WOMEN, & INFLUENCE & POWER IN LAW™



September 21-23, 2016

INTERNET OF THINGS

DATA BREACH SITUATION ROOM

Sharon R. Klein, Partner In Charge – CIPP
Pepper Hamilton LLP

Julie Bernard – Principal, Cyber Risk Services
Deloitte

Alma Murray, Esq., Senior Counsel, Privacy, CIPP
Hyundai Motor America

Cindy Donaldson, Chief Operating Officer
LS-ISAO

September 22, 2016

What is the "Internet of Things"

"Devices or sensors that connect, communicate or transmit information with or between each other through the Internet"

FTC Report on Internet of Things "Privacy & Security in a Connected World"
https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices

RANGE OF ENTERPRISE RISKS

FTC Enforcement

- Section 5 of FTC Act
- Unfair and Deceptive Trade Practices
  - Unfair=not following industry practices
  - Deceptive=failure to do what you promised

FACTS

- Cozy Cam is a manufacturer of home automation products and offers services which allow consumers remote access to view the inside and outside of their home.

FACTS

- Judy is a Cozy Cam customer.
- Bought product at Home Depot with a Home Depot credit card.
- **Sept. 11** – her home was burglarized.

FACTS

- **Sept. 3** – Cozy Cam upgraded its software
- **Sept. 6** – Cozy Cam received report that one customer could view the inside and outside of a home which was not theirs and could access profile information of another customer.
- **Sept 13** – Cozy Cam's security protocols which were disabled for one week are repaired.

FACTS

- **Sept. 15** – Cozy Cam sent breach notices.
- Judy's lawyer asks Cozy Cam for detailed information about the security defect.

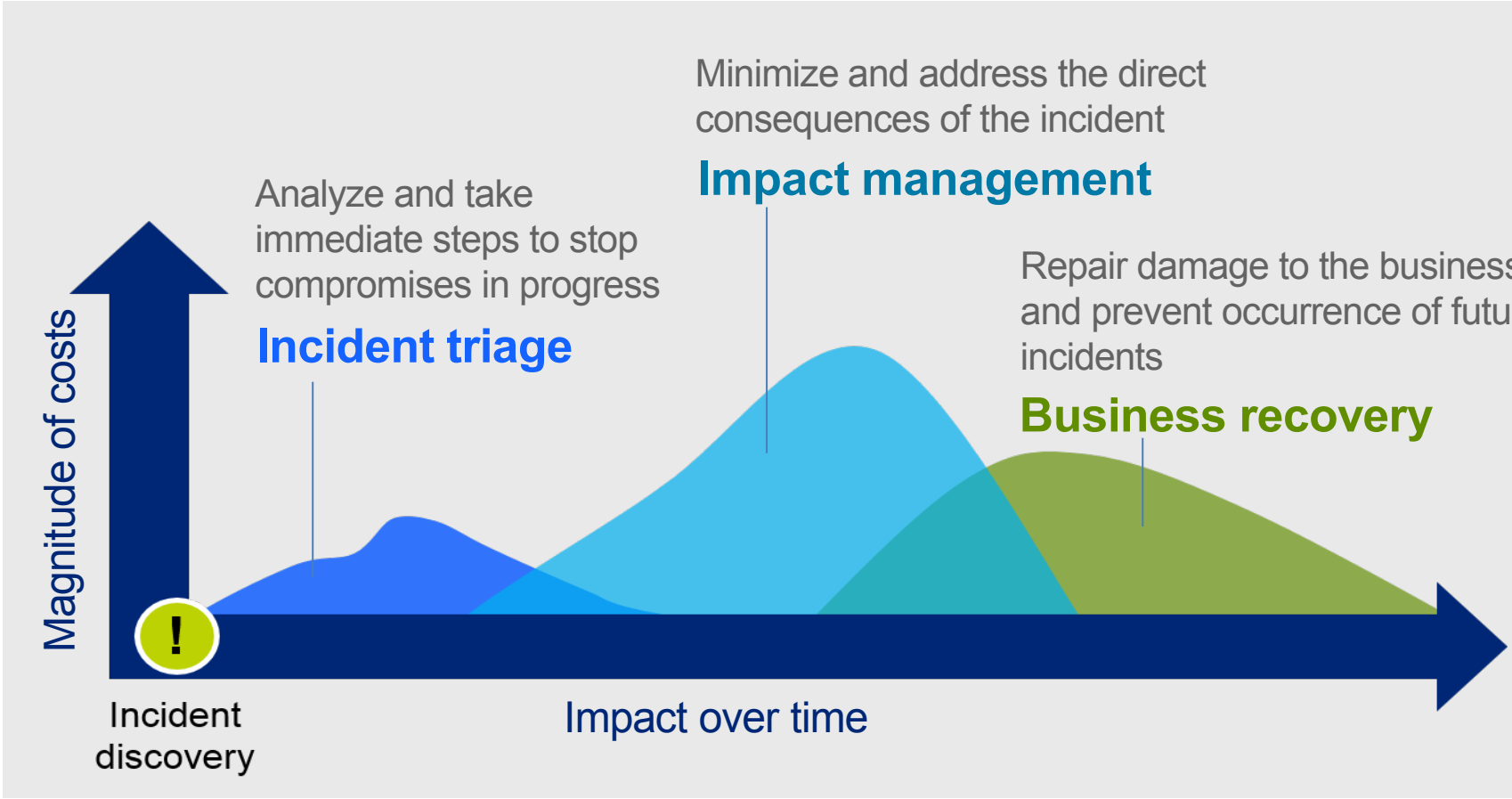
A narrow lens on cyberattacks can leave organizations unprepared for the broader potential costs

