Real Cybersecurity and Managing and Reporting Metrics

William Favre Slater, III

Chicago, Illinois

United States of America

March 31, 2022

Table of Contents

Executive Summary

This brief article explains some basic concepts to improve the cybersecurity services that are provided in your organization, and some examples of how to measure, manage, and report the metrics that describe those services.

Introduction

Obviously, cybersecurity is one of the most important topics in business today. With all the headlines about cyberattacks, ransomware attacks, cyberwarfare, and data breaches, everyone who uses a computer that is connected to the Internet is thinking about how they be more secure. In addition, the people who are cybersecurity leaders are constantly challenged to demonstrate to management that the security services they are managing and delivering offer real quality and value for the budget expenditures required to deliver these services.

This article will provide useful information about how to deliver better cybersecurity services. It will also provide expert insights from notable security practitioners / authors about measuring and managing cybersecurity services and how to report these metrics to upper management so they will understand what they are getting for the money they have allocated for cybersecurity, and how these expenditures are increasing the required levels of security in the organization.

Real Cybersecurity

Nearly all of us in the cybersecurity career field as well as those who are being trained to enter field as a career direction, have been trained to understand the important facets of cybersecurity, namely Confidentiality, Integrity, and Availability, frequently described as “CIA”. We have been taught that any cybersecurity solution is not complete unless it has the design and controls that protect the organization in there three areas.

Have you ever considered that there might be more to these three requirements for cybersecurity. Well, in fact there are at least three additional facets that should be considered to offer the best possible cybersecurity. Those are Utility, Authenticity, and Control. Coupled with the CIA, these additional three facets form the Parkerian Hexad. This is named after one of the founders of the cybersecurity profession, Mr. Donn B. Parker. Mr. Parker was hacking computers and software since the 1960s. He was also a prolific lecturer and his videos are still available on YouTube.

The facet of Utility has to do with the idea that your data and systems are Usable. You cannot get work done with data that is not usable.

The facet of Authenticity has to do with the idea that the data or information you have is genuine. In the day and age of Deep Fakes, this would be a valuable thing to know. For example, as recently as March 2022, Deep Fake Videos of Ukraine's President Zelenskyy have appeared on the web, making statements that he never said.

The facet of Control has to do with the fact that the data or information you need is actually under your control. In the day and age of malware and trojan software, it is important to have the peace of mind that you have control over the data and information and systems for which you are responsible.

So adding these three additional facets can help you and your cybersecurity Team build solutions that are far superior to those who are only doing the CIA part of the Parkerian Hexad.

W. Krag Brotby – Information Security Management Metrics

Brotby's Information Security Management Metrics classifies metrics according to the following scheme:

- Program Development Metrics
  - Policy Management Metrics
  - Process Maturity Metrics
- Support Metrics
  - Personnel Support Metrics
  - Resources Support Metrics
- Operational Metrics
  - Operational Readiness Metrics
    - Management Readiness Metrics
    - Technical Readiness Metrics
  - Operational Practices Metrics
  - Operational Environment Metrics
- Effectiveness Metrics
  - Metrics for Technical Target of Assessment
    - Metrics for Strength Assessment
      - Metrics for Features in Normal Circumstances
      - Metrics for Features in Abnormal Circumstances
    - Metrics for Weakness Assessment
      - Risk Metrics
      - Operational Limitation Metrics

From Information Security Management Metrics, W. Krag Brotby, 2007.

Brotby is the only security author / practitioner in this article to introduce the concept of a Capability Maturity Model for measuring and managing the effectiveness of information security metrics. The maturity levels in this model are defined as

1. Initial
2. Repeatable
3. Defined
4. Managed
5. Optimizing

Lance Hayden, PhD – IT Security Metrics

Dr. Hayden advocates the creation of a Security Process Management (SPM) Framework to be used to monito all aspects of IT Security Management. The table shown below is an example of IT organizational goals mapped to example metrics that can be captured to measure the performance of a Security Operations Team:

Goal	Metric
Budget & Personnel	
Understand the prioritization of and investment in security as a function of IT operations.	Percent of IT budget devoted to IT security
Understand the connection between IT security activities and the business.	Percent of IT security budget covered through internal charge back, by unit
Understand the prioritization of and investment in security as a function of IT operations.	Ratio of full-time IT staff resources devoted to IT security
Understand one general level of security personnel expertise.	Ratio of certified to noncertified IT security staff members
Processes & Projects	
Understand the level of visibility into routine security operational activities.	Ratio of security business processes that are documented
Understand the utilization of existing IT security staff.	Number of security measurement or improvement projects undertaken during time period
Understand the prioritization of and investment in security as a function of IT operations.	Ratio of security measurement or improvement projects to overall IT measurement or improvement projects
Understand project size and duration for IT security projects.	Average resource utilization (in staff hours) for security measurement or improvement projects undertaken during time period
Systems & Vulnerabilities	
Understand deviation from established baselines.	Percent of systems compliant with current configuration standards
Understand gaps in existing security posture.	Number or ratio of systems containing vulnerabilities as a result of assessment
Understand threat levels for vulnerable systems.	Average count and severity of vulnerabilities per assessed system or defined set of systems
Understand threat levels for vulnerable systems.	Number of probes, attempted attacks, and penetrations during time period
Understand vulnerabilities posed by wireless connectivity.	Ratio of secured to unsecured wireless access points present on network

Change & Remediation	
Understand systemic changes to security baseline over time.	Number of configuration change or exception requests per time period
Understand security reaction posture and impact on IT security staff.	Number of security incidents (escalated or investigated) per time period
Understand what kind of security vulnerabilities are most prevalent in the environment.	Ratio of vulnerability types identified (access, denial-of-service, data loss or corruption, fraud, and so on)
Understand lag time between vulnerability discovery and mitigation.	Average time required to remediate identified security vulnerabilities

From IT Security Metrics, Lance Hayden, 2010.

Dr. Hayden's book is filled with many more great examples of best practices for managing IT Security Metrics. It is very accessible and useful for IT security staff and managers at all levels of experience.

Andrew Jaquith – Security Metrics

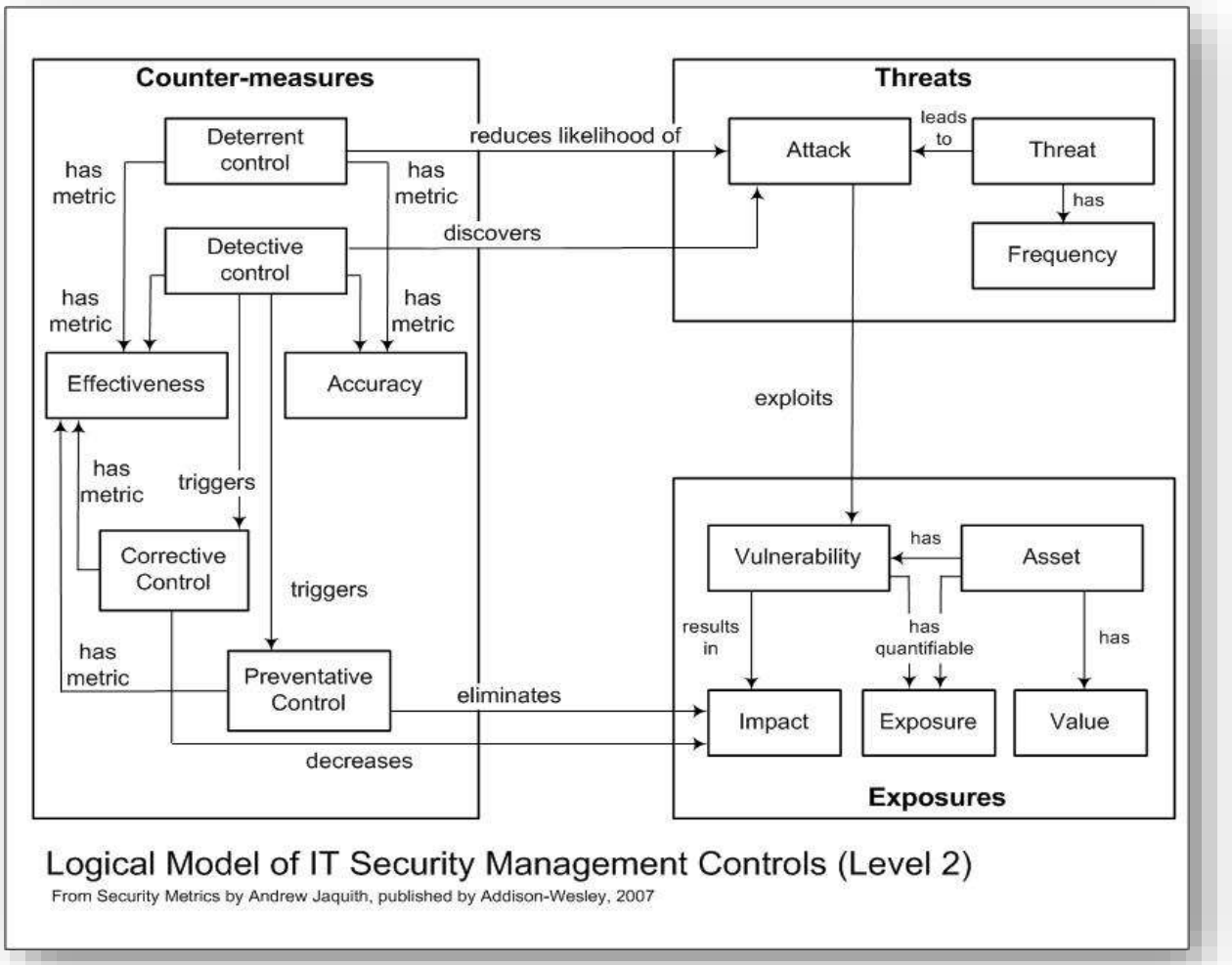
Andrew Jaquith is one of the best known Security Metrics people in the Information Technology world. This statement from his book is a good summary of the purpose of Security Metrics:

> ***"Security metrics are the servants of risk management, and risk management is about making decisions. Therefore, the only security metrics we are interested in are those that support decision making about risk for the purpose of managing that risk."***

Jaquith is also known for his ability to perform deep statistical analysis on monitoring and other essential IT security metrics. He believe there are even more valuable insights to me gained by measuring the measurements of the processes themselves. Jaquith cites the COBIT IT Management Framework to shed light on the importance of the Monitoring control domain: It is the governance activities an organization performs to understand how well its processes operate:

> ***"All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain addresses performance management, monitoring of internal control, regulatory compliance, and providing governance." (COBIT)***

Jaquith is also well known for his information diagram that elucidates the relationship between IT Threats, Security Management Controls, and Assets (Exposures). That elegant diagram is shown below.



Logical Model of IT Security Management Controls (Level 2)

From Security Metrics by Andrew Jaquith, published by Addison-Wesley, 2007

NIST SP 800-55rev1 – Performance Measurement Guide for Information Security

The NIST SP 800-55rev1 document contains invaluable tips for building a framework to measure and management a information security management program. It's not only authoritative and well-written by cybersecurity experts, and also freely available from the web. See the References section for the link. The diagram below shows NIST's concept about building a Information Security Measurement Program.

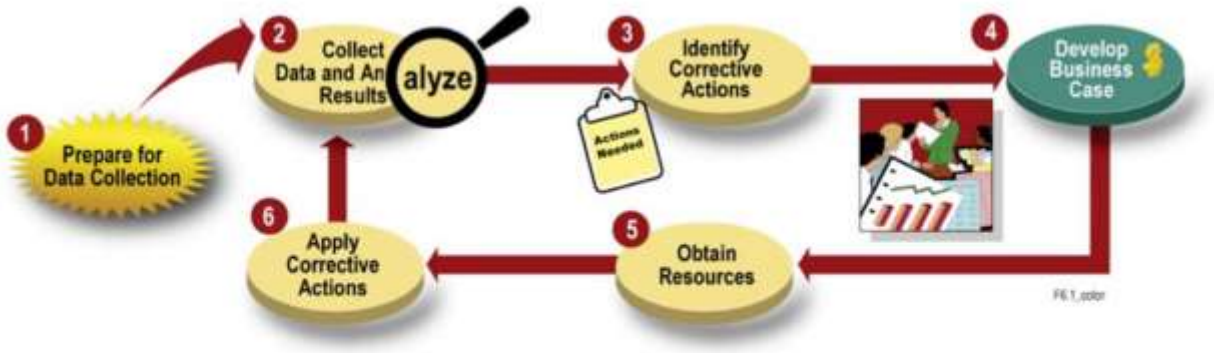


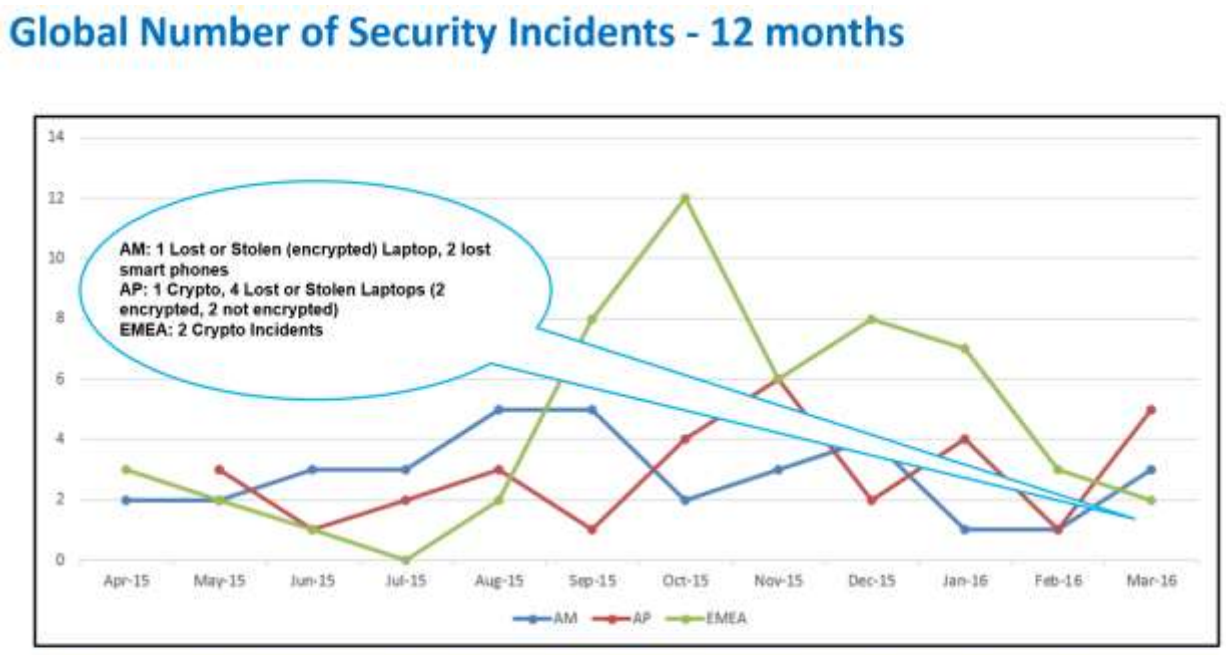
Figure 6-1. Information Security Measurement Program Implementation Process

William Slater – Personal Experience and Observations

This section covers some of my own experiences with metrics.

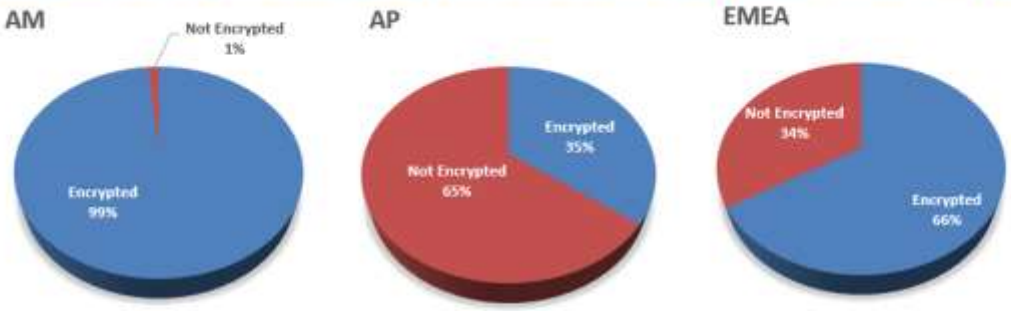
Examples of IT Security Related Metrics

From 2015 – 2016, I managed the Global Security Team for a large company in Chicago. It was a job I inherited, so I did not have to opportunity to design the monthly metrics reports I was producing. Still, many may find the example slides from the monthly report slide deck interesting. The collection, formatting, and analysis of this data required many hours of my time each month, but it was what our Global Executives expected to see each month.



Region	Apr-15	May-15	Jun-15	Jul-15	Aug-15	Sep-15	Oct-15	Nov-15	Dec-15	Jan-16	Feb-16	Mar-16
AM	2	2	3	3	5	5	2	3	4	1	1	3
AP		3	1	2	3	1	4	6	2	4	1	5
EMEA	3	2	1	0	2	8	12	6	8	7	3	2
Global Totals	5	7	5	5	10	14	18	15	14	12	5	10

Regional Number of Windows Systems with Encryption - AM, AP, and EMEA



AM

State (System)	Number of Managed Systems	Percentage
Encrypted	11903	99%
Not encrypted	168	1%
Total encryptable devices	12071	
Filtered	2745	
Total devices	14816	

