Keys to Building a Robust Data Security Plan

Cris V. Ewell, Ph.D.
Seattle Children's
CISO

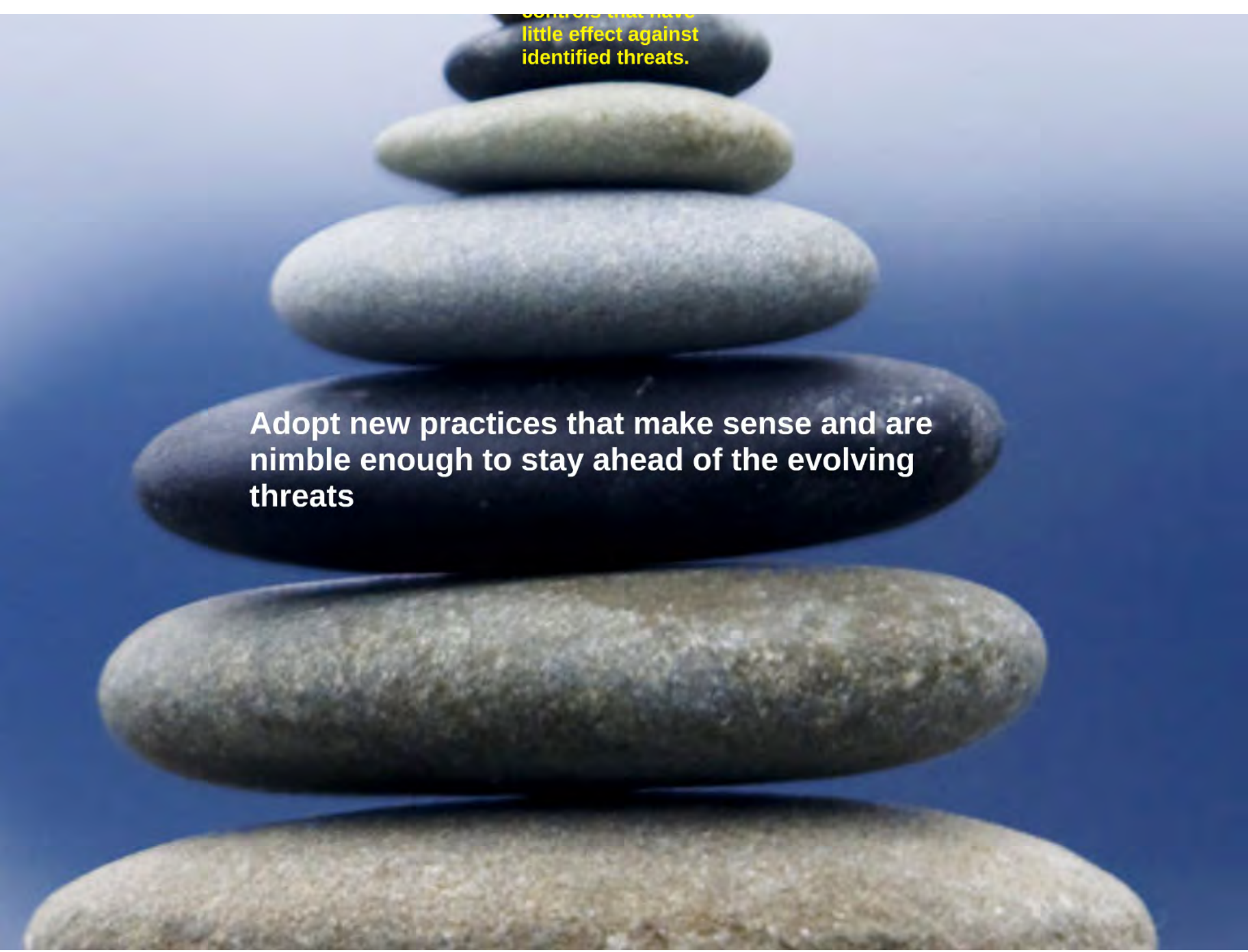
Why do we need new practices?

