

# So You Have an Information Sharing Capability...

DATA  
Global Network

A1

Model A1

INNOVATION

## Now What?

DATA

# About Me

- ▶ Husband, father, podcaster, political junkie, and IndyCar fan
- ▶ A board member of the Nation Council of Registered ISAOs and the Cyber Resilience Institute
- ▶ An Information Security Instructor for CIAS at UTSA
- ▶ Have presented at the previous two IISC conferences:

**Disclaimer:** All views and opinions are mine and not those of any organization that I may not represent!

# About this presentation

My goal is to provide insights into how you can turn information into something that is actionable and valuable for your organization!!!

```
padding: 4px 6px;  
text-align: left;  
  
&:hover {  
    color: $c-link-hover;  
}  
  
&.selected {  
    background-color: $c-action;  
    color: white;  
}  
  
.amount {  
    float: right;  
    font-weight: bold;  
}  
  
&.last-child {
```

Before we begin, lets assume...



```
padding: 4px 6px;  
text-align: left;  
&:hover {  
  color: $c-link-hover;  
}  
ed {  
  background-color: $c-action;  
  color: white;  
}  
{  
  text-align: right;  
  font-weight: bold;  
}  
&:last-child {
```

# Assumption 1

Your organization has spent time and resources to establish an information sharing capability. This includes:

- ▶ Joining an Information Sharing and Analysis Organization (ISAO)
- ▶ Establishing relationships with businesses
- ▶ Working with law enforcement/other government entities
- ▶ Joining multiple online community forums

## Assumption 2

- ▶ The purpose of our information sharing program is to have better situational awareness about the threats that the organization is facing in order to be able to be better prepare, identify, protect, respond and recover.
- ▶ This capability is about reducing the organization's cybersecurity risk and improving the overall cybersecurity posture.

## Its a lot of work

- ▶ Developing a relationship with or joining an ISAO or other organizations
- ▶ Establishing processes, protocols, polices, and procedures
- ▶ Procuring, testing, and implementing technologies

# Don't let it go to waste

- ▶ The last thing that we want is to have this information, more so this capability sit stagnant
- ▶ Don't let that information get stuck in the blue nowhere or some black hole
- ▶ By not utilizing this capacity risks are going unaddressed and if you are in a regulated industry you could be compounding your organization's risk

```
padding: 4px 6px;  
text-align: left;
```

```
&:hover {  
    color: $c-link-hover;
```

```
&.selected {  
    background-color: $c-link-selected;  
    color: white;
```

```
    }  
    amount {  
        float: right;  
        font-weight: bold;
```

```
    }
```

```
&:last-child {
```



# Information Sharing Lifecycle



I would like to introduce my view on the Information Sharing life cycle.

- ▶ Visualize the different steps in how information is processed.
- ▶ Adds context by mapping the steps to technology, people, and processes.
- ▶ Guides the developing KPIs and metrics to build around the program.

# Information Sharing Lifecycle

## Collect

- ▶ The ingestion, collection, or gathering of data from one or multiple sources. This can be automated or manual. This part of the process can be initiated by the push or pull of information.

## Triage

- ▶ Sorting, classifying, and categorization of the information. Can be automated and/or manual.

## Analyze

- ▶ A detailed examination of data to identify malicious activity and an assessment of the identified malicious activity to existing threat information to say something greater about the data at hand <sup>1</sup>.

1. ISAO 100-1 Introduction to Information Sharing and Analysis Organizations (ISAOs) v1.01

# Information Sharing Lifecycle

## Act

- ▶ The response or action taking by an organization to address or mitigate the information.

## Measure

- ▶ Determining the outcomes of the action(s) taken by the organization as a result of the information.