AP

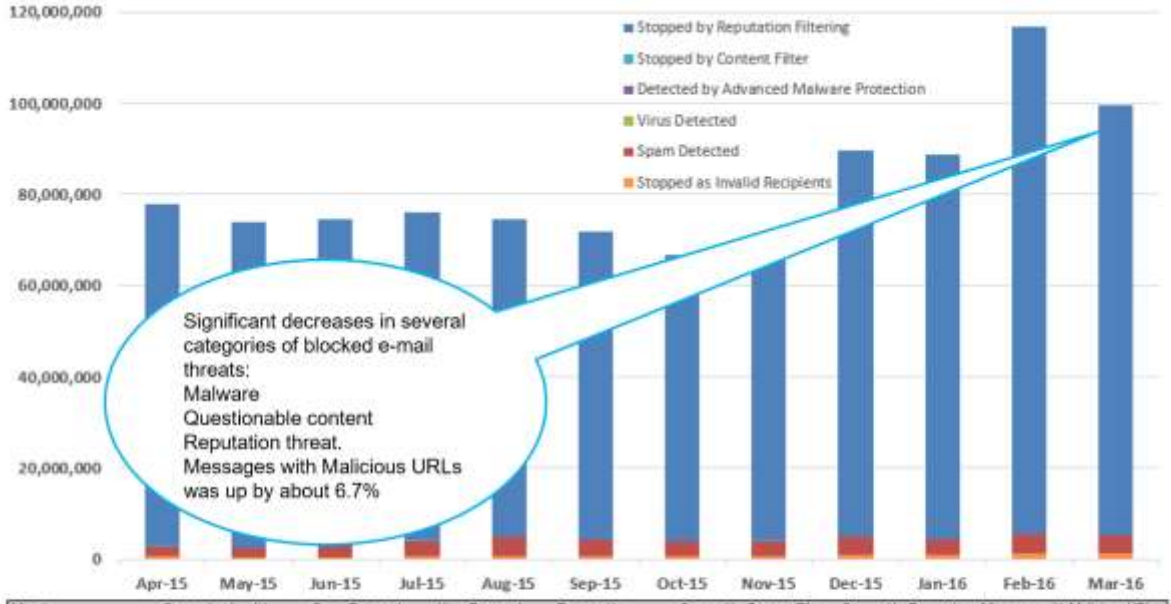
State (System)	Number of Managed Systems	Percentage
Encrypted	3141	35%
Not encrypted	5769	65%
Total encryptable devices	8910	
Filtered	549	
Total devices	9459	

Changes from February 2016:
AM up 2%
AP up 1%
EMEA up 3%

EMEA

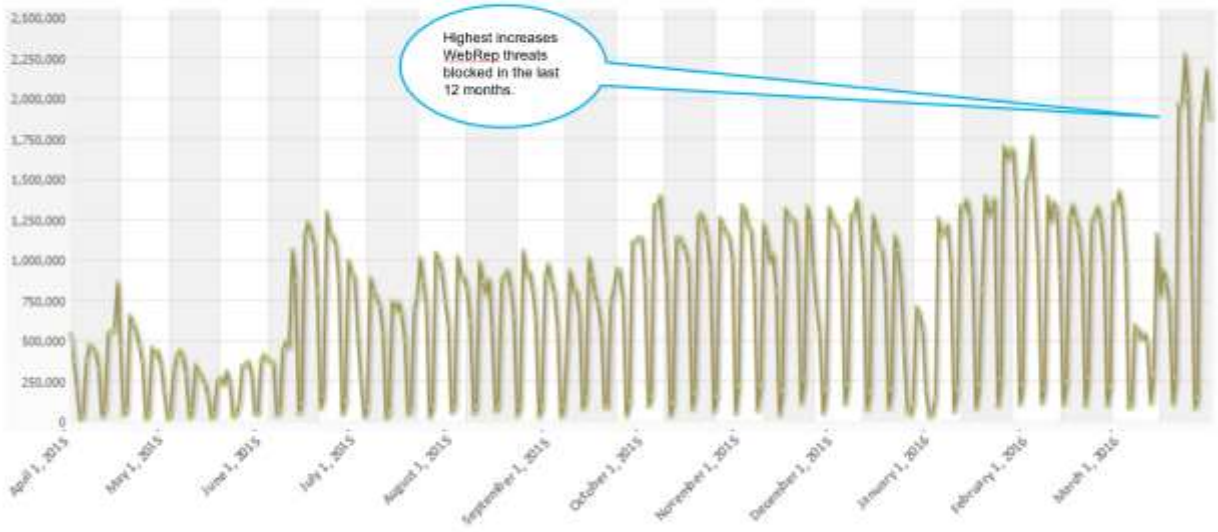
State (System)	Number of Managed Systems	Percentage
Encrypted	7102	66%
Not encrypted	3629	34%
Total encryptable devices	10731	
Filtered	815	
Total devices	11546	

