CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL

Volume 2, No. 1
April 2023
ISSN: 2832-1006

In this issue:

iscap
Information Systems & Computing Academic Professionals

The **Cybersecurity Pedagogy and Practice Journal** (**CPPJ**) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (https://cppj.info). Our sister publication, the proceedings of the ISCAP Conference (https://proc.iscap.info) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point, papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal.

While the primary path to journal publication is through the ISCAP conference, CPPJ does accept direct submissions at https://iscap.us/papers. Direct submissions are subjected to a double-blind peer review process, where reviewers do not know the names and affiliations of paper authors, and paper authors do not know the names and affiliations of reviewers. All submissions (articles, teaching tips, and teaching cases & notes) to the journal will be refereed by a rigorous evaluation process involving at least three blind reviews by qualified academic, industrial, or governmental computing professionals. Submissions will be judged not only on the suitability of the content but also on the readability and clarity of the prose.

Currently, the acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

Editors

2023 Review Board

Measurement, reporting, and monitoring in organizational security governance from the security professional's perspective

Kevin Slonka
kslonka@francis.edu
Computer Science & Cyber Security Department
Saint Francis University
Loretto, PA 15940 USA

Sushma Mishra
mishra@rmu.edu

Peter Draus
draus@rmu.edu

Natalya Bromall
bromall@rmu.edu

Computer and Information Systems Department
Robert Morris University
Moon Township, PA 15108 USA

Abstract

The constantly increasing number of security incidents and threats warrant organizational security governance (OSG) practices rooted in data that allow quick and reliable decision-making to quickly adapt to the changing landscape of security management. Measurement, reporting, and monitoring of security controls across organizations provide a data-driven governance approach that enables leaders to scale security tools and measures aligned to organizational business objectives. This research identifies standard practices under measurement, reporting, and monitoring and provides insight into how these domains come together to enhance overall OSG practices. Interviews are conducted with security professionals in multiple organizations. Qualitative analysis of the data suggests underlying themes for each domain. Results indicate that the three domains under study form the basis of data governance and play a key role in aligning the OSG objectives with security controls. Implications for research and practice are drawn, and future research directions are suggested.

Keywords: organizational security governance, data governance, measurement, reporting, monitoring, qualitative, thematic analysis

1. INTRODUCTION

Security measurement, reporting, and monitoring are critical components in all organizational security governance (OSG) strategies. Implementation of constant security monitoring enhances employees' security assurance behavior and awareness (Ahmad et al., 2019). Effective security measurement in all fields of the organizational IT infrastructure leads to effective

information security management (You, Cho, & Lee, 2015). Finally, a successful reporting strategy is a glue that holds together all other areas of information security governance. With the increased number of cyber-attacks, top organizational management becomes more and more involved in security governance and requires constant reporting on (1) what was done to reduce vulnerabilities and (2) how effective these measures are (Garigue & Stefaniu, 2003). At the same time, even the involvement of top management does not guarantee effective prevention of cyber-attacks. Corris (2010) noted that organizations continue to fall victim to phishing, stolen data, employee negligence, and other security issues. While there is a solid OSG theoretical framework, few studies report the match between this framework and its practical implementation.

Researching the way organizations implement OSG measures will have multiple benefits. First, it will help close the gap between theoretical frameworks and the real issues organizations face with their implementation. Second, it will reveal the aspects of OSG that companies encounter the most difficulties. For example, previous research shows that OSG implementation is often inefficient due to either not formulating its specific objectives or not communicating them to all involved parties (Mishra, 2015). Finally, it will help the researchers provide recommendations for making OSG implementation more effective.

In this research, we use the theoretical framework of OSG defined by AlGhamdi (2020). This model includes seven critical domains (1) Responsibility & accountability, (2) Awareness, (3) Compliance, (4) Assessment & auditing, (5) Measurement, (6) Reporting, and (7) Monitoring. The research goal is to explore the practical implementation of the last three domains: organizations' measurement, reporting, and monitoring. The research goal yields three research questions, which will be answered in this study:
RQ1: How does security measurement structure influence Organizational Security Governance (OSG) practices?

RQ2: How do reporting initiatives influence OSG practices?

RQ3: How does monitoring influence organizations' OSG practices?

