



# Security #SquadGoals

---

Applying the Information Management Hierarchy to  
Your Talent Placement & Acquisition Strategy Will  
Improve Organizational Security

**August 2018**

**Authored by:**

**Parham Eftekhari, Executive Director, Institute for Critical Infrastructure Technology**

**Drew Spaniel, Lead Researcher, Institute for Critical Infrastructure Technology**

---

# Security #SquadGoals

## Applying the Information Management Hierarchy to your Talent Placement & Acquisition Strategy Will Improve Organizational Security

August 2018

Authored by

Parham Eftekhari, Executive Director, Institute for Critical Infrastructure Technology

Drew Spaniel, Lead Researcher, Institute for Critical Infrastructure Technology

---

Copyright 2018 Institute for Critical Infrastructure Technology. Except for (1) brief quotations used in media coverage of this publication, (2) links to the [www.icitech.org](http://www.icitech.org) website, and (3) certain other noncommercial uses permitted as fair use under United States copyright law, no part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For permission requests, contact the Institute for Critical Infrastructure Technology.

## Support ICIT

Through objective research, publications and educational initiatives, the Institute for Critical Infrastructure Technology, a 501(c)(3) cybersecurity think tank located in Washington, D.C., is arming public and private sector leaders with the raw, unfiltered insights needed to defend our critical infrastructures from advanced persistent threats, including cyber criminals, nation states, and cyber terrorists.

Our mission is to cultivate a cybersecurity renaissance that will improve the resiliency of our Nation's 16 critical infrastructure sectors, defend our democratic institutions, and empower generations of cybersecurity leaders.

Financial capital from generous individual and corporate donors is the lifeblood of the institute and a force multiplier to our efforts. With your support, ICIT can continue to empower policy makers, technology executives, and citizens with bleeding-edge research and lift the veil from hyper-evolving adversaries who operate in the dark.

Together, we will make quantum leaps in the resiliency of our critical infrastructures, the strength of our national security, and the protection of our personal information.

<http://icitech.org/support-icit/>

## Contents

Introduction .....	4
What's Really Driving the Increase in Cybersecurity Spending? .....	4
Layers of the Information Management Hierarchy .....	6
Information Assurance .....	6
Information Security .....	8
Cybersecurity.....	8
IT .....	9
Conclusion.....	10

## Introduction

Despite an incessant onslaught of insider threats, social engineering attacks, breaches, and other security incidents, some organizations do not recognize that a significant flaw in their security paradigm could be the imprecise definition of Information management roles which leads to an inefficient delegation of relevant responsibilities among security personnel. Firms fail to understand their risk profile according to the hyper-evolving threat landscape, and as a result, base decisions on an assumed risk appetite that does not accurately reflect the reality of their security posture. One recurring example of this occurs in industrial environments; owners and operators are just now beginning to understand the depth of the impact of IT / OT convergence on resiliency and what it means for cybersecurity decision making and operational functions. Consequently, many time-sensitive security decisions are still made with partial or inadequate understanding of the threat landscape and digital environment. As a result, IT/ OT microcosms are often not protected according to their value or potential harm if compromised.

Misunderstandings of information and risks may result in C-level directives that sacrifice essential security initiatives in favor of budget limitations. Consequently, in order to minimize the security budget, either talent is acquired at the least cost or information governance, management, and security responsibilities are irresponsibly delegated to personnel who are inadequately qualified, equipped, and authorized to ensure the confidentiality, integrity, and availability of the data at all stages of its lifecycle.

No matter what security solutions the organization employs and no matter how much they spend, security incidents will continue to occur so long as misinformed decisions are made, such as tasking IT staff with security or burdening cybersecurity staff with high-level policy determinations. As a best practice, it is critical that at each level, qualified talent is positioned to meet the needs of the organization. This will only happen, however, if organizations understand the layers of information hierarchy and map their information security teams according to these generally accepted principals.

People are simultaneously the strongest and weakest link in the security of the company. Ensuring the optimal assignment of roles and responsibilities to qualified personnel is essential for the minimizing of risk and the mitigation of threats. Simply put, security strategies only work when the right people are positioned in the right job.

