Bon Secours

HIPAA SUMMIT 2018

Taming the Wild West: Application Risk Assessments

2018

CORL technologies

CORL technologies

Introductions:

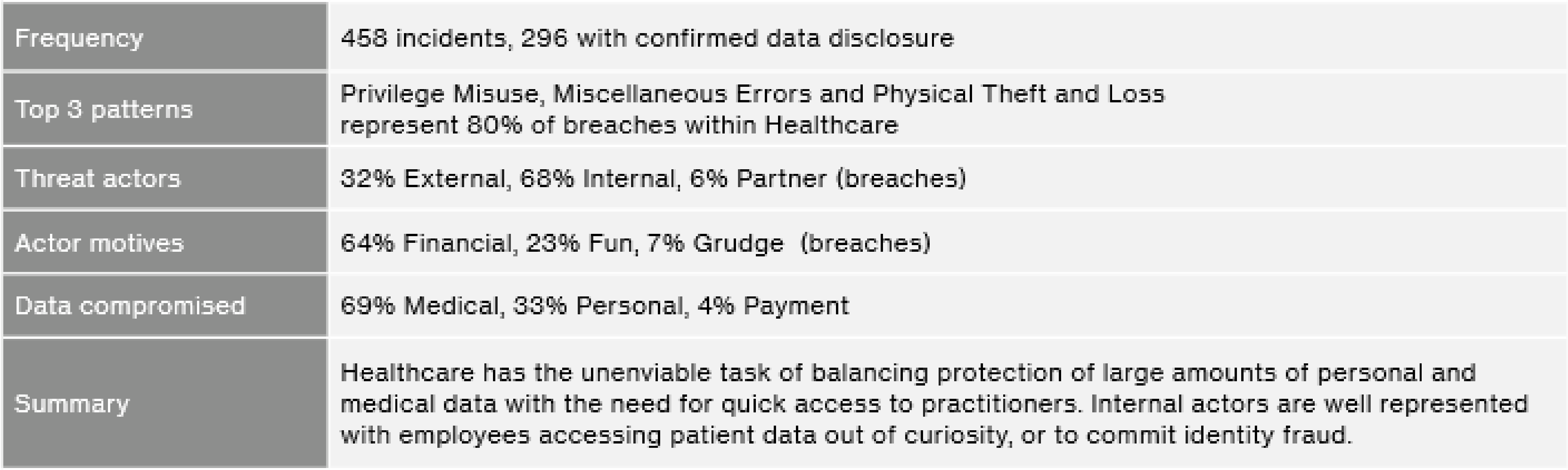
Tracy Griffin

Director, Information Security Risk Management, Bon Secours Health Systems, Richmond, VA
Tracy_Griffin@bshsi.org

Cliff Baker

Chief Executive Officer, CORL Technologies, Atlanta, GA
cliff.baker@corltech.com
vendorsecurity.com

