Managing Advanced Threats in the Digital Age

Addressing security, risk and compliance for U.S. Public Sector executives

John W. Lainhart
Partner
Cybersecurity, Governance, & Privacy
IBM Global Business Services

Christopher Ballister
Associate Partner
Cybersecurity, Governance, Privacy, & Risk
IBM Global Business Services

Managing Advanced Threats in the Digital Age

Addressing security, risk and compliance for U.S. Public Sector executives

Table of Contents

Introduction 3
External threats 4
Internal threats 4
Compliance requirements 5
A holistic security intelligence approach 5
A three-point plan for the C-Suite 8
Building “security intelligence” in waves 12
Conclusion: Real risks demand an integrated C-suite 15
References 15

Introduction

Recent media attention has highlighted a series of high-profile security breaches such as the Department of Veterans Affairs (VA) data loss[1], the Office of Personnel Management (OPM) data hack[2], the Postal Service data breach[3], the F-35 military fighter jet data leak[4], and Presidential helicopter data hack[5] all of which have affected U.S. government agencies and their contractors, and severely damaged the public trust and confidence in our federal government. These attacks are relentless, aggressive and constantly evolving, and have clearly shown that federal agencies and organizations are struggling in managing security threats, despite the stricter security protocols that are often in place at government agencies. Cyber threats are "among the most urgent dangers to America's economic and national security," President Obama was quoted as saying in a Wall Street Journal article in 2015. No longer relegated to the IT organization of classical defensive products and tools within the enterprise firewall, security is now unquestionably a C-suite priority across an information ecosystem. Federal agencies and organizations need to move toward a more systematic and proactive approach to addressing evolving security threats and managing compliance requirements in today's economy.

As the world has become more digitized and interconnected, U.S. federal government agencies and organizations have also become more electronically digitized, performing public services over the internet, and as a result, the door to emerging threats and leaks has opened wider. Today, there are more than three billion individual Internet users and seven billion mobile-cellular phone subscriptions.[6] More than 50 billion objects are expected to be digitally connected by 2020, including cars, appliances and cameras.[7] Intensifying this complex mix, the amount of digital information created and replicated in the world will grow to an almost inconceivable 35 trillion gigabytes by 2020.[8]

Not only has the amount of data increased, but the corresponding value of digital assets has increased as well. Sensitive healthcare and customer information, intellectual property and even the physical objects – devices, vehicles, and machinery-embedded with electronics, software, and network connectivity (commonly knowns as Internet of Things or IoT) are all increasingly found to collect and exchange critical data. Attacks that affect these assets are much more likely to have a material impact on the entire organization, as opposed to simply the IT department. Take, for example, the hacking of the Ukrainian electrical grid where a cyber attack brought down critical infrastructure and resulted in power outages for over 225,000 Ukrainians.[9] This incident demonstrates that targeted action against an organization's technological infrastructure can clearly impact critical operations.

Other factors are making it critical for enterprises to change how they manage security and compliance as well. The valuable data embedded within organizations is a target of people who attack systems, whether for criminal reasons such as economic gain, personal reasons such as revenge or frustration, or political reasons such as terrorism. The damage to information and its processing infrastructure is occurring more often and with a high degree of "professionalism" in increasingly organized ways.

New technologies also introduce new risks, in fact, businesses are adopting cloud and mobile technologies at unprecedented rates. This influx of new innovation, technologies, and end-points push more and more business transactions outside company walls and

completely transform enterprise security as we know it. As the traditional network perimeter around the data center permanently dissolves, it is more difficult to defend an organization's data from the increasing gaps in security, and to verify that users accessing data are authorized and have appropriate rights to the data being accessed.

So it has become more important, yet more difficult, to secure and protect critical information and related assets. No longer can enterprise security programs rely on "if it's not broke, don't fix it." The bad guys could already be inside your systems, stealing your data or probing to get in. Security programs need effective protection of valuable information and prevention of breaches, and to comply with the increasing federal compliance requirements. Security has quickly ascended the C-level attention scale, and developing *security intelligence* – the ability to proactively predict, identify and react to potential threats – is undeniably taking on a new priority in the digital age.

Security challenges are greater than ever

With the massive increase in data, technologies, devices and connections, security challenges are increasing in number and scope. Security has become a multidimensional threat, especially in the federal space. The challenges fall into three major categories: external threats, internal threats and compliance requirements.

