Abstract

Addressing cybersecurity and information security is becoming increasingly important within the DoD and beyond. With software systems constantly talking amongst themselves and across various networks, concern is growing about the protection of our sensitive data and applications. But one must also consider how much security is too much and when the 'right' degree of cybersecurity has been achieved. This paper discusses cyber and information security and presents measurements and metrics suitable for accessing mitigation strategies.

Introduction

Cybersecurity and information security dominate the news these days. As software solutions become ubiquitous and highly interconnected via networking, the internet, cloud solutions, remote computing, etc., the chance for breaches is increasing at an alarming rate.

> "*Since 1988's Morris Worm, which infected 10% of the estimated 60,000 computers connected to the internet, cybersecurity has grown into an industry expected to exceed $1 trillion in global spending between 2017 and 2021.* "[1]

Cybercrime will cost the global business market an estimated average of $6 trillion annually through the same time frame [1].

Every entity at every level of industry and government is aware of the perils of ignoring cyber and information security threats. But organizations are asking themselves the following questions: How much security is enough? How will we know when we get there? How much will it cost? Where is the tipping point where our expenditures exceed the value added through cyber and information security initiatives? In order to answer these questions, organizations must assess their current state and begin to develop a security focused measurement system to track the progress, successes and failures of their cybersecurity investments and to effectively predict costs and benefits of future initiatives.

The savvy organization in 2019 understands that investment in cyber and information security is essential and measurement is a vitally important aspect to their cybersecurity related initiatives. Measurement will justify these investments, measure the impacts of initiatives, facilitate continuous improvement of cybersecurity security processes and practices, and create a framework to predict costs and benefits of future investments. Many of these same organizations struggle to figure out where to start down this road. According to the 2017 State of Cybersecurity Measurement Annual Report [2][1], more than half of the respondents (58%) scored a failing grade when self-evaluating their efforts to measure investments and performances against best practices. More disturbing, less than twenty percent (18%) gave themselves an A.

This paper begins with a brief discussion around cybersecurity and information security; what these concepts mean, how they are alike and different, and how they have evolved over time. Following this, the concept of measurement in the cyber and information security context will be discussed and a framework for evaluating potential metrics will be presented. Some potential cyber and information

[1] based on a survey of over 400 global business and security executives

security metrics will be defined, aligned with the International Standards Organization/International Electrotechnical Committee (ISO/IEC) 27K Standards along with some thoughts on the strengths and weaknesses of those metrics. The paper will conclude with some general thoughts on the future of measurement and cost estimation in the world of cybersecurity.

Cybersecurity and Information Security

History

As computers began to rise in popularity around the middle of the twentieth century, early models were not generally connected to other systems, making cybersecurity a non-issue. Information security efforts were focused on managing user IDs and passwords for mainframes and shared servers. It was a simpler time where users either had access to an application or they didn't; there were not a lot of varying roles assigned to users based on their need to know or need for access. Computers were a tool, not the lifeblood of the organization. Except for backups, not much thought was given to business continuity as it pertained to the computer systems in use. During the 1980's, as personal computers (PCs) began to flourish along with the demand to connect them to servers, the need for firewalls and antivirus software emerged and grew. During these times some forward thinking Information Technology (IT) folks[2] began to think about measurements around data and information security. With the concept of security being so immature, it was hard to determine what the right things to measure were. Often the answer was to go with easy and cheap. The 90's virus and hacking incidents started making the news; organizations started to understand that their data and information was as important to protect as their physical IT systems. From the 2000's on, as technology progresses, the internet is more and more ubiquitous, cloud computing is emerging as a standard in many industries, and information is flowing freely and furiously through the ether. Cybersecurity and information security are regular features in the nightmares of the C-level executives of many organizations, large and small.

Definitions

Cybersecurity and information security are often used interchangeably though they have different meanings:

- Information security is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. The information or data may take any form, e.g. electronic or physical. [3] Early information security efforts were mostly compliance based. The basic focus of information security is to ensure confidentiality, integrity and availability in an efficient manner without affecting productivity.
    - Confidentiality is maintained when information is not accessible, available or disclosed to people, entities or processes.