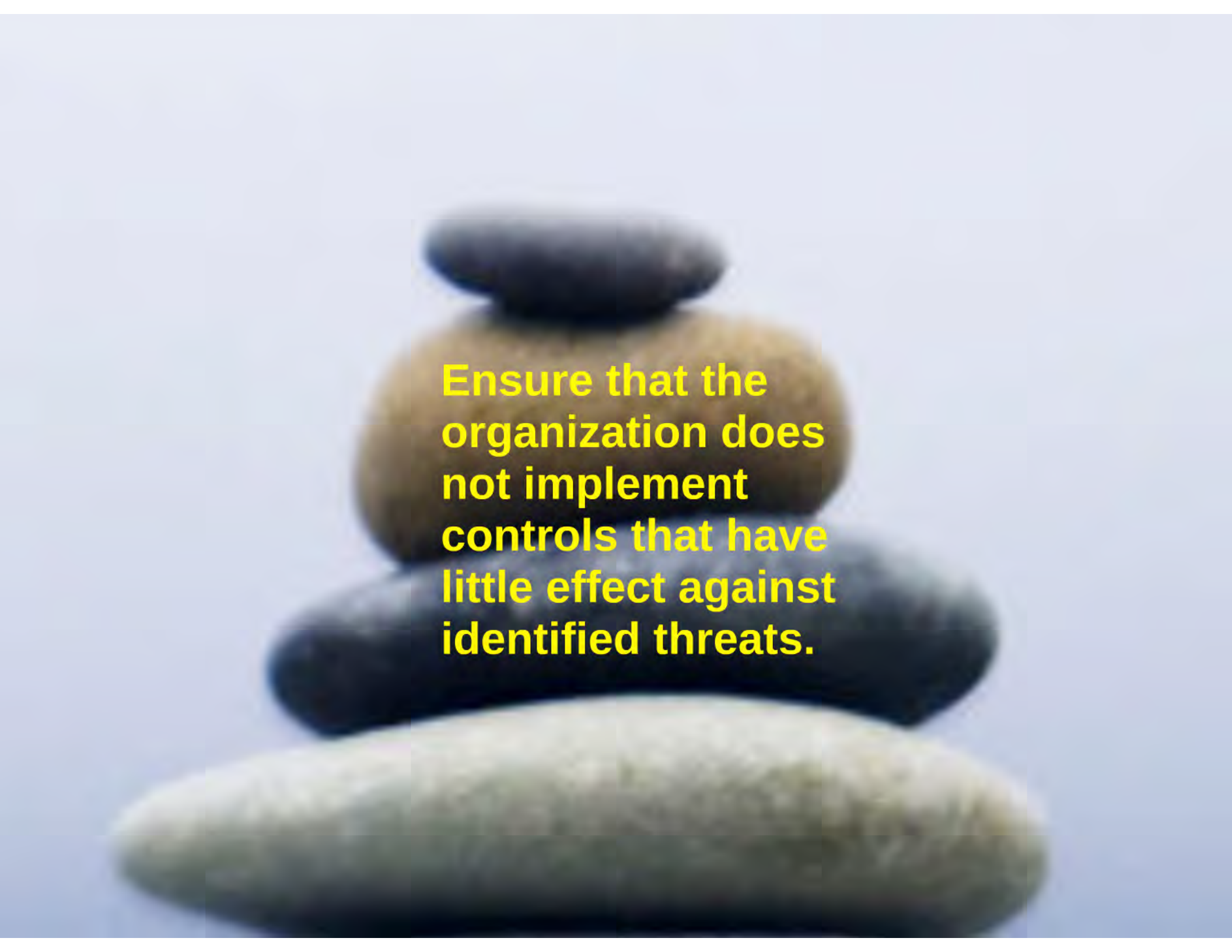
Traditional information security strategies and standards

- diminished effectiveness
- disproportionately technical
- do not adequately address rapidly evolving threat landscape