## What's Really Driving the Increase in Cybersecurity Spending?

Gartner forecasts that worldwide, enterprise security spending will exceed \$96.3 billion in 2018, an increase of 8 percent from 2017. Gartner also predicts that by 2020, more than 60 percent of organizations will invest in multiple data loss prevention, encryption, and other data-centric security tools – a 25 percent increase from current investments. The increase is believed to

result from new regulations, shifting buyer mindsets, and increasing awareness of emerging and evolving threats. Overall, however, the increase is the result of fear of reputational harm and of "the next big breach." Malware such as WannaCry, NotPetya, Spectre, Meltdown, and numerous others as well as fear of incidents such as Equifax, etc. drive organizations to allocate additional budgetary resources towards improving their defensive posture against the cyber threat landscape [1].

Increases in security spending and investment will amount to a minimal reduction in cybersecurity incidents if the implemented mitigation and remediation solutions are not designed, acquired, implemented, or managed by qualified personnel who are assigned duties commensurate with their positions. Staffs are - and will forever remain - the strongest and weakest link in the holistic information security architecture. The acquisition and retention of qualified personnel remain a challenge for firms of every size. Consequently, spending on outsourcing security and IT services increased 11 percent in 2018 to an estimated total of \$18.5 billion. By 2019, outsourced services will account for 75 percent of all spending on security software and hardware products, an increase of 12 percent from 2016. The shift towards the reliance on external IT and security staff is due to skill shortages and talent burnout [1]. If roles were defined according to more appropriate requirements, then talent would be easier to acquire and retain.

Neither spending more on security solutions nor outsourcing to third-party firms has significantly reduced the risk to organizations or the threat of malicious adversaries. The focus on appropriating more and more solutions has led to the development of "snake-oil" faux experts offering "silver-bullet" solutions. Third-parties are often the primary target of attackers intent on laterally compromising an organization. Adversaries remain at least one step ahead of network defenders and law enforcement. For the most part, Information Security is still focused on responding to adversarial efforts; though, enterprise budgets are slowly shifting focus to detection and predictive response. At best, the increase in spending forces threat actors to adopt even more sophisticated methodologies and to hyper-evolve more expeditiously.

Rather than risk the reputation and security of the organization by relying primarily on third-parties or vendor solutions for security, perhaps organizations should reassess their posture. Comprehensive and effective security strategies depend on clearly defined roles and visibly delaminated responsibilities. Instead of trying solution after solution only to discover that a breach already happened, organizations should first ensure that their strategy and methodology is designed, implemented, managed, and maintained by qualified staff.

Managing and securing valuable information cannot be done with a single step or initiative. It is a dynamic multi-stage process that CISOs must reassess regularly to evolve with the changing threat landscape. Similarly, the responsibilities of managing and securing the data cannot be

delegated to one employee or staff. Devastating breaches remain a consistent occurrence because many organizations ignore the best practice of hiring qualified personnel for specific roles in the organization according to the hierarchy of information personnel, the responsibilities of each role, and the needs of the organization. Rather than pass all security and data governance to “the IT guys,” roles and responsibilities should be judiciously assigned hierarchically. Information Assurance personnel dictate strategic policies based on the needs of the company concerning topics such as privacy, risk, threat mitigation, compliance, physical security, and other areas. The Information Security team implements, enforces, and otherwise makes actionable the instructions and priorities of Information Assurance staff. Cybersecurity staff manages the security solutions acquired and implemented by the Information Security team. Finally, Information Technology personnel manage and maintain the company PCs, servers, and other systems so that the other staff can focus on securing information and mitigating risk. Ignoring any layer of Information management hierarchy stresses the other layers and opens the organization to risk. Adversaries exploit the vulnerabilities resultant from the overexertion and knowledge deficiencies that inevitably occur when the Information management hierarchy is ignored.

## Layers of the Information Management Hierarchy

Acknowledgment and understanding of the Information management hierarchy are still developing. Discrepancies in definitions and delimitations in topics exist; nevertheless, at a high-level, the structure of the hierarchy remains resolute. The barriers confining these topics are fluid and nebulous because they shift according to the hyper-evolving threat landscape. Even academic and industry experts experience frequent difficulty differentiating the terminology and fields. As a result, communication between stakeholders may be inhibited by differences in interpretations or preconceived delineations. Worse, since strategic talent acquisition depends on defining problem areas and hiring personnel according to the needs of the organization, imprecise terminology and incomplete understandings of the nuances of the fields and the skillsets of professionals in those fields, could result in talent placement that leaves the needs of the organization unfulfilled and that renders sensitive systems and data vulnerable to adversarial compromise. The brief definitions below are an attempt to clarify the boundaries between the layers of the hierarchy so that organizations can make better informed organizational and talent acquisition and placement decisions.