[2] Though the term information technology was not an oft use term, if at all

  - Integrity is maintained by ensuring that data remains accurate and complete throughout the lifecycle of the data.
  - Availability is maintained when data is accessible at the time and place where it is needed. This means all the systems required to make data available function properly.
- The word cybersecurity was first used in 1989 in reference to the Morris Worm and other early attacks. Cybersecurity refers to measures taken to protect a computer or computer system (as on the internet) against unauthorized access or attack [4]. Cybersecurity measures are focused on protecting cyberspace[3] from any criminal action intended to compromise information or other computer assets.

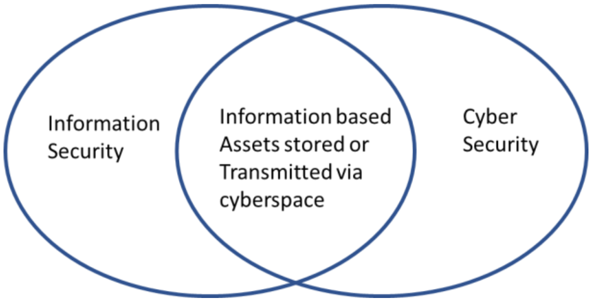
Information Security
Information based Assets stored or Transmitted via cyberspace
Cyber Security

Figure 1:Intersection of Cyber Security and Information Security

Figure 1 represents the intersection of these two concepts. This intersection is significant because most of the information we are securing is saved electronically and most cybersecurity breaches are intended to obtain confidential information, to compromise the integrity of information or prevent access to information. Many information security initiatives have definite implications for cybersecurity as well. From the perspective of measuring cyber and information security successes and process improvements, there is a significant overlap as well. Over time, the two notions appear to be merging together, generally referred to as cybersecurity and in many cases replacing compliance-based approaches with approaches based on risk mitigation and avoidance.

Measurement in the Cybersecurity Context

Measurement in an environment that is in constant flux is a complex problem to overcome. The discipline of cybersecurity certainly falls squarely into this category.

> "*Without sound metrics, we are in the position of a passerby who encounters a man swinging plucked chickens around his head while he stands on a street corner: asked why he is doing that he answers, 'To keep the flying elephants away.' 'But there are no flying elephants' responded the befuddled observers. He crows triumphantly 'See? It works!'" [5]*

The unfortunate truth is that there is no simple, easy answer to the question "What are the right things to measure to ensure that security initiatives are successful, efficient and cost effective?" There are many reasons for this but the most obvious one is that every organization has different requirements for security and within every organization there are a plethora of metrics consumers who, based on their roles within the organization, have different requirements for what is important to them. There may also be external

[3] Cyberspace defined – a virtual computer world, more specifically an electronic medium used to form a global computer network to facilitate online communications

customers for whom information security metrics are important. (credit card customers, tightly coupled business to business partners, patients of a health care practice, etc.)

Before discussing specifics of a measurement initiative, it is important to think about what we mean by measurement, metrics and metametrics.

- Measurements are objective, concrete parameter values for something (e.g. length, weight, area, etc.) usually in a specific unit of measure (inches, pounds, etc.)
- Metrics are more subjective than measurements and are often determined in relation to several points of reference. Measurements are facts about a process, data item, or thing; metrics offer useful information about that process or thing based on the value of those measurements (e.g. dollars per pound, Lines of code per hour, etc.). Metrics are focused on empowering decision makers, identifying and measuring process improvement initiatives, and increasing accountability.
- Metametrics represent information about metrics. In the same way that one would summarize a data set with information (e.g. mean, standard deviation, min, max, etc.), one would want to summarize a metric with information (e.g. cost to collect, believability, actionability, usefulness, etc.).