External threats

The Nation faces a proliferation of external attacks against major companies and government organizations. In the past, these threats have largely come from individuals working independently. However, these attacks have become increasingly more coordinated, and launched by groups ranging from criminal enterprises to organized collections of hackers to state-sponsored entities. Attackers' motivations can include profit, prestige, political agenda or espionage. These attacks target ever-more critical organizational assets, including citizen databases, intellectual property, and even physical assets that are driven by information systems.

These external attacks have significant consequences, resulting in IT, legal and regulatory costs. For example, the theft of OPM background investigation data on millions of federal employees and contractors has created a massive threat to U.S. national security that will last for decades and cost billions of dollars to monitor [10]. Many of these attacks use sophisticated tactics, techniques and procedures, and take place slowly but persistently over time, masked as normal activity. For example, the Department of Veteran Affairs' database has been hacked numerous times by at least eight foreign organizations in recent years[11, 12]. These threat vectors known as Advanced Persistent Threat (APT) require specialized continuous monitoring methods to detect threats and vulnerabilities prior to breaches or loss of sensitive data.

Internal threats

In many situations, breaches in information security are not perpetuated by external parties, but by insiders. Insiders today can be employees, contractors, consultants and even business partners and service providers. These breaches range from careless behavior and administrative mistakes (such as giving away their passwords to others, losing back-up tapes or laptops or inadvertently releasing sensitive information), to deliberate actions taken by

disgruntled employees. As the F-35 and some of the OPM background investigation leaks have regrettably demonstrated, your organizations are only as safe as each of your business partners, suppliers, or contractors are reliable.

These actions can lead to harm as or more dangerous than external attacks. For example, the Wikileaks incident, which involved the unauthorized release of classified records, has reportedly cost the U.S. government millions of dollars and damaged relations with foreign governments around the world.[13] And the Snowden breach of NSA classified records is another example of damaging relations with foreign governments around the world and even worse consequences to the U.S. intelligence community.[14]

Compliance requirements

Public Sector enterprises, federal agencies and organizations in particular, face a steadily increasing number of federal, industry and local mandates related to security, each of which have their own standards and reporting requirements. These many mandates include the Federal Information Security Management Act (FISMA), the Privacy Act, National Institute of Standards and Technology (NIST) Standards and Special Publications (SP), Office of Management and Budget (OMB) mandates, Federal Acquisition Regulation (FAR) and (Defense Federal Acquisition Regulation) DFAR clauses, Federal Risk and Authorization Management Program (FedRAMP), Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health (HITECH), various state privacy/data breach laws, IRS Publication 1075, Statement on Standards for Attestation Engagements (SSAE) No. 16, COBIT®, various ISO/IEC international standards, and European Union (EU) privacy directives, etc. Complying with these requirements often takes a significant amount of time and effort to prioritize issues, developing appropriate policies and controls, and monitoring compliance.

A holistic security intelligence approach

Security threats and compliance requirements will have a significant impact on the ability of individuals in the public sector C-suite to deliver on their key priorities. As technology plays an increasingly important role, the challenges associated with information security go well beyond the province of the CIO. For example, 70% of executives expressed concern about cloud and mobile security. [15] Theft or loss of mobile devices, privacy concerns associated with cloud, and accidental sharing of sensitive data are some of the key fears. The discussions with more than 13,000 C-suite executives since 2008 show that each member of the executive team is impacted by security issues (see Figure 1).

	CEO	CFO/COO	CIO	CHRO	CMO
CxO priority	• Maintain competitive differentiation	• Comply with regulations	• Expand use of mobile devices	• Enable global labor flexibility	• Enhance the brand
Security risks	• Misappropriation of intellectual property • Misappropriation of business sensitive data	• Failure to address regulatory requirements	• Data proliferation • Unsecured endpoints and inappropriate access	• Release of sensitive data • Careless insider behavior	• Stolen personal information from customers or employees
Potential impact	• Loss of market share and reputation • Criminal charges	• Audit failure • Fines, restitutions and criminal charges	• Loss of data confidentiality, integrity and/or availability	• Violation of employee privacy	• Loss of customer trust • Loss of brand reputation

Source: Over 13,000 face-to-face executive interviews conducted as part of IBM Institute for Business Value C-level studies.