State of Healthcare Security

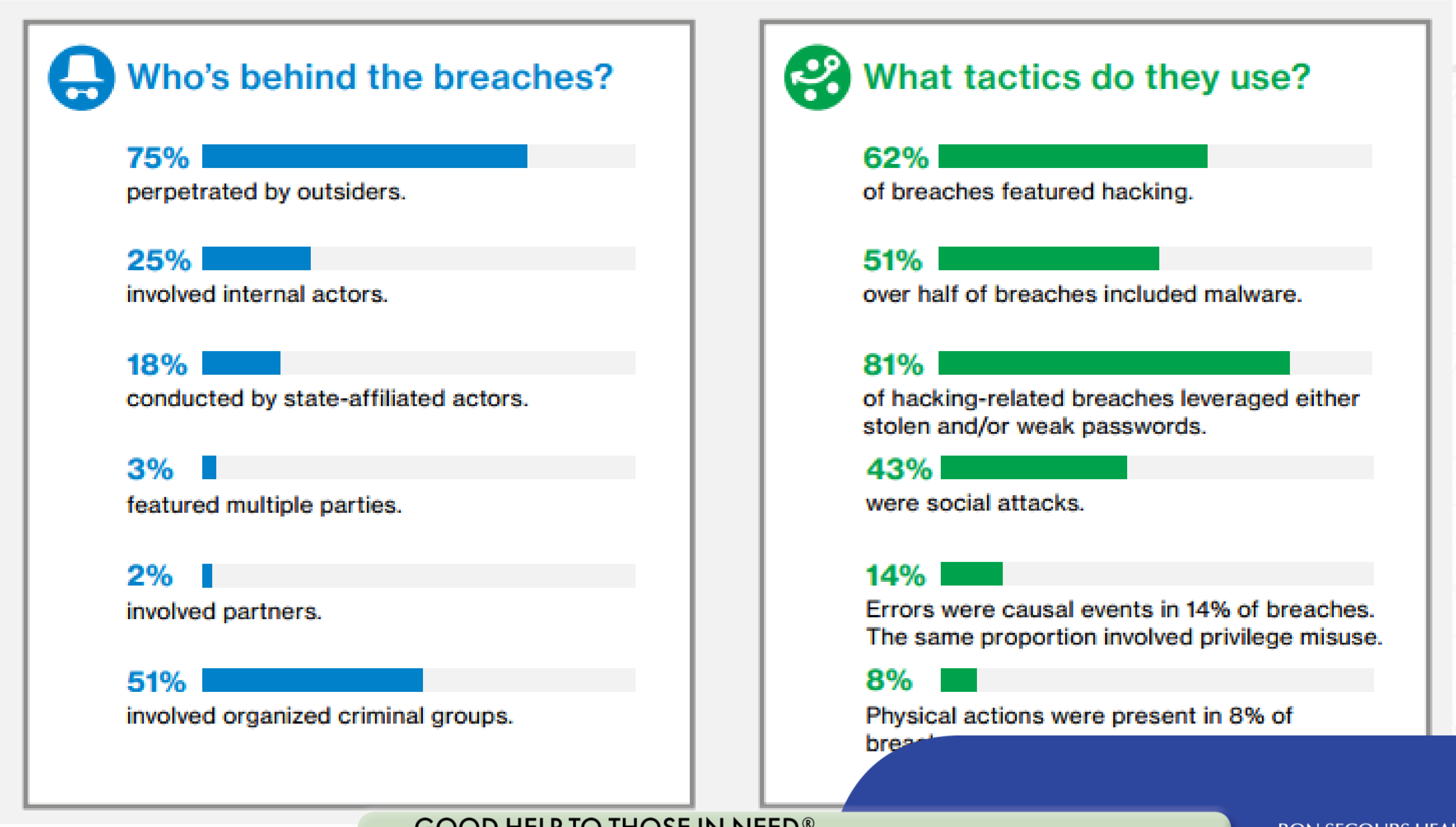


Frequency	458 incidents, 296 with confirmed data disclosure
Top 3 patterns	Privilege Misuse, Miscellaneous Errors and Physical Theft and Loss represent 80% of breaches within Healthcare
Threat actors	32% External, 68% Internal, 6% Partner (breaches)
Actor motives	64% Financial, 23% Fun, 7% Grudge (breaches)
Data compromised	69% Medical, 33% Personal, 4% Payment
Summary	Healthcare has the unenviable task of balancing protection of large amounts of personal and medical data with the need for quick access to practitioners. Internal actors are well represented with employees accessing patient data out of curiosity, or to commit identity fraud.

Verizon 2017 Data Breach Investigations Report

Breach Data Trends

Verizon 2017 Data Breach Investigations Report



Who's behind the breaches?

75% perpetrated by outsiders.

25% involved internal actors.

18% conducted by state-affiliated actors.

3% featured multiple parties.

2% involved partners.

51% involved organized criminal groups.

What tactics do they use?

62% of breaches featured hacking.

51% over half of breaches included malware.

81% of hacking-related breaches leveraged either stolen and/or weak passwords.