2. LITERATURE REVIEW

Organizational Security Governance

Organizational Security Governance is part of the overall organizational Governance. Blum (2020) lists the main functions as "Charter or mandate the security program," "Manage, control, and report on risk," Coordinate security projects and manage issues," Manage security policy," and "Allocate security budgets and resources." It is essential to recognize that this is a governance activity and not simply a framework for IT security. Schinagl, S., & Shahim, A. (2020) noted the move from the technical level to the top board, strategic level when they wrote, "landscape has shifted 'from the basement to the boardroom,' that is, from a narrowly focused technical issue towards a strategic business issue and a top priority item for the board" (Schinagl & Shahim, 2020, p. 283).

Another driving force behind the expansion into the boardroom is the increasing number of laws and regulations impacting data, privacy, and security. Khoo, Harris, & Hartman (2010) wrote, "Organizations must elevate the issue to a corporate governance priority to systematically strengthen information security at all levels of the organization" (p. 51). Yaokumah & Brown (2014) looked at the relationship between strategic information security governance and information security governance and concluded that "effective information security governance strategic alignment greatly improves organizations' risk management, resource management, performance measurement, and delivers business value" (Yaokumah & Brown, 2014 p. 51).

Frameworks

As the importance to the organization of the information and information infrastructure grew, and the governance structures expanded, some form of the system was needed to help organize the growing complexity. Multiple frameworks were utilized in this endeavor; some were part of the general organizational governance structure, and some were specific to the information security realm. Some of the frameworks, such as ISO/IEC 38500 and COSO, have high levels of abstraction and are focused more on governance itself, while others, such as ISO/IEC 17779 and ITIL, are focused more on IT tactics and strategy. Of course, this framework's more detailed and focused nature makes it more prevalent among technical managers and not overall organizational governance (Von Solms, 2005). Other frameworks cover higher governance levels down to the tactical level and are in the middle of the abstraction layer, such as COBIT 4/5 (De Haes,

Van Grembergen, & Debreceny, 2013). Al-Fatlawi (2021) looked at using COBIT 5 to improve security in accounting information systems and noted that the framework included the governance and implementation processes.

While COBIT is a prevalent and successful framework, other researchers have found deficiencies in its use for information security (Pratiwi, Indah, Jauhari, & Firdaus, 2020). AlGhamadi (2020) reviewed the literature in this area and found seven critical success factors when using frameworks for information security governance: 1) Responsibility & Accountability, 2) Awareness, 3) Compliance, 4) Assessment & Auditing, 5) Measurement, 6) Reporting, and 7) Monitoring.

Problems with the Current Situation

Some of the problems with the current situation in Information Security Governance include the lack of oversight by top organization leaders. One group of researchers, after reviewing security governance in the healthcare industry, concluded that the increasingly complex laws and regulatory environment exasperated the problems, writing, "The preponderance of healthcare-related laws, compliance regulations, and security guidance frameworks serve to complicate the cybersecurity challenge further and too often results in senior leadership assuming a state of blissful ignorance" (Abraham, Chatterjee, & Sims, 2019, p.539).

In addition to the breadth of the framework, others have noted the difficulty in measurement and reporting. To try and help solve this problem, some researchers have focused on developing methodologies to assist the security assessors in their duties. They found that the data was "deeply influenced by the expertise of the assessor and his/her sensitivity" (Angelini, Bonomi, Ciccotelli, & Palma, 2020, p. 1). The complexity of the entire process and the disconnect from the everyday work of most employees was also listed as an issue by Ridley, Young, and Carroll (2004). Sadok, Alter, & Bednar (2020) conclude that "Security practices remain an illusory activity in their real-world contexts" (p. 18).

Measurement & Monitoring

When gathering data for security evaluation, it still isn't clear what the measurement should be. Lidster & Rahman (2018) performed a comprehensive literature review and concluded a lack of a good measure of alignment between practices and governance still exists. It is not just governance that can be improved by including the upper level of the organization. A group of researchers found that the quality of the security is enhanced as the quality of the relationship between the auditors and upper management improved (Steinbart, Raschke, Gal, & Dilla, 2018).

One area where adherence to governance policies is the area of phishing attacks. Testing and data gathering in this area is easy and done across many organizations. Instead of looking at actual testing, some researchers have suggested gathering data on the user's knowledge of phishing and their understanding of different situations using scenario-based analysis. In this way, they hope to collect data on the employees' broader understanding of the issues and opportunities for data loss (Das, Nippert-Eng, & Camp, 2022).