Figure 1: **Addressing security and compliance needs is a priority across the C-suite.**

Responsibilities for security issues that may have been more clearly delineated in the past now overlap organizational silos, as does the potential damage if things go wrong. Although different federal agency executives do need to have higher priorities for some security challenges than others, enterprises cannot afford to ignore the need to act in a cohesive way to address today's security risks. Most classic defensive weapons of cyber security and traditional information assurance approaches are backward-looking, and hence lag in their ability to protect against, and respond to, emerging or evolving threats. Public sector enterprises, and federal agencies and organizations in particular, now need to modernize security approaches beyond the perimeter-focused "moats and walls" approach to a holistic and proactive security approach that focuses on "using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes,"[16] For example, public sector enterprises should emphasize detection, identification, protection, response, supply chain transparency, security intelligence, predictive analysis, data encryption, and a "zero trust network" philosophy[17]. The integrated and intelligent approach provides effective security protection and risk management of the enterprise ecosystems through continuous monitoring of critical systems and high value data, advanced analytics and security intelligence (see Figure 2).

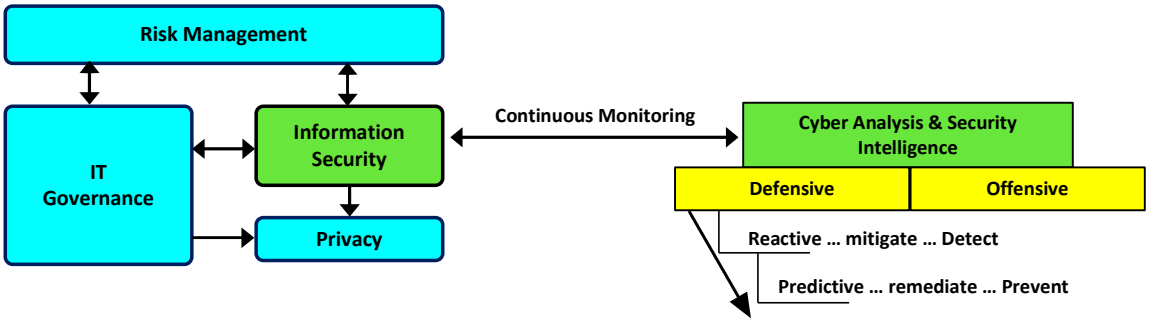


Figure 2: A holistic proactive security management approach.

- ***Risk Management*** identifies critical business processes that are most important to an agency's mission success, as well as threats and vulnerabilities that can impact critical business processes. Information security risk management needs to be part of the organizational culture and needs to be managed through an organization-wide approach with risk-informed and risk-based policies, processes and procedures. NIST SP 800-37, Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach is a Joint Task Force Transformation Initiative developed by an Interagency Working Group with representatives from the Civil, Defense, and Intelligence Communities in an ongoing effort to produce a unified information security framework for the federal government. This guide transforms the traditional Certification and Accreditation (C&A) process into the six-step Risk Management Framework (RMF).
- ***Information Technology (IT) Governance*** is a key enabler of successful cybersecurity protection. It provides the consistency, processes, standards, and repeatability needed for effective IT operations at the lowest possible cost within compliance requirements. IT Governance must be part of Enterprise Governance, a discipline that addresses all stakeholder needs, conditions and options to ensure they are evaluated for determining balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives.[18] On October 21, 2008, OMB Memorandum M-09-02 required that each agency have in place an Information Technology Management Structure and Governance Framework. So not only is it the right thing to do but it is backed up by an OMB mandate. Consistent and standardized security and privacy processes, controls and technology configurations support better protection at a lower cost.
- ***Information Security*** is a program managed by the Department/Agency Chief Information Security Officer (CISO) according to Federal Laws and Directives such as FISMA, OMB directives and memorandums, and NIST standards and special publications. Information security encompasses efforts to protect data and information systems from inappropriate access, manipulation, modification, and destruction. NIST's *Framework for Improving Critical Infrastructure Cybersecurity* focuses on using business drivers to guide cybersecurity activities while considering cybersecurity risks as part of the organization's risk management processes. NIST SP 800-53r4 *Security and Privacy Controls for Federal Information Systems and Organizations* provides a catalog of security and privacy controls for federal information systems and organizations. It includes a process for selecting controls to protect

organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors. The controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk. NIST SP 800-53r4 was also issued by an interagency working group with representatives from the Civil, Defense, and Intelligence Communities. In order for the information security program to achieve an acceptable level of risk to operate, IT Governance must incorporate a minimal level of maturity.