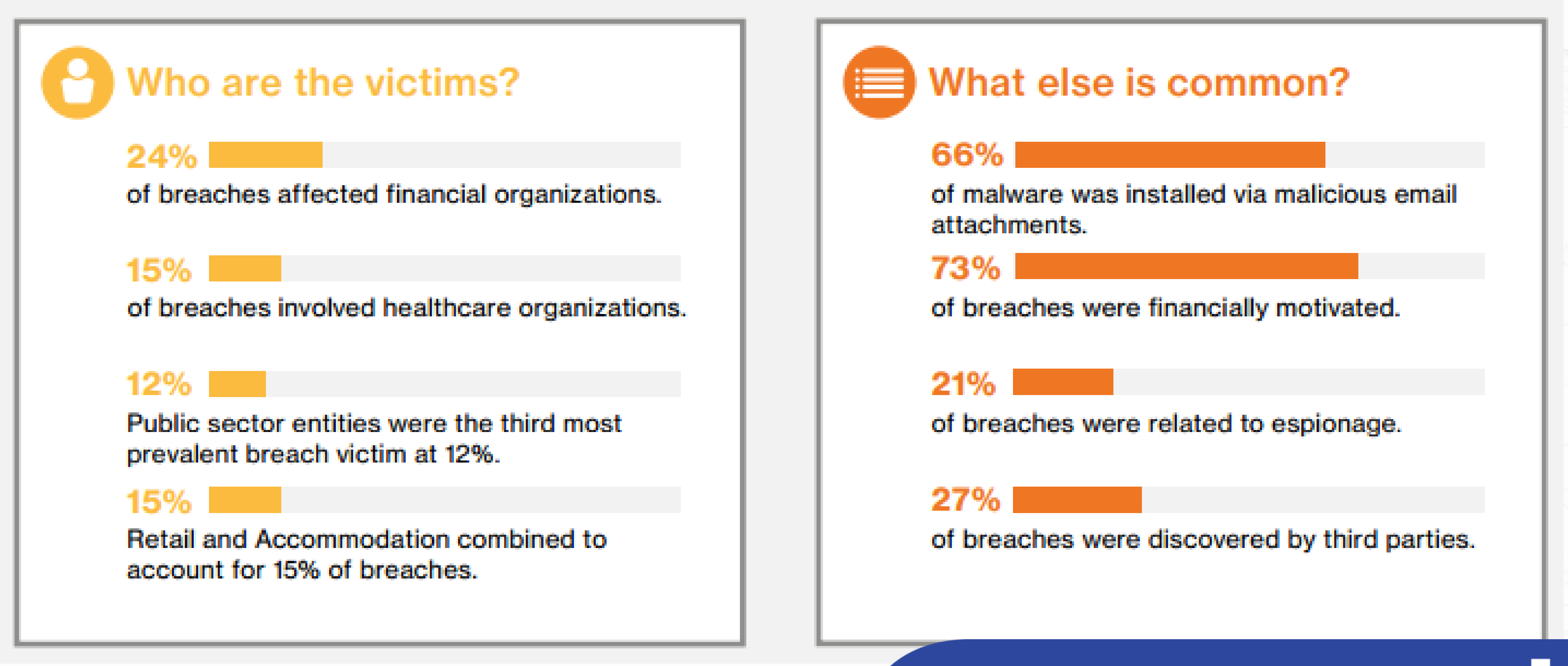
43% were social attacks.

14% Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8% Physical actions were present in 8% of brea

Breach Data Trends

Verizon 2017 Data Breach Investigations Report



Who are the victims?

24%

of breaches affected financial organizations.

15%

of breaches involved healthcare organizations.

12%

Public sector entities were the third most prevalent breach victim at 12%.

15%

Retail and Accommodation combined to account for 15% of breaches.

What else is common?

66%

of malware was installed via malicious email attachments.

73%

of breaches were financially motivated.

