Cybersecurity Framework Workshop 2017
National Institute of Standards and Technology, Gaithersburg MD

May 16-17, 2017

The Communications Sector – Cybersecurity Through the Risk Management Measurement Prism

Panelists

Moderator: Robert Mayer, USTelecom Vice President Industry and State Affairs
Chris Boyer, AT&T, AVP Global Cybersecurity Policy
Kathryn Condello, CenturyLink, Director of NS/EP
John Marinho, CTIA, Vice President Technology & Cybersecurity
Matt Tooley, NCTA, Vice President, Broadband Technology
Jesse Ward, NTCA Director, Industry & Policy Analysis

COMMUNICATIONS SECTOR COORDINATING COUNCIL

NIST National Institute of Standards and Technology U.S. Department of Commerce

AGENDA

- CSRIC IV WG4 Sector Adaptation of NIST Framework
- The Challenges of Measuring Cybersecurity PLUS Risk Management
- Panel Discussion
- Questions and Answers

COMMUNICATIONS SECTOR COORDINATING COUNCIL

CSCC WG4 Measurement Working Group

C. WHY IS MEASURING SECURITY DIFFICULT?

Based on practitioner experience in establishing and operating security measurement programs there are several reasons why measuring cybersecurity may be a challenge:

- Cybersecurity is not an exact science and does not provide for exact measurement such as water, temperature, or network throughput. In many cases, it is difficult to determine the success or failure of a given practice, or even if recommended practices are having an impact.
- Inputs, outputs, and outcomes of cybersecurity are separated in time, making authoritative measurement challenging. In other words, protective controls such as security training, access control, or firewalls are believed to work; however, it is very difficult to pinpoint cause and effect. This makes outcomes difficult to articulate and quantify.
- Correlation does not imply causation. For example, the increase in a number of attacks or incidents may simply mean that the intrusion detection and prevention systems have been updated and tuned and are registering a greater number of events which might have gone unnoticed before.

- Different organizations have different risk environments, goals for cybersecurity, and tools that they use to capture measures, and therefore comparing organizations is challenging and may not be meaningful.