- Customer breach notification
- Post-breach customer protection
- Regulatory compliance costs
- Public relations costs
- Attorney fees and litigation
- Cybersecurity improvements
- Cost of lost customers

- Impact to current contracts
- Devaluation of trade name
- Loss of IP
- Impact of operational disruption and/or destruction
- Insurance premium increases
- Increased cost to raise debt

…and unprepared for the duration of recovery efforts

Costs are incurred and impacts are felt over years, in several phases



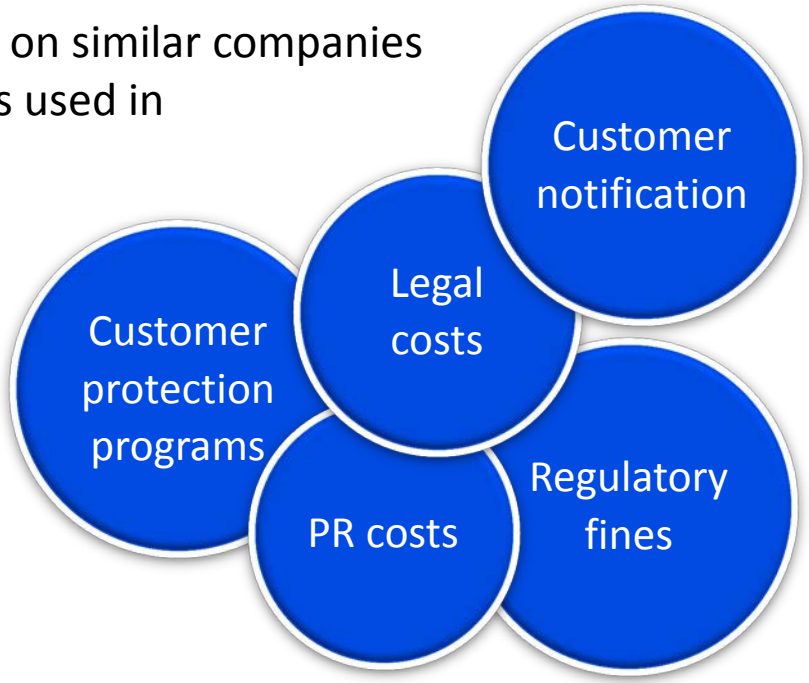
Estimating financial impact of the attack

Deriving cost and duration data

- Leveraged experience helping companies recover from major cyberattacks
- Developed fictitious profiles and scenarios based on industry knowledge
- Used publicly available information on similar companies as benchmark data to derive factors used in direct cost and valuation equations