"What gets measured gets done, what gets measured and fed back gets done well, what gets rewarded gets repeated" (John E. Jones). When considering a cybersecurity measurement initiative, or any measurement initiative for that matter, there are several important things that need to be considered:

- Metrics need to be selected to answer important organizational concerns and be balanced across a spectrum of objectives that are:
  - Strategic – big picture metrics focused on ensuring that business goals can be achieved
  - Management focused – high level metrics for senior management focused on supporting decisions regarding governance, risk management and guiding strategy.
  - Operationally focused – low level metrics designed to facilitate smooth day to day operation of the information systems and their applications.
- Metrics need to provide information important to one or more stakeholders
- Metrics need to provide quantifiable and actionable information
- The process for gathering data for metrics cannot be expensive or labor intensive.
- Measurement data needed for metrics needs to be available, easily accessible and the measurement process needs to be repeatable
- Metrics need to be meaningful and useful to the consumer. A metric that is simple and easy to understand will be more useful and actionable than one that is complicated and hard to explain.

Selection of the right metrics is crucial to an organization's ability to monitor, improve, and predict the cost of cybersecurity initiatives. In [5], the authors propose a framework for an organization to use to make intelligent, informed, repeatable and defensible decisions as to what are the best metrics for their organization with their particular security requirements and business objectives.[4] This framework presents a set of metametrics against which proposed metrics can be graded. They also propose a set of

[4] This book is a great resource for an organization looking to learn more about measurement for cyber and information security

guidelines to guide the grading activity, although they are quick to point out that their guidelines may need to be tailored to align with the business and its risks, security requirements, and constraints.

The framework proposed is the PRAGMATIC method which considers the following nine metametrics proposed by the authors as a comprehensive way to evaluate and compare metrics for suitability:

- Predictive: A metric is considered predictive if it provides foresight rather than hindsight. A metric that can detect and prevent an incident before it occurs would score high on the predictive scale. A metric such as 'number of known risks currently untreated/unresolved' is likely be considered predictive.
- Relevant: A metric is considered relevant if it meets one or more of the organizations needs with respect to cybersecurity. A metric for which there is management consensus that it provides useful information to manage the business would score high on the relative scale. A metric such as 'percentage of security controls that may fail silently' is likely to be considered relevant.
- Actionable: A metric is considered actionable if it informs as to the appropriate response to a situation and inspires action. A metric such as 'number of security artifacts with committed owners' is likely to be considered actionable.
- Genuine: A metric is considered genuine if it provides objective, credible and straightforward information. The more a metric is informed by auditable facts the higher it would score on the genuine scale. A metric that compares 'discrepancies between physical location and logical access location'[5] is likely to score high on the genuine scale.
- Meaningful: A metric is considered meaningful when it is usable by the recipient of the metric. An important factor of a metric's influence is how well it can be used to communicate with decision makers. A metric such as 'annual cost of cybersecurity controls' is likely to score high on the meaningful scale
- Accurate: A metric is considered accurate if it responsibly and repeatedly provides a value that is 'right' within the context of the metric. A metric that reports the 'frequency that access control matrices for applications are reviewed' is likely to score high on the accurate scale.
- Timely: A metric is considered timely if it is available to decision makers in a fashion that facilitates them making corrective decisions prior to an incident. A metric such as 'percentage of critical business processes that have business continuity arrangements' is likely to score high on the timely scale.
- Independent: A metric that is independent is one that is not encumbered with bias and is unlikely to be 'gamed' by the provider. It offers an honest and trustworthy assessment of a situation. Independence, in this context, is about the perception of the metric consumer as to how much the metric provider can evaluate it fairly. A metric such as 'cybersecurity budget variance' is likely to score high on the independent scale.
- Cost: A metric will score high on cost if the benefits it brings to the business exceed the cost to the business to maintain this metric. Some metrics are very easy to collect (thus inexpensive) but offer little value to the business; others are expensive but add potential value that justifies the high cost. Clearly businesses need to look across a suite of proposed metrics to determine what

[5] How often people who are not in a facility with physical access control) appear to be logged in locally

set will offer optimal value within resource constraints. A metric such as 'cybersecurity ascendency'[6] is likely to score high on the cost scale.

The PRAGMATIC metametrics outlined above represent a comprehensive collection of information that should be useful to an organization in the process of identifying a suitable suite of metrics. Clearly one could argue that some of these metametrics are a bit 'squishy' and would require some structure around the actual method of measurement and calculation to facilitate fair comparisons across competing metrics. Some organizations may find some of these metametrics of little or no value, may deem some very important and some less important or they may have metametrics that resonate better with their business. For these reasons, the methodology presented is quite easily tailorable.