Regional email attacks blocked - IronPort - 12 months - AM



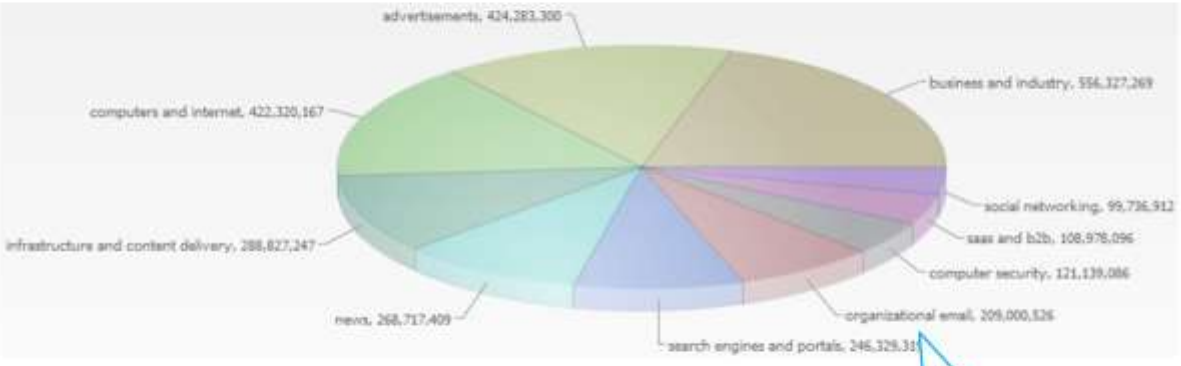
Month	Stopped as Invalid Recipients	Spam Detected	Virus Detected	Detected by Advanced Malware Protection	Stopped by Content Filter	Stopped by Reputation Filtering	Messages with Malicious URLs (subset of Stopped by Reputation Filtering)
Apr-15	677,492	2,250,823	0	0	49,085	74,724,424	0
May-15	480,574	1,980,097	0	0	46,371	71,424,424	0
Jun-15	514,149	2,626,967	14	104	70,528	71,423,565	3,608
Jul-15	579,285	3,489,623	542	174	92,157	71,870,354	61,763
Aug-15	618,783	4,199,385	1,325	176	38,968	69,717,957	80,589
Sep-15	699,421	3,621,199	2,704	135	81,974	67,302,108	99,196
Oct-15	775,463	3,163,183	4,064	734	178,433	62,468,490	109,418
Nov-15	830,249	3,279,791	2,507	330	233,668	64,862,067	148,071
Dec-15	1,067,395	3,851,712	52,285	94	28,790	84,444,771	135,061
Jan-16	998,286	3,244,214	3,793	1,959	21,233	84,561,862	159,950
Feb-16	1,135,721	4,408,397	3,932	5,792	95,364	111,166,162	113,212
Mar-16	1,139,361	4,044,111	2,729	307	44,158	94,352,976	120,899

Global Internet Browsing Attacks Blocked by Cisco CWS – 12 months



WebRep Threats Blocked

Global Internet Browsing Attacks Blocked by Cisco CWS – 12 months



Blocked Malware includes these categories:
PUA, Spyware, Adware, and Viruses

12 months of data shown. Notable here is that most of the categories are not nefarious in nature, meaning that CWS is blocking a lot of website threats where we would not normally expect threats to lurk. This data only reflects users that are connected directly to the JLL infrastructure.

Global Attacks / Nefarious Activity Identified by QRadar – March 2016

SIEM Malware can include events where a virus is detected or other malware is detected. It could also be related to the Crypto events highlighted earlier.

SIEM Suspicious can include the detection of User Activity Suspicious Patterns IP Spoofs Suspicious ICMP Protocol usage or Unknown Suspicious Event.

Tickets Created by Category:	Total	AM	AP	EMEA
SIEM Authentication	5	2		3
SIEM DDoS	2		1	1
SIEM Malware	11	8	2	1
SIEM Recon	3	3		
SIEM Suspicious	10	9		1
SIEM System	1	1		
SIEM Threats	1		1	
SIEM Worm	3	3		
Grand Total	**36**	**26**	**4**	**6**

The number of tickets in March 2016 were reduced from the February 2016 count of 45 due to the improvements in tuning efforts.