As with so many other aspects of the information arena, the collected data must be stored, sorted, and ready for analysis. For security issues, reports of flaws are stored in multiple open databases, such as the Common Vulnerabilities and Exposures (CVE) and National Vulnerability Database (NVD). Security policies developed from the governance models can refer to these vulnerabilities when ensuring that systems securities are up to date. Dong et al. (2019) found inconsistencies in the data between these two repositories, making auditing difficult.

As the information infrastructure grows and data is no longer stored in central locations but on devices scattered all over, such as in an IoT environment, security and measurement become an even more significant hurdle. IoT devices are built by smaller companies, each with data and security standards. They lack the resources to match standards for every customer. The expanded usage of such devices outstrips the regulatory and governance as demand pressure increases (Vitunskaite, He, Brandstetter, & Janicke, 2019).

The issue is more than the framework but the organization's security practices. Orehek and Petric (2020) stress that the goal of measurement should not just be on individual metrics but that all the data should be evaluated to measure the organization's security practices. Others have noted that by extending the security practices, workers are working to meet specific security metrics and improve the entire organizational security levels (Tan, Ruighaver, & Ahmad, 2010, September), leading to reporting such overall levels.

Reporting

One of the most basic IT security reports is a security audit. While the audit may or may not look at the governance model, it still collects data on security policies and adherence. Bongiovanni et al. (2022) argue that the problem is not in the data gathering but in quantifying and organizing the data to align with the organizational governance model. They proposed a model to quantify existing security data to an existing security governance model. They tested their model on multiple organizations and confirmed that such a model worked as proposed and tracked well across industries. Instead of developing a new reporting model, Herath, Herath, & Cullum (2022) proposed using the Balanced Scorecard model and applying it to security governance. One of the advantages of this method is that all of the previous work could be leveraged in the deploy reporting scheme. Another positive is the inclusion of the financial return on the investment in security governance that is inherent in this model.

Alotaibi, Furnell, & Clarke (2019) proposed a reporting model that assigns points to end-users based on their security compliance and awareness of security policies and risks. The intriguing aspect of this model is that the issues are not just used as a measurement and reporting function but are used to assign both penalties and rewards.

One of the significant areas of reporting is a risk. Spremic (2011) pointed out that IT risk is a function of both the asset itself and the threat and vulnerability. Three parts of the proposed corporate IT risk management model are: "Corporate governance policies for managing IT risks," "Procedures for managing IT risks on business units level or functional level," and "Operational (technical) activities."

Organizational Security Governance Practices

As demonstrated earlier, changing the practices to increase the upper levels of management in the security governance improves security levels. Still, other researchers have found more of a sense of complacency. After interviewing 187 employees in 39 organizations about their security practices, Sadok, Alter, & Bednar (2020) found that the corporate policies were disconnected from the security activities of the workers and that the security policies don't have a high priority. They concluded that "Security practices remain an illusory activity in their real-world contexts." Sadok, Alter, & Bednar (2020 p.1). The organization's security practices are more than the policies and governance structure; it is also how the employees interact with the guidelines. What is said and rewarded in all organizations is not always the same. Khatib & Barki (2021) surveyed over 300 workers concerning their activities in hypothetical scenarios and found their response was motivated more by any benefits than any costs based on non-compliance. This would fit with the model proposed by Alotaibi, Furnell, & Clarke (2019).

Efficient OSG practices are not just an organization's security policies but encompass the training and everyday interactions with the guidelines; some of those interactions increase the security level, and some decrease the organization's security level (Da Veiga et al., 2020). Other researchers have moved beyond security practices and looked at the interplay between security practices and the general practices of the organization and information security awareness. They found a high correlation between the general practices and the security practices, suggesting that training efforts on security practices alone should be a more effective use of resources (Wiley, McCormac, & Calic, 2020). Of course, the security practices depend on a top to bottom security governance framework. After reviewing industry and academic security practices, Veiga & Eloff (2007) made the critical recommendation that "The first step in developing an information security culture and empowering the workforce to be aware of their responsibilities towards protecting information assets would be to implement a comprehensive Information Security Governance framework" (p. 370).

To fully understand an organization's Information Security Governance, we need to gather data about the structure and policies and conduct interviews concerning all aspects of the organization's security practices.