What is really compelling about the notion of the PRAGMATIC method is not so finely ingrained in the metametrics proposed[7], but rather the fact that it offers a logical and repeatable process for assessing relative value of metrics within the context of an organization's requirements. While this methodology is not exclusive to metrics concerning cybersecurity, it appears that it might represent a shining beacon to those security professionals who are struggling in the constantly changing wild-wild west atmosphere in which they are currently working.

Cybersecurity Metrics

It would be impossible and impractical to list all the possible cybersecurity metrics here because the field is still constantly evolving. It is possible that metrics considered very good today may be replaced by far better ones by the time this paper goes to press. The intent of this section of the paper is to introduce a set of potential metrics that are likely to have broad appeal to various types of organizations. Organizations, security management, and security professionals should realize that while some of these metrics may work well for them, there are some that are not going to make sense given particulars of the organization, security goals, risk aversion and resources available to devote to security focused measurement. Realize as well, that there may be many other metrics that are better suited to the needs of some organizations. Identifying the right suite of metrics for an organization is not an exercise, but rather a journey. It is a journey that should never end, as metric needs will evolve with changing technology and an organization's emerging maturity in cybersecurity practices.

The metrics that follow come from various sources. Some of these metrics were described in or adapted from the text that introduced the PRAGMATIC approach [5] where over 150 examples were introduced and rated based on the authors experiences. The ones presented here are a subset of the high scoring ones with cybersecurity implications. Other metrics known to the author have been included in this section as well to address changes in cybersecurity, technology and cloud computing since the publication of the book. The intent is not to be comprehensive but to offer some breadth and depth to the readers knowledge of the possibilities.

As in the referenced book, the metrics presented are aligned with the International Standards Organization/International Electrotechnical Committee (ISO/IEC) Standard 27002 structure [6]. The areas

[6] This metric simply traces the levels of hierarchy in an organization between the CEO and the most senior cybersecurity executive.

[7] Though they do seem to be good choices

of concern in the National Institute for Standards and Technology (NIST) Special Publication 800-171[7] are covered by the metrics presented. This standard established guidelines and best practices for initiating and maintaining a cyber and information security organization by focusing on the following areas:

- **Cybersecurity Risk Management**

  While it is true that most security metrics should be considered risk management metrics, these selected metrics focus more on the metrics that provide insight into how an organization assesses and deals with cybersecurity risks.

  - Number of known risks currently untreated or unresolved: This metric represents the proactiveness and effectiveness of the security function. Watching trends of this metric over time provides a window into the health of the organization within the security context.
  - Cybersecurity budget variance: This metric allows management to follow and access trends in the security budget to assess whether security risks are being appropriately managed over time. Significant increases or decreases in this budget should trigger further investigation.
  - Number of unpatched technical vulnerabilities: This metric indicates, for a given time period, the amount of patch work that still needs to be accomplished. When viewed over time it also tells the story of whether risks are being sensibly managed. This metric is useful in predicting future workload for the completion of known patches.

- **Cybersecurity Policy**

  Policies, standards and procedures are a necessary evil to create a disciplined environment where the employees understand and respect that cybersecurity is the responsibility of all members of the staff.

  - Percent or number of security artifacts (policies, standards, procedures, metrics, etc.) with committed owners: This metric goes to the core of the organization's commitment to health with respect to security. When an artifact does not have a committed owner there is no one championing that artifact, making sure there is awareness of that artifact or updating that artifact as changing conditions in the security climate require.
  - Traceability of policies, control objectives, standards and procedures: This metric provides insight into how well these artifacts are linked together and consistent with each other. Across an organization there are likely to be multiple policies, standards, etc. that have

security implications. These artifacts may have different owners or multiple owners; a high degree of traceability reduces the risk of conflicts across these artifacts and how they are used.

- Policy coverage of frameworks such as ISO/IEC 27002: This metric communicates the extent to which an organization's cybersecurity policies comply with externally sanctioned industry standards. It also provides indications of the organization's security health.