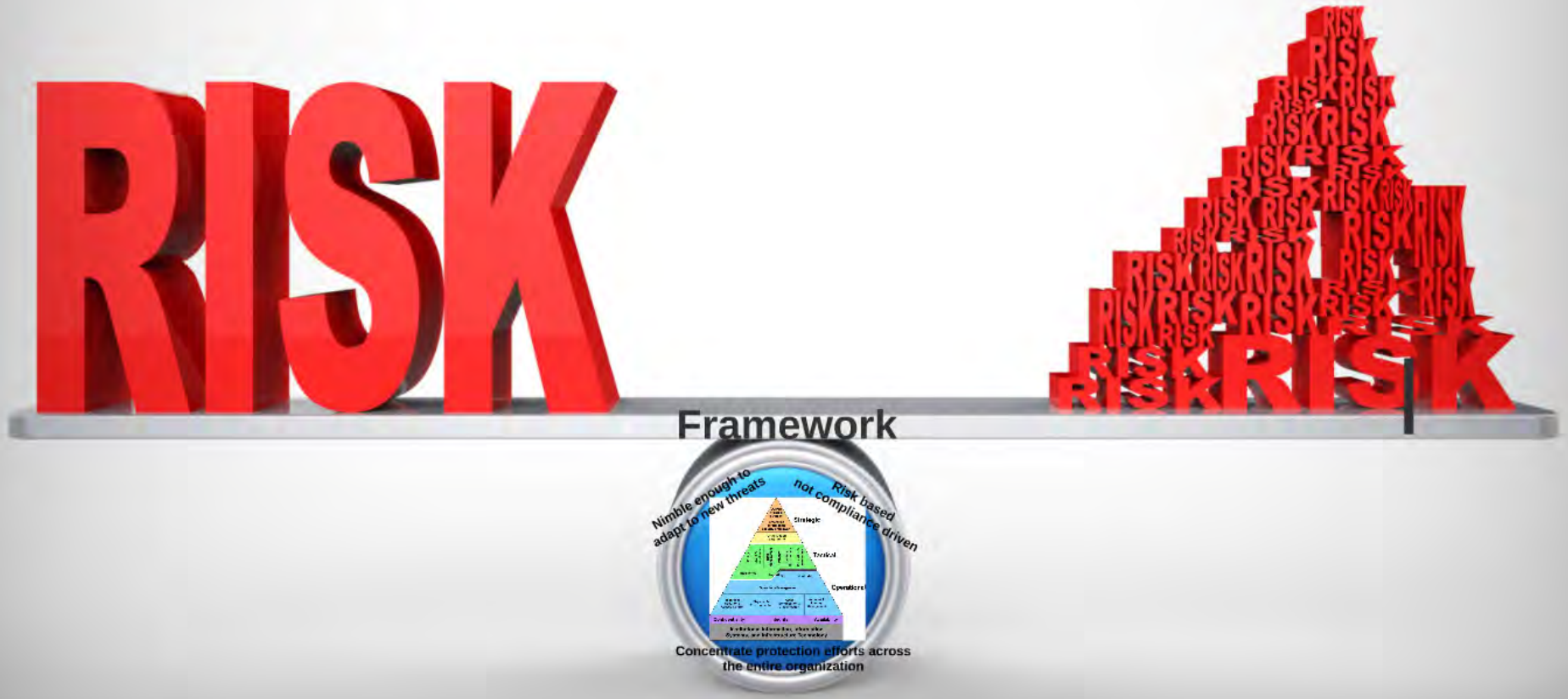

Information security practice goals
Ensure that the organization does not implement controls that have little effect against identified threats.
Adopt new practices that make sense and are nimble enough to stay ahead of the evolving threats
Based on actual conditions, business objectives, and risk appetites specific to each organization.


Based on actual conditions, business objectives,
and risk appetites specific to each organization.


little effect against
identified threats.
Adopt new practices that make sense and are nimble enough to stay ahead of the evolving threats


Ensure that the organization does not implement controls that have little effect against identified threats.