3. METHODOLOGY

Data Collection and Analysis

To collect the data, we conducted 10 interviews with security and organizational governance managers, which were sufficient to cover small, medium, and large businesses. The discussions included questions about the managers' experience with security measurement, reporting, and monitoring. Each interview included three groups of questions matching the three domains. Each question included multiple talking points (Table 1), which were normally covered by the respondents. In case any talking points were skipped, the interviewer asked

additional questions related to the missing information.

Question 5: How does measurement influence OSG practices?

• How does your organization measure its performance against their Organizational Security Objectives?
  ○ Can you give some examples of the types of data that is gathered to help measure this performance?
  ○ IS the data actually used to try and alter performance?
  ○ Does the data only flow upward, or do all employees have access to at least some of these performance measures?
  ○ Do you have any examples of this downward flow?

• In what ways are employees measured on their awareness and commitment to the Organizational Security Objectives?
  ○ Is the measurement itself meant to influence their performance?
  ○ Can you give any details?

• Does your organization gather data from outside to assess their Organizational Security Objectives?
  ○ Can you give some details?
  ○ Does this data influence practice as well as data gathering techniques and measures?

Table 1: Interview Questions Structure

The interviews were recorded as audio files and later converted to text with the help of a transcribing tool. The answers were grouped by the three domains and the respondents within each domain. During the first stage of the further analysis, we listed the themes that emerged after the initial reading. A theme was recorded on the list if it was mentioned multiple times, either by the same respondent or multiple respondents. The responses were specifically matched to the recorded themes during the second stage.

The results of the data analysis are presented in the following section.

The subjects' demographic information is given in Appendix A. The majority of the ten interviewed subjects represent either the top management or executive management highly involved in information security decision-making. Most respondents represent medium to large organizations (1000 or more employees) and have substantial (10 or more years) experience in their field. The organizations were very diverse and included healthcare, pharma, defense, financial services, engineering/IT, and non-profit.

4. RESULTS

This section presents the results of our data analysis. The data is presented research question-wise.

Domain: Measurement

Theme 1: Performance	• Dashboard with metrics for each area • Different areas of performance: people, process, and knowledge • Delivery of completed projects • Projects within budget • Frameworks provide metrics • Internal audit performs measurement. • Key risk indicators • KPIs are measured but do not get much of an executive view-operational nature, such as VM and phishing. • Good code passing through pipeline offering good service
Theme 2: Awareness of OSG	• Maintain situational awareness through different channels • Reputation awareness
Theme 3: External	• Third-party measures • Security campaigns impact • Training impact • Scans the internet-facing systems for threat vectors • Provide a score to reflect the health of the system • Ranks highest risk systems to prioritize • Sends assessment reports to clients directly

Table 2: Measurement Domain Themes

A well-designed OSG program needs to be constantly aligned with the organization's risk appetite. Measurement of governance practices in control effectiveness, risk score, policy effectiveness, and operational efficiency ensure that the OSG objectives are realized after implementation. Performance and changes in an organization must continually evaluate whether the OSG principles, policies, and procedures are

working according to predefined indicators and criteria (Alghamdi et al., 2020). Research literature suggests many measures, such as employees' awareness and training in doing their job, clarity in business processes (Mishra, 2015), knowing who to approach in adverse situations, and commitment to responsibilities (Nicho, 2018). These measurements assure top management that the OSG program is on track and acts as an incentive to garner more resources for the enhancement of the program.

Our data for the Measurement domain shows three emergent themes: 1) Performance, 2) Awareness of OSG, and 3) External (Table 2).

Theme one covers the performance measurement indicators and practices. Our data suggest that most organizations use dashboards with metrics for each performance area. These areas are people, processes, and knowledge. Multiple types of metrics are used, such as the delivery of completed IT projects, the number of projects within budget, and key risk indicators, such as the number of phishing attacks, malware attacks, etc. The internal audit division performs measurements of control effectiveness in many organizations. Most of the leading IT governance frameworks provide key metrics. Key performance indicators (KPI) are measured, funneling data to dashboards. Operational KPIs include whether the code passing through the pipeline is good, whether managers use vulnerability management, or detecting phishing attacks. In contrast, dashboard data is provided to C-Level executives.

Theme two is about employees' awareness of OSG practices. Our data suggest that it is essential to maintain situational awareness through different channels in various contexts. Understanding what is being measured, why it is being measured, and how it impacts day-to-day tasks goes a long way in making measurement more effective. Employees' reputation awareness creates a sense of pride in their daily work performance.