- ***Privacy*** provides, within a secure enterprise, controls to ensure that only properly designated personnel access information governed under privacy laws, and encompass efforts to protect an individual's ability to determine how their personal information is collected, used, stored, and disclosed. Information security and IT Governance directly impact the success of a privacy program. Privacy cannot exist without information security. Privacy must be considered in all information security programs -- the NIST Cybersecurity Framework includes a "Methodology to Protect Privacy and Civil Liberties" (Section 3.5), which specifically addresses individual privacy and civil liberties implications that may result from cybersecurity operations. NIST SP 800-53r4 includes "Appendix J PRIVACY CONTROL CATALOG: PRIVACY CONTROLS, ENHANCEMENTS, AND SUPPLEMENTAL GUIDANCE," which specifically provides a structured set of controls for protecting privacy and serves as a roadmap for organizations to use in identifying and implementing privacy controls concerning the entire life cycle of Personally Identifiable Information (PII), whether in paper or electronic form. Finally, privacy must be part of the organization's IT Governance program to ensure that it is adequately addressed in all discussions where PII is involved.
- ***Continuous monitoring*** (required by OMB and NIST mandates) ***with cyber analytics*** proactively highlights risks and identifies, monitors and addresses threats. As agencies and organizations bolster their security defenses, security intelligence plays an increasingly important role to develop actionable insights and help identify, in a near real-time basis, internal and external threats, including advanced persistent threats, while implementing governance and automated enterprise risk processes to meet compliance requirements.
- ***Collaboration and information sharing*** across different functional components within the approach, and organizationally across federal agencies and organizations and stakeholders are critical, and highly encouraged and supported by the approach, to ensure that accurate, current information and insights are being distributed, communicated, and consumed to improve security posture before a security breach occurs.

A three-point plan for the C-Suite

C-suite executives of public sector enterprises, and federal agencies and organizations, need to take three important steps toward building security intelligence:

- **Get informed.** Take a structured and collaborative approach to assessing business and IT risks across the extended enterprise.
- **Get integrated.** Integration is the new foundation that puts security into context and automates protection through unifying existing tools and infrastructures to reduce the complexity, improve the efficacy, and lower the cost. Integration implements and enforces security excellence across the extended enterprise.

- **Get intelligent.** Intelligence is the new defense that uses deep analytics and real-time security intelligence to proactively highlight risks, timely identify, monitor and address threats and disrupt targeted attacks, and make knowledgeable decisions.

1. Get informed

Getting informed involves assessing and addressing IT security risk as part of the larger Enterprise Risk Management Framework as guided by the NIST Risk Management Framework for federal agencies and organizations.

The NIST Risk Management Framework, supplemented by other NIST guidelines, provides a structured approach and guidelines to assessing business and IT risks. The Risk Management Framework:

- Promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes;
- Encourages the use of automation to provide senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational information systems supporting their core missions and business functions;
- Integrates information security into the enterprise architecture and system development life cycle;
- Provides emphasis on the selection, implementation, assessment, and monitoring of security controls, and the authorization of information systems;
- Links risk management processes at the information system level to risk management processes at the organization level through a risk executive (function); and
- Establishes responsibility and accountability for security controls deployed within organizational information systems and inherited by those systems (i.e., common controls).

Case example:
IT technology risks and security challenges spark IT security and governance revamp

The U.S. Department of Veterans Affairs was facing significant challenges for the functional capacity of the IT systems and overall security of the systems spread geographically across the continent. The Congress and the Government Accountability Office, were concerned about the age, efficiency and security of the Department's IT systems, and had been calling for a major IT realignment and upgrade, especially, after the security breach that compromised confidential information for about 26.5 million veterans.

As a result, the Department implemented a comprehensive, strong IT governance program based on industry best practices, as well as a system to help ensure the new controls were regularly updated and improved. The process began with a comprehensive evaluation of the Department's security and entire system of controls, including IT general controls, application controls and IT governance. The organization's information security governance was assessed, including reviewing security processes and writing or updating policies, standards and procedures.

The overhaul at the Department started with the creation of an IT governance plan and the adoption of a full set of IT best practices that the agency ultimately adopted, resulting in a more secure, integrated, reliable and responsive IT environment. The Department followed

the best practices and federal guidelines, and used a structured approach to review and assess the business and IT risks across all business units and systems aimed at efficiently delivering high quality health care services and other benefits to veterans, while supporting the thousands of health care professionals who work for the agency. Under the plan, the agency centralized all it budgeting, planning and development, while placing a premium on encrypting, securing and accounting for every piece of computer hardware in the system.