Calculating direct costs

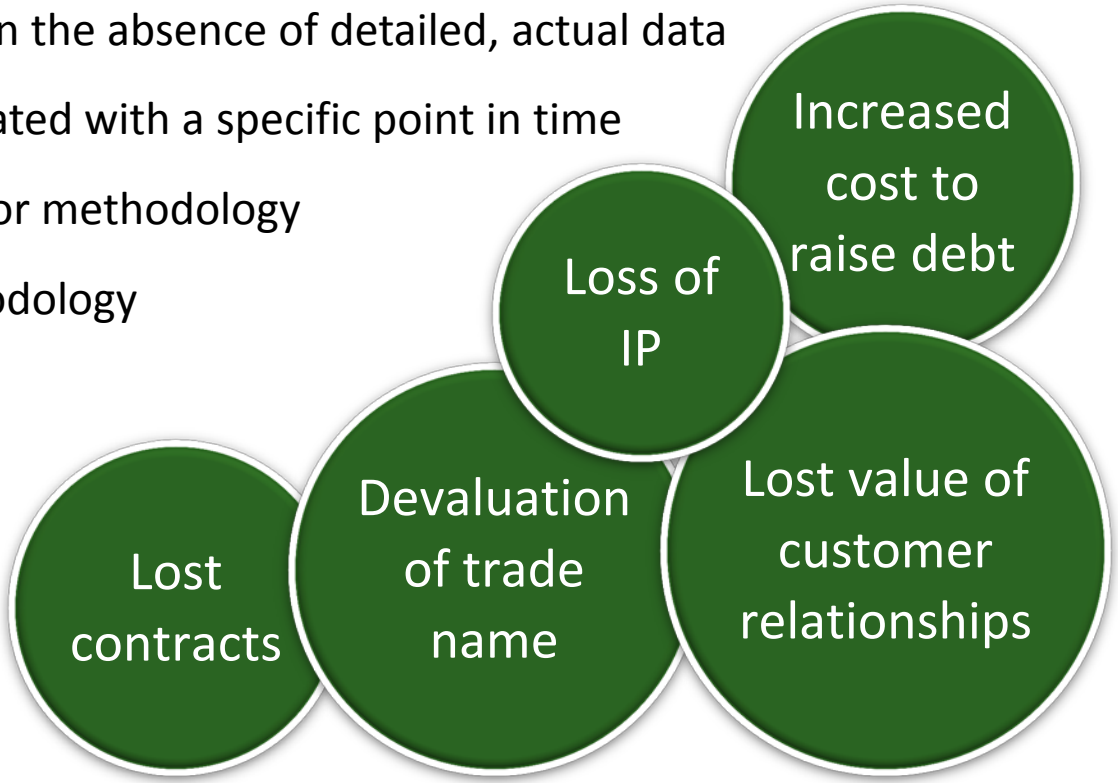
- Relatively simple to approximate based on publicly available information
- Leveraged existing studies



Modeling potential cyberattack impact

Calculating intangible impacts

- Applying professional judgement, accepted financial modeling methods and reasonable assumptions in the absence of detailed, actual data
- Financial impact is associated with a specific point in time
- With-and-without / But-for methodology
- Relief-from-royalty methodology
- Reliance on assumptions



What does it cost?

Total potential impact >$4B

- Many of the costs commonly associated with PII-type data breaches do not factor in
- Greatest impacts are intangible costs
- The value of lost IP is not the major cost, but the theft of IP has rippling impacts