## Disseminate/Report

- ▶ Distributing the outcomes, new information, or finds internally or externally. This information can also be used to compare and compile with new information that is received in.

customer.scss	54
layout.scss	55
product-terms.scss	56
pricing_conditions.scss	57
product-list.scss	58
request-profile.scss	59
review.scss	60
search.scss	61
show.scss	62
widget.scss	63
...	64
...	65
...	66
...	67
...	68
...	69
...	70

```
padding: 4px 6px;  
text-align: left;  
  
&:hover {  
    color: $c-link-hover;  
}  
  
&.selected {  
    background-color: $c-action;  
    color: white;  
}  
  
.amount {  
    float: right;  
    font-weight: bold;  
}  
  
&.last-child {
```

Back to the title of the presentation...


So now what?

# What do we do now that we have this capability?

First, don't lose sight of why the program was established in the first place.

- ▶ Keep focused on the vision, mission, and goals of the information sharing program in the forefront of our minds.





## What do we do now that we have this capability?

- Second, we need to continually show the value of this capability to the organization.
- Showing the return on the investment and effort will be a key activity for establishing future growth of the program.

# How do we show value?

The image shows a digital display board with a grid of data. The text is in Arabic. The visible data points include:

Company Name	Value 1	Value 2	Value 3	Value 4	Value 5	Value 6	Value 7
شركة طيران أبوظبي	2,930	27,000	2,180	5,690	4,500	5,420	0.000
شركة أبوظبي	2,180	1,225	5,350	0.410	584,494	0.450	0.000
شركة أبوظبي الوطنية للتعا	5,340	0	0.000	2,750	92,464	2,600	0.000
شركة الحظية للبيضة	0.450	30,393	2,440	1,830	56,512	1,600	0.000
شركة أبوظبي الوطنية للتأمين	2,600	5,000	1,600	2,310	128,544	2,290	0.000
الأممك	1,600	73,778	2,300	3,100	874,820	3,090	0.000
	0.000	0.000	0.000	0.000	0	2,950	0.000
						1,450	0.000

```
padding: 4px 6px;  
text-align: left;  
  
&:hover {  
    color: $c-link-hover;  
}  
  
&.selected {  
    background-color: $c-action;  
    color: white;  
}  
  
.amount {  
    float: right;  
    font-weight: bold;  
}  
  
&.last-child {
```

Simply comes down to Metric, Metrics, Metrics!



# Tracking performance

What are some examples of KPIs for an Info Sharing Program?



Accuracy of the information



Reputation of the source



Relevance of the information



Program effectiveness



```
padding: 4px 6px;  
text-align: left;  
  
&:hover {  
  color: #000000;  
}  
  
&.selected {  
  background-color: $c-action;  
  color: white;  
}  
  
.amount {  
  float: right;  
  font-weight: bold;  
}  
  
&:last-child {
```



# Accuracy & Quality

There are number of different ways to measure data accuracy and data quality





# Reputation of the source

## GitHub

👁 Watch 36   ★ Star 539   🍴 Fork 378

## Infraguard

Rating
4.5
4.66

## Shodan

Top Voted

11,142

**Webcam**  
best ip cam search I have found yet.

webcam surveillance cams 2010-03-15

4,523

**Cams**  
admin admin

cam webcam 2012-02-06

## ThreatConnect's CAL

Additional Owners		
Name	Threat Rating	Confidence Rating
Bambenek	👤👤👤👤👤	50
IR0b1terate SRC	👤👤👤👤👤	



# Information Relevance & Program Effectiveness

- Is the information relevant to our environment?
- Did the information being shared with us result in some sort of action that protected our systems?
- Did this information help solve our problems, reduce our risk, and improve our security?

# What are the metrics supporting the KPIs?

## Examples

- ▶ # of False Positive by source
- ▶ % accuracy of the information by source
- ▶ # of True Positives by source
- ▶ Community rating of the source
- ▶ # of threats stopped as a direct result of this information



# What do we do with this capability?

Operationalize the data that is collected.