The agency successfully implemented the IT governance program that directs and controls the enterprise in order to achieve its missions with strong risk, security and privacy management. The agency also made substantial progress in consolidating planning, budgeting and personnel and in securing all the information contained in its massive IT systems. The success story and its well-informed IT governance, risk and security management model has been used by other large-scale public sector entities to modernize and consolidate similarly unwieldy and dispersed systems.

2. Get integrated

Security does not stop at the organizational boundaries. Integration is the new foundation that puts security into context and automates protection through unifying existing tools and infrastructures to reduce the complexity, enhance the efficacy, and lower the cost. Integration implements and enforces security excellence across the extended enterprise.

Federal agencies need to implement, collaborate, and enforce security excellence across the extended enterprise. This includes involving key stakeholders, including:

- Customers – Develop and communicate personal information policies. Remain transparent and rapidly address privacy breaches.
- Employees and Contractors – Set clear security and privacy expectations. Provide education to identify and address security risks. Manage the access and usage of both systems and data.
- Partners – Work with partnering organizations and service providers across the supply chain to develop and implement security standards. Report on and manage risks, including security incidents, as a normal part of business operations.
- Auditors – Align enterprise and IT risk. Contribute to controls frameworks. Conduct regular reviews of regulatory and enterprise policies.
- Regulators – Manage regulatory risks and demonstrate compliance with existing regulations. Review and modify existing controls based on changing requirements.

Case example:
Effective, integrated security management aids federal regulatory compliance and improves organizational security posture

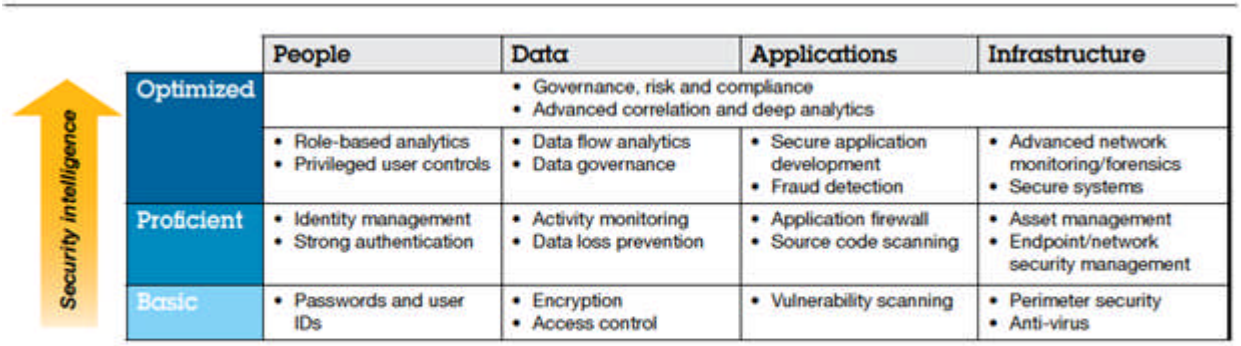
The U.S Department of Health and Human Services' Centers for Medicare and Medicaid Service has been faced with a multitude of regulatory requirements and security audits each year, such as those relating to FISMA and HIPAA. The agency wanted to proactively manage risk, implement and maintain prudent controls for its large-scale, complex and mission critical healthcare integrated general ledger financial accounting program, instead of having to react to each federal audit as a one-off. In addition, it strived to improve the organizational security posture and stay ahead of and reduce the impact these audits had on normal operations.

The solution involved an overhaul of the agency's IT security management program structure. As part of this undertaking, the agency instituted IT security and governance controls required by federal regulations that span all of its program operations and processes, and integrated all facets of the program environment, including users, contractors, partners, service providers, applications, systems, processes, and infrastructure, across the extended supply chain and service operations. The risk-informed and adaptive process was used, which identified risk and defined the control framework by establishing, implementing and operating the security controls and governance procedures; testing them; and, finally, monitoring, correlating and reporting outcomes.

The security controls implementation and maintained not only helped the agency monitor and manage compliance with federal regulations and successfully pass relevant federal audits, they also helped the agency align business and IT and manage the risk and security posture with more complete context and insights to make informed decisions for corrective actions. The agency now has a more efficient, consistent response to audits – and has reduced the amount of effort needed for audit response by approximately half, and more importantly, resulted in a more robust security posture.