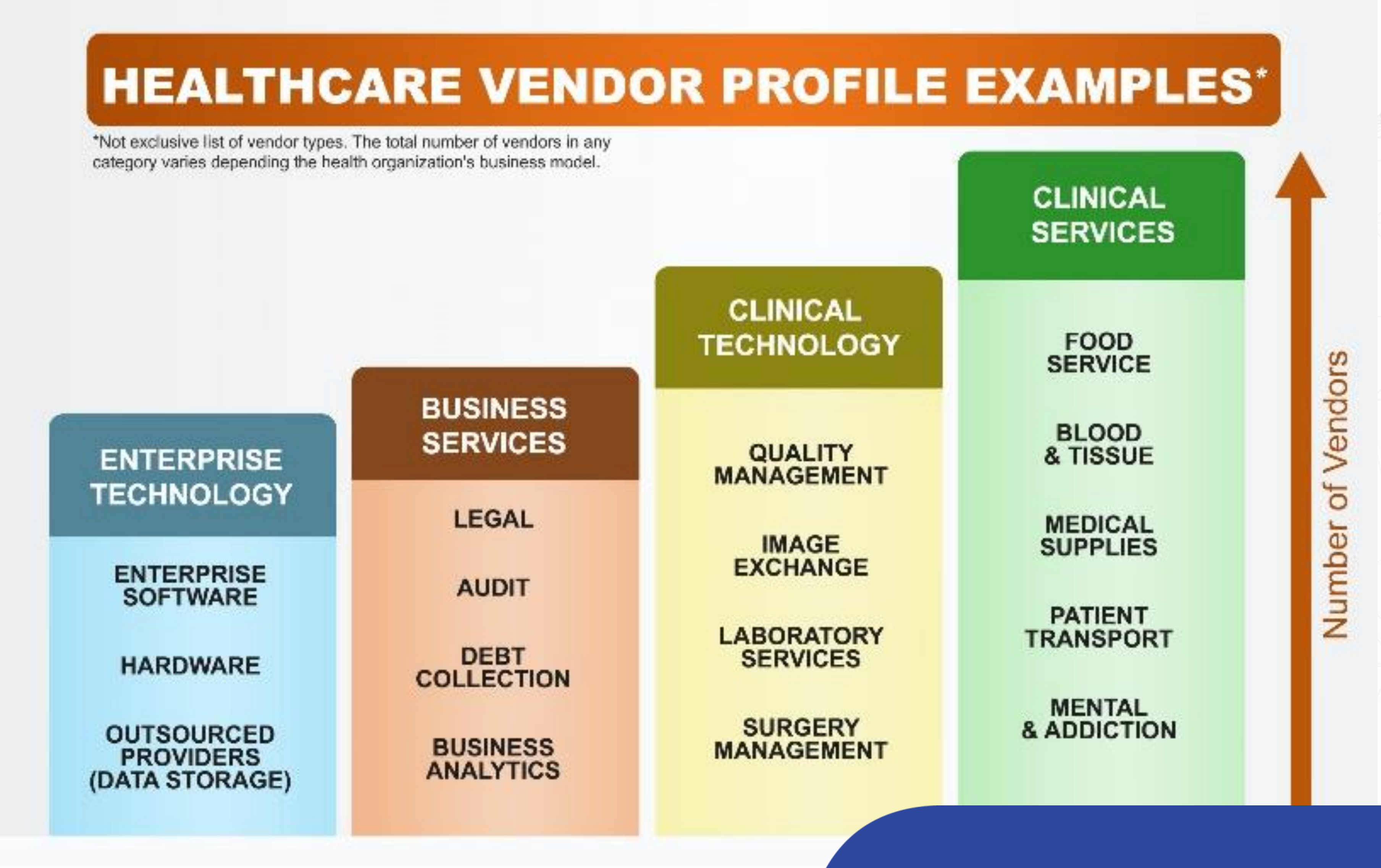
21%

of breaches were related to espionage.

27%

of breaches were discovered by third parties.

PHI Everywhere



HEALTHCARE VENDOR PROFILE EXAMPLES*

*Not exclusive list of vendor types. The total number of vendors in any category varies depending the health organization's business model.

ENTERPRISE TECHNOLOGY

- ENTERPRISE SOFTWARE
- HARDWARE
- OUTSOURCED PROVIDERS (DATA STORAGE)

BUSINESS SERVICES

- LEGAL
- AUDIT
- DEBT COLLECTION
- BUSINESS ANALYTICS

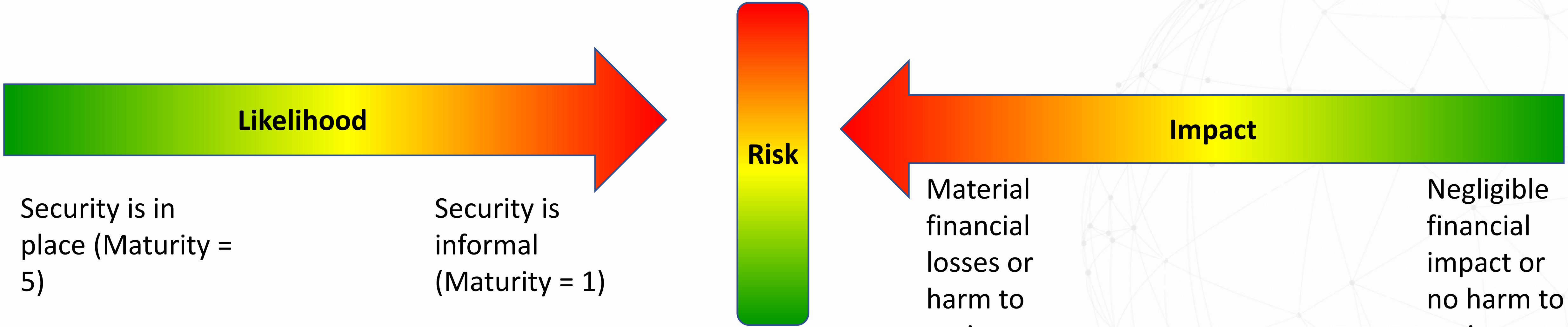
CLINICAL TECHNOLOGY

- QUALITY MANAGEMENT
- IMAGE EXCHANGE
- LABORATORY SERVICES
- SURGERY MANAGEMENT

CLINICAL SERVICES

- FOOD SERVICE
- BLOOD & TISSUE
- MEDICAL SUPPLIES
- PATIENT TRANSPORT
- MENTAL & ADDICTION

Key Risk Concepts – Likelihood and Impact



Security is in place (Maturity = 5)

Security is informal (Maturity = 1)