CSCC Measurement Working Group

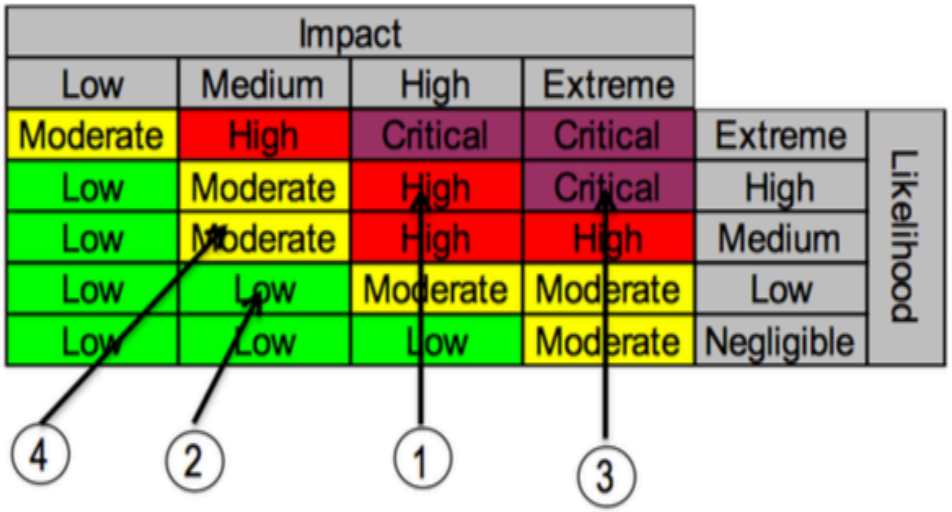
Risk Management

The Challenges of Measuring Cybersecurity PLUS Risk Management

COMMUNICATIONS SECTOR COORDINATING COUNCIL

Qualitative vs Quantitative

Real World Example



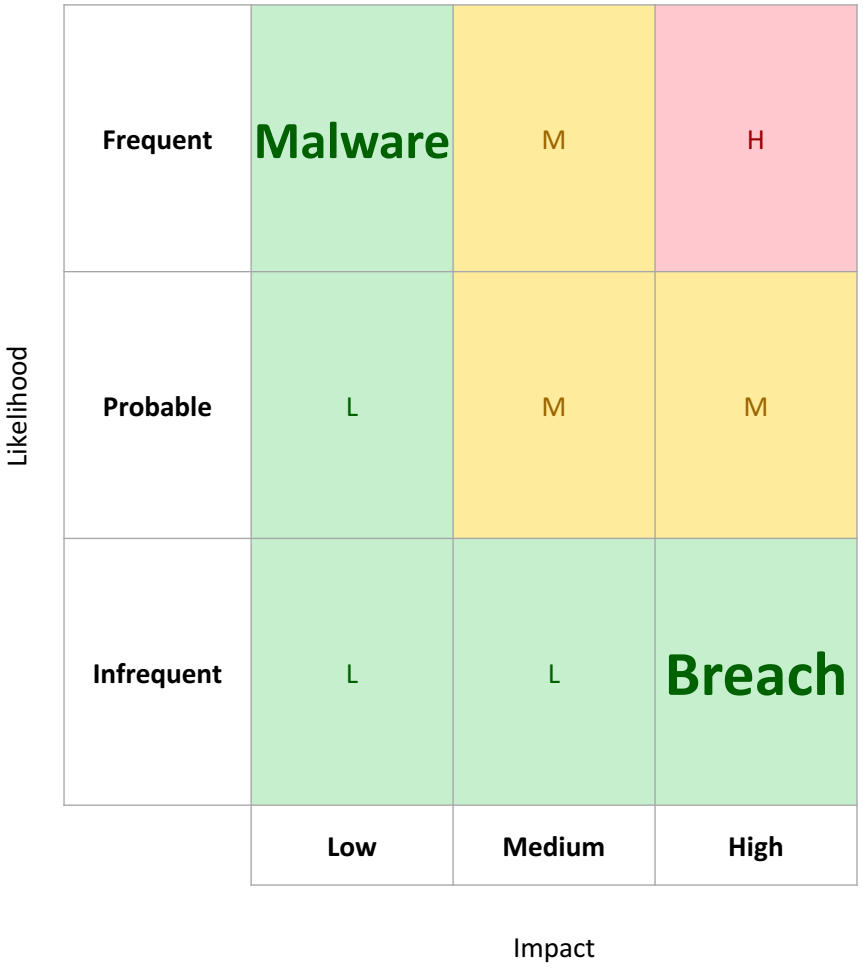
Most standards and certification tests promote risk analysis as a type of ordinal scoring method

The "**Risk Rating Methodology**" on **OWASP.org** states:

- "Once the tester has identified a potential risk and wants to figure out how serious it is, the first step is to estimate the "**likelihood**". At the highest level, this is a rough measure of how likely this particular vulnerability is to be uncovered and exploited by an attacker. It is not necessary to be over-precise in this estimate. *Generally, identifying whether the likelihood is low, medium, or high is sufficient* ."

COMMUNICATIONS SECTOR COORDINATING COUNCIL

Risk Matrix Example



- Commodity malware infections
  - Happen every day
  - Relatively inexpensive to remediate
- Data breach
  - Happens infrequently
  - Much higher impact if it does

Which one is more important?

Do Numbers Make It Better?

Frequent 67-100%	L	M	H
Probable 34-66%	L	M	M
Unlikely 0-33%	L	L	L
	Low	**Medium**	**High**
	0-$100k	100k-$1m	> $1m

Examples with Numbers

Frequent 67-100%	**Malware**	M	H
Probable 34-66%	L	M	Small Breach
Unlikely 0-33%	L	L	Large Breach
	Low	**Medium**	**High**
	0-$100k	100k-$1m	> $1m

Risk = Impact * Likelihood

According to the matrix, commodity malware and a data breech are the same level of risk.

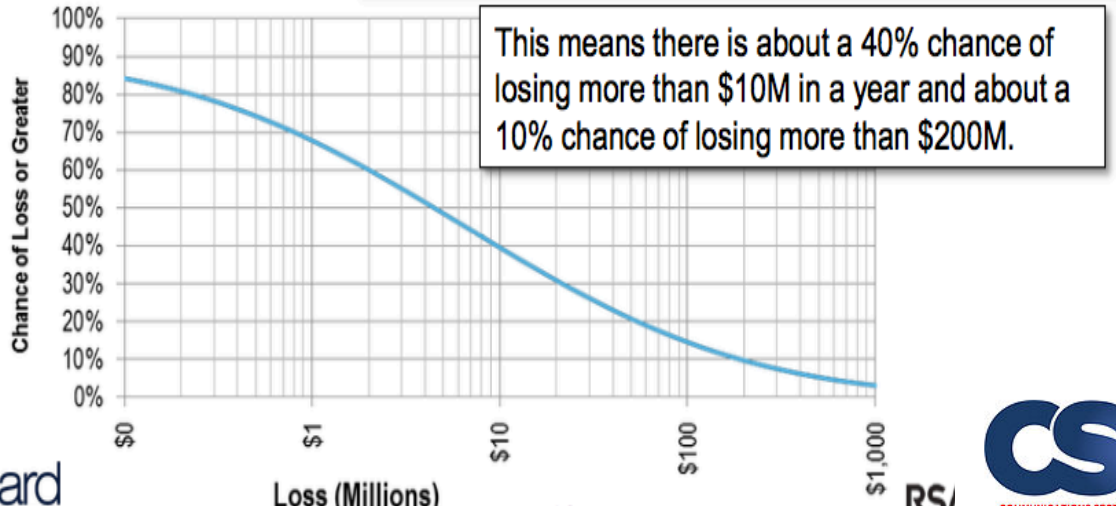
Quantitative

What If We Could *Actually Measure Risk* in Cybersecurity?

