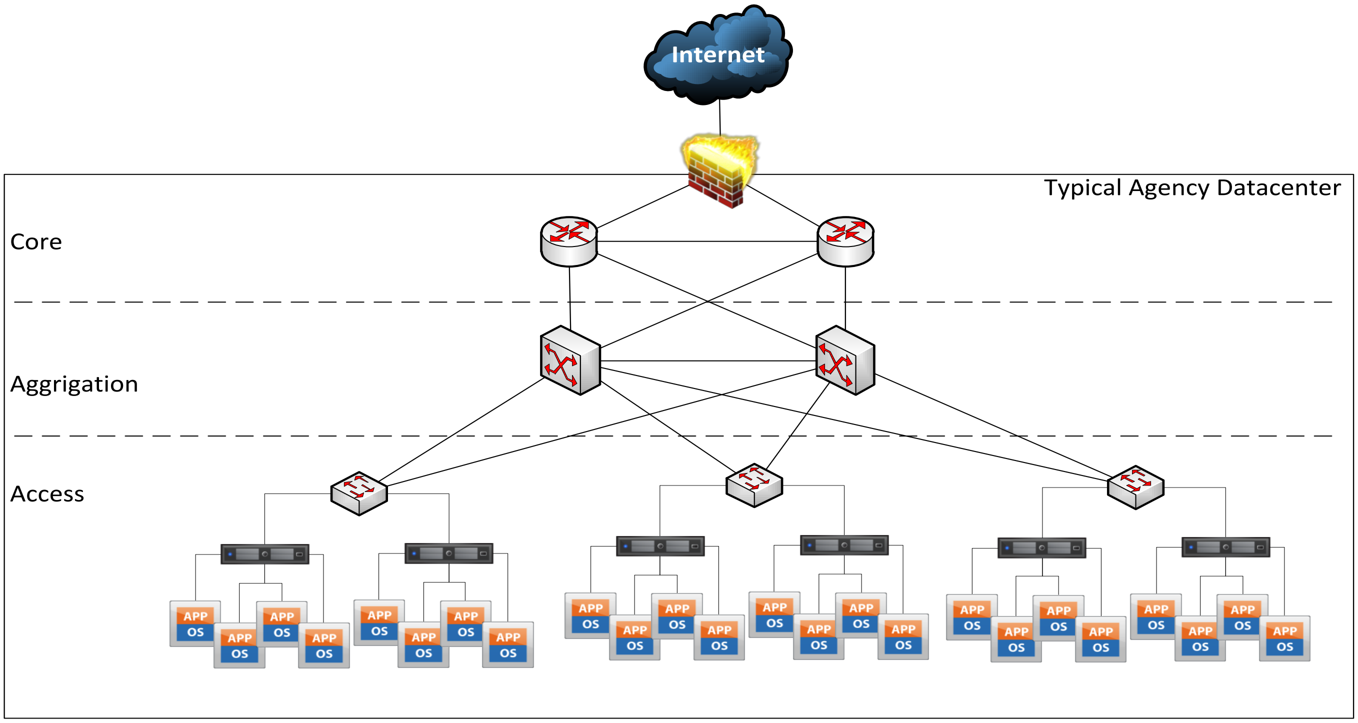
IT Alliance for Public Sector
A Division of ITI

Appendix of Supporting Materials

Sophisticated and aggressive cyber-attacks by criminal entities and foreign governments represent a clear and present security threat to businesses and governments alike. Mitigating these threats requires a change in the way we build, operate, and secure data center networks.

Like an ancient city, data center networks have traditionally been built on the concept of a strong perimeter defense. For example, firewalls (often called "network devices") are positioned at the data center perimeter to prevent intruders from entering the network and gaining access to data. Like a siege on an ancient city, there is typically a common single point of firewall failure that allows a breach and entry into data center. This creates a strong outer defense, but there is no network resiliency once the attack is inside. Once the intruder has penetrated the firewall there is no simple, quick, or automated means to stop malicious activity within the data center without disruption to the agency's mission.