## Information Assurance

Information Assurance (IA) focuses on the high-level strategy of Information management and protection. It focuses on the big picture of an organization’s security posture. Organizations conduct Information Assurance to ensure that sensitive information remains secure and private. At a high-level, it encapsulates the identification of assets and the recognition of risk

and threat appetite. Decisions based on the conclusions of risk assessments, conducted by Information Security personnel, may be considered as part of Information Assurance. For instance, part of Information Assurance might include estimating how susceptible information assets are to adversarial attack, disclosure (a loss of *confidentiality*), modification (a loss of *integrity*), or disruption (a loss of *accessibility*), and the monetary quantification of the impacts of those events with consideration of the probabilistic likelihood of an event occurring according to real-time monitoring of the hyper-evolving threat landscape. The processes of Information Assurance, like the processes of Information Security, Cyber Security, and Information Technology, are cyclical and iterative. For example, decisions about how much to invest in security solutions might depend on the latest Indicators of compromise and other data from the Cyber Security layer and the risk analysis and relevant context from the Information Security layer [2].

IA dictates that strategies and policies should exist for topics such as privacy, risk, threat mitigation, audits, compliance, physical security, and other focus areas. Information Assurance includes measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities [4] [5] [3]. Information Assurance professionals assess risks and vulnerabilities and put together management plans for minimizing issues [6]. IA professionals do not concern themselves with technical specifics such as operating system exploits or zero-day vulnerabilities; instead, they familiarize themselves with what data the company possesses, how that data is stored, shared, and employed, the value of the information, and other factors that help guide the organization to prioritize and protect information without disrupting daily operations. Information Assurance experts measure the effectiveness of solutions implemented in the Information Security, Cyber Security, and Information Technology layers of the organizational structure [2].

Information Assurance professionals focus on the business of what to protect and how to protect it, but they generally are not concerned with the technical details. Their job focuses on the high-level management, planning, auditing, and governance. The technical strategy and governance of valuable information is the purview of Information Security professionals. They ensure that regardless of its container or state, information remains secure throughout every stage of its lifecycle. They determine and sometimes create the necessary architecture, operating systems, applications, file systems, and hardware platforms used to house and secure information at rest and in transit. The Information Security team makes actionable the priorities the Information Assurance professional crafted and budgeted to protect the organization's information assets. They also conduct the audits and compliance assessments ordered by the Information Assurance expert. While the Information Assurance expert must understand the



business needs and budget constraints, the Information Security professional must possess comprehensive technical knowledge of binary representation, computer organization, file structures, instruction processing, communications protocols, risk analysis frameworks, threat actor methodologies, and other more in-depth knowledge that facilitates the protection of information. Though some argue that Information Security staff need not know technical minutia to be effective, the reality is that a more encompassing and holistic knowledge base significantly improves the effectiveness of the hired talent and the security of key assets [2].

## Information Security

Information Security (IS) concerns how risk is analyzed, mitigation strategies are developed and implemented, security solutions are evaluated and acquired, policies are created and implemented, and how other key stakeholder decisions are made. Information Security governs how information and information systems are protected from unauthorized access, use, disclosure, disruption, modification, or destruction. The fundamental foundations of Information Security are protecting the confidentiality, integrity, and availability of information wherever it is stored, during processing, or while in transit [7] [8] [9] [10] [3] [11] [12] [13]. Confidentiality refers to preserving authorized restrictions on access and disclosure, including the means for protecting personal privacy and proprietary information. The Integrity of data is preserved by guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. Availability is ensured so long as information can be reliably accessed promptly [4] [14]. The configurations of security parameters of Cyber Security and Information Technology solutions are set according to the governance of the Information Security program.

## Cybersecurity

Cyber Security refers to the ability to defend against cyber-attacks, protect resources, and prevent cyber-attacks. Cybersecurity professionals defend systems, networks, and devices, secure internal and external communication, and detect, evaluate, and analyze malicious code [6]. "Cyber Security" and "Information Security" are all too often used as synonyms in security terminology and create a lot of confusion among security professionals due to discrepancies in interpretations and understanding. As of 2017, the terms "Information Security" and "Cyber Security" were used at relatively the same rates in the United States, Russia, India, and across most of the world. The term "cybersecurity" was used significantly less in the search volume of each nation [15].