Theme three is about using external factors and agencies to measure OSG practices' impact. Several third-party measures are used in organizations. Third parties are often used to track the impact of security campaigns or training employees. On the network side, scanning the internet-facing systems for threat vectors allows for measuring network efficiency. On the process side, frameworks entail guidelines that will enable creating a score on processes to reflect the system's health. The prioritized ranking for different controls allows for better decision-making. For DoD-related organizations, external agencies directly send the report of OSG practices to the clients to maintain transparency in the process.

Domain: Reporting

Reporting allows the actual data from measurement to flow upwards in the organization such that decision-making is informed and timely. Reports show the results of the assessment and measurement activities in the organization, which can assist top management in understanding the return on investment in the organization's protection (Alghamdi et al., 2020). Research literature argues for proper reporting channels in the context of OSG to achieve the intended benefits of the controls (Mishra, 2020; Nicho, 2018). Most widely used frameworks such as COBIT, NIST, or even in-house versions of such frameworks provide a rich array of metrics for reporting purposes.

Our results suggest three main themes for the reporting domain: 1) Standard procedure, 2) operations, and 3) action related to reports (Table 3).

Theme one is reporting on standard procedures at different levels of an organization. Our data suggest that monthly operational reporting is funneled up through metrics and KPIs to management. Teams of people create reports through Tableau (or similar tools) for CEOs for strategic decision-making. Once a month, data is reported at a C-level meeting without daily operational details. Quarterly reports with crucial metrics for the board are also generated. In larger organizations, there are separate reporting groups specializing in reporting on anything that occurs in the organization; for example, risk assessment reports based on the state of controls are generated for auditors. In some organizations, reporting depends on who is asking and what is being asked; it is in response to what is being sought. There are no standardized formats for enterprise-wide reporting. Rather, departments have their standards of reporting. Some organizations follow reporting standards provided by frameworks such as US-CERT.

Theme two is operational reporting for task management activities at a higher granularity. Our data suggests that organizations use multiple tools to obtain any kind of report aligned to security process and control. It could be vulnerability reports from the third party or real-time information on all domains of cybersecurity

that are essential for daily tasks to be completed. Measuring all the controls in multiple manners allows consistent control appraisal in a given control domain.

Theme three alludes to actions taken in response to these reports. The organizational focus is to refine and improve the OSG process through reports and metrics. The flow of information upwards and downwards through the hierarchy depends on the information's value or nature and urgency. High-risk situations are acted upon in real-time. Compliance with policies is an expectation, followed up diligently in reporting. Non-compliance with controls or unexpected conditions, such as a breach, warrants more training for staff to deal with the situation. There could be a reward system to encourage employees to do the right things. It is good to recognize employees for due diligence in reporting incidents or unexpected situations.

Domain: Monitoring

Continuous monitoring provides agility to an organization's response to an aberration in its systems or processes. Monitoring allows responding to situations if preventive controls have been bypassed deftly. Monitoring control allows for quick remediation of the problem and minimizes damage in an unwarranted case (Mishra, 2021). Monitoring provides business continuity and recovery plans to be executed without interrupting day-to-day business (Alghamdi, 2020). Monitoring also allows for oversight of the users' behavioral patterns within the organization to ensure that data is confidential and integrity is maintained (Mishra, 2015).

Our data suggest three themes in the domain of monitoring: 1) continuous monitoring, 2) action in deviation situations, and 3) monitoring training (Table 4).

Theme one is about continuously monitoring the IT environment using multiple tools. Organizations implement zero-trust security, which results in everything and everyone being monitored on the network. Tools are used to scan many terabytes of data daily. Baseline parameters are configured, and the dashboard captures the anomalies that need attention. Automated recurrent monitoring allows for ensuring that controls are operating effectively. All monitoring data feeds into reports directly for compliance purposes.