Material financial losses or harm to patients

Negligible financial impact or no harm to patients

Calculating Risk Rating

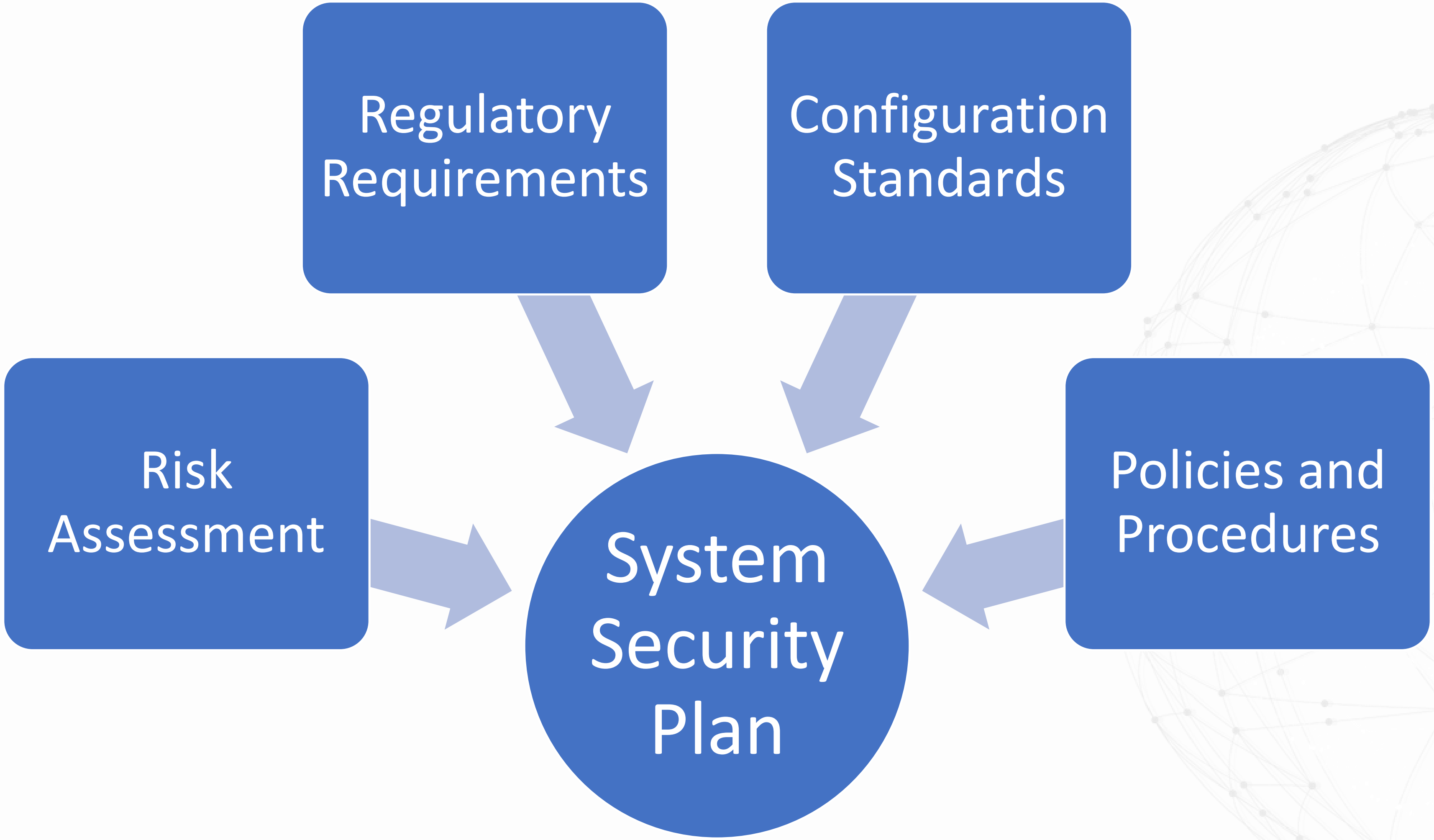
Unacceptable level of risk

Likelihood	Almost Certain	15	19	**23** **X**	**24** **X**	**25** **X**
	Likely	13	14	20	**21** **X**	**22** **X**
	Possible	8	12	16	17	18
	Unlikely	6	7	9	10	11
	Highly Unlikely (Rare)	1	2	3	4	5
		Negligible	Minor	Moderate	Major	Material

Impact

Risk	Rating
High	🟥
Medium	🟧
Low	🟨
Managed	🟩

Application Risk Assessments



Sensitive vs. Non-Sensitive

CORL technologies

Sensitive

- These systems have additional or enhanced controls
- For example, these systems have encryption requirements

Non-Sensitive

- Every system has these common controls
- For example, these systems are not required to implement encryption