One key differentiator between Cyber Security and information security relies upon the distinction between information and data. Data is raw facts and figures, independent of their meaning. Information comes about when we interpret and combine data to interpret meaning. Without context, each datum is not information. Collectively, the data can be called

information when it is interpreted in a context and given meaning. For example, the string of numbers "12011992" may be data, but the application of relevant context could allow the audience to recognize the string as a birth date (12-01-1992). In short, information is one or more pieces of data that have some meaning. Information security focuses on protecting the confidentiality, integrity, availability (CIA) of the information; meanwhile, Cyber Security concerns the protection of the underlying systems that store, process, and transport data.

Cyber Security is agnostic of the context of the secured data. The hardware and software applied to secure data should be proportional to the value of the data, but after the determination of applicable solutions, the context of the data is irrelevant from a Cyber Security perspective. The most significant difference between the fields is that Cyber Security only pertains to data and information contained in the digital realm while Information Security considers the security of any information container whether it be digital, analog, or even people [15].

Though some may argue that Cyber Security exists outside the purview of Information Security because it also applies to non-information elements such as cars, traffic lights, etc., these sources failed to consider the holistic microcosm. The secure coding best practices, policies of IoT security, native security controls, and other facets of the design and operation of the aforementioned devices were Information Security decisions that become Cyber Security issues once the device becomes operational. If an adversary were to compromise one of the systems, they would have to exploit a vulnerability and modify, destroy, or disrupt data values or systems with some level of context about the meaning of the values; otherwise, their attack would prove fruitless as they altered irrelevant data.

Cyber Security personnel defend systems, reverse engineer malicious code, and monitor for threats, regardless of the context of the data. They are also able to create the off-the-shelf solutions that Information Security professionals select, deploy, and maintain. Cyber Security specialists are also usually better qualified to address vulnerabilities associated with non-traditional computing devices, such as automated vehicles, IoT, and other systems [2].

## IT

At an even more granular level, Information and Communication Technologies, sometimes referred to as IT or ICT, is the configuration, management, and sometimes the protection of information technologies. In order to meet budget constraints, some organizations hire low-level IT personnel instead of qualified Information Security talent. IT systems, when not protected by Information Security or Cyber Security, are a primary target for potential attackers because the vulnerable systems serve as unparalleled beachheads for multi-stage attack campaigns that leverage sophisticated malware to laterally compromise systems across multiple company departments or between affiliated organizations [15]. Information

Technology staff maintain servers and other systems that are protected by the Cyber Security solutions implemented by the Information Security team at the direction of the Information Assurance leader. Their primary role is to ensure that systems remain operational and to handle non-security related tasks so that the other Information staff can focus on the security posture of the company and the evolving threat landscape.

## Conclusion

Security does not have to be governed primarily by spending precious budgets on solutions or third-parties that may not protect the company from digital or physical threat actors.

Organizations, hired talent, clients, data subjects, and the community at large benefit from firms' understanding and adhering to the Information management hierarchy.

When qualified talent is strategically positioned in the appropriate roles with the commensurate responsibilities, the risk is minimized, security solutions efficiently protect information assets, and corporate resource allocation is optimized. When the hierarchy is ignored, the risk is transferred to each stakeholder. Any perceived fiscal savings that result from inefficient positioning are illusory gains; significant long-term costs offset the short-term savings. Worse, customers, clients, partners, employees, and others who trust the organization to secure sensitive information become the victims of one or more malicious threat actors.

While every organization may not have resources to hire one full time employee for each of the roles in the hierarchy described in this paper, it does not diminish the importance of building these concepts into both short-term and long-term operational and hiring plans to delineate responsibilities to drive the best security outcomes. In short, to improve the security posture of the organization:

1. Understand the roles and responsibilities governing the information stored, processed, and transmitted by the organization.
2. Hire, train, and retain specialized staff who are dedicated to protecting the firm against adversarial efforts.

Security has - and always will be - about people. Does your firm have the right people to mitigate and respond to evolving and emerging threats or are you dependent on the unverified promises and assurances of third-party vendors and service providers?