- **Cybersecurity Management and Governance**

  Security management and governance comes down to the security controls[8] that are in place and how well they are performing their jobs. This function is responsible for making sure the right controls are in place addressing the right security risks, that they control what they are expected to control, and that the amount of resources spent on security controls is adequate but not excessive.

  - Percentage of security controls that may fail silently: This metric provides visibility of the organization's risk that changes in threat, technology, configuration, platforms, etc. will make controls disabled or ineffective. While this seems to be something that would be expensive to track, it is compelling and worthwhile that an organization could understand and address any trends in this area before they lead to an incident. It also can be part of the analysis to predict future costs to address the implied vulnerabilities.
  - Cybersecurity ascendency: This metric offers visibility into how seriously the organization takes cyber security by determining how important the highest-ranking security executive is considered in the overall organization. It is easy to measure because it is simply the number of levels in the organization chart from CEO to most senior security executive. Organizations that bury security functions several layers down are sending a message that cybersecurity is not a top priority.
  - Days since the last serious cybersecurity incident: This metric, when tracked over time, could be useful in identifying impacts of process improvement initiatives focused on preventing serious security incidents. It could also be used as a measure to predict resources required to address incidents in the future.
  - Number of security metrics being tracked by category: This metric provides insight to management as to the extent and comprehensiveness of the cybersecurity measurement program in the organization. Trends may provide interesting information about the organization's maturity in the security arena.
  - Percentage of critical third-party vendors whose contracts include cybersecurity requirements commensurate with the organizations policies. This metric provides insight into how vulnerable the organization is making itself by taking advantage of cloud services or other third-party service providers. There are surely concerns that security can be compromised when operations are moved to the cloud; the security savvy organization makes contractual agreements to mitigate such risks.

[8] Security controls are safeguards or countermeasures to avoid, detect, counteract or minimize security risks to physical property, information, computer systems or other assets.

- **Information Asset Management**

  Cybersecurity assets include intellectual property, personally identifiable information (PII), personal health information, strategic and security plans and procedures, financial plans, etc. A good measure of an organization's cybersecurity practices is how their important information assets are protected by ensuring that the right people have direct responsibility for those assets and that there are direct consequences if those assets are compromised.

  - Percent or number of orphaned information assets without an owner: This metric communicates the number of information assets that have no owner because the owner moved on and no replacement was appointed. If this number is high this could indicate that assets which were once deemed critical no longer have a committed owner. This is like the 'percent of security artifacts with committed owners' metric. The difference is that this metric applies to information assets while the previous mentioned metric applies to the security policies, procedures, metrics, etc.
  - Proportion of information assets not classified: This metric provides insight into how comfortable the organization should feel about the above metric. Information assets need to be classified as to their importance to the organization in order to determine which assets require ownership.
  - Unowned information asset days: This metric acts as a companion to the first metric in this section as it provides additional context around the orphaned assets. Presumably an asset that was previously determined to need an owner, should get a new owner when orphaned. The longer such assets go without ownership, the greater the vulnerability of those assets which may speak to breakdowns in the security function.

- **Human Resources Security**

  Paramount to the success of any cybersecurity initiatives is buy-in from the top of the organization. If the person at the top refuses to wear a name badge or leaves his/her password on a sticky note on his/her monitor, this sets a tone in the organization that security policies and procedures are not a top priority. Organization's that establish and maintain a culture that makes security concerns an intricate part of day to day operations are much more likely to reduce incidents and improve response when incidents occur

  - Security awareness level: This metric is intended to indicate how conscious of security best practices the employees are. This can be measured via surveys, through learning management systems, by tracking how often sites with security policies and procedures are visited and for how long, by tests devised to trick employees into releasing sensitive information, etc. The more systemic the employee's understanding and acceptance of their own role in good security, the better the security footprint of the organization.
  - Rate of change in employee turnover or frequent absences: This metric is intended to help management keep a pulse on possible unrest or dissent throughout the organization or within one or more departments. If this is the case, the result could be sloppiness in executing security policies and procedures, or even worse actual malicious acts as retaliation for perceived poor treatment. However, this metric, while it is an easy (cheap)

thing to track, could also serve to be misleading since turnover and absences could be completely unrelated to employee discontent.