Theme 1: Standard procedure	• Monthly operational reporting funneled up through metrics and KPIs to management. • Reporting depends on who is asking and what is being asked. • Not standardized. Departments have their standards of reporting. • Team of people creating reports through Tableau for CEOs • Reports quarterly with crucial metrics for the board • Once a month, data is reported at a C-level meeting. • A separate group presents a technical report on anything important that is ongoing. • Risk assessment reports based on the state of controls • Follow US-CERT reporting standards.
Theme 2: Operations	• Tools allow obtaining any kind of report aligned to security process and control. • Vulnerability reports from the third party • Real-time reports on all domains of cybersecurity • Constant Control appraisal in a given control domain
Theme 3: Action related to reports	• The focus is to refine and improve the process through reports and metrics • Depends on the value of the information. High-risk situations are acted upon in real-time. • Compliance is an expectation. Follow it diligently • Non-compliance or unexpected situations warrant more training. • Recognize employees for due diligence in reporting incidents or unexpected situations

Table 3: Reporting Domain Themes

There are structures in place, such as a change advisory board, that allow what is monitored and how the data is being consumed for decision making.

Theme 1: Continuous monitoring	• Continuously monitoring our environment. • Zero trust security-everything and everyone is monitored. • All data feeds into reports for compliance. • Change advisory board allows what is monitored. • Tools are used to scan many terabytes of data daily. • Automated recurrent monitoring to ensure controls are operating effectively
Theme 2: Action in deviation situations	• Employees know what to do. • In deviation, act according to policies. • Sensitive information is flagged and put in the proxy area. • Human intervention is required to clear the doubt. • Advisory decides actions based on the situation. • Something gets flagged, then a report is sent to everyone
Theme 3: Monitoring training	• What to do in a deviation situation is a part of awareness training • Specific training is required to allow what changes can go through. • Vulnerable to phishing attacks-needs to be trained

Table 4: Monitoring Domain Themes

Theme two is about actions taken in an unexpected situation. Our data suggest that there is training so that employees know what to do in unexpected situations. If there is no clarity for a given scenario, then employees are trained to follow policies as guidelines. In many cases, human intervention is required to clear the ambiguity in action. Monitoring allows the organization to flag sensitive information traveling in the network and put it in a proxy area for further review. There are advisory groups in organizations that decide what actions are best based on the situation. In most cases, if something gets flagged, then an alert is sent to everyone.

Theme three is about specific training for monitoring purposes. Employees on monitoring teams need to be provided specialized training in a) recognizing that a situation is not normal and b) what should be the course of action in a situation like this. It could be a vulnerability or phishing training that provides detailed steps on what changes can be allowed and what cannot be done.

5. DISCUSSION

Each of the three domains (bolded in Table 5) in this study has implications for practice. The first domain, measurement, can be considered the gatekeeper to the remaining domains. Without proper measurement, there can be no reporting or monitoring. This study suggests that measurement must be implemented at various levels within an organization in order to be effective. At the operational level, software engineers need measurement of their code as it passes through the CI pipeline. Compliance staff needs measurement of security control implementation for audit purposes. At a higher level, managers use KPIs and KRI's to ensure that organizational goals are being met and risks are being mitigated. At the strategic level, completed projects and budgets must be measured to achieve proper prioritization. While organizations may need to develop certain metrics in-house, there are various external resources that offer frameworks containing sets of common measures that every organization should implement (Chew et al., 2008; Bodeau et al., 2018). Organizations, however, should ensure that they are not merely implementing measurement for its sake; "inappropriate levels of precision and stability" (Snyder et al., 2020, p. 42) increase for little to no gain. Only measurements that help achieve business goals should be implemented, monitored, and reported.

Performance Awareness of OSG External	**Measurement**
Standard procedure Operations Action related to reports	**Reporting**
Continuous monitoring Action in deviation situations Monitoring training	**Monitoring**

Table 5: Domain Theme Summary

Just as measurements, suggestions for proper reporting can be found in external frameworks. Organizations will find that these are merely suggestions and will be highly customized depending on the recipient. C-Suite executives may want reports that are infrequent and high-level, while middle managers may want reports that are frequent and detailed. Some reporting may even be conducted in real-time, such as critical vulnerability reports from the cyber team. The same rule applies with reporting as it did with measuring, don't go overboard. Over-reporting can lead to report fatigue, leading to critical reports being glossed over or deleted without being read. This can have catastrophic effects on a business.