The figure below depicts a typical data center that relies on perimeter security to protect the data from unauthorized users. In this example, the perimeter firewall (the red brick wall on fire) is analogous to the wall around an ancient city. The primary function of that wall is to deny unauthorized entry by anyone that does not belong in the "city"/data center. However, once the wall is breached/hacked, the intruder is free to move throughout the city unabated. This is called "lateral movement" within the network.



In the past, data centers were able to deploy perimeter security systems around the data center with a 1:1 relationship between physical devices (e.g. one firewall to one server). Today, technology has advanced to enable the ability to utilize previously wasted resources within the datacenter by consolidating unused resources into a common "pool" for all to use. This pooling of common resources is known as "virtualization." Attempting a 1:1 ratio in today's virtualized data center is not practical due to the complexity and cost – especially when there is a complimentary and far more cost efficient "zero-trust" solution available.

A zero-trust environment prevents unauthorized lateral movement by increasing compartmentalization or segmentation within the data center. To build on the analogy above, compartmentalization is equivalent to securing each home in the city with biometric locks while eliminating access between homes. Therefore, limiting an intruder's ability to move around freely within the city/data center significantly contains the magnitude of a perimeter security breach.

Zero-trust security represents a new approach to data center security that compliments and enhances traditional perimeter security. You still have the wall around the city, but now every home has its own, automated security system as well. Enabling a zero-trust environment uses software to secure the interior exit/entry points of each system within the data center to the most granular level possible. This approach effectively segments the networks to enable a great security posture that was never possible before now. This security posture allows networks to continue to operate and maintains network resiliency. Also, zero-trust security and network segmentation allows entities to leverage existing infrastructure, and avoid expensive "tech-refresh" investments in additional perimeter security hardware.

The National Institute of Science and Technology

Developing a Framework to Improve Critical Infrastructure Cybersecurity

In Response to:

RFI# 130208119-3119-01

Submitted On: 04/08/2013

Prepared for:

The National Institute of Science and Technology (NIST) within the Department of Commerce (Commerce)

Submitted By:
Forrester Research, Inc.
60 Acorn Park Dr.
Cambridge, MA 02140

Phone: 703-584-2628
Fax: 617-613-5200
Point of Contact Mark Western,
Vice-President of Sales
E-mail: mwestern@forrester.com
www.forrester.com

NAICS: 519190
GSA Schedule: GS-35F-4900H
CAGE: 1W0J5
TIN: 04-2797-789
DUNS: 10-6765-928
Business Size: Large

Overview

In February 2013 President Obama's Cybersecurity Executive Order (EO) made public the clear and present danger of cyber warfare. The President called for the Federal Government and its Agencies to lead the fight against cyber criminals. As part of this call to action, President Obama asked the National Institute of Standards and Technology (NIST) to gather industry and Federal feedback to create a set of voluntary policies to help develop the US's cybersecurity framework.

In order to keep up with the continually changing cybersecurity landscape, the Federal Government and organizations in important industries such as finance, utilities, and Federal contractors must fundamentally shift the way in which they think about cybersecurity. The traditional mindset does not take into account the current environment; changes like mobility and big data have made "building stronger walls" an expensive farce that will not adequately protect networks.

To help answer the cybersecurity questions of today while allowing for proactive growth in the future, Forrester has outlined our proprietary "Zero Trust Model" (Zero Trust) of information security. Zero Trust changes the way that organizations think about cybersecurity and better protects valuable information while allowing for free interactions internally. The major benefits of Zero Trust to the Federal Government include:

- **Zero Trust is applicable across all industries and organizations** – It is an easy to implement way to improve safety that any organizations can implement.
- **Zero Trust is not dependent on a specific technology or vendor –** Zero Trust is a vendor neutral design philosophy that allows maximum flexibility to create architectures that meet specific demands.
- **Zero Trust is scalable** – Vital information is protected while public facing data travels freely.
- **There is no chance of violating Civil Liberties** – Zero Trust focuses on keeping internal data safe and would not result in any foreseeable encroachment on Civil Liberties.