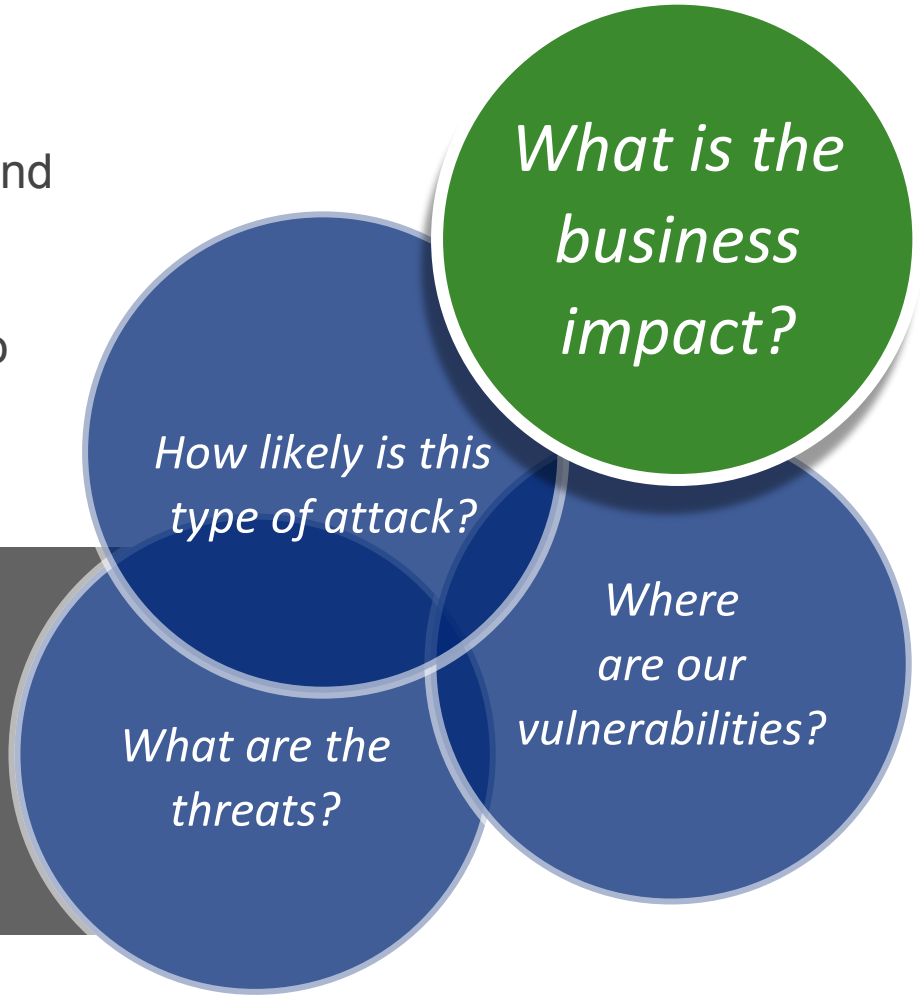
	Cost Factors	Cost (millions)	% Total
Known costs	Customer breach notification	--	--
	Post-breach customer protection	--	--
	Regulatory compliance	--	--
	Public relations	$1.00	0.02%
	Attorney fees and litigation	$11.30	0.24%
	Cybersecurity improvements	$13.00	0.27%
Hidden costs	Insurance premium increases	$1.00	0.02%
	Increased cost to raise debt	--	--
	Operational disruption	$1,200.00	25.09%
	Lost value of customer relationships	--	--
	Value of lost contracts	$1,617.00	33.81%
	Devaluation of trade name	$1,697.00	35.48%
	Loss of intellectual property	$242.50	5.07%
	Total	**$4,782.80**	100.00%

There's a big disconnect with the business

Cybersecurity programs continue to focus on the threats, vulnerabilities and probability.

Often, not enough attention is paid to the true damages a particular type of cyberattack can cause.

By looking realistically at the potential costs, business leaders can right-size investments to better protect their most valuable assets.



Internal View of Compliance

- Where does compliance fit within the corporation
  - Governance
  - Interdisciplinary
  - Cross business unit
  - Team meetings
  - Incident response

What Litigation Issues May Be Implicated?

- Class Action Lawsuits
- Products Liability Claims
  - Negligence/Strict Liability
  - Design/Manufacturing Defect
  - Failure to Warn
  - Breach of Warranty

How to Bring it all Together

- Establish Core Team Members
- Attend Joint Meetings

External View of Compliance

- ISAO Model
  - How they work
  - What benefits they bring

What is an ISAO?

- An ISAO is a group created to gather, analyze, and disseminate cyber threat information. ISAOs are not directly tied to critical infrastructure sectors, as outlined in **Presidential Policy Directive 21** (2/13/2015).
- ISAOs offer a more flexible approach to self-organized information sharing activities amongst communities of interest such as the legal sector and other business sectors across industry.

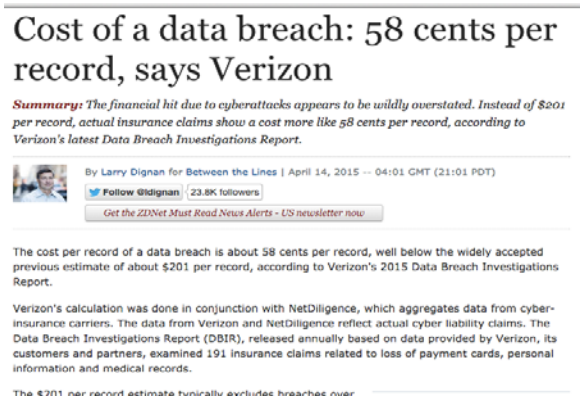
The Need for Info Sharing is Increasing

Increasing Attack Volume, Complexity

Rising Breach Costs

Growing Regulatory Pressures

Exploding Threat Indicator "Noise"



Cost of a data breach: 58 cents per record, says Verizon

Summary: The financial hit due to cyberattacks appears to be wildly overstated. Instead of $201 per record, actual insurance claims show a cost more like 58 cents per record, according to Verizon's latest Data Breach Investigations Report.