Information security program needs to be built on a risk based framework and integrated into operations



Framework

Nimble enough to adapt to new threats

Risk based not compliance driven

Concentrate protection efforts across the entire organization

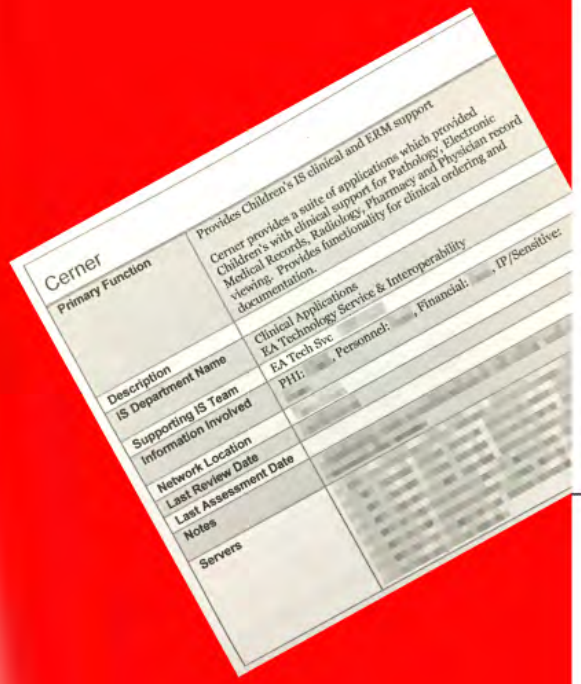
Identify, document, and maintain a clear understanding of the assets

- Asset Profiling and Inventory Listing
- Clearly Defined Asset Ownership Role
- Asset-Based Focus for Risk Mitigation Priorities
- Minimization of the Electronic Attack Surface

- Asset Profiling and Inventory Listing
- Clearly Defined Asset Ownership Role
- Asset-Based Focus for Risk Mitigation Priorities
- Minimization of the Electronic Attack Surface

Asset profiling and inventory

- Intellectual Property
  - Value
  - Number of people with access
- Key Service or Products
  - Type (HVAC for example)
  - Social political volatility
  - Applicable laws/compliance requirements
  - Volume of users/service community
  - Key dependencies
- Application(s)
  - Electronic footprint/profile
  - Number of transactions hosted
  - Number of admin/user access (Ext/Int)
  - Key dependencies
- Business Partner(s)
  - Level of implied trust
  - Condition of contract/liability
  - Key dependencies
- Key Individual(s)
  - Role
  - Security acumen
  - Data/physical access
  - Key dependencies
- Data
  - Applicable laws/compliance requirements
  - Type of data involved
  - Volume of data
  - Location/replicated (extent)
  - Key dependencies



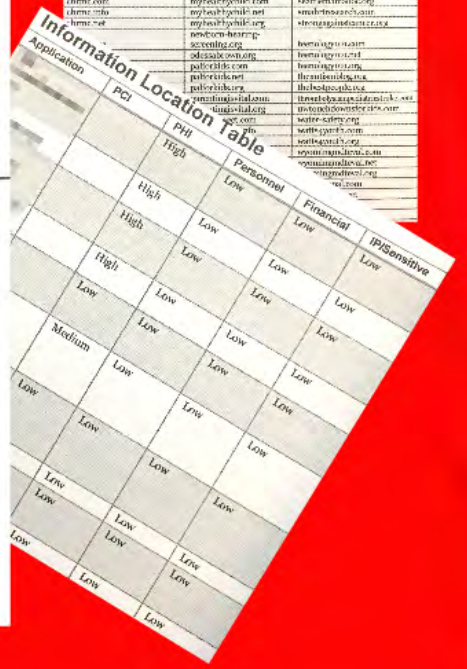
Seattle Children's
HOSPITAL · RESEARCH · FOUNDATION