- ▶ There are a few ways an organization can take action on the data they have collected from this capability



# What do I do with all this data?

- ▶ Build intelligence, knowledge, and ultimately wisdom from this information
  - ▶ Data → Information → Knowledge → Wisdom (DIKW Framework) Going from who, what, when, where to how, and ultimately to why
- ▶ Apply the external data to our internal data and fuse it into business intelligence

# What do I do with all this data?

- ▶ Take this intelligence and turn it into institutional knowledge.
- ▶ Build your Security Awareness and Training programs.
- ▶ Create use cases from situations, issues, threats that have been experienced within your organization.
- ▶ Build training scenarios from those real-life examples.





## What are some outputs?

- ▶ Daily, Monthly, Quarterly, and/or Yearly
  - ▶ Analytical Reports
  - ▶ In person or webinar briefings
- ▶ Dashboards
  - ▶ KPIs
  - ▶ Trends
- ▶ Internal threat bulletins
- ▶ Program success stories
- ▶ Lessons Learned case studies
- ▶ Policy, procedure, and standards recommendations
- ▶ Conference presentations

# Give back to the Community

- ▶ Share what you learn and find with the ISAO community
  - The Good
  - The Bad
  - And the Ugly
- ▶ Create and share threat bulletins to distribute outward
- ▶ Host webinars, in person briefings, and other meetings

# Something to think about

- ▶ Some potential agencies to share with:
  - ▶ NCCIC
  - ▶ State Level ISAOs
  - ▶ Fusion Centers
  - ▶ State and Local Law Enforcement
  - ▶ FBI
  - ▶ State and/or Local Government Depts. of Homeland Security
  - ▶ (if legal will allow it).
- ▶ Involving Law Enforcement could help them in cases they are already working.

```
padding: 4px 6px;  
text-align: left;  
  
&:hover {  
    color: $c-link-hover;  
  
&.selected {  
    background-color: $c-action;  
    color: white;  
}  
  
.amount {  
    float: right;  
    font-weight: bold;  
}  
  
&:last-child {
```

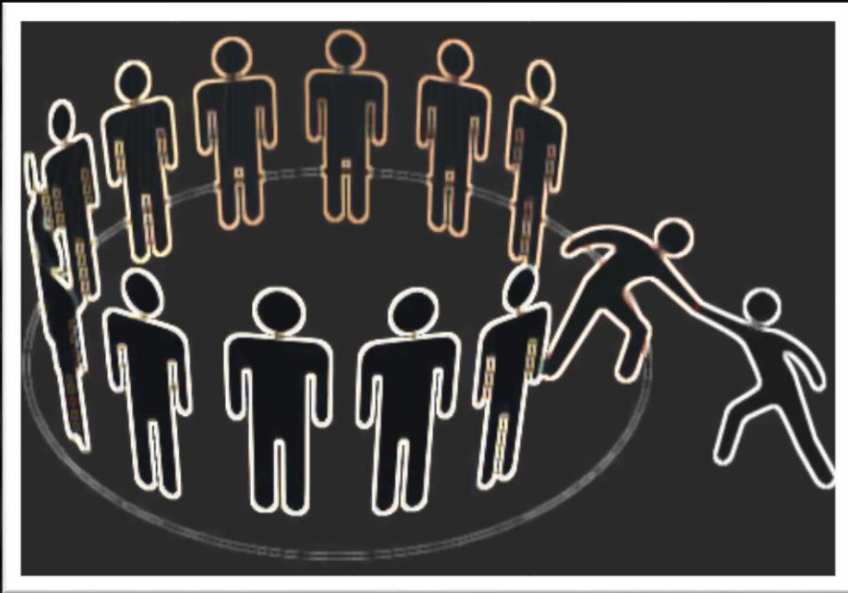
customer.scss	54
layout.scss	55
product-terms.scss	56
pricing_conditions.scss	57
product-list.scss	58
request-profile.scss	59
review.scss	60
search.scss	61
show.scss	62
widget.scss	64
archive.scss	66
override	67
vendor	68
stack	69
card	70

```
padding: 4px 6px;  
text-align: left;  
  
&:hover {  
    color: $c-link-hover;  
}  
  
&.selected {  
    background-color: $c-action;  
    color: white;  
}  
  
.amount {  
    float: right;  
    font-weight: bold;  
}  
  
&.last-child {
```

