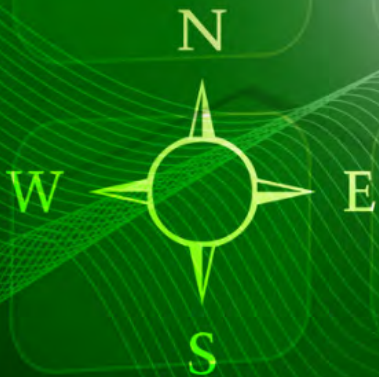
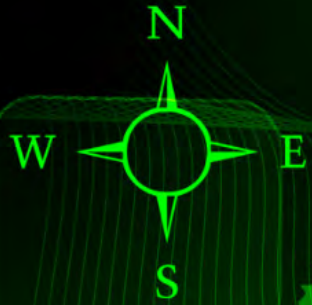


Keys to Building a Robust Data Security Plan



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

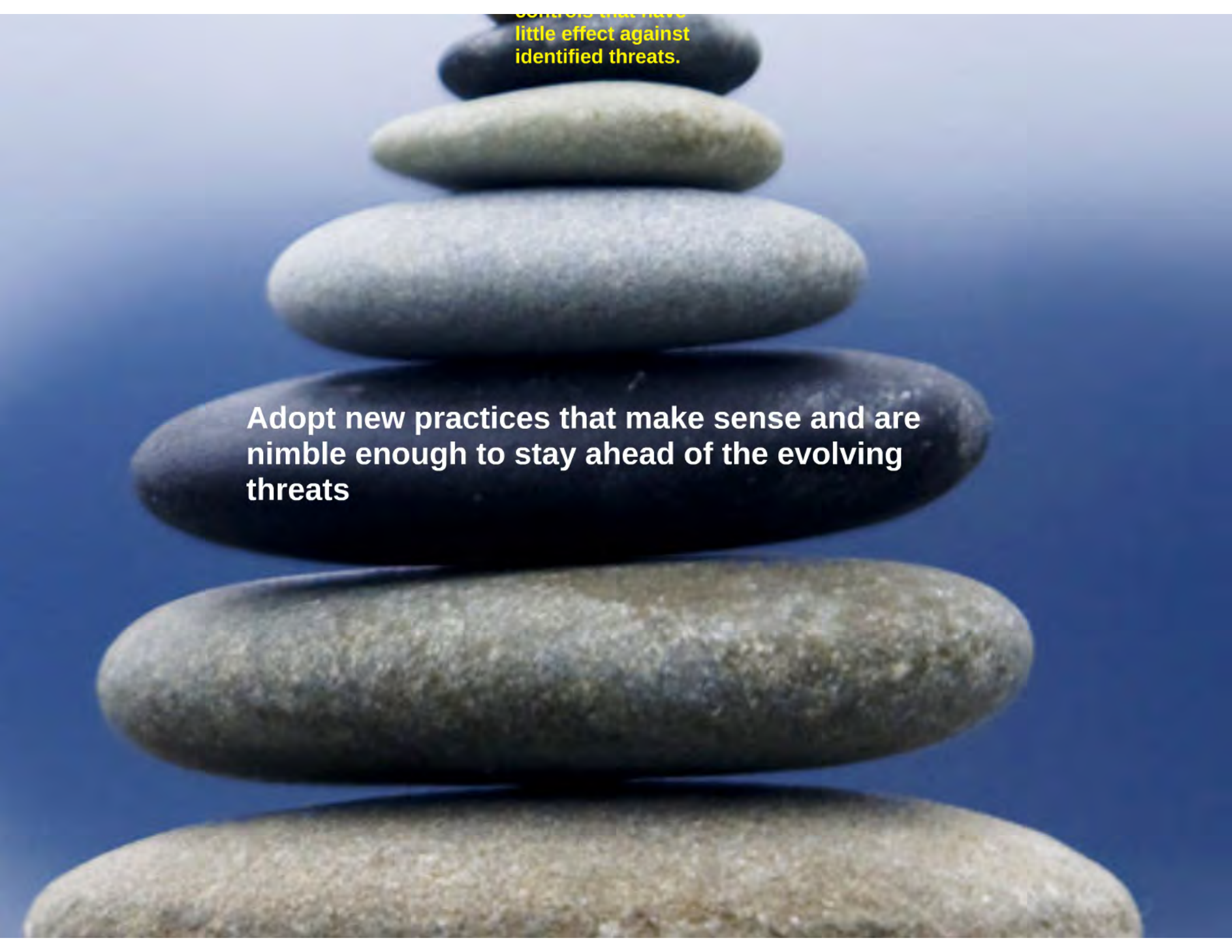
Ensure that the organization does not implement controls that have little effect against identified threats.