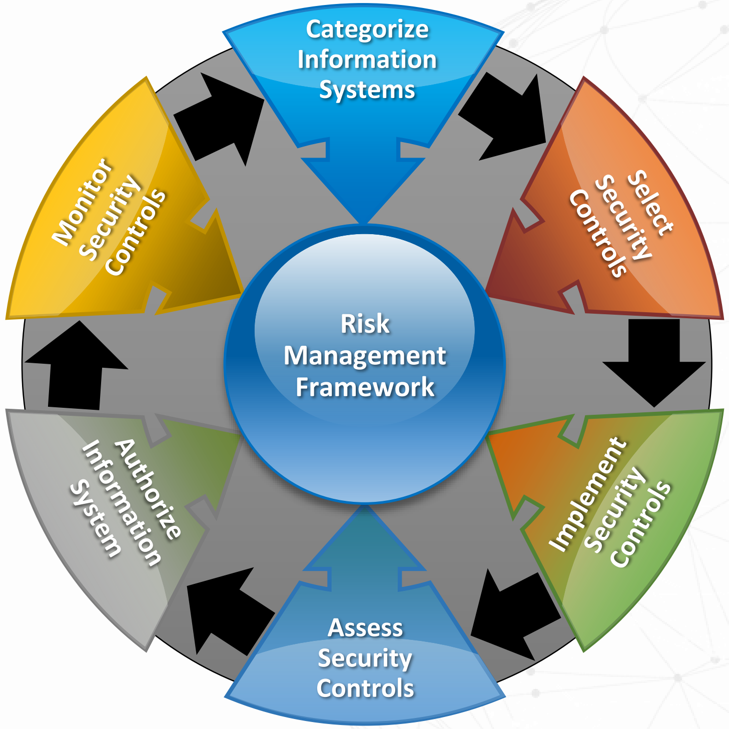
BSHSI's Risk Management Standards requires the classification of all IT systems and data according to their sensitivity with respect to the following three criteria:

- Confidentiality, which addresses sensitivity to unauthorized disclosure
- Integrity, which addresses sensitivity to unauthorized modification
- Availability, which addresses sensitivity to outages

BSHSI Risk Management Framework

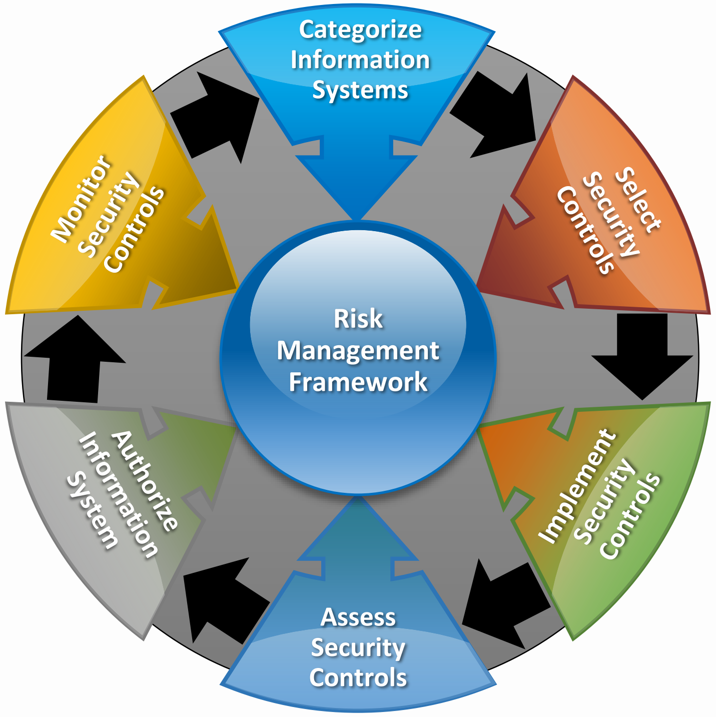
BSHSI adopted a six-step risk management framework process

- Categorize Systems
- Select Controls
- Implement Controls
- Assess Controls
- Authorize Information System
- Monitor Controls


Categorize Information Systems
Select Security Controls
Implement Security Controls
Assess Security Controls
Authorize Information System
Monitor Security Controls
Risk Management Framework

Note: Based on NIST 800-37r1, 800-39r1 and 800-53r4

System Security Plans: Application Risk Assessment


Categorize Information Systems
Select Security Controls
Implement Security Controls
Assess Security Controls
Authorize Information System
Monitor Security Controls
Risk Management Framework

CATEGORIZE INFORMATION SYSTEM

- Categorize the information system and document the results SSP
- Describe the information system (including system boundary) and document SSP
- Register the information system