# What else can I do?

Going beyond the internal actions

# Get involved



- ▶ Join a working group
- ▶ Engaged in community forums
- ▶ Go to conferences
- ▶ Attend training sessions
- ▶ Build your network

# Get your leadership involved

- ▶ Regularly communicate with your organization's leadership.
  - ▶ Promote your successes
  - ▶ Provide regular reports on the critical issues.
- ▶ Get them involved in the ISAO and the other members of the ISAO.
- ▶ Conduct executive level table top exercises – use real life examples of issues your organization has seen.



# What About the Lawyers?

- ▶ Work with your legal council to ensure that your sharing capability protects you under the Cyber Information Sharing Act (CISA) of 2015.
- ▶ Involve them in the Incident Management and Response processes.

```
padding: 4px 6px;  
text-align: left;  
  
&:hover {  
    color: $c-link-hover;  
}  
  
&:selected {  
    background-color: $c-action;  
    color: white;  
}  
  
.amount {  
    float: right;  
    font-weight: bold;  
}  
  
&:last-child {
```

# What About the Lawyers?

- ▶ Ensure that proper agreements are established and executed.
  - ▶ Non Disclosure Agreements (NDA)
  - ▶ Memorandum of Understanding (MOU)
- ▶ Having your legal council's support in maintaining awareness of privacy and legal concerns surrounding information sharing is paramount.

```
padding: 4px 6px;  
text-align: left;  
  
&:hover {  
    color: $c-link-hover;  
  
&.selected {  
    background-color: $c-action;  
    color: white;  
  
.amount {  
    float: right;  
    font-weight: bold;  
  
&.last-child {
```



# Don't forget about the front line



Work with the front line techs and analysts to get their buy in

- ▶ Have them beta test tech
- ▶ Get their input on procedures
- ▶ Have them present to management
- ▶ Provide incentives through recognition and awards



# Continue to grow the capability

The work is never done!

- ▶ Grow and mature the program
- ▶ Reinvest time and resources
- ▶ Make adjustments as needed
- ▶ You get out off it what you put in to it

# Resources

- ▶ Cybersecurity and Information Sharing: Legal Challenges and Solutions
  - ▶ <https://fas.org/sgp/crs/intel/R43941.pdf>
- ▶ ISAO-SO Publications
  - ▶ <https://www.isao.org/resources/published-products/>
- ▶ American Bar Association - Cybersecurity
  - ▶ [https://www.americanbar.org/advocacy/governmental\\_legislative\\_work/priorities\\_policy/civil\\_liberties/cybersecurity/](https://www.americanbar.org/advocacy/governmental_legislative_work/priorities_policy/civil_liberties/cybersecurity/)
- ▶ US-DHS Information Sharing
  - ▶ <https://www.dhs.gov/cisa/information-sharing-vital-resource>

# Bio



- Currently a Director of Information Security for IU Health and IU School of Medicine. Nick has over 15 years' experience in Information Technology, 9 years in Cybersecurity, 9 years in Law Enforcement, and 10 years in State Government.
- B.S. in Management Information Systems – ISU '03 & M.S. in Cyber Forensics – Purdue '15
- Experience in incident response, digital investigations, criminal investigations, digital media recovery, law enforcement, data governance, end point protection, network and log analysis, vulnerability management, security operations, incident management, project management, as an instructor, and service implementation of managed security services.
- Supported multiple industries and sectors including, academia, State\Local\Tribal\Territorial (SLTT) Governments, health care, Information Technology and Manufacturing.