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.

A photograph of three smooth, rounded stones stacked vertically on a light-colored wooden surface. The stones are of varying shades: the top one is dark grey, the middle one is a lighter tan, and the bottom one is a dark blue-grey. The background is a clear, bright blue sky. The text is overlaid on the bottom stone.

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



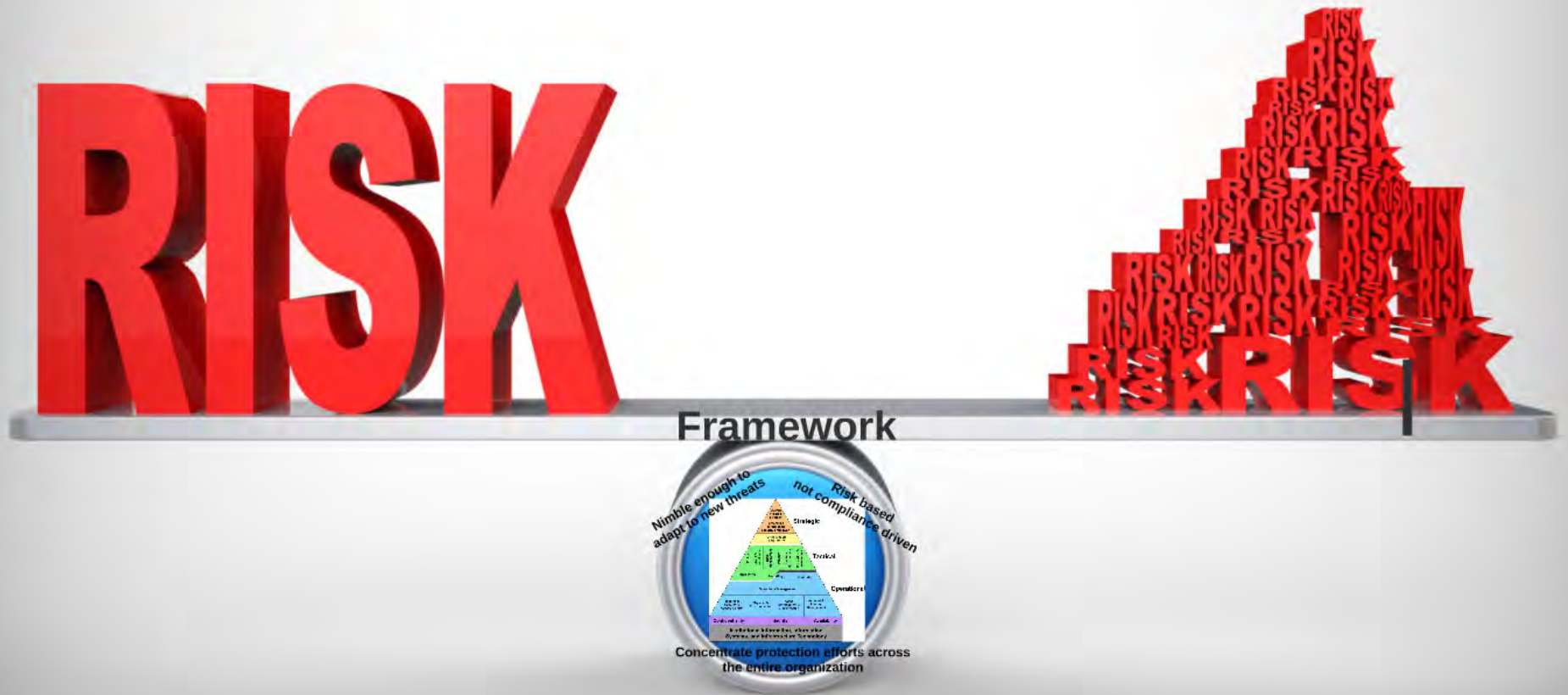
controls that have
little effect against
identified threats.

**Adopt new practices that make sense and are
nimble enough to stay ahead of the evolving
threats**



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**

A black rectangular graphic tilted at an angle, containing the word "ASSETS" in a colorful, brush-stroke style font. The letters are red, yellow, green, and blue. A white horizontal line is positioned below the text.