The Dark Side of IT Metrics: 80% vs 93%

If you wondered if there is a "dark side" to security metrics, there certainly can be. Many years ago, when I was managing a Data Center and also doing system administration for a very large energy company, our Service Level Agreement contract specified that our Team members would meet there pair and restoration metrics at least 80% of the time. Example, production servers that were classified as "Gold" had to be restored to service within four hours. If that window was exceeded, it was called a busted SLA, and the customer was constantly keeping score. We were a Team with almost 300 members, all of whom were talented and highly motivated, so we met our SLA performance obligations 93% of the time. One day, our Management Team had a mandatory meeting and told us we were doing a great job, and in fact, too good of a job. They said feedback from the customer was that if we could achieve 93% performance, in the customer's opinion that meant we have too many people on the Team, so maybe it was time for headcount reduction. Consequently, our Management Team advised the Team Members to slow down, not work so hard, and bring the successful SLA metrics down to around 80%.

5700 Remedy Tickets in 12 Months

Another metric that is frequently used in the world of IT metrics is the Cost-Per-Ticket. A great example of this is the Messaging Team that I led at a large U.S. Government Agency from November 2006 – March 2008. There were 24 messaging engineers on the Team, and we had an annual contract budget for technical messaging services that was valued at $4.3 million. When you divide that $4.3 million by 5700 Remedy Tickets, it comes out to about $754.39 per ticket. It turns out that this is not only an important number, but it can be used by a Services Company and the Government to discuss the quality of service as well as the compensation for the average engineer on the contract. In fact, Management may come back and say, “We expect to pay no more than $690 / per ticket.”. Again, this can and well lead to some serious conversations, so be aware and be ready to have such discussions if you aspire to leadership positions.

Randy Steinberg – Measuring ITIL

In 2006, Mr. Randy Steinberg published a book that provided valuable insights and a framework for measuring the management functions related to the Information Technology Infrastructure Library (ITIL). The book also includes a CD containing an Excel file that provides workbooks for each ITIL management area, and these workbooks roll up data into a dashboard that can be used to quickly identify the performance of an Information Technology Department where ITIL has been implemented. Metrics for Incident Management are show below, including Operational Metrics, Tolerance Levels, KPIs, and Critical Success Factors. In 2009 I was on a project at Peterson Air Force Base several years ago, implementing what became known as the world's largest ITIL implementation, and the workbooks in this Excel spreadsheet became the basis for measuring ITIL, and providing progress reports to our management and project stakeholders. It was and still is an extremely valuable tool. I highly recommend it. The Incident Management Metrics shown below are from Mr. Steinberg's Excel file.

Incident Management Metrics:

Operational Metrics

Total Number Of Incidents
Average Time To Resolve Severity 1 and Severity 2 Incidents (Hours)
Number Of Incidents Resolved Within Agreed Service Levels
Number Of High Severity/Major Incidents
Number Of Incidents With Customer Impact
Number Of Incidents Reopened
Total Available Labor Hours To Work On Incidents (Non-Service Desk)
Total Labor Hours Spent Resolving Incidents (Non-Service Desk)
Incident Management Tooling Support Level
Incident Management Process Maturity

Tolerance Levels

Number Of Incident Occurrences
Number Of High Severity/Major Incidents
Incident Resolution Rate
Customer Incident Impact Rate
Incident Reopen Rate
Average Time To Resolve Severity 1 and Severity 2 Incidents (Hours)
Incident Labor Utilization Rate
Incident Management Tooling Support Level
Incident Management Process Maturity

Key Performance Indicators (KPIs)

Number Of Incident Occurrences
Number Of High Severity/Major Incidents
Incident Resolution Rate
Customer Incident Impact Rate
Incident Reopen Rate
Average Time To Resolve Severity 1 and Severity 2 Incidents (Hours)
Incident Labor Utilization Rate
Incident Management Tooling Support Level
Incident Management Process Maturity

Critical Success Factors

Quickly Resolve Incidents
Maintain IT Service Quality
Improve IT And Business Productivity
Maintain User Satisfaction

Conclusion

This article has provided some guidelines to provide better cybersecurity services for your organization, and discussed to importance of measuring and reporting on IT services, especially those related to cybersecurity. Your Management Team and the related stakeholders want to be able to measure the value and quality of the technical services you and your Team will be delivering. To optimize your Team's performance consider multiple sets of metrics reporting techniques discussed in this article, and get on top of this important aspect of cybersecurity leadership.

Finally, to paraphrase Sigurjon Arnason and Keith Willett, having a well-managed, structured information security program that you are routinely monitoring, measuring, and reporting on is no guarantee that you will not get breached or come under cyberattack, however, it will assist in litigation management to show a judge and a potential jury that your organization takes risk management seriously.

References

Arnason, S. T. and Willett, K. D. (2008). How to Achieve 27001 Certification. Boca Raton, FL: Auerbach Publication.