By Larry Dignan for Between the Lines | April 14, 2015 -- 04:01 GMT (21:01 PDT)

Follow @ldignan 23.8K followers

Get the ZDNet Must Read News Alerts - US newsletter now

The cost per record of a data breach is about 58 cents per record, well below the widely accepted previous estimate of about $201 per record, according to Verizon's 2015 Data Breach Investigations Report.

Verizon's calculation was done in conjunction with NetDiligence, which aggregates data from cyber-insurance carriers. The data from Verizon and NetDiligence reflect actual cyber liability claims. The Data Breach Investigations Report (DBIR), released annually based on data provided by Verizon, its customers and partners, examined 191 insurance claims related to loss of payment cards, personal information and medical records.

The $201 per record estimate typically excludes breaches over

CRAIN'S NEW YORK BUSINESS

Login

CURRENT ISSUE EVENTS DATA & LISTS VIDEO NEWSLETTERS CUSTOM CONTENT TV

Real Estate Small Business Health Care Politics Technology More Industries

Balancing the weight of big decisions?

The insight you need to make decisions of impact

Deloitte Growth Enterprise Services

Deloitt

JPMorgan cybersecurity costs doubling

nds $250 million a year on computer security, was recently hacked.

BRIEFING ROOM ISSUES THE ADMINISTRATION PART

Home • Briefing Room • Statements & Releases

The White House

Office of the Press Secretary

E-Mail Tweet

For Immediate Release

FACT SHEET: Executive Order Promoting Private Sector Cybersecurity Information Sharing

1,554

Number of installations of FS-ISAC's Soltra Edge information-exchange platform in the first four months after it was launched Dec. 3

12 million

Number of threat indicators in FS-ISAC's cyberthreat repository as of Oct. 1, a fivefold increase from a year earlier

10,000+

Number of daily manual

Benefits of Information Sharing

Sharing Practices | TLP

The **Traffic Light Protocol** (TLP) is used to encourage greater sharing of sensitive information. The originator determines how widely they want their information shared, if at all.

