Metricon X

# 9:45-10:30 A Calibrated Severity Score for Breach Impacts

**Score Calibration via Explorations**

1. Correlated/ co-occuring/ redundant indicators
   1. Simple: Correlation Matrix
   2. Sophisticated: Iterated VIF
   3. Correlated/ co-occuring/ redundant indicators
2. Linear Model for # Disclosed Records 🡪 Serious problems
3. Constrained Optimization (Still working on this)
   1. Use existing weights as “initial condition”
   2. Use “disclosed records” cases as constraints
   3. Function to maximize:
      1. Sum of all weights
   4. Gradient function
4. Inference on Evidence via BayesNet

# 10:30-11:15 Defensible Metrics for Improved Network Resilience Scoring to Include Lateral

**Network Resilience: currently being abused like ML and AI**

**We’ve lost sight of Business Resilience**

* Metrics maximizing IT network security lack alignment
* Non-linear and dynamic relationship between business processes, revenues, and the supporting IT/OT systems need to be rationalized

**A more holistic approach for measuring resilience**

* Financial
* Business Process
* IT/OT

**Methodology: Surpassing NIST CSF &FAIR to reach AMA/SMA Compatible Models**

* NIST CSF Assessment
* FAIR Framework
* AMA Compatibility

**Leveraging Telemetry**

**Enriching Telemetry**

**Initial Criticality Values with Axiomatic Rules**

1. Arbitrary risk assignments
2. Inferring key relationships and collective criticality between nodes (sub-graphs)
3. Overlaying expert judgement
   1. Always add more or extend model/ algorithms

**Blast Radius**

* Includes the utilization of heuristics and k-shortest path algorithms
* Blast Radius: Filtered for one hop out

**Customizable Criticality & Risk Profile Scoring**

**Real Tas & Your Network**

* Fine-tune criticality and vulnerability weighting values for organization-specific assessment

**Risk Reduciton with Kerberos Instrumentation**

* Prevention/ Hardening
  + Active Directory Monitoring (ADMON)
    - Identify commonly exploited attack paths
    - Reduce potential for lateral movement via intentional access management
* Integrity
  + Kerberos Protocol Validation (KV)
    - External verification of all authentication transactions
    - Reduce dwell time from months to minutes when internal credentials are compromised
* This methodology enables a living, breathing model for continuous testing and assessment of enterprise-wide and organization-specific risk
* Supports extensions beyond network resilience in the IT world to real operational and financial impact to the P&L
* Eliminates the need for massive one-time or periodic consulting exercises
* Supports incremental refinement of threat models, inventories, and business process understanding

# 11:30-12:15 Metrics and Standards: Report from the Trenches

* 8 frameworks, but only 3 “Wholistic” Information Security Frameworks with published metrics

ISO Identifies

* 2 Kinds of measurements
  + Performance
  + Effectiveness

Process:

* Evaluation
* Analysis
* Measurement monitoring

13:30-14:15 MSRC Case Study

Microsoft security response report- write-up will give with problem, which trisge team will evaluate to create a case

Responsible disclosure: where they go to vendor before going to the public

Team inform people

Bug bounties- Pay people money to find issues and bugs. Cannot be paid always so they also inform the public about it because it helps people with jobs sometimes

MSRC 100- measure a very big deal

Success disasters- its not just how many time or things you’ve reported to Microsoft, but its also about how actionable it is, how is it helping.

Also helps with rediscovery of flaws, to support a master list created when it is first reported

Do you have people reverse engineer the system to rank higher on MSRT – Yes, they’d like if that’s happening. Current model is reactive and they’ve made sure to explain the process to calculate the Top 100.

How to do evaluate a chain attack- Can be calculated by vulnerability index.

**Present criteria for Top 100-**

Short time frame to judge(12 months)

Make sure it goes directly to Microsoft

Severity levels

**Leveraging Top 100-**

Looking to encourage exploring ventures they’ve not worked with yet

Telling people where they would like research rather than just the info they’re giving

Take into account to helpful behaviour- like really good research should be encouraged as opposed to someone who does really good once in a while but just a lot of background noise other times

14:15-15:00 Integrating Cyber Insurance into your cyber security Arsenal

**Integrating Cyber Insurance into your cyber security Arsenal**

* Biggest vulnerability is user. Training the users is no more enough due to successful attempts made by outsiders to access secured systems
* Regulations: stress on protecting information stored by companies and prevent data breaches
* Insurance: study of Canadian insurance companies – their coverage about cybersecurity insurance – Cyber and privacy liability
* Privacy breaches insurance – if insurance policies are provided, would the insured become lazier and laxer in their digital security hazards?
* How do you formulate these policies to formalize to machine processable language?