The following is a brief overview explaining what the Zero Trust Model is, and why it is more applicable to the current discussion than traditional cybersecurity approaches. For additional information, please see **Appendix A: Relevant Forrester Articles**.

Corporate Experience

Founded in 1983, Forrester Research, Inc. (Forrester) is an American-owned, publically traded (NASDAQ: FORR), independent research and advisory firm that provides forward-thinking research and advice primarily to global leaders of Federal agencies, international Non-Global Organizations (NGOs), and $1 Billion+ companies. Forrester's mission is to help our clients succeed every day. We accomplish our mission with actionable research and advice that targets 17 key roles across organizations, including security and risk professionals. These roles focus on leaders in Information Technology (IT), Marketing and Strategy (M&S), and the Technology Industry (TI). George Colony, Forrester's current CEO and founder, based the company on five concepts that form our core values: Client, Courage, Collaboration, Service, Integrity, and Quality (3CSIQ). Thanks to these values, Forrester has continued to be profitable year over year, growing to over $292 million in 2012. Today Forrester serves a global network of over 3,000 organizations with actionable advice to help them overcome the complex challenges brought on by changes in the international IT market, best practices, and the ways that today's population use technology.

Forrester has maintained a Federal presence since 2001 and a formal Federal Practice with offices in the DC metro area since 2005. Since its inception, this practice has experienced consistent year over year income growth and our Federal Practice workforce has doubled. Currently, Forrester works with 86% of the Cabinet Level Departments and approximately 100 different Federal organizations. We also work with key Federal partners including major integrators and Federal IT policy leaders.

With a majority of our Federal team located in the DC area (in our Tysons Corner office), Forrester is able to provide ample onsite time during engagements. Forrester routinely brings Research Professionals onsite to Federal Agencies. As part of this effort, Forrester has an annual Research Professional Road Show that brings the most sought after Analysts to the Washington, DC area to speak with Federal Clients on Federal specific topics.

Forrester provides broad, global, analysis and experience regarding cybersecurity coupled with a deep understanding of how changes in the IT environment will affect the Federal Government's workforce and ultimately its mission.

Forrester's Security and Risk Principal Analyst John Kindervag is a 25-year veteran of the high-tech world. He is the leading expert in the areas of wireless security, intrusion detection and prevention, and voice over IP hacking. During John's tenure at Forrester he has developed Forrester's Zero Trust model of information security. Forrester's Zero Trust model will help the Government rethink how to approach defensive cybersecurity; rather than having to rely on constant vigilance alone. The Zero Trust model of information security will provide the Government with a modular and cost-effective approach to cybersecurity to protect vital industries and segments of the Government without layering additional technology on top of the flawed systems in place today. Zero Trust will require the Government to go through a state of transformation by eliminating the idea of a trusted network regardless of whether it is an internal or external network, and redesigning networks from the inside out. In the Zero Trust Model of information security, we assume that all traffic is untrusted. This approach demands that you build security into the DNA of your IT architecture by investing in situational awareness, and developing robust vulnerability and incident management capabilities. For more information regarding Forrester's Security and Risk Team, please see **Appendix B Relevant Team Biographies**.

Problem: Current Trust Models and Approaches Are Broken

There's an old saying in information security: "We want our network to be like an M&M, with a hard crunchy outside and a soft chewy center." This philosophy is widespread today, accompanied by the mantra "trust but verify." This mantra and M&M philosophy of information security is based on trust and the assumption that malicious individuals cannot pass the "hard crunchy outside." The thought process around this philosophy was that additional internal security measures were unnecessary because it was unlikely that an intruder would be able to get sustained access to a network, and it was also unlikely that they would be able to move from area to area once in an organization. In today's new threat landscape, this M&M and "trust but verify" model of information security is no longer an effective way of enforcing security.