SELECT SECURITY CONTROLS

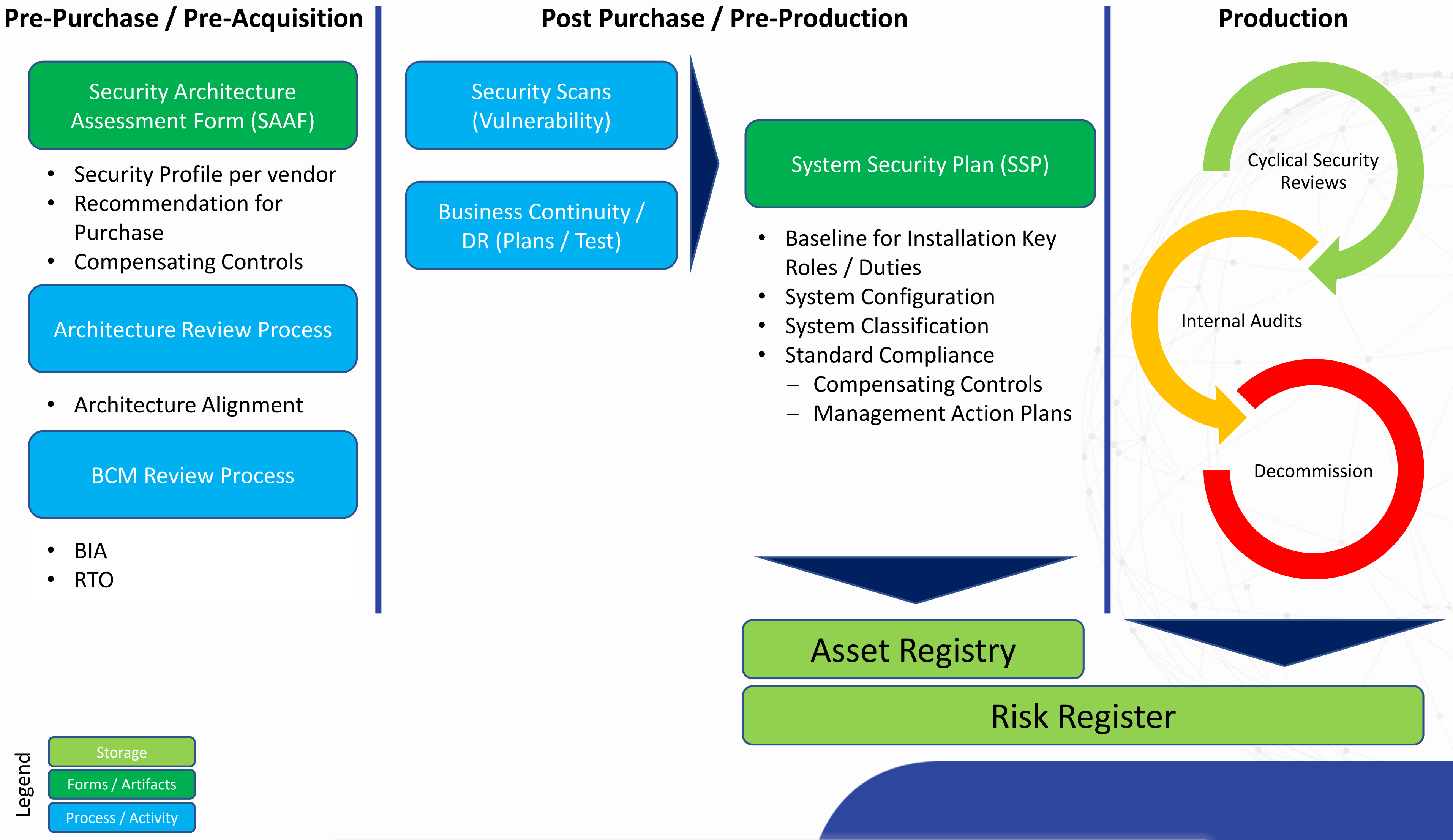
- Identify the security controls that are provided by the organization as common controls for organizational information systems and document SSP
- Select the security controls for the information system and document SSP
- Develop a strategy for the continuous monitoring of security control effectiveness and any proposed or actual changes to the information system and its environment of operation. SSP
- Review and approve the security plan SSP

IMPLEMENT SECURITY CONTROLS

- Implement the security controls specified in the security plan. SSP
- Document the security control implementation, as appropriate, in the security plan, providing a functional description of the control implementation SSP

System Risk Assessment Flow

CORL technologies



Pre-Purchase / Pre-Acquisition

Security Architecture Assessment Form (SAAF)

- Security Profile per vendor
- Recommendation for Purchase
- Compensating Controls

Architecture Review Process

- Architecture Alignment

BCM Review Process

- BIA
- RTO

Post Purchase / Pre-Production

Security Scans (Vulnerability)