Brotby, W. K. (2009). Information Security Management Metrics. Boca Raton, Florida: CRC Press.

Ebrary.net. (2022). Parkerian Hexad. Retrieved from the web at https://ebrary.net/26648/computer_science/parkerian_hexad.

Hayden, L. (2010). IT Security Metrics. New York, NT: McGraw-Hill.

ISACA. (2022). COBIT. Retrieved from the web at https://www.isaca.org/resources/cobit.

Jaquith, A. (2007). Security Metrics. Upper Saddle River, NJ: Pearson Education.

NIST. (2008). NIST SP 800-55 Rev. 1 – Performance Measurement Guide for Information Security Retrieved from the web at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf.

Parker, D. B. (1998). Fighting Computer Crime: A New Framework for Protecting Information. Indianapolis, IN: Wiley.

Slater, W. F. (2016). Professional career artifacts.

Steinberg R, (2013). Measuring ITIL – Illustrated. Bloomington, IN: Trafford Publishing.

Bio

William Favre Slater, III

M.S., MBA, PMP, CISSP, CISA, SSCP, CDCP, ISO 20000, ITIL, IPv6

William Slater, President & CEO of Slater Technologies, Inc. He is based in Chicago, IL. He is a seasoned IT professional with more than four decades of experience. Since 2001, his primary focus areas have been Data Centers, Cybersecurity, Networking, Application Development, Service Management, Project Management, Program Management, Executive Leadership (CISO, CIO, and CTO) and Blockchain (since 2012). Mr. Slater is a patriotic American and a former U.S. Air Force Officer. In fact, he was one of the very first Cyberwarriors in the U.S. Air Force. He has been an Adjunct Professor for over 18 years, and holds three graduate degrees, including an M.S. in Cybersecurity, and 80 professional certifications, including CISA, CISSP, SSCP, and PMP. His professional experience includes: the U.S. Air Force, Northrop, Digital Equipment Corporation, BP, Department of Veterans Affairs, Microsoft, IBM, and McDonald's. He is a member of $(ISC)^2$, PMI. ISACA, and the Internet Society. He is a strong supporter of Internet Freedom and the fact that "The Internet Is for Everyone."

You can see much more about Mr. Slater's career and his work at https://billslater.com/interview, https://billslater.com/career and at https://billslater.com/writing.

Mr. Slater is very happily married to Ms. Joanna Roguska (a native of Warsaw, Poland) since December 2000. He is a devoted husband, a non-denominational Christian, a musician and songwriter, a published technical writer, a teacher, and a Black Belt and certified instructor in Kodokan Judo. He is also friends with and one of the biggest fans of Mr. Andreas Vollenweider (from Zurich, Switzerland) and his music since 1985. When he is not doing technical work in IT, or teaching, Mr. Slater and his wife enjoy traveling to other countries and places in the U.S. where they haven't been. Since 2000, they have traveled to the following places together:

States and Places in the United States	Countries and Places
Alaska	Antarctica
Arizona	Argentina
Arkansas	Australia
California	Bahamas
Cherokee, NC	Buenos Aries
Colorado	Canada
Florida	Cayman Islands
Georgia	Chile
Hawaii	Bogota, Colombia
Idaho	Costa Rica
Indiana	Cuba
Iowa	Czech Republic
Kentucky	Egypt
Louisiana	Falkland Islands
Massachusetts	France
Michigan	Iceland
Minnesota	Ireland (2)
Mississippi	Jamaica
Missouri	Japan
Montana	London, United Kingdom
Nebraska	Mexico (3)
Nevada	New Zealand
New Mexico	Panama
New York City	Poland
North Carolina	Portugal
North Dakota	Scotland
Oregon	Spain
South Carolina	Turkey
Tennessee	Uruguay
Texas	
Utah	
Virginia	
Washington State	
Washington, DC	
Wisconsin	
Wyoming	

Contact Information

William Favre Slater, III
MBA, M.S. in Cybersecurity, PMP, CISSP, SSCP, CISA, ISO 27002, ISO 20000, ITIL v3, IPv6
CISO, Sr. IT Security Consultant / Project Manager / Program Manager
slater@billslater.com
williamslater@gmail.com
wslater@protonmail.com
Career Page: http://billslater.com/interview
LinkedIn: https://www.linkedin.com/in/william-sequoyah-slater-556b6220b/
312 - 342 - 2626 - Mobile - 01
312 - 758 - 0307 - Mobile - 02
312 - 275 - 5757 - FAX
1515 W. Haddon Ave., Unit 309
Chicago, IL 60642
United States of America
41.9021954° N, 87.665722° W