  - Percent of people in the organization who are not up to date on security training: This metric provides an excellent window into how seriously the organization is taking cybersecurity. Many incidents are triggered by employees who don't know or don't understand the security policies and procedures within the organization.

- **Physical and Environmental Security**

  All the best policies, procedures, firewalls, sophisticated controls and valuable security metrics offer very little real protection if bad actors can walk into a facility and gain physical access to critical assets. It should be a no brainer that propping open the door, allowing unknown people access to the server room or sharing facility access codes with others is a bad idea. People still do these things either for convenience, sloppiness or with malicious intent. Most metrics in this category fall outside of the intersection between cybersecurity and information security but the following bears mention.

  - Discrepancies between physical locations and logical access location: This metric reports how often system accesses are suspicious. For example, when an employee appears to have logged in via a local network when security logs indicate that employee is not on the premises. This could be an indication that a user has shared their login credentials or left their login information in a public place or that their login information has been hacked; it could also be an indication that someone held the door for them on arrival that morning, resulting in their card not being swiped. This metric is a relatively cheap and easy way to watch trends that may indicate intrusions or bad security behavior.

- **Information Technology Security**

  The attention and responsiveness of the IT function with respect to cybersecurity is paramount to ensuring that an organization's operations are not hindered or suspended due to security related incidents.

  - Proportion of systems checked and fully compliant to technical standards: This metric provides visibility into the extent and success of compliance testing. It should provide insight into how mature the compliance testing process is and how many systems are compliant to standards.
  - Time from change approval to change: This metric is intended to highlight potential inefficiencies in the approval process to get changes into the system. Many changes are focused on addressing security issues by fixing bugs or other vulnerabilities in the system. The longer changes stay in the queue, the longer vulnerabilities are there to exploit
  - Average number of changes per category received per time period: This metric provides insight into how often change notices of varying degrees of criticality are received. It not only provides insight into the stability of third-party applications but also can be predictive of resources required to handle critical and near critical changes in the future.
  - Rate of change of emergency change requests: This metric provides insight into how quickly the IT group reacts to change requests that are classified as emergency or urgent.

  - Presumably these are necessary to address near real-time possibilities of a serious incident or attack and the change process should be accelerated accordingly.
  - Proportion of highly privileged/trusted users: This metric provides management an indication of how vulnerable the system is based on how many people can effectively 'go anywhere' when they are logged in. Users should be granted access commensurate with their roles, their responsibilities and their need to access certain information and applications. Giving people greater access to more areas, applications, data, etc. then they need to do their jobs could be a recipe for disaster and IT professionals should make it a priority to limit access accordingly.
  - Maximum tolerable downtime: This metric represents the point in time where the impact of downtime becomes severe or intolerable. Understanding this for all critical business systems will create justification for investments in cybersecurity initiatives.
- **Access Control**

  As important as locking the doors, access controls prevent unauthorized users from logging into systems and keeps authorized users contained to the areas of the system necessary to do their jobs.

  - Rate of messages received at central access logging/alerting system: This metric keeps a pulse on potential threats by monitoring issues associated with failed logins. To be timely this metric needs to be monitored frequently and responded to quickly when there are indications that access is being sought nefariously.
  - Days since logical access control matrices for application systems were last reviewed: This metric reports on how timely IT department employees are with reviewing who has access to what applications. As employees often change roles within an organization, a regular review of who has access to what is imperative to keep application access limited to those with a current need to know/use.
  - Number of days to deactivate former employee credentials: This metric represents the average amount of time from when an employee leaves the organization to when their account is fully deactivated. Accounts that linger present potential for unauthorized access into the system and its associated networks.
  - Frequency of review of third-party access: This metric indicates how much attention the organization is paying to external entities who have (or had at one time) legitimate reason to be granted access. Lack of scrutiny in this area indicates a less than stellar third-party policy and could lead to unauthorized accesses that more vigilance could have prevented.
  - Percent of business partners with effective cybersecurity policies: This metric indicates how vulnerable an organization may be if they are granting access to business partners but not holding them to their same standards for cybersecurity.
- **Software Security**

  The application layer continues to be one of the most vulnerable areas with respect to cybersecurity breaches. Most vulnerabilities in software applications are a direct result of defects or faults that are injected into the software during the requirements analysis, design, code and test activities during development. Having good software development processes in place, which integrate security practices throughout the software development lifecycle, is a very effective way to eliminate vulnerabilities that have direct impacts on cybersecurity.