One of the reasons to change is the explosion in mobile technology use. Mobile technology is more susceptible to theft and human error than traditional technology. A "trust but verify" approach does not compensate for these types of intrusions because the threat would come from what is a “trusted source.” In many cases, by the time organizations realizes that the source is no longer trusted, it is often too late.

Zero Trust takes into account the possibility of threats coming from internal as well as external sources and protects the organization from both types of threats. Cybersecurity must fully integrate with an organization’s network because organizations must contend with malicious insiders who are often in positions of “trust.” Data from Forrester’s annual Forrsights security survey shows that insiders (whether through malicious or accidental actions) were more likely than external attackers to be cause of breach across North American and European enterprises and SMBs (see Figure 1 below).

Once an attacker gets past the M&M shell of today’s networks, he has insider access to all the resources in the network. The Government has built strong perimeters, but well-organized cybercriminals have recruited insiders and developed new attack methods that stretch thin their current resources and penetrate current security protections used to protect important industries like defense, financial services, and utilities. To confront these new threats, cybersecurity professionals must eliminate the soft chewy center by making security ubiquitous throughout the network, not just at the perimeter.

In summary, “trust, but verify” is obsolete. Forrester has found that many cybersecurity professionals trust often but verify very little. In addition, “trust” simply does not apply to packets. Identity at the network level is merely an assertion of certain attributes that may be true or false, forged or real. However, all we can truly know about network traffic is what is contained in packets, and packets cannot tell us about the veracity of the asserted identity, let alone the intentions or incentives of the entity generating the packets.

Issues of trust aside, Zero Trust is better than traditional cybersecurity philosophies because it takes into account organizations’ desire to share data quickly. Zero Trust does not hold up the transfer of data so that it can be “verified.” It allows data to move freely, reducing the likelihood of siloing.

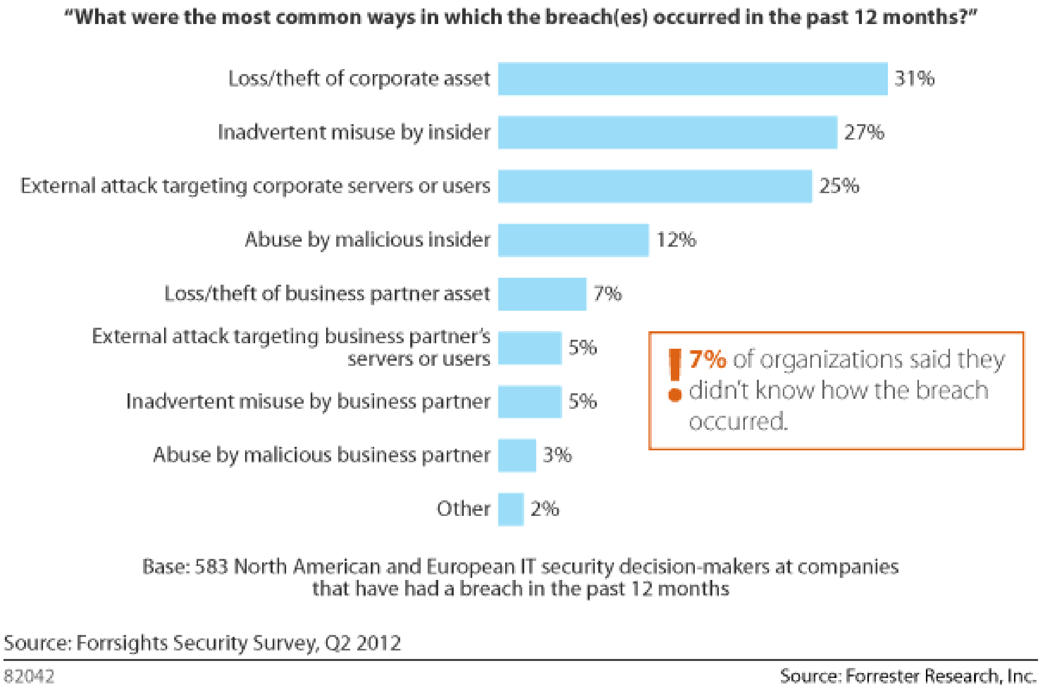


Figure 1. Our data shows that the main threat comes from within organizations, not outside