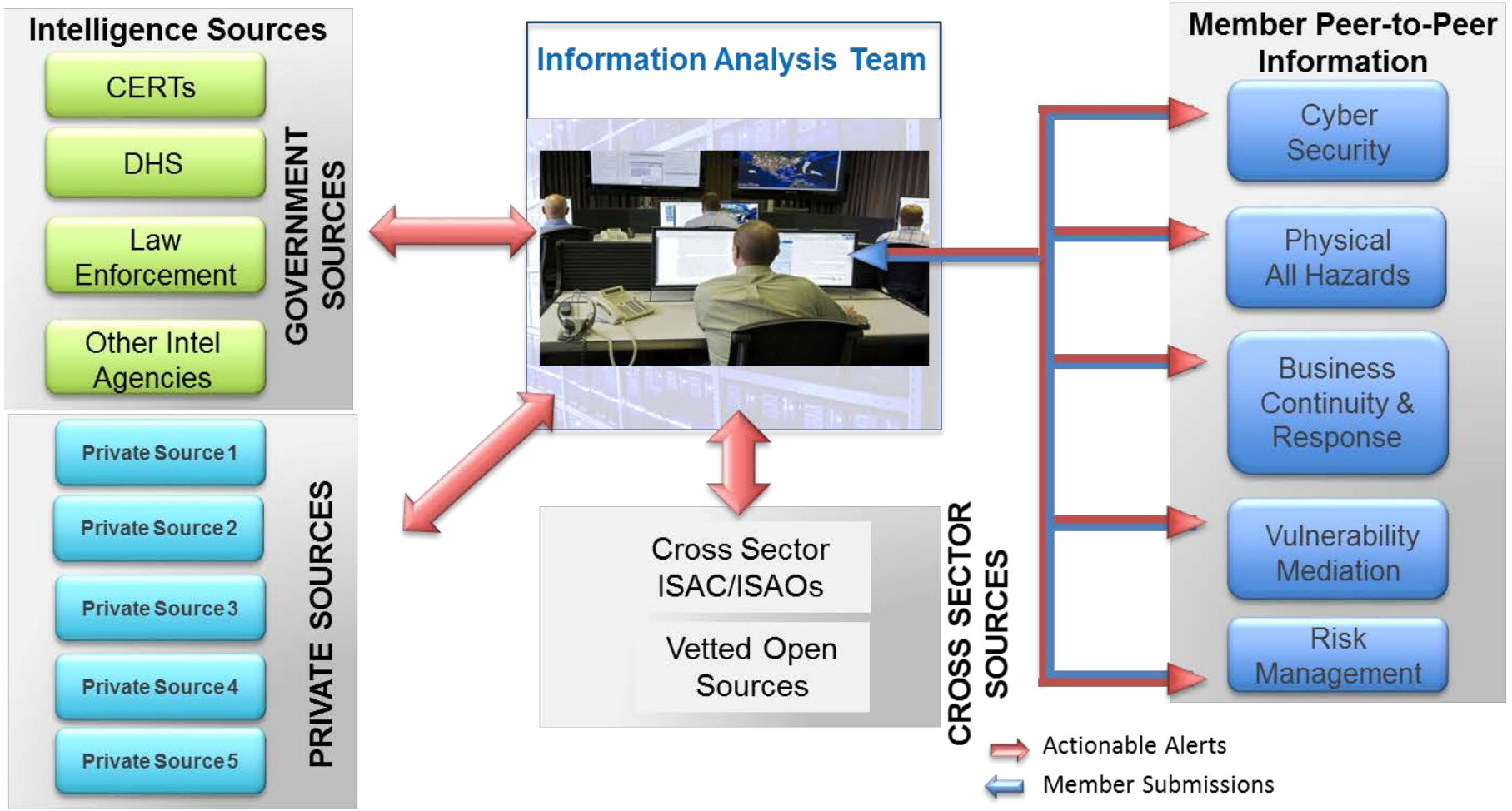
Current Member Benefits

ListServ Subscriptions	Participate on the intelligence sharing listserv.
LS-ISAO Portal	Alerts providing relevant and actionable threat information, vulnerabilities and advisories from vendors and government agencies are circulated via email through the LS-ISAO Portal.
Member Submissions | Anonymous or with Attribution	Members can submit via email/phone/portal with an appropriate TLP classification. Submissions are processed and shared as Cyber Incident (CYI), Cyber Threat (CYT), Collective Intelligence (COI) and/or Request for Information (RFI) on cybersecurity and industry specific issues.
Indicator of Compromise Information	Sources include closed-source government agencies, open source intelligence, and vetting member submissions with additional investigations, research and analysis.
Customized Email Notification Profile	Portal Alerts will be sent to portal user(s) based on assigned roles.
Sector Specific Alerts (government, private partners and other ISAC/ISAOs)	Non-classified products from NCCIC, US-CERT, ICS-CERT and other ISACs. (LS-ISAO has applied for a DHS CRADA, allowing full access to all sharable DHS analytic products from the US-CERT portal).
Crisis Information Notification System	Industry incident response and recovery communication support (via phone/email).
Threat and Vulnerability Reports	Cyber Incident (CYI), Cyber Threat (CYT) and Collective Intelligence (COI)

Current Member Benefits

ListServ Subscriptions	Participate on the intelligence sharing listserv.
Vulnerability Analyses, Alerts and Risk Mitigation	Cyber Vulnerability (CYV).
Collective Intelligence Reports	Available trend and state of intelligence reports focused on security awareness.
Interactive Threat/Vulnerability Catalogues	Available in the LS-ISAO Portal.
Member Directory	Available in the LS-ISAO Portal.
Secure Portal Chat	Available in the LS-ISAO Portal; allows for private sector interest groups to focus on single topic.
Secure Portal Document Repository	Available in the LS-ISAO Portal.
Member Surveys	Supports community requests for information.
Member Meeting Events and Networking Opportunities	Available to members only and scheduled throughout the year.
Participation in Member Committees	Governance and subject focus groups contribute to health and growth.

Intelligence Flows are Bi-Directional



FTC IoT Tips

- Start with the Fundamentals
- Take advantage of what experts have already learned about security
- Design your product with authentication in mind
- Protect the interfaces between your product and other devices or services

FTC IoT Tips

- Consider how to limit permission
- Take advantage of readily available security tools
- Test the security measures before launching your product
- Select the secure choice as your default setting
- Use your initial communication with customers to educate them about the safest use of your product

FTC IoT Tips

- Establish an effective approach for updating your security procedures
- Keep your ear to the ground
- Innovate how you communicate
- Let prospective customers know what you're doing to secure customer information

QUESTIONS