3. Get intelligent

Security Intelligence is the new defense that uses cognitive-based systems, deep analytics and real-time security intelligence to proactively highlight risks, timely identify, monitor and address threats and disrupt targeted attacks, and make informed decisions. As public sector enterprises and federal agencies bolster their security defenses, the use of predictive analytics plays an increasingly important role (see Figure 5). They can do sophisticated correlation to detect advanced persistent threats, have a sense of governance and have automated enterprise risk processes in place – critical building blocks for enabling security intelligence.



	People	Data	Applications	Infrastructure
Optimized		• Governance, risk and compliance • Advanced correlation and deep analytics		
	• Role-based analytics • Privileged user controls	• Data flow analytics • Data governance	• Secure application development • Fraud detection	• Advanced network monitoring/forensics • Secure systems
Proficient	• Identity management • Strong authentication	• Activity monitoring • Data loss prevention	• Application firewall • Source code scanning	• Asset management • Endpoint/network security management
Basic	• Passwords and user IDs	• Encryption • Access control	• Vulnerability scanning	• Perimeter security • Anti-virus

Figure 5: **Using analytics to proactively highlight risks and identify, monitor and address threats.**

Case example:
Analytics help upgrade security risk capabilities

The Department of Transportation's Federal Aviation Administration (FAA) developed a system to protect large digital and physical computer infrastructures such as the nation's

civilian aviation system from cyberattacks. The project introduced first-of-a-kind security analytics technologies and entirely new approaches to safeguard against hacking, botnets, cyber spy networks and other cyber threats. The flexible model looked retrospectively at event occurrences and system compromises, and was able to correlate historical traffic patterns with dynamic data from monitors, sensors and other devices capturing information about network traffic and user activity in real time.

Specific system capabilities included the ability to:

- Continuously aggregate and process web-based traffic, data flowing through FAA networks, and information from security devices such as monitors and sensors in real time
- Look retrospectively at event occurrences and security alerts and correlate to dynamic user activity on the networks to gain better insights about the security posture of networks in real time
- Increase situational awareness by continually monitoring network workload characteristics
- Visually and instantly represent information on event occurrences and malware findings via customized dashboards
- Store real-time data in a data warehouse for later analysis and supervised learning

The combination of historical and dynamic analysis served as an additional filtering process to help the FAA eliminate false positives and spend more time identifying specifics about events or incidents of interest. The additional benefits of blending historical and dynamic analysis allowed threats to be identified in a predictive manner that would normally go undetected until an incident is identified and reactive damage control must be initiated.

Building "security intelligence" in waves

To address both the proliferation and magnitude of risks, organizations need to consider a more automated, proactive approach to security. In short, they need to incorporate security intelligence as an essential part of the business. This requires a comprehensive approach involving a range of issues, such as physical security, data classification, employee awareness and control.

In many organizations, security intelligence evolves across three levels. These represent a shift from manual approaches to the use of increasingly automated processes for identifying, tracking and addressing threats. The trend is toward more proactive anticipation of security issues rather than reactive approaches (see Figure 3).

- Basic – Organizations focus on employing perimeter protection, which regulates both physical and virtual access. Perimeter protection provides input into manual reporting of incidents and violations. Enterprises at the Basic level are deploying firewalls, antivirus, access control and manual reporting, which are valuable first steps. However, they operate in a reactive and manual operating mode with little insight on their actual security posture.

- Proficient – Security is layered into the fabric of IT applications and business operations. This wave includes incorporating security into key applications, databases and business processes. At the Proficient level, security is becoming more comprehensive; but at the same time, complexity is added to an organization's security efforts. As a result, enterprises still fall short regarding their security intelligence, as security becomes more diffuse and less coordinated.
- Optimized – Organizations use predictive and automated security analytics to drive toward security intelligence. Security is Optimized as this wave includes the profiling of past intrusions, employee activity and other data sources to anticipate where potential breaches could occur and prevent occurrences before they happen.

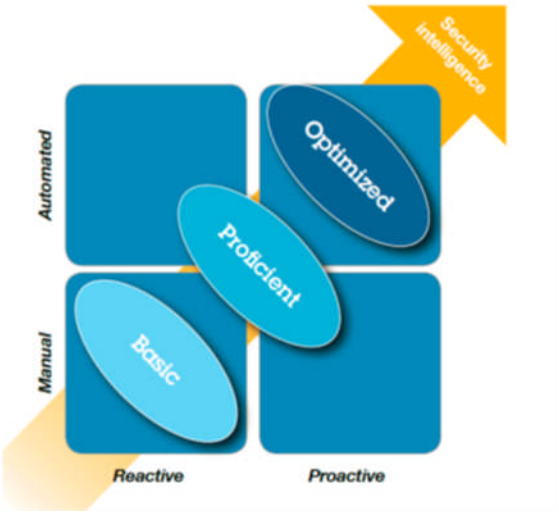


Figure 3: A structured, three-level approach to building security intelligence.

