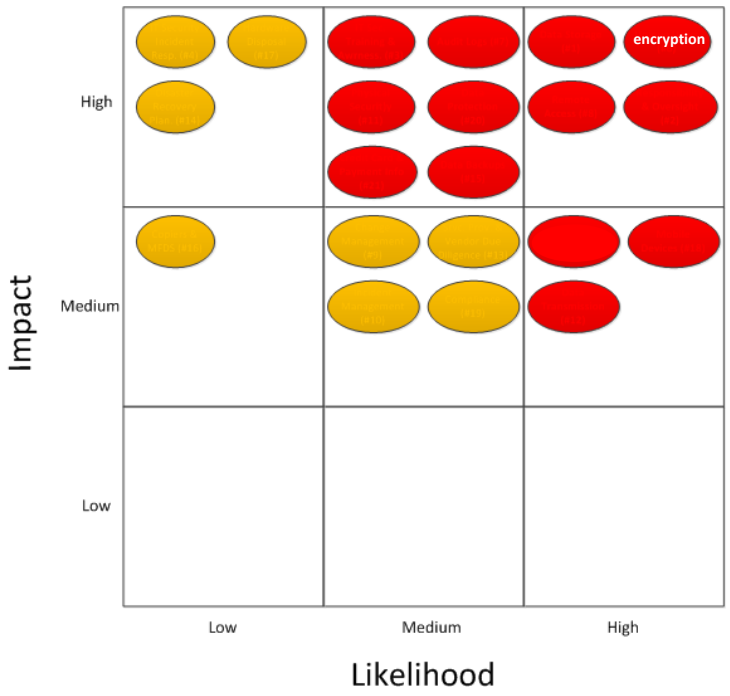
Populated before analysis

Description of the Vulnerability	Risk Summary	Likelihood and Impact	Risk Rating	Analysis Results	Residual Risk and Recommendations
Encryption The client does not have their entire inventory of devices encrypted.	Without encryption, a lost or stolen device has greater potential for PHI to be obtained.	**Likelihood**: **High** **Impact**: **High**	**High**	Lost or stolen devices are the most frequent cause of a HIPAA breach. Not only is encryption an addressable safeguard under the security rule, but without encryption in place, the client increases the likelihood that someone could gain unauthorized access to a device and it's PHI.	**Residual Risk:** **Low** **Recommendation:** The client should deploy a centrally managed device encryption across their entire population of devices working from mobile devices back to fixed work stations.