  - Percentage of controls tested realistically: This metric monitors the thoroughness of testing coverage of security controls in applications. This not only indicates how well security best practices are integrated in the software development process but also how effective that integration is.
  - Software quality assurance (QA) maturity: This metrics provides insight into the maturity of the software development groups QA processes on the assumption that a mature QA group will holistically embrace security objectives as part of their mission. In the same way that the architects and designers typically generate” use cases” describing how software is anticipated to be used, security architects and designers can generate “misuse cases” describing how software is anticipated to be attacked, compromised or otherwise misused [8].
  - Extent to which cybersecurity is incorporated into software development process: This metric measures how tightly cybersecurity is integrated into the software development lifecycle. Security should be built into software from the ground up, starting with concept and requirements, not treated as something that should be addressed during integration and test. This metric is important in an organization that does a lot of their own software development as the implications can be consequential.
  - Security testing coverage: This metric represents the extent of security focused testing for a software application. Many malicious attacks are made possible through vulnerabilities that are coded into applications.

- **Incident Management**

  Organizations need to run on the assumption that incidents will occur. Timely discovery and proper response are paramount to minimizing the impact of the incident on employees, users, customers and business partners. Once an incident has been responded to successfully, the organization should take the time to post-mortem the process from discovery through return to status quo as part of continuous process improvement.

  - Time taken to remediate security incidents: This metric indicates the average amount of time taken from discovery to close of ticket for all incidents with a significant security element. Successful recording of this metrics requires that incidents be classified as to whether security was a factor in that incident. The value of this metric is that it not only helps an organization plan for incident recovery when they occur, its trends also provide a way of determining how security initiatives in this area are working.
  - Mean time between security incidents: This metric provides insight into how often security incidents occur. As a trend, this metric offers an excellent cost-effective means of assessing the efficacy of process improvement initiatives. This metric in concert with the previous metric facilitates planning for resource requirements for future incidents.

- **Business Continuity**

  Business continuity refers to the steps taken by an organization to ensure that operations and activities essential to the business can continue despite an incident or can recover sufficiently before the impact of the incident becomes excessive or intolerable. Disaster recovery, disaster management and contingency planning are all part of business continuity.

  - Coverage of business impact analysis: This metric reports the percent of the business process landscape studied to determine what the impacts of a cybersecurity incident would be. Presumably coverage applies to the critical business systems and operations. This metric gives leadership an excellent window into how well their security professionals have assessed the situation. Trends overtime indicate how well this process of analyses is being maintained.
  - Percentage of business processes having defined recovery Time Objectives (RTOs) and recovery point objectives (RPOs): This metric provides insight into how much of the business process landscape has well defined objectives for recovery in the event of an incident. RTO refers the how long it should take the business process to be recovered and RPO indicates how far back in time that recovery needs to address[9].
  - Uptime: This metric indicates overall availability of business systems. This is a cost efficient and highly relevant and meaningful metric in that it gives a quick look into low or erratic availability, which while not necessarily caused by a security incident, should be viewed as an indicator that investigation is appropriate.
  - Disaster recovery test results: This metric reports on the results of disaster recovery testing. This tells its consumer two things, if disaster tests are being performed and how well does the organization perform when tested.

- **Security Compliance and Assurance**

Since May 2017, US federal government agencies and organizations doing business with them have been struggling to adhere to the President's executive order for immediate implementation of the highest standards in cybersecurity seen to date, the Federal Information Security Modernization Act (FISMA). This act adds some meat to the proposition that:

> *"An effective enterprise risk management program promotes a common understanding for recognizing and describing potential risks that can impact an agency's mission and the delivery of services to the public" [9]*

Most organizations, whether they are working with the federal government or not, have compliance and assurance standards they are required to meet. Some of these are internal and are hopefully focused on forwarding the business objectives of the organization. Some of these are external and may, depending on the extent and cost of complying with them, create a risk management decision for the organization. They need to consider a balance between investing in compliance over the cost and consequences of non-compliance. In some cases, this is a no brainer, in others it's a practical deliberation.