A New Approach: Introducing Forrester’s Zero Trust Model for Cybersecurity

The Zero Trust Model is simple: cybersecurity professionals must stop trusting packets as if they were people. Instead, they must eliminate the idea of a trusted network (usually the internal network) and an untrusted network (external networks). In Zero Trust, all network traffic is untrusted. The Zero Trust Model has three key concepts:

1. **Ensure all resources are accessed securely regardless of location.** Assume that all traffic is threat traffic until your team verifies that the traffic is authorized, inspected, and secured. In real-world situations, this will often necessitate using encrypted tunnels for accessing data on both internal and external networks. Cybercriminals can easily detect unencrypted data; thus, Zero Trust demands that security professionals protect internal data from insider abuse in the same manner as they protect external data on the public Internet.
2. **Adopt a least privilege strategy and strictly enforce access control.** When we properly implement and enforce access control, by default we help eliminate the human temptation for people to access restricted resources. Today, role-based access control (RBAC) is a standard technology supported by network access control and infrastructure software, identity and access management systems, and many applications. Zero Trust does not explicitly define RBAC as the preferred access control methodology. Other technologies and methodologies will evolve over time. What is important is the concept of minimal privileges and strict access control.
3. **Inspect and log all traffic.** In Zero Trust, someone will assert their identity and then we will allow them access to a particular resource based upon that assertion. We will restrict users only to the resources they need to perform their job, and instead of trusting users to do the right thing, we verify that they are doing the right thing. In short, Zero Trust flips the mantra "trust but verify" into "verify and never trust." Zero Trust advocates two methods of gaining network traffic visibility: inspection and logging. Many security professionals do log internal network traffic, but that approach is passive and does not provide the real-time protection capabilities necessary in this new threat environment. Zero Trust promotes the idea that you must inspect traffic as well as log it. In order to do so, network analysis and visibility (NAV) tools are required to provide scalable and non-disruptive situational awareness. NAV is not a single tool, but a collection of tools that have similar functionality. These NAV tools include network discovery tools for finding and tracking assets, flow data analysis tools to analyze traffic patterns and user behavior, packet capture and analysis tools that function like a network DVR, network metadata analysis tools to provide streamlined packet analysis, and network forensics tools to assist with incident response and criminal investigations.

Zero Trust Network Architecture Traits

Current designs merely overlay existing networks with more and more controls in an attempt to create a semblance of a secure network. We need to build networks from the inside out: Start with the system resources and data repositories that we need to protect as well as the places where we need to be compliant, and then build a network out from that.

To rethink the network requires a willingness to set aside preconceived notions about what the network should be and think about what the network could be. By taking network design down to the trust level, we can create the Zero Trust network. Zero Trust will enable security throughout your network by addressing three concepts that will empower secure networking in the future:

1. **Easily managed and segmented for security and compliance.** Compliance and performance issues demand a segmented network, but hierarchical networks are difficult to segment. This is because the focus on switch fabrics and high-speed backplanes does not provide a way to break apart the backplane for segmentation purposes. Some networkers advocate the use of virtual LANs (VLANs) for segmentation purposes, but they are highly insecure. Think of VLANs as the yellow line on the road. Traffic is not supposed to cross that yellow line, but nothing prevents a vehicle from doing so. In the same way, VLANs define a network traffic isolation policy, but they are not technologically capable of preventing a malicious actor from moving between VLANs and gaining access to privileged information. Therefore, new ways of segmenting networks must be created because all future networks need to be segmented by default.
2. **Built with multiple parallelized switching cores.** The traditional switch fabric is the bottleneck that keeps us from building inherently secure and efficient networks. A unified switch fabric and massive backplane are, in fact, antithetical to multicore processing and parallelization. The actual problem is the existence of the very switch fabric organizations so focused on, organizations must disabuse themselves of the notion that the network is all about the backplane, we will begin to think about networks in a completely different way. Having a several-hundred-gigabyte backplane on a core switch is of little value today because all those packets are going to different destinations, which reduces traffic efficiency. Modern laptops have multicore processors. If we use laptops as an example of distributed processing in which the OS provides centralized management, we can extrapolate that model to the network.
3. **Centrally managed from a single console.** In the early command-line days, centralized device management was not practical or possible. The prevailing solution was to combine numerous switches into a single chassis that shared the same backplane so that networking professionals could manage all the switches from a single device. Unfortunately, this creates traffic congestion as the network shoves all types of traffic onto the same road, regardless of destination. Organizations do not have to have all traffic aggregated together on the same backplane any longer. The need to manage better data created the idea of a massive backplane Central management of all networking elements is the key to creating the network of the future. In tomorrow's network, the centralized management solution becomes the network backplane.

How to Build a Zero Trust Network Architecture

The Zero Trust network architecture is a theoretical adaptation of the Zero Trust Model of information security. Not all of the technology and components described below are available today — at least not yet. While you cannot go out and simply buy a Zero Trust network, cybersecurity professionals can use the architectural design components of Zero Trust to help get past today's biases about how we should build networks and begin looking at network design from a new point of view. Key architectural components of Zero Trust include:

1. **An integrated "segmentation gateway" as the nucleus of the network.** A network segmentation gateway (SG) takes all of the features and functionality of individual, standalone security products (firewalls, IPS, WAF, NAC, content filtering gateways, VPN gateways, and other encryption products) and embeds them into the very fabric of the SG. By embedding a packet-forwarding engine, we have a device that can sit at the very center of the network. The SG's larger value lies in its ability to properly segment networks in a secure manner and build security into the very DNA of the network. This is a radical concept, because although it takes some of its inspiration from

traditional unified threat management (UTM) designs, an SG takes embedded security to the next level.

A UTM is a perimeter control. An SG becomes the nucleus of the network. To be successful, a segmentation gateway would need to be very high-speed, support multiple 10 Gig interfaces, and have the ability to provide QoS or packet shaping to maintain performance. As hardware components such as network processors and other silicon drop in price and increase in speed, vendors could potentially tune their existing devices to function much like the SG Forrester envisions. Vendors such as Palo Alto Networks, Xceedium, Fortinet, Crossbeam Systems, and Dell SonicWall all have innovative, high-speed products that are poised to function as segmentation gateways.