ASSETS

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

Architecture Handbook

CISM Reference Manual

Corporate Information Security Management

4/13/2015

Cerner	
Primary Function	Provides Children's IS clinical and ERM support
Description	Cerner provides a suite of applications which provided Children's with clinical support for Pathology, Electronic Medical Records, Radiology, Pharmacy and Physician record viewing. Provides functionality for clinical ordering and documentation.
IS Department Name	Clinical Applications
Supporting IS Team	EA Tech Svc
Information Involved	PHI, Personnel, Financial, IP/Sensitive
Network Location	
Last Review Date	
Notes	
Servers	

Observed Owned Domains		
Domain	IP	Location
childrenshospital.com	192.168.1.1	Seattle, WA
childrenshospital.org	192.168.1.2	Seattle, WA
childrenshospital.net	192.168.1.3	Seattle, WA
childrenshospital.edu	192.168.1.4	Seattle, WA
childrenshospital.gov	192.168.1.5	Seattle, WA
childrenshospital.mil	192.168.1.6	Seattle, WA
childrenshospital.us	192.168.1.7	Seattle, WA
childrenshospital.ca	192.168.1.8	Seattle, WA
childrenshospital.uk	192.168.1.9	Seattle, WA
childrenshospital.au	192.168.1.10	Seattle, WA
childrenshospital.jp	192.168.1.11	Seattle, WA
childrenshospital.in	192.168.1.12	Seattle, WA
childrenshospital.br	192.168.1.13	Seattle, WA
childrenshospital.mx	192.168.1.14	Seattle, WA
childrenshospital.ar	192.168.1.15	Seattle, WA
childrenshospital.co	192.168.1.16	Seattle, WA
childrenshospital.ec	192.168.1.17	Seattle, WA
childrenshospital.ve	192.168.1.18	Seattle, WA
childrenshospital.ve	192.168.1.19	Seattle, WA
childrenshospital.ve	192.168.1.20	Seattle, WA
childrenshospital.ve	192.168.1.21	Seattle, WA
childrenshospital.ve	192.168.1.22	Seattle, WA
childrenshospital.ve	192.168.1.23	Seattle, WA
childrenshospital.ve	192.168.1.24	Seattle, WA
childrenshospital.ve	192.168.1.25	Seattle, WA
childrenshospital.ve	192.168.1.26	Seattle, WA
childrenshospital.ve	192.168.1.27	Seattle, WA
childrenshospital.ve	192.168.1.28	Seattle, WA
childrenshospital.ve	192.168.1.29	Seattle, WA
childrenshospital.ve	192.168.1.30	Seattle, WA
childrenshospital.ve	192.168.1.31	Seattle, WA
childrenshospital.ve	192.168.1.32	Seattle, WA
childrenshospital.ve	192.168.1.33	Seattle, WA
childrenshospital.ve	192.168.1.34	Seattle, WA
childrenshospital.ve	192.168.1.35	Seattle, WA
childrenshospital.ve	192.168.1.36	Seattle, WA
childrenshospital.ve	192.168.1.37	Seattle, WA
childrenshospital.ve	192.168.1.38	Seattle, WA
childrenshospital.ve	192.168.1.39	Seattle, WA
childrenshospital.ve	192.168.1.40	Seattle, WA
childrenshospital.ve	192.168.1.41	Seattle, WA
childrenshospital.ve	192.168.1.42	Seattle, WA
childrenshospital.ve	192.168.1.43	Seattle, WA
childrenshospital.ve	192.168.1.44	Seattle, WA
childrenshospital.ve	192.168.1.45	Seattle, WA
childrenshospital.ve	192.168.1.46	Seattle, WA
childrenshospital.ve	192.168.1.47	Seattle, WA
childrenshospital.ve	192.168.1.48	Seattle, WA
childrenshospital.ve	192.168.1.49	Seattle, WA
childrenshospital.ve	192.168.1.50	Seattle, WA
childrenshospital.ve	192.168.1.51	Seattle, WA
childrenshospital.ve	192.168.1.52	Seattle, WA
childrenshospital.ve	192.168.1.53	Seattle, WA
childrenshospital.ve	192.168.1.54	Seattle, WA
childrenshospital.ve	192.168.1.55	Seattle, WA
childrenshospital.ve	192.168.1.56	Seattle, WA
childrenshospital.ve	192.168.1.57	Seattle, WA
childrenshospital.ve	192.168.1.58	Seattle, WA
childrenshospital.ve	192.168.1.59	Seattle, WA
childrenshospital.ve	192.168.1.60	Seattle, WA
childrenshospital.ve	192.168.1.61	Seattle, WA
childrenshospital.ve	192.168.1.62	Seattle, WA
childrenshospital.ve	192.168.1.63	Seattle, WA
childrenshospital.ve	192.168.1.64	Seattle, WA
childrenshospital.ve	192.168.1.65	Seattle, WA
childrenshospital.ve	192.168.1.66	Seattle, WA
childrenshospital.ve	192.168.1.67	Seattle, WA
childrenshospital.ve	192.168.1.68	Seattle, WA
childrenshospital.ve	192.168.1.69	Seattle, WA
childrenshospital.ve	192.168.1.70	Seattle, WA
childrenshospital.ve	192.168.1.71	Seattle, WA
childrenshospital.ve	192.168.1.72	Seattle, WA
childrenshospital.ve	192.168.1.73	Seattle, WA
childrenshospital.ve	192.168.1.74	Seattle, WA
childrenshospital.ve	192.168.1.75	Seattle, WA
childrenshospital.ve	192.168.1.76	Seattle, WA
childrenshospital.ve	192.168.1.77	Seattle, WA
childrenshospital.ve	192.168.1.78	Seattle, WA
childrenshospital.ve	192.168.1.79	Seattle, WA
childrenshospital.ve	192.168.1.80	Seattle, WA
childrenshospital.ve	192.168.1.81	Seattle, WA
childrenshospital.ve	192.168.1.82	Seattle, WA
childrenshospital.ve	192.168.1.83	Seattle, WA
childrenshospital.ve	192.168.1.84	Seattle, WA
childrenshospital.ve	192.168.1.85	Seattle, WA
childrenshospital.ve	192.168.1.86	Seattle, WA
childrenshospital.ve	192.168.1.87	Seattle, WA
childrenshospital.ve	192.168.1.88	Seattle, WA
childrenshospital.ve	192.168.1.89	Seattle, WA
childrenshospital.ve	192.168.1.90	Seattle, WA
childrenshospital.ve	192.168.1.91	Seattle, WA
childrenshospital.ve	192.168.1.92	Seattle, WA
childrenshospital.ve	192.168.1.93	Seattle, WA
childrenshospital.ve	192.168.1.94	Seattle, WA
childrenshospital.ve	192.168.1.95	Seattle, WA
childrenshospital.ve	192.168.1.96	Seattle, WA
childrenshospital.ve	192.168.1.97	Seattle, WA
childrenshospital.ve	192.168.1.98	Seattle, WA
childrenshospital.ve	192.168.1.99	Seattle, WA
childrenshospital.ve	192.168.1.100	Seattle, WA