Architecture Handbook

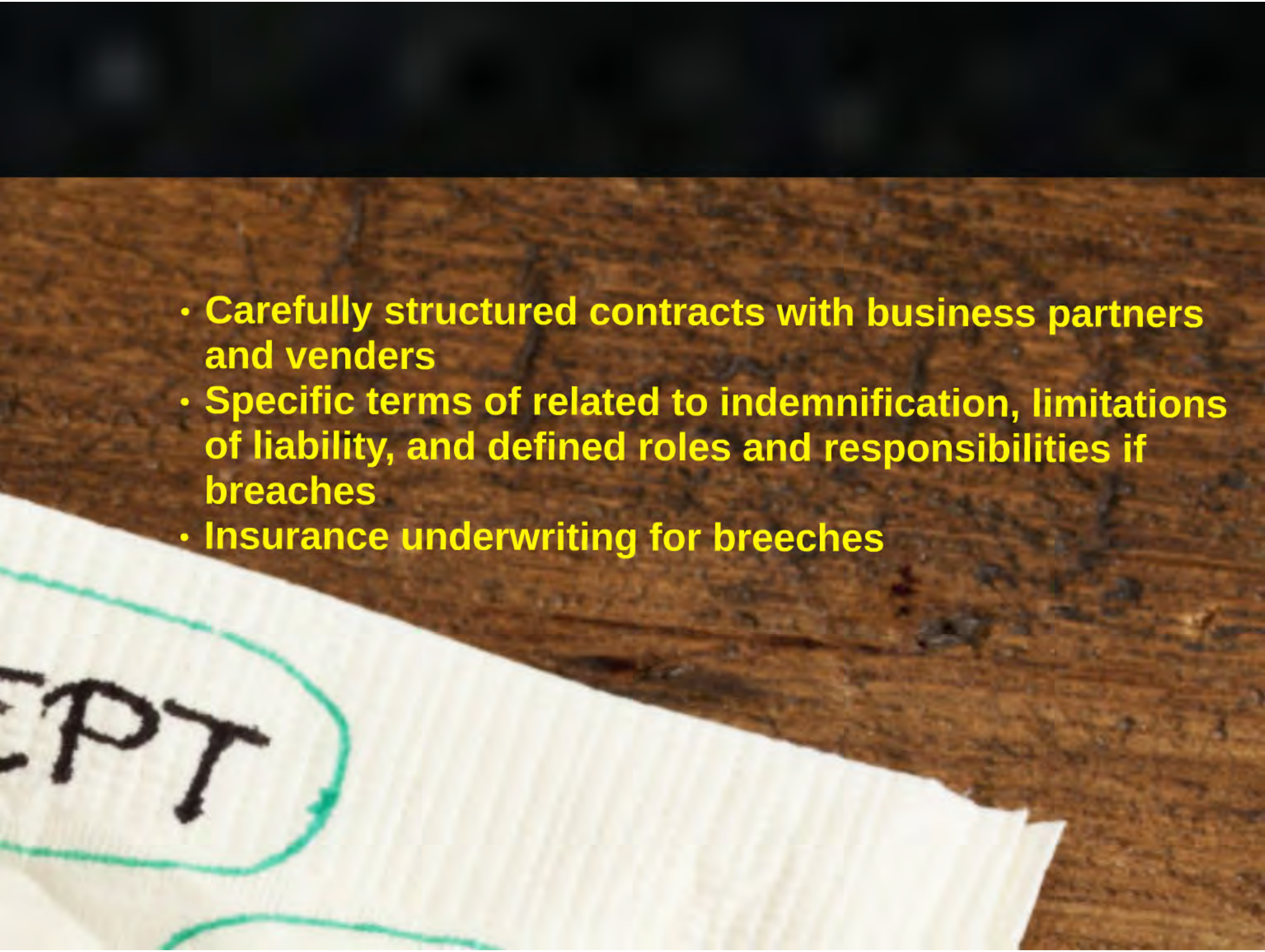
CISM Reference Manual

Corporate Information Security Management

4/13/2015

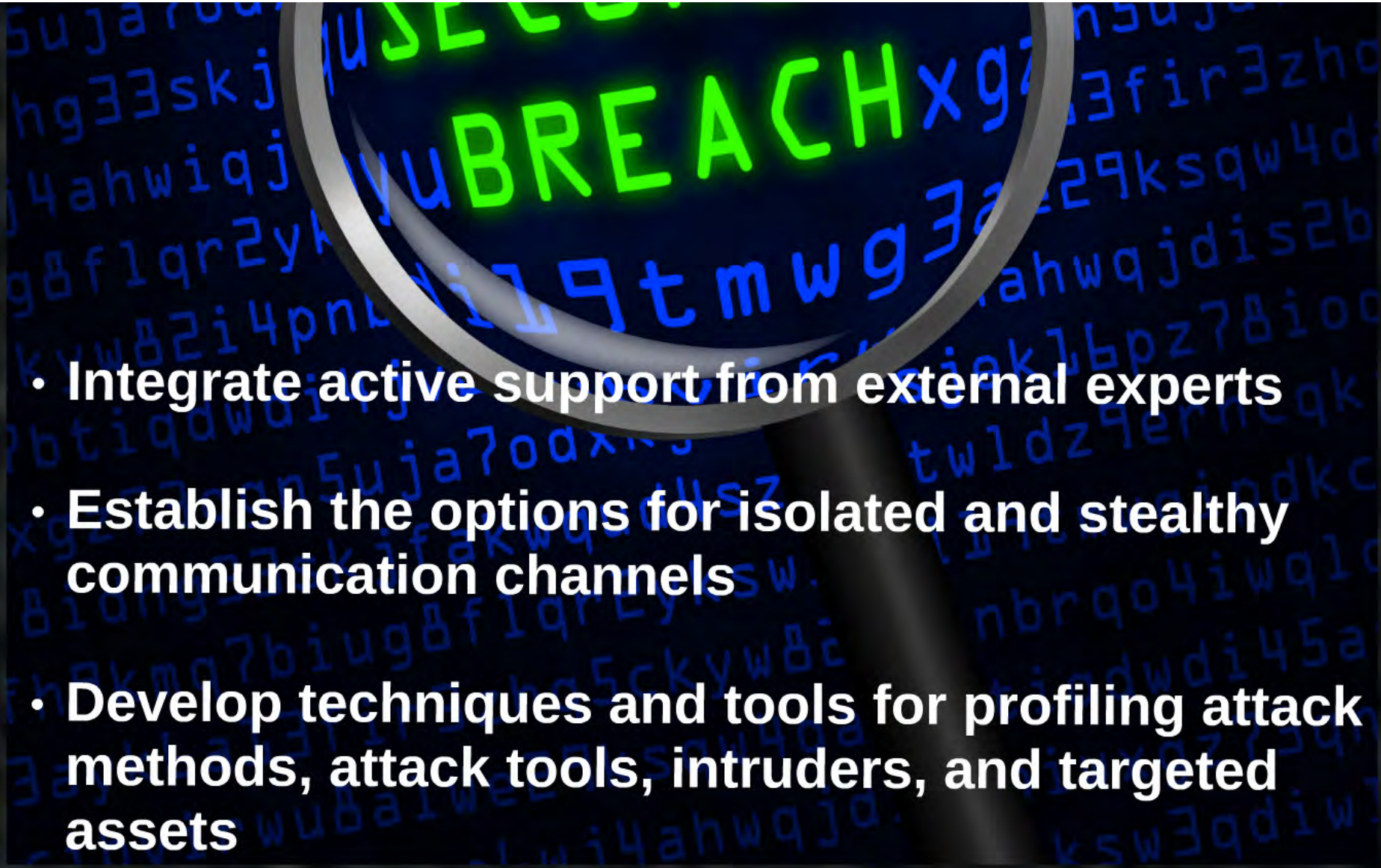


Aggressive Risk Transfer Strategies


• Carefully structured contracts with business partners and venders
• Specific terms of related to indemnification, limitations of liability, and defined roles and responsibilities if breaches
• Insurance underwriting for breeches
EPT

Advanced Incident Response and Management

- Integrate active support from external experts
- Establish the options for isolated and stealthy communication channels
- Develop techniques and tools for profiling attack methods, attack tools, intruders, and targeted assets



- Integrate active support from external experts
- Establish the options for isolated and stealthy communication channels
- Develop techniques and tools for profiling attack methods, attack tools, intruders, and targeted assets

Intelligence

- Provide forecasting and analysis of threats and conditions
- Establish reliable sources and news feeds
- Develop active and trusted network of strategic partners and experts


• Provide forecasting and analysis of threats and conditions
• Establish reliable sources and news feeds
• Develop active and trusted network of strategic partners and experts