[9] Does the process state need to go back to the time of failure or is yesterday or last week adequate?

- Breakdown of exceptions and exemptions: This metric communicates degree of noncompliance with existing policies, processes, systems, etc. An exemption is noncompliance that has been sanctioned by management; an exception is noncompliance which has not been officially sanctioned. This measurement gives leadership an excellent view of the risks associated with current noncompliance and a window into how lax the organization is with respect to compliance.
- Number and severity of findings in audit reports, reviews, assessments, etc.: This metric conveys the health and maturity of the organization with respect to security issues and insight into the adequacy and coverage of security controls.
- Status of compliance with externally imposed security obligations: This metric applies specifically to compliance from without and gives specific insight into external risks the organization should consider.

As stated earlier, these metrics represent possibilities that an organization may want to consider. They do represent a sensible and manageable set of metrics for a business with no better options to get started. It is quite likely that they do not represent the perfect set of metrics for any specific organization, security department or security executive. Metrics always need to be defined within a context based on the perspective of the business towards cost, requirements and risk.

Conclusions and Next Steps

Cybersecurity and information security are not easy topics to grapple with. The landscape is rapidly changing as technology is constantly improving while bad actors keep getting better at defeating this technology. Organizations are being regularly challenged to protect their computer systems, networks, information assets, employees and business partners in a cost effective and practical manner.

Business leaders are constantly challenged with understanding cyberspace and determining the best ways to conquer the potential evils therein. Measurement and metrics are part of the solution. This paper provides a framework for presenting information to decision makers that informs as to the current state of the organization with respect to cyber and information security. Included are a set of proposed metrics that will provide a representation of the current state and predictive trends and analysis of the future state. These metrics represent a set of talking points for IT and security professionals to engage in conversations about what investments are working, what are not and what the next best set of investments should be for the future security needs of the organization.

This paper is merely a start into understanding and accessing value around cyber and information security investments. The first step involves understanding what activities, processes and practices are important to get one’s head around what these notions mean and to put them into a context where they can be measured, assessed and understood. This sets the stage for assessment of current state and understanding the value of cybersecurity investments. Research is underway to address the next step in this process which is to evaluate which measure and metrics are best suited to understanding cost and developing cost estimating relationships to help decision makers with cost benefit analyses as organizations look to improve and update their cyber and information security practices.

References

[1] “Cybersecurity Performance: 8 Indicators”, Carnegie Mellon University Software Engineering Institute – Insider Threat Blog, March 25, 2018, available at https://insights.sei.cmu.edu/insider-threat/2018/03/cybersecurity-performance-8-indicators.html, retrieved 1/21/2019

[2] “The 2017 State of Cybersecurity Metrics Annual Report”, Thycotic, available at https://thycotic.com/resources/cybersecurity-metrics-report-2017/, retrieved 1/15/2019

[3] https://en.wikipedia.org/wiki/Information_security

[4] https://www.merriam-webster.com/dictionary/cybersecurity

[5] Brothby W.K., Hinson GG, “*PRAGMATIC Security Metrics: Applying Metametrics to Information Security”,* CRC Press, Taylor & Francis Group, LLC; Boca Raton, FL, 2013

[6] ISO/IEC 27002 *Information Technology – Security Techniques – Code of Practice for Information Security Management, International Standard Organization/International Electrotechnical Committee, 2013*

[7] “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations”, NIST Special Publication 800-171*,* Joint Task Force Transformation Initiative, April 2013

[8] McGraw, G., Software Security: Building Security In, Addison-Wesley, New Jersey, 2006

[9] “Best Practices for Cybersecurity Compliance Audits”, BlackStratus, https://www.blackstratus.com/best-practices-cybersecurity-compliance-audits/, Dec 2018, retrieved Feb 2019