Using cyber analytics to proactively highlight risks and identify, monitor and address threats and vulnerabilities helps to achieve predictive and preventive cybersecurity capabilities. However, cyber analytics can also be greatly enhanced, using cognitive-based systems to build knowledge and learn, understand natural language, and reason and interact more naturally with human beings. Cognitive computing has the ability to tap into, and make sense of, all the security data that has previously been dark. It also is able to put content into context with confidence-weighted responses and supporting evidence. It can quickly identify new patterns and insights and reduce false positives. As a result, security professionals can provide more precision, speed and accuracy in stopping cyber attacks.

Specifically, cognitive solutions have these three critical capabilities that are needed to achieve security intelligence:

1. Engagement: These systems provide expert assistance by developing deep domain insights and presenting the information in a timely, natural and usable way.
2. Decision: These systems have decision-making capabilities. Decisions made by cognitive systems are evidence-based and continually evolve based on new information, outcomes and actions.
3. Discovery: These systems can discover insights that perhaps could not be discovered otherwise. Discovery involves finding insights and connections and understanding vast amounts of information, including structured data and most importantly, unstructured data, not previously available.

Moving up the levels to Optimized, adds an additional layer of preparation against both inadvertent and deliberate security incidents. To identify and close security gaps throughout the enterprise ecosystem, organizations will need to explore and exploit analytics capabilities to meet their most pressing needs. An in-depth evaluation of four "security domains" can

guide organizations toward security intelligence by systematically improving governance, risk management and compliance (see Figure 4).

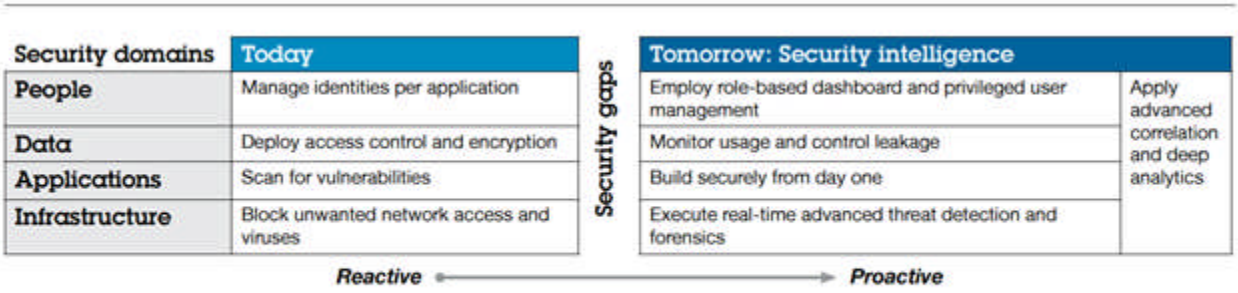


Figure 4: **A balanced approach is needed to manage physical, technological and human assets.**

- People – Switch from controlling access on an application-by-application basis via passwords to a role-based approach that controls user access through dashboards, privileged user controls and user behavior analysis.
- Data – Move beyond basic access controls and encryption methods to protect data by improving data governance, protecting high value data, and managing data usage and flow.
- Applications – Evolve from reliance on scanning for vulnerabilities in existing applications to detecting fraud, designing security into new applications, real time source scanning, and anomaly detection.
- Infrastructure – Replace reactive methods like blocking unauthorized access and viruses with proactive methods that secure systems by enabling advanced network monitoring and forensics and taking advantage of cognitive-based systems.

Are you building security intelligence?

Based on the potential for threats, and the opportunities to mitigate these risks using more advanced security intelligence, organizations should consider their answers to the following questions:

Across security domains

- What is your plan to assess your security risks?
- How are you able to detect threats and report compliance across domains?
- Do you have a log retention and audit capability?
- Which processes do you use to handle incident response and disaster recovery?
- How do you involve key internal and external stakeholders in security matters?

People

- To what extent have you rolled out an identity program?
- How do you know what authorized users are doing?
- What is your plan to automate identity and role-based management?

Data

- In what ways have you classified and encrypted sensitive data?

- How do you know if sensitive data leaves your network?
- How do you monitor access to data, especially privileged access?

Applications

- How is security built into your application development process from day one?
- How do you regularly test your website for vulnerabilities?
- What is your approach to test legacy applications for potential exposures?