## ICIT Contact Information

Phone: 202-600-7250

E-mail: <http://icitech.org/contactus/>

## ICIT Websites & Social Media



[www.icitech.org](http://www.icitech.org)



<https://twitter.com/ICITorg>



<https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit->

## Sources

- [1] R. van der Meulen, "Gartner Forecasts Worldwide Security Spending Will Reach \$96 Billion in 2018, Up 8 Percent from 2017", *Gartner.com*, 2018. [Online]. Available: <https://www.gartner.com/newsroom/id/3836563>. [Accessed: 07- Aug- 2018].
- [2] R. Klump, "Information Assurance vs. Cyber Security vs. Information Security: Clarifying the Differences", *Lewis University*, 2018. [Online]. Available: <https://www.lewisu.edu/experts/wordpress/index.php/information-assurance-vs-cyber-security-vs-information-security-clarifying-the-differences/>. [Accessed: 31- Jul- 2018].
- [3] "Committee on National Security Systems (CNSS) Glossary", *Committee on National Security*, 2015. [Online]. Available: <https://www.cnss.gov/CNSS/openDoc.cfm?zQeg4RjbLYRH/Tw9LO4NJw==>. [Accessed: 31- Jul- 2018].
- [4] "Information Assurance versus Information Security", *NovaInfosec*, 2011. [Online]. Available: [https://www.novainfosec.com/2011/08/30/information-assurance-versus-information-security/?doing\\_wp\\_cron=1533049927.8281159400939941406250](https://www.novainfosec.com/2011/08/30/information-assurance-versus-information-security/?doing_wp_cron=1533049927.8281159400939941406250). [Accessed: 31- Jul- 2018].
- [5] "SP 800-59: Guideline for Identifying an Information System as a National Se | CSRC", *Csrc.nist.gov*, 2003. [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-59/final>. [Accessed: 31- Jul- 2018].
- [6] "Cyber Security vs. Information Assurance: Which One is Right for You?", *American Intercontinental University*, 2015. [Online]. Available: <https://www.aiuniv.edu/blog/2015/april/cyber-security-vs-information-assurance>. [Accessed: 31- Jul- 2018].
- [7] "SP 800-37 Rev. 1, Applying RMF to Federal Info Sys: Security Life Cycle Approach | CSRC", *Csrc.nist.gov*, 2010. [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final>. [Accessed: 31- Jul- 2018].
- [8] "NVD - 800-53", *Nvd.nist.gov*, 2018. [Online]. Available: <https://nvd.nist.gov/800-53>. [Accessed: 31- Jul- 2018].
- [9] "SP 800-53A Rev. 4, Assessing Security & Privacy Controls for Fed Info Sys & Orgs | CSRC", *Csrc.nist.gov*, 2014. [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-53a/rev-4/final>. [Accessed: 31- Jul- 2018].

- [10] "SP 800-60 Vol. 2 Rev. 1, Mapping Information/System Types to Security Categories | CSRC", *Csrc.nist.gov*, 2008. [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-60/vol-2-rev-1/final>. [Accessed: 31- Jul- 2018].
- [11] "FIPS 200, Minimum Security Requirements for Federal Info and Info Systems | CSRC", *Csrc.nist.gov*, 2006. [Online]. Available: <https://csrc.nist.gov/publications/detail/fips/200/final>. [Accessed: 31- Jul- 2018].
- [12] "FIPS 199, Standards for Security Categorization Federal Info and Info Sys | CSRC", *Csrc.nist.gov*, 2004. [Online]. Available: <https://csrc.nist.gov/publications/detail/fips/199/final>. [Accessed: 31- Jul- 2018].
- [13] "Federal Information Security Management Act", *Dni.gov*, 2018. [Online]. Available: <https://www.dni.gov/index.php/ic-legal-reference-book/federal-information-security-management-act>. [Accessed: 31- Jul- 2018].
- [14] "SP 800-66 Rev. 1, Introductory Guide for Implementing the HIPAA Security Rule | CSRC", *Csrc.nist.gov*, 2008. [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-66/rev-1/final>. [Accessed: 31- Jul- 2018].
- [15] "Understanding difference between Cyber Security & Information Security", *Cisoplatform.com*, 2016. [Online]. Available: <http://www.cisoplatform.com/profiles/blogs/understanding-difference-between-cyber-security-information>. [Accessed: 31- Jul- 2018].