15:15-16:00 Metrics that Matter: help management improve decision making and improve the organization’s security posture

* Metrics – what are the right information, data we investigate such that they are action oriented and bring value?
* How secure are we? What are the threats on high risk areas?
* Quantitative measurement to back up everything
* Drive cyber hygiene
* Self service platform that enables decision making
* Overview of Information Security Metrics Program
  + Define requirements – identify data sources – analyze – dashboard
  + Manage risk and compliance with quantitative measures to support decision making
  + Scope of metrics
  + Metrics (Content, KPI, KRIs)
  + Clear and compelling story – help them take action
  + Domain – outcome – metric – raw data
  + Quant + qualitative measurements – gap analysis, improvement areas, area to invest and focus on
  + Identify sensitive information assets
  + Identify most critical infrastructure and applications
  + Prioritize vulnerability assessment and remediation
  + Prioritize compliance assessment and remediation
* Automation and reduce overhead
* Focus more
* Stakeholder interaction and engagement
* Report on actions taken and impact
* Next steps: key questions + define requirements + list data sources + define potential metrics + create sample reports + identify quick wins

16:00-16:45 Assigning Probability to Cybersecurity Risk

* Augment probability to cybersecurity risk measurement
* ERM framework standards
* Framework – how cybersecurity risk management affects decisions
* Observations - Controls – people – assessments – events – issues => cybersecurity risk
* DBIR – database – summary, severity

Day 2

09:10-09:55 Why does Application Security take so long?

* The entire presentation was curve graph based.
* Take the information data from the customers and ask them questions- what do they want to know and then perform research to come up with the advice
* Fixing flaws are the most time consuming
* Overall, 4.4m findings were closed out of 6.3m flaws findings after 500 days of finding the product
* The time is wasted when the people scans the incorrect branch which closes less than 10 findings. They have to go back and scan the correct branch to get a mass closure.
* Survival analysis: Percentage of flaws closed- 75%-21 days, 50%- 121 days, 25%- 472 days.
* The survival curve is better for the 50 scans per year than 1-12 scans per year (based on scan frequency)
* An unanswered question is what is the nominator for the question, the organization or the applications?
* Future: Longer term - correlation of activity to individual developer activity.

Questions:

Do you have the data that were never closed?

* Yes

Is there a way to find and let the people know if the flaws are removed from the production?

* It’s a lot of data but the data needs to be entered, so there is a possibility, but really scarce

09:55 – 10:40 Communicating Cyber Risk to the Board

* The target audience for the cyber balance sheet -Board of directors and CIO’s
* Source Tracking – Minimize the bias list to get the results and data collection – Send it to separate individuals to get the response and data
* Factors that made it easier/harder to convey value

Board Awareness

Board Support

Business Enabler

Presentation skills

**Other Justification - most valuable as it can make it the hardest**

Conservative spends

Prior breach

* Review of 2017 Study
* Boards lack confidence in the security program (Directors get the overwhelming impression that investment on security cannot guarantee security)
* They prefer Business level Security Metrics
* Organizational risk drivers
  + Growth strategy
  + Risk Philosophy
  + Regulatory Pressure
* Cyber Risk in perspective – Cyber risk has the maximum risk and is at the top of other enterprise risk
* Expression of Cyber Risk at the board level – Most of the board are mainly expressing the security risk as a story with no proper numbers
* Security incidents and losses metrics / Compliance status ad findings are mainly reported to the board
* It is difficult to translate security metrics into business terms
* Threats are #1 for the financial services and #9 for communication and tech. Based on the type of organization, there can be different types of metrics in the boardroom
* 2017 report was open questions that they answered, and the responses have been used to derive the categories that they choose from in the 2018 report.
* Most of the board level are satisfied with the board level security metrices, which is contradicting to the fact that they are not confident in their security program.
* The risk metrics are not necessarily helping the board to increase their confidence and make them more enable to provide the necessary oversite of cyber risk for their organization.
* Most board are not sure what are the right questions to ask for.

11:00 – 11:45 Communicating Cyber Risk to the Board: Privileged Access and Data Science

Problem- Show control over privilege access in 18 months

Rank business applications-

Focus on Crown Jewel application stack

Define control set for Crown Jewels

Establish ground truth

Inc visibility on privilege allocation

Clean up privilege

Track progress

Expand to next set of critical applications

**Fundamental layers of achieving effective CCM**

Data Collection

Data unification

Asset inventories

Control Coverage

Measurement

Controls catalogue & frameworks

Continuous Control Monitoring

After ranking, its important to **build up inventory**

Discovery tool

Network

Endpoint agent

Configuration management/ patching

Authentication services

Building the graph-

Asset inventory

Local Admin

Identity and Access Management

HR

Authentication Services

Simple graph measure-

Number of devices with no graph

No. of accounts with Direct Privileged Access

Include classification of account type

No. of accounts with inherited access

Via group membership

No. of humans with access

No. of paths to privileged access