2. **Parallel, secure network segments.** A segmentation gateway defines global policy and requires multiple high-speed interfaces. This embeds security into the segmentation gateway fabric. In the Zero Trust network, we call each of the switching zones attached to an interface a "microcore and perimeter" (MCAP). Each segmented zone is its own microcore switch, and you can consider each zone as a microperimeter because all the resources within a specific microcore share similar functionality and global policy attributes. You centrally manage all MCAPs by aggregating all the switches within all the MCAPs into a unified switching fabric.
3. **Centralized management as the network backplane.** In the Zero Trust network, security is the nucleus of the system, with the switch fabric placed around the central security element — the segmentation gateway. This is antithetical to the hierarchical network, where the switch infrastructure is at the center of the network and security professionals try to wedge adequate controls on top of an inflexible fabric. In the Zero Trust network, the transparent and unified management of all MCAPs defines the backplane. The Government must move from command-line management of individual elements to a centralized intuitive management system that empowers our IT staff to manage expensive networks. Juniper Networks has rebuilt its management software, and its Junos Space offering can centrally manage Juniper's switches and security devices. EMC Smarts Network Configuration Manager is a standalone software platform that can manage network devices from multiple vendors to create this new management backplane.
4. **A data acquisition network (DAN) to gain complete network visibility.** An essential concept of Zero Trust is that you must inspect and log all traffic to and from each MCAP. To facilitate this, Forrester is proposing the creation of a new type of network called a "data acquisition network" (DAN). Today, numerous types of networks exist: local area networks (LANs), metropolitan area networks (MANs), wireless LANs (WLANs), and wide-area networks (WANs). To enforce Zero Trust, organizations should consider creating a DAN. A DAN facilitates the extraction of network data — typically, packets, syslog, or SNMP messages — to a single place where you can then inspect and analyze it in near real time. A DAN is an attractive concept; anybody who has had to troubleshoot networks knows how hard it is to capture packets in a network effectively. Because all traffic traverses the segmentation gateway, which interconnects all MCAPS, data acquisition can be accomplished efficiently. All of this traffic can be mirrored and forwarded to a DAN MCAP where security information management (SIM) and network analysis and visibility (NAV) tools centrally capture, analyze, and log all traffic traversing the network. NAV, along with traditional SIM tools, provides a type of network omniscience that is imperative in today's threat environment. Lancope, Narus, Niksun, RSA, and Solera Networks are among the varied players in this NAV space.

The Data Security, Control, and Privacy Imperative

Email addresses and passwords, credit card numbers, Social Security Numbers, account login credentials, and personal information are all pieces of information that cybercriminals can use to commit a wide range of crimes from identity theft to fraud to reselling in the underground market economy. As awareness increases, consumers, business executives, IT leaders, and law enforcement are taking countermeasures and cutting profits for cybercriminals. As risks increase and profits decline, cybercriminals look for new markets for new types of stolen information. Confidential company information, such as customer lists, product plans, and strategy road maps, financial information, and intellectual property such as trade secrets and formulas are even more attractive. In addition, organizations today cannot overlook the possibility that state-sponsored actors are also targeting their intellectual property. Regardless of the source — insiders, rival business entities, organized crime, nation-states — intellectual property and confidential company information can mean a big payday, whether such information is turned over for immediate financial rewards or used to further an attacker's own future economic interests.

In addition, while securing or protecting an individual's personally identifiable information (PII) from unauthorized use or theft is critical, it is just one aspect of privacy. The most common complaint about privacy that we hear from our clients is that the plethora of privacy laws in various jurisdictions and industry bodies are difficult to understand and sometimes in conflict with each other. Business, security, and privacy leaders are just now beginning to understand the issues around data residency. There are no geographical borders on the Internet, so it is extremely difficult to secure and protect data using traditional geographic paradigms. The policies governing the storage and transport of nation-specific data will become critical if organizations are to meet these requirements.

A New Framework: Introducing Forrester's Data Security and Control Framework

There are only two types of data that exist in your organization:

1) Data that Someone Wants to Steal
2) Everything Else

The first type is sensitive or toxic data, which can be easily identified with the equation 3P + IP = TD. The three P's stand for personally identifiable information (PII), personal health information (PHI), and personal cardholder information (PCI); IP is intellectual property; and TD is toxic data. Forrester breaks the problem of securing and controlling data down into three areas:

1. **Defining the data.** This involves data discovery and data classification. Security and risk professionals, together with their counterparts in legal and privacy, should define data classification levels based on toxicity. This allows security to protect properly data based on its classification once it knows where that data is located in the enterprise.
2. **Dissecting and analyzing the data.** This involves data intelligence (extracting information about the data from the data, and using that information to protect the data) and data analytics (analyzing data in near real time to protect proactively toxic data). Look for security information management (SIM) and network analysis and visibility (NAV) solutions to intersect with big data to enhance security decision-making.
3. **Defending and protecting the data.** Data defense is the fundamental purpose of cybersecurity, and is the area where organizations focus most today. To defend your data, there are only four levers you can pull — controlling access, inspecting data usage patterns for abuse, disposing of data when the

organization no longer needs it, or “killing” data via encryption to devalue it in the event that it is stolen.