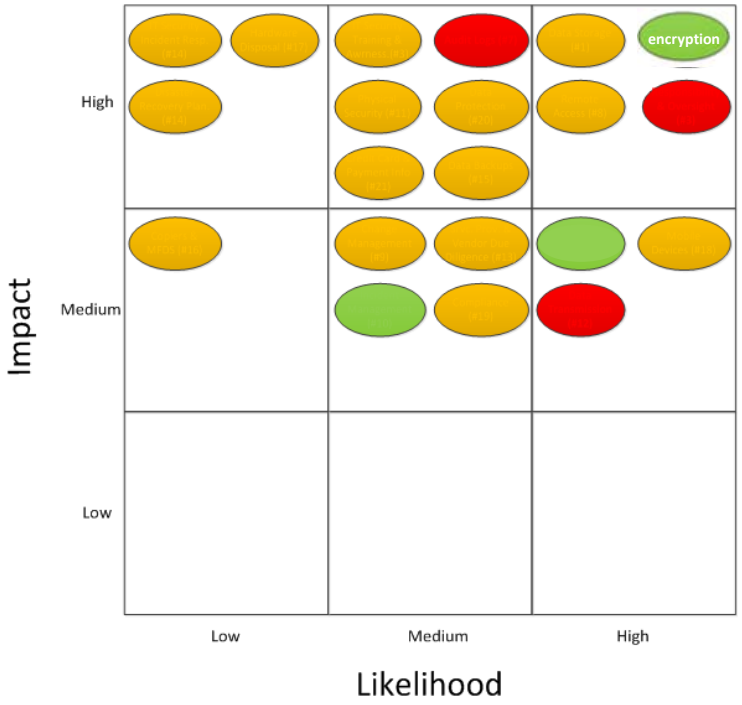
Populated during analysis

HEAT MAPS

Inherent



Residual



4

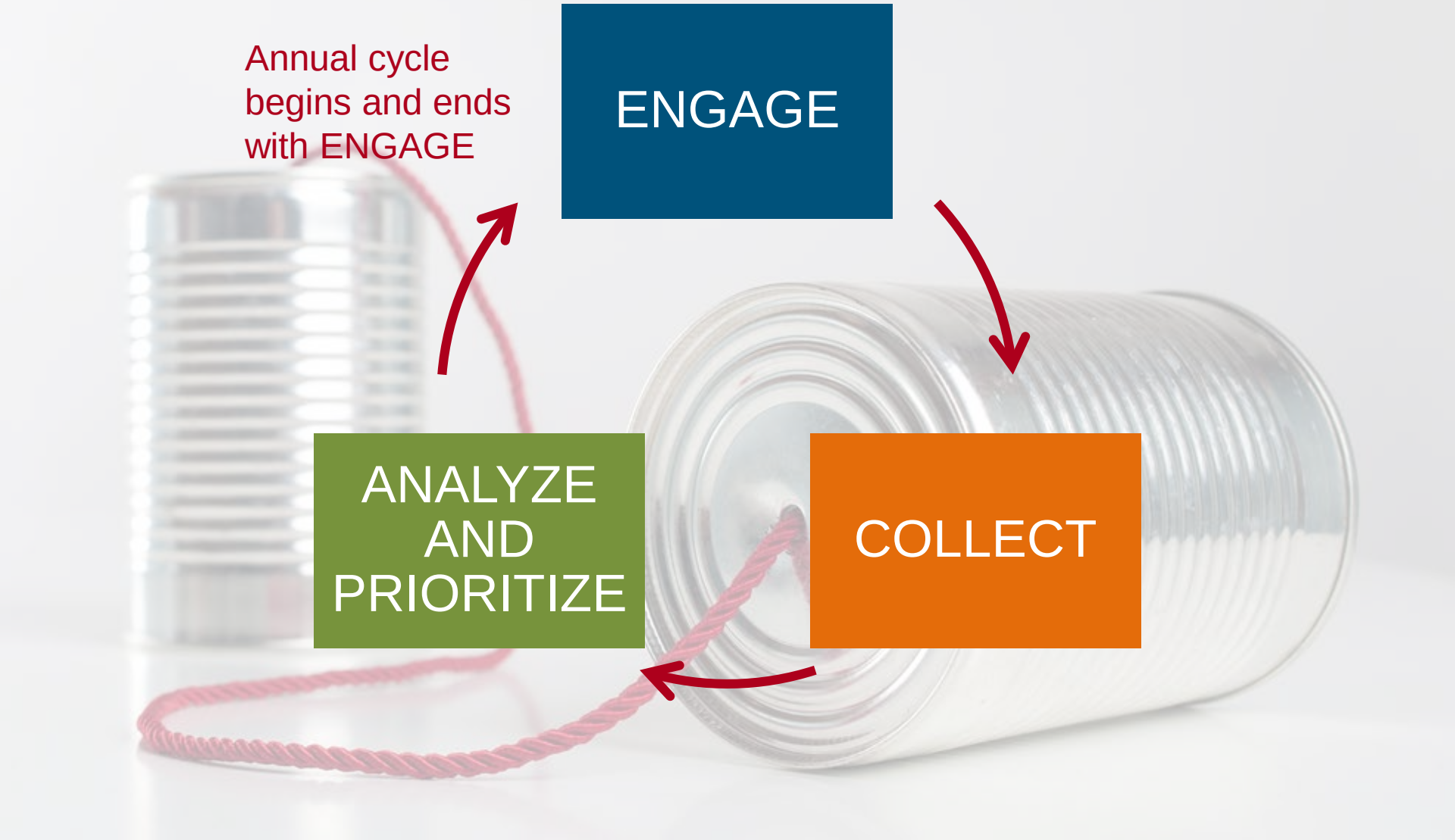
REPORT

Finalize reports with Project Team

Present outcomes and discuss next steps with stakeholders, including meetings with

- IT leader
- Key committees
- Assessment participants

THE RISK ASSESSMENT CYCLE



OUTCOMES

Collaboration

Sustainable Approach

Security Awareness

Priorities

TAKEAWAYS

It is getting riskier

Engagement of stakeholders is critical

More than compliance... It's about reducing ***likelihood*** and ***impact***

Doesn't have to be complicated

QUESTIONS

INTERESTED IN MORE?

We are always available for your questions

vmorrill@berrydunn.com

cdavies@berrydunn.com