Application	PCI	PHI	Personnel	Financial	IP/Sensitive
Application 1	High	High	Low	Low	Low
Application 2	High	Low	Low	Low	Low
Application 3	High	Low	Low	Low	Low
Application 4	Low	Low	Low	Low	Low
Application 5	Medium	Low	Low	Low	Low
Application 6	Low	Low	Low	Low	Low
Application 7	Low	Low	Low	Low	Low
Application 8	Low	Low	Low	Low	Low
Application 9	Low	Low	Low	Low	Low
Application 10	Low	Low	Low	Low	Low
Application 11	Low	Low	Low	Low	Low
Application 12	Low	Low	Low	Low	Low
Application 13	Low	Low	Low	Low	Low
Application 14	Low	Low	Low	Low	Low
Application 15	Low	Low	Low	Low	Low
Application 16	Low	Low	Low	Low	Low
Application 17	Low	Low	Low	Low	Low
Application 18	Low	Low	Low	Low	Low
Application 19	Low	Low	Low	Low	Low
Application 20	Low	Low	Low	Low	Low

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



Aggressive Risk Transfer Strategies

- **Carefully structured contracts with business partners and vendors**
- **Specific terms related to indemnification, limitations of liability, and defined roles and responsibilities in the event of breaches**
- **Insurance underwriting for breaches**

CEPT

Advanced Incident Response and Management

Think outside of the normal
incident response practices

A magnifying glass with a silver rim is centered over the words 'SECURITY' and 'BREACH'. The words are written in a bright green, blocky font. The background is a dark blue field filled with faint, light blue alphanumeric characters, resembling a digital or data stream. The magnifying glass has a slight shadow and highlights the text it is focused on.

SECURITY
BREACH

- 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



BREACH

- **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

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

Threat Actors

- External (No trust or privilege)
 - 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

Context for Predictive Analytics

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

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

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

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



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



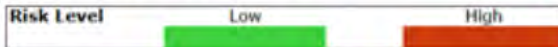
Attack Vector Risk

- 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



Compliance Risk

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

Status - Performance Measures

	Last	Current	Trend
Improve High Risk Applications			↑
Reduce Network Environment Risk			↓
Maintain Program Health			→
	Last	Current	Trend

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	

	Measure #2			Measure #3		
	Last	Current	Trend	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