What if we could measure risk more like an actuary – "The probability of losing more than $10 million due to security incidents in 2016 is 16%"

What if we could prioritize security investments based on a "Return on Mitigation"?

	Expected Loss/Yr	Cost of Control	Control Effectiveness	Return on Control	Action
DB Access	$24.7M	$800K	95%	2,832%	Mitigate
Physical Access	$2.5M	$300K	99%	727%	Mitigate
Data in Transit	$2.3M	$600K	95%	267%	Mitigate
Network Access Control	$2.3M	$400K	30%	74%	Mitigate
File Access	$969K	$600K	90%	45%	Monitor
Web Vulnerabilities	$409K	$800K	95%	-51%	Track
System Configuration	$113K	$500K	100%	-77%	Track



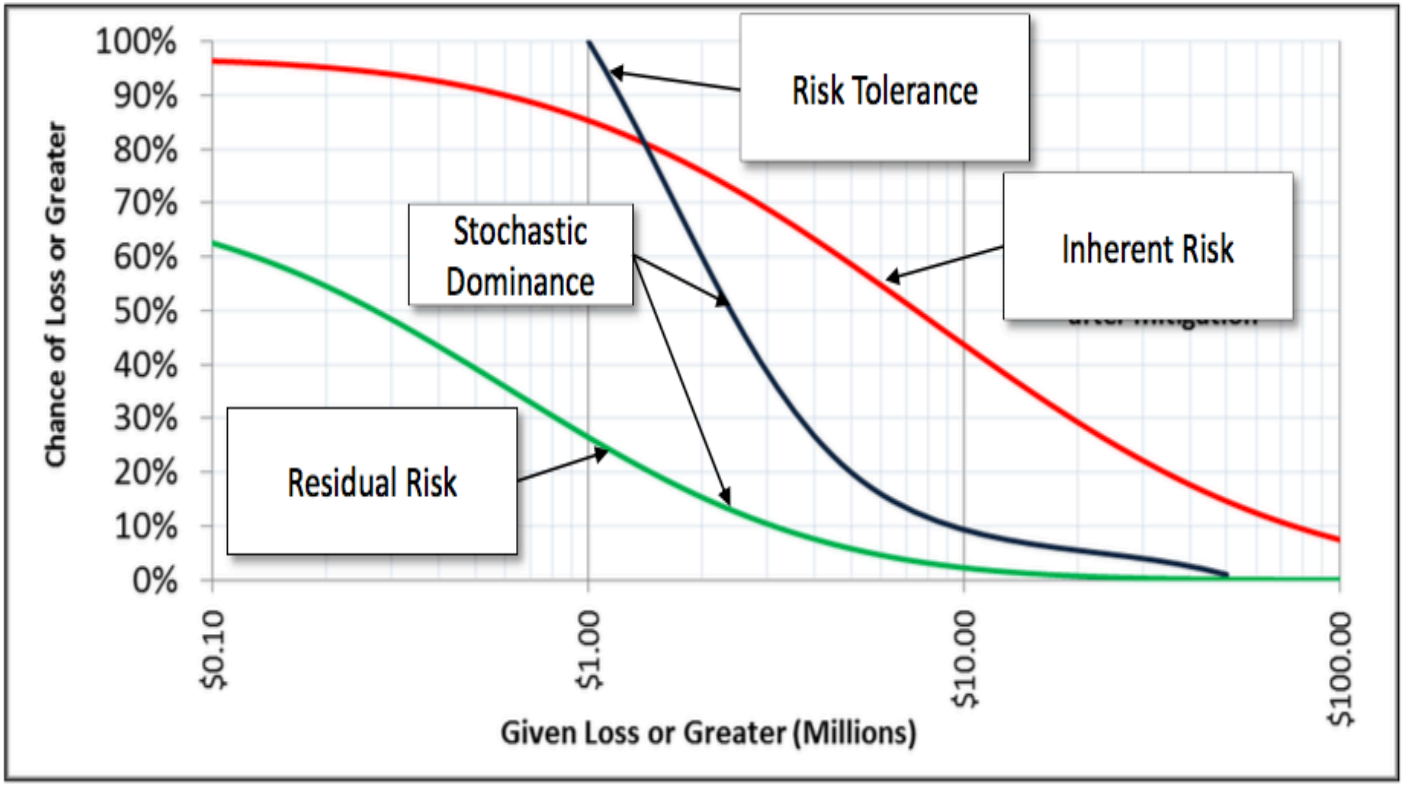
This means there is about a 40% chance of losing more than $10M in a year and about a 10% chance of losing more than $200M.