Newer cyber frameworks have given birth to the younger brother of reporting: continuous monitoring. While reports offer insights into an organization's operations on a periodic basis, critical activities can occur between those periods. Organizations must implement tools and processes to ensure that their environment is monitored 24/7 for changes to baseline performance (National Institute of Standards and Technology, 2018). This can be everything from increasing processor and memory usage on a production database server to detecting changes to a configuration file on a domain controller. Unwanted change on a network can wreak havoc, and employees must be properly trained to respond to such incidents. The existence of an incident handling team to respond to cyber breaches is one such way an organization can prepare for negative changes (Cichonski et al., 2012). In a more proactive sense, an organization should have a configuration control board (CCB) to approve or deny any change to the network, ensuring that proper testing is done and the change will not negatively affect the organization's security posture (Johnson et al., 2011).

6. CONCLUSION

This study makes abundantly clear that proper OSG is mandatory for organizations to succeed in today's threat landscape. Key aspects of measuring, reporting, and monitoring were uncovered and the existence and usefulness of these three domains were validated. Given the sheer quantity of effort required to implement these three domains alone, it is evident that proper OSG cannot be achieved with fractional IT staff nor with one- or two-person IT departments. It takes a team (optimistically many teams) of adequately educated and trained cyber experts to ensure a resilient security posture and protect an organization from ever-changing threats. Future research should be conducted that takes results from all seven domains from the seminal study and produces a set of minimum guidelines for implementing of an OSG program within an organization.

7. REFERENCES

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the US healthcare industry. *Business Horizons*, *62*(4), 539-548.

Ahmad, Z., Thian, S. O., Tze, H. L., & Norhashim, M. (2019). Security monitoring and information security assurance behavior among employees: An empirical analysis. *Information and Computer Security, 27*(2), 165-188.

Al-Fatlawi, Q. A., Al Farttoosi, D. S., & Almagtome, A. H. (2021). Accounting information security and it governance under cobit 5 framework: A case study. *Webology, 18* (Special Issue on Information Retrieval and Web Search), 294-310.

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & Security, 99*, 1-39.

Alotaibi, M. J., Furnell, S., & Clarke, N. (2019). A framework for reporting and dealing with end-user security policy compliance. *Information & Computer Security, 27*(1),2-25.

Angelini, M., Bonomi, S., Ciccotelli, C., & Palma, A. (2020). *Toward a Context-Aware Methodology for Information Security Governance Assessment Validation*. International Workshop on Cyber-Physical Security for Critical Infrastructures Protection, Springer, 171-187.

Bodeau, D. J., Graubart, R. D., McQuaid, R. M., & Woodil, J. (2018). *Cyber resiliency metrics, measures of effectiveness, and scoring*. MITRE Corporation. https://www.mitre.org/sites/default/files/publications/pr-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf

Bongiovanni, I., Renaud, K., Brydon, H., Blignaut, R., & Cavallo, A. (2022). A quantification mechanism for assessing adherence to

information security governance guidelines. *Information & Computer Security.*

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., & Robinson, W. (2008). *Performance measurement guide for information security*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer security incident handling guide*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Corris, L. (2010). *Information security governance: Integrating security into the organizational culture*. Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies, 35-41.

Das, S., Nippert-Eng, C., & Camp, L. J. (2022). Evaluating user susceptibility to phishing attacks. *Information & Computer Security, 30*(1), 1-18.

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security, 92*, 1-23.

De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems, 27*(1), 307-324.

Dong, Y., Guo, W., Chen, Y., Xing, X., Zhang, Y., & Wang, G. (2019). *Towards the detection of inconsistencies in public security vulnerability reports*. 28th USENIX Security Symposium (USENIX Security 19), 869-885.

Garigue, R., & Stefaniu, M. (2003). Information security governance reporting. *Information Systems Security, 12*(4), 36-40.

Herath, T. C., Herath, H. S., & Cullum, D. (2022). An Information Security Performance Measurement Tool for Senior Managers: Balanced Scorecard Integration for Security Governance and Control Frameworks. *Information Systems Frontiers*, 1-41.

Johnson, A., Dempsey, K., Ross, R., Gupta, S., & Bailey, D. (2011). *Guide for security-focused configuration management of information systems*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf

Khatib, R., & Barki, H. (2021). How different rewards tend to influence employee non-compliance with information security policies. Information & Computer Security, 30(1), 97-116.

Khoo, B., Harris, P., & Hartman, S. (2010). Information security governance of enterprise information systems: An approach to legislative compliant. *International Journal of Management & Information Systems (IJMIS), 14*(3).