Business Continuity / DR (Plans / Test)

System Security Plan (SSP)

- Baseline for Installation Key Roles / Duties
- System Configuration
- System Classification
- Standard Compliance
  - Compensating Controls
  - Management Action Plans

Production

Cyclical Security Reviews

Internal Audits

Decommission

Asset Registry

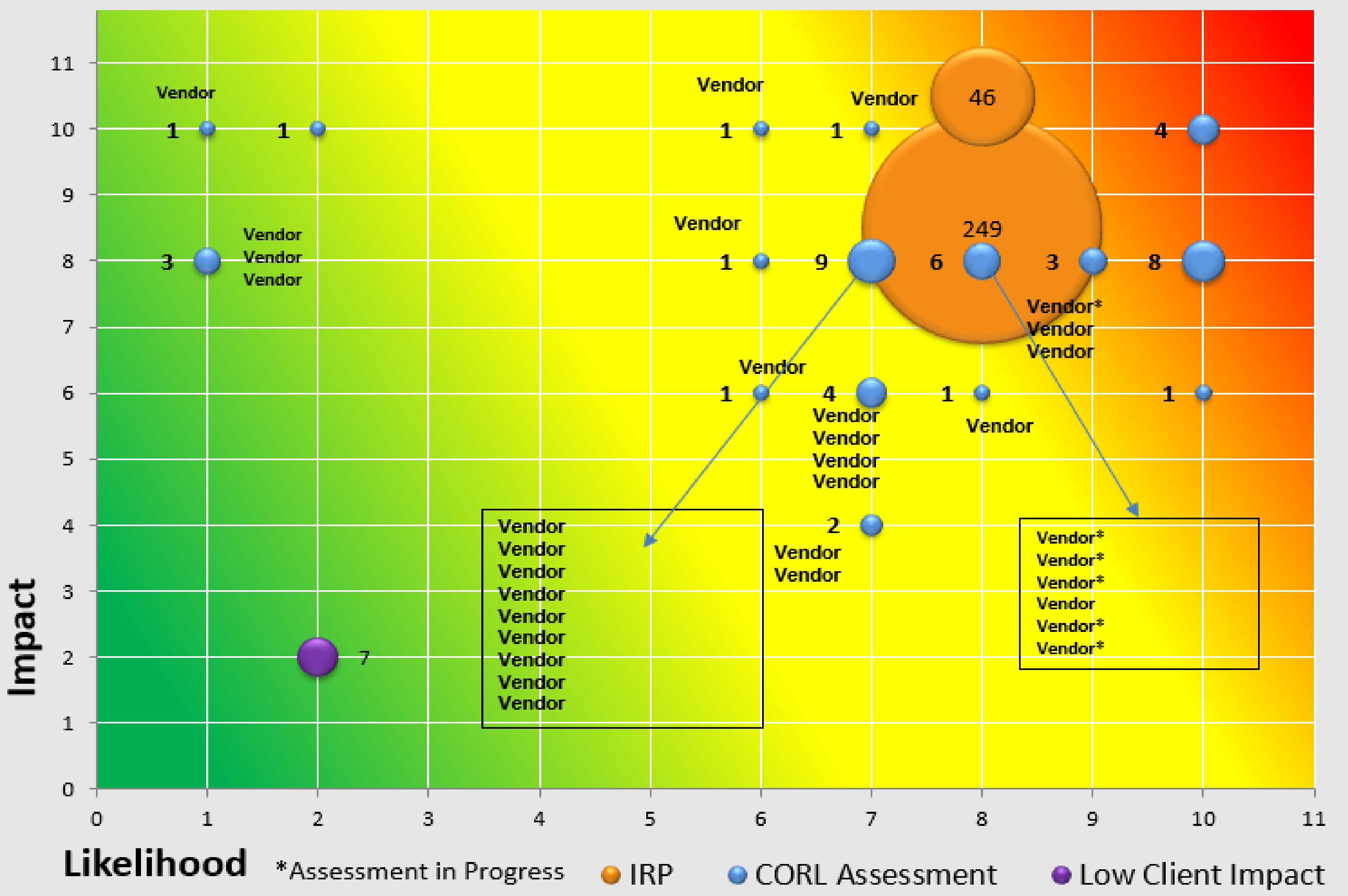
Risk Register

Legend

- 🟩 Storage
- 🟩 Forms / Artifacts
- 🟦 Process / Activity

Overall Risk Program Management

- Clear vision of vendor/application security risk management objectives
- Executive level communication
- Program effectiveness



CORL technologies

QUESTIONS?

GOOD HELP TO THOSE IN NEED.®

BON SECOURS HEALTH SYSTEM