Hubbard Decision Research

CSCC COMMUNICATIONS SECTOR COORDINATING COUNCIL

Loss Exceedance Curves: Before and After

How do we show the risk exposure after applying available mitigations?



Call To Action For Cybersecurity!

- Organizations should stop using risk scores and risk matrixes and standards organizations should stop promoting them
- Adopt simple probabilistic methods now: They demonstrate a measurable improvement over unaided intuition and they have already been used. So there is no reason not to adopt them.
- Build on simple methods when you are ready – always based on what shows a measurable improvement.

Hubbard Decision Research

RSAC

CSCC COMMUNICATIONS SECTOR COORDINATING COUNCIL

The Risk Management Paradox….

- **So what does the risk management paradox tell us?**
  - Being a risk manager is a thankless job and may also lead to being a scapegoat when things go wrong
  - You cannot prove a negative and in risk management there is only a chance that something is going to happen so when it doesn't – is that a result of good risk management?
  - **It is very difficult to measure the effectiveness of the risk management program because if nothing is going wrong, management will put it down to their superb management initiatives and not to sound risk management**
  - If you are a risk manager and you are expecting a ticker tape parade you are going to be sadly disappointed

The Premise .....

- **For us to be able to measure the value of risk management to our organization:**
  - We need to understand our objectives
  - We need to be able to measure performance against our objectives

RIMS the risk management society

CSCC COMMUNICATIONS SECTOR COORDINATING COUNCIL

Measurement – the Methodology

- **The measurement of risk management performance can be divided into three distinct categories:**
  - ***Compliance***. This measures whether the organization is complying with its own risk management policy directives
  - ***Maturity***. This measures the maturity of the risk management program within the organization against industry best practice
  - ***Value Add***. This measures the extent to which risk management is contributing to the achievement of the organization's objectives and outcomes

So the Challenge

- We must have sound, measurable objectives
- We must have a sound performance measurement framework
- We must continue to measure performance
- We need a way to measure the maturity of our risk management program that is repeatable
- We need to measure performance against our performance measures each time we measure maturity

- If we do not have these things in place, we will NEVER be able to confidently answer our boss' question

Conclusions

Measuring cybersecurity is a complex topic as we learned in FCC CSRIC WG#4 and doesn't lend itself to a prescriptive or one-size fits all approach. The NIST cybersecurity framework is inherently flexible. One of the primary reasons for the success of the framework is that it avoids being a checklist and is more of a risk management program that can be implemented in a variety of ways to meet differing business needs. NIST should maintain that structure as it considers metrics.

Any metrics that NIST proposes should be process oriented, to help companies determine if their risk management processes are adequate given the risks. There is a wide variety of research into how to evaluate the effectiveness of processes. NIST can use the framework process to help companies best determine if their risk management process is sufficient to mitigate their risk.

In order to help companies measure their risk management programs NIST could propose examples of how companies measure these programs today but shouldn't try to standardize or identify best practices. Similar to the point above, companies are best positioned to understand their cyber risk and internal risk management programs and NIST can help them evaluate the effectiveness of those programs by sharing how others in industry measure the effectiveness of their risk management programs today but should avoid a one-sized fits all approach to measurement.

CSCC
COMMUNICATIONS SECTOR COORDINATING COUNCIL

Conclusions

NIST's proposals like mean time to detection and other measures have been looked at in the past and could potentially be futile It is difficult to calculate those types of measures because in many cases companies, for example, don't even know if they have a cyber issue until they find out. In that context the actual method of calculating the metric may be confusing and not relevant to addressing the attack.

Any metrics that companies use have to be outcome based and related to an actual issue that is within the scope and control of the entity that is being measured. This was a key finding in Working Group #4. Metrics need to be actionable for that particular business. For example, communications companies routinely measure things like service outages and from a service outage the mean time to restore service and other related measures. In that case the communications service provider is responsible for and has control over when their service is restored. Thus the companies are measuring an outcome that is within their span of control. Example of this in evaluating a risk management process may be metrics like # of employees trained on risks etc.

COMMUNICATIONS SECTOR COORDINATING COUNCIL