Lidster, W. W., & Rahman, S. S. (2018, August). *Obstacles to implementation of information security governance.* 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 1826-1831.

Mishra, S. (2015). Organizational objectives for information security governance: a value focused assessment. *Information & Computer Security, 23*(2), 122-144.

Mishra, S. (2020). Examining Organizational Security Governance (OSG) Objectives: How strategic planning for Security is undertaken at ABC Corporation? *Journal of Information Systems Applied Research, 13*(2), 13-24.

Mishra, S. (2021). Interpreting Organizational Security Governance Objectives for Strategic Security Planning, *Journal of Information Systems Applied Research, 14*(3), 30-43.

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Nicho M. A process model for implementing information systems security governance. *Information & Computer Security. 2018, 26*(1), 10–38.

Orehek, Š., & Petrič, G. (2020). A systematic review of scales for measuring information security culture. *Information & Computer Security, 29*(1), 133-158.

Pratiwi, A., Indah, D. R., Jauhari, J., & Firdaus, M. A. (2020, May). *Security capability assessment on network monitoring information system using COBIT 5 for*

information security. In Sriwijaya International Conference on Information Technology and Its Applications (SICONIAN 2019), 167-171.

Ridley, G., Young, J., & Carroll, P. (2004, January). *COBIT and its Utilization: A framework from the literature*. In 37th Annual Hawaii International Conference on System Sciences, 1-8.

Sadok, M., Alter, S., & Bednar, P. (2020). It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs. *Information & Computer Security, 28*(3), 467-483.

Schinagl, S., & Shahim, A. (2020). What do we know about information security governance?"From the basement to the boardroom": towards digital security governance. *Information & Computer Security, 28*(2), 261-292.

Snyder, D., Mayer, L. A., Weichenberg, G., Tarraf, D. C., Fox, B., Hura, M., Genc, S., & Welburn, J. W. (2020). *Measuring cybersecurity and cyber resiliency*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2703/RAND_RR2703.pdf

Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both?. *Computers & Security, 24*(2), 99-104.

Spremic, M. (2011, July). *Standards and frameworks for information system security auditing and assurance.* In Proceedings of the World Congress on Engineering, 1, 251-266.

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. Accounting, Organizations and Society, 71, 15-29.

Tan, T. C., Ruighaver, A. B., & Ahmad, A. (2010, September). Information security governance: When compliance becomes more important than security. In IFIP International Information Security Conference (pp. 55-67). Springer, Berlin, Heidelberg.

Veiga, A. D., & Eloff, J. H. (2007). An information security governance framework. *Information systems management, 24*(4), 361-372.

Vitunskaite, M., He, Y., Brandstetter, T., & Janicke, H. (2019). Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. *Computers & Security, 83*, 313-331.

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security, 88*, 1-8.

Yaokumah, W., & Brown, S. (2014). An empirical examination of the relationship between information security/business strategic alignment and information security governance domain areas. *Journal of Law and Governance, 9*(2), 50-65.

You, Y., Cho, I., & Lee, K. (2015). An advanced approach to security measurement system. *The Journal of Supercomputing, 72*(9), 3443-3454.

Zaini, M. K., Masrek, M. N., & Sani, M. K. J. A. (2020). The impact of information security management practices on organisational agility. *Information & Computer Security, 28*(5), 681-700.

Editor's Note:

This paper was selected for inclusion in the journal as the CONISAR 2022 Best Paper The acceptance rate is typically 2% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2022.

APPENDIX A
Participants – Demographics

Participants	Relevant years of experience	Industry	Size	Title	Education level
P1	10+	Pharma	40,000+	Information Security Manager	Master
P2	10+	Financial services	1000+	Cyber Risk advisory manager	Doctoral
P3	6+	Financial services	10,000+	Senior cyber security investigative analyst	Master
P4	20+	Healthcare services	10,000+	VP security	Master
P5	3-5	Engineering/IT	80	Studio lead	Bachelors
P6	15	Non-profit R&D (fed contractor)	65	President/CEO	Doctoral
P7	7	Financial services	200,000+	VP cyber security operations	Masters
P8	23	Defense/ aerospace	400	CISO & CIO	Bachelors
P9	9+	Technology consulting	Global/big	Global Director Security Architecture and Governance and Cloud Security and Compliance Services for Digital Solutions	Bachelors
P10	25	Healthcare	90,000+	Information Security Manager	Master