Infrastructure

- How do you promptly patch connected devices?
- In what ways do you monitor in- and out-bound network traffic?
- How are you building security into new initiatives (such as cloud, mobile and the like)?

Conclusion: Real risks demand an integrated C-suite

In today's increasingly complex and interconnected world, risks are real and increasing exponentially. An enterprise that delegates security matters solely to the CIO is compounding its risk factors. More than ever, each member of the enterprise's leadership owns a significant stake – and a powerful role – in securing the data and intellectual capital that flows through the organization. There is one common denominator – security today is more than a purely technical issue. Rather it requires a frank discussion about risk, investment and taking a preventative approach to security issues.

The ultimate goal is to prevent security risks from impacting high value data, ultimately public trust and confidence by:

- Knowing the impact and risk implications of adverse security events and breaches
- Evaluating the impact related to IT system(s) disruptions on ongoing operations
- Understanding the fallout effects of information security lapses within the enterprise and across the entire Federal government.

Clearly, not every potential risk and contingency can be addressed in a cost-effective manner. Organizations must prioritize the business impact of potential risks instead of trying to protect against every conceivable threat. However, this prioritization depends on input from multiple C-suite executives who provide unique perspectives on their particular disciplines.

References

1 EPIC.org, "Veterans Affairs Data Theft." https://epic.org/privacy/vatheft/

2 Levine, Mike and Date, Jack. "22 Million Affected by OPM Hack, Officials Say." ABC News. July 9, 2015. http://abcnews.go.com/US/exclusive-25-million-affected-opm-hack-sources/story?id=32332731

3 Chiacu, Doina. "U.S. Postal Service data breach may compromise staff, customer details." REUTERS. November 10, 2014. http://www.reuters.com/article/us-cybersecurity-usps-idUSKCN0IU1P420141110

4 Bender, Jeremy. "Chinese Data Theft Could Be 'Disastrous' For The US Military's Most Expensive Fighter Jet." Business Insiders. March 14, 2014. http://www.businessinsider.com/stolen-f-35-technology-used-china-fighter-2014-3

5 Moscaritolo, Angela. “Blueprints of Obama's Marine One helicopter leaked on P2P.” SC Magazine. March 2, 2009. http://www.scmagazine.com/blueprints-of-obamas-marine-one-helicopter-leaked-on-p2p/article/128109/

6 International Telecommunications Union. “The key 2005-2015 ICT data for the world.” http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2015/ITU_Key_2005-2015_ICT_data.xls

7 Ericsson. “More than 50 billion connected devices – taking connected devices to mass market and profitability.” February 14, 2011. http://www.ericsson.com/news/110214_more_than_50_billion_244188811_c

8 IDC. “Digital Universe Study,” sponsored by EMC. May 2010.

9 Gunter, Chase. “Protecting physical infrastructure with cyber.” FCW – The business of Federal Technology. April 27, 2016. https://fcw.com/articles/2016/04/27/nppd-cyber-infrastructure.aspx?s=fcwdaily_280416

10 Russell, Richard A. “What OPM isn't saying about the true cost of data breaches.” Fedscoop. July 10, 2015. http://fedscoop.com/what-opm-isnt-saying-about-true-cost-of-data-breaches

11 Associated Press. “Official: rampant hacking at VA.” POLITICO. June 4, 2013. http://www.politico.com/story/2013/06/computer-hacking-veterans-affairs-department-092227

12 Brino, Anthony. **“**VA hacked by foreign orgs, security needs standardization.” Government Health IT. June 5, 2013. http://www.govhealthit.com/news/va-hacked-foreign-orgs-security-needs-standardization

13 Fildes, Jonathan. “What is Wikileaks?” BBC. December 7, 2010. http://www.bbc.co.uk/news/technology-10757263

14 Gellman, Barton, Blake, Aaron, and Miller, Greg. “Edward Snowden comes forward as source of NSA leaks.” The Washington Post. June 9, 2013. https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html

15 IBM Global C-Suite Study. http://www-935.ibm.com/services/c-suite/study/

16 NIST. “Framework for Improving Critical Infrastructure Cybersecurity” Version 1.0. February 2014.

17 IT Alliance for Public Sector (ITAPS), ITI. “OPM-OMB-NSC Recommendations.” July 2015.

18 COBIT5®, ISACA, 2012. http://www.isaca.org/cobit/pages/cobit-5-framework-product-page.aspx.