Enterprise risk concepts

Cris V. Ewell, Ph.D.
December 2012

Threat Actors

- External (No trust or privilige)
  - Organized crime
  - State sponsored
  - Former employee or partner
  - Terrorist group
  - Lone hacker
  - Environmental
- Partners (Implied trust and privilege)
  - Suppliers
  - Business partner
  - Hosting vendor
  - Outsourced support
  - Other vendor
- Internal (Trust and privilege)
  - Workforce member
  - Contractors

Attack Vectors

- Authorized account misuse
- Cryptographic and password
- Data interception
- Denial of service
- Implied trust exploitation
- Malicious software
- Misjudgment or error
- Natural, environmental, and other
- Operating system and application
- Physical
- Social engineering
- Supply chain compromise

Organization

Capabilities*

- Organization & Authority
- Policy
- Audit & Compliance
- Risk Management
- Privacy
- Incident Management
- Education & Awareness
- Intelligence, Reporting, & Monitoring
- Operational Management
- Technical Security & Access Control
- Physical & Environmental
- Asset Identification & Classification
- Account & Identity Management

Context for Predictive Analytics

- Asset/Target critical attributes
- Threat actors
- Attack vectors
- Organization external footprint
- Targeted or opportunistic
- Implemented controls
- Organizational verticle
- Other ...

Threats*

- Organization & Authority
- Policy
- Audit & Compliance
- Risk Management
- Privacy
- Incident Management
- Education & Awareness
- Intelligence, Reporting, & Monitoring
- Operational Management
- Technical Security & Access Control
- Physical & Environmental
- Asset Identification & Classification
- Account & Identity Management

*Categories

Organizational Risk

Chance of threat actor successfully using attack vector resulting in compromise of asset or target

Assets or Targets

- Intellectual property
- Key service or products
- Application(s)
- Business partner
- Key person
- Data

Sample Information Security Dashboard

Overall Risk

Info Security Program Risk

- Intelligence, Reporting, and Monitoring
- Operational Management
- Technical Security and Access Control
- Asset Identification and Classification
- Account & Identity Management
- Audit and Compliance
- Education and Awareness
- Policy
- Incident Management
- Risk Management
- Privacy
- Organization and Authority
- Physical and Environmental Security

Attack Vector Risk

- Social Engineering
- Implied Trust Exploitation
- Authorized Account Misuse
- Denial of Service
- Malicious Software
- Operating System and Application
- Misjudgment Or Error
- Physical
- Supply Chain Compromise
- Data Interception
- Cryptographic and Password

Organization / Asset Risk

- Applications
- Business Partners
- Data
- Business Type
- Key People
- Mission/Activity
- Intellectual Property
- Key Service or Products

Risk Level	Low	High

Compliance Risk

	Last Period		Current Period		Trend
	Gap	Goal	Gap	Goal	
HIPAA					↑
PCI					→

Status - Security Initiatives

	Open	Close	Status
Information Security Plan	Nov-14	Sep-17	
Mobile Protection	Jun-14	May-15	
Enterprise Monitoring	Apr-14	Jun-15	
DMZ Security Plan	Dec-14	Sep-15	
Security Incident Handling	Dec-14	May-15	

Status - Performance Measures

		Last	Current	Trend
Vulnerability Management	Improve High Risk Applications			↑
	Reduce Network Enviornment Risk			↓
	Maintain Program Health			→
Measure #2		Last	Current	Trend
Measure #3		Last	Current	Trend

Incidents

Incident Type	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Disclosure of information	12	12	13	13	15	10	8	7	14	10	5	5
Hacking/Malware	6	4	8	8	7	10	14	10	8	10	8	14
IS incident	4	5	2	7	3	5	7	9	8	8	5	7
Loss of information	4	4	2	1	8	1	3	5	5	1	7	0
Theft of information	11	1	3	4	5	1	0	4	1	0	1	6
Unauthorized use	1	4	3	2	2	3	2	5	1	4	2	1
TOTAL	38	30	31	35	40	30	34	40	37	33	28	33
Reportable Incidents	1	4	0	0	1	2	1	0	0	0	2	0

Confidential

Keys to Building a Robust Data Security Plan

Cris V. Ewell, PhD
Seattle Children's
(206) 987-5077
cris.ewell@seattlechildrens.org