Security professionals apply most controls at the very edges of the network. However, if attackers penetrate your perimeter, they will have full and unrestricted access to your data — and thanks to big data, it will all be in one place. By placing controls as close as possible to the data store and the data itself, you can create a more effective line of defense.

Measuring the Effectiveness of Data Privacy Programs

The emotional aspect makes it difficult to evaluate privacy concern: Directly asking about a privacy issue may result in an emotional and biased response. This effect may be partly responsible for the dramatic privacy concern ratings coming from recent surveys — ratings that often seem to be at odds with user behavior. Managing inconsistent requirements across a global enterprise is nothing new; CISOs are quite familiar with it, but that does not make it simple. It is important to understand that privacy protection, which can often seem abstract and inconsistent, consists of identifiable information assets, repeatable processes, and specific security controls. Once an organization identifies information assets, processes, and controls, it becomes easier to measure the state of privacy in the enterprise.

Forrester organizes security metrics into three categories: readiness, response, and recovery. There are eight widely accepted principles of privacy. Two organizations, the Organization for Economic Co-operation and Development (OECD) and The United States Department of Health, Education, and Welfare (now the Department of Education and the Department of Health and Human Services), identified the need for a system- and network wide approach to address the need for privacy. The OECD Privacy Guidelines released in 1980 apply to any personal data that is in the public or private sector where the nature of the intended use presents a potential "danger to the privacy of individual liberties." We can use this same framework in conjunction with the eight principles of privacy to create a two-dimensional matrix to measure the state of privacy in the organization. We refer to this as Forrester's Privacy Metrics Framework, and the types of metrics (readiness, response, and recovery) organizations should develop are outlined below:

- **Accountability.** Regulators and customers demand the ability to audit privacy compliance. Management should support these audits. Capture the outcome of periodic privacy audits and the level to which the audits enforce accountability for the safe collection, access, and disposition of the private information. Look for trends in the audit data to determine if your privacy program is continuously improving that state of privacy management in your organization.
- **Collection.** Organizations should limit the amount and type of personal data that they collect and ensure that they obtain it by lawful and fair means. Record the number of times that the organization collected information that exceeded the stated need for the information and track the disposition of this information.
- **Data quality.** Personal data should be correct, complete, and relevant to the organization's needs. Perform periodic audits of collected information to determine the level of quality. This could include the number of times the organization collected information without getting prior consent, informing the individual what they intended to use the information for, or telling the individual for how long they intended to keep the information.
- **Openness.** Regulators and customers demand that firms explain how they handle PII. Measure the frequency with which the company informs individuals on the type of information held, the

procedures they use to protect the sensitive information, and the individual's right to see the information.

- **Participation.** Employees and customers should understand what information a company holds about them and how it manages this information. Measure the time it takes to answer an individual's request for information, including copies of and corrections to the information.
- **Purpose.** When companies collect data, they should be upfront regarding how they will use it. Measure the accuracy, completeness, and currency of personal data held by the organization. Information captured should include data such as the date of most recent verification activity and the percentage of data found to be accurate, complete, and current during most recent verification activity.
- **Security safeguards.** Organizations should protect personal data against unauthorized access, destruction, use, modification, and disclosure. Measure the distribution of times the organization did or did not dispose of personal data in a secure manner after the end of the stated usage time interval.
- **Use limitation.** Organizations should not use personal data for any purpose other than the uses the law allows or ethics require. Measure the number of times that the organization put personal data to a new use without first obtaining the individual's approval.

Appendix A: Relevant Forrester Research

Kindervag, J. and Holland, R. (November 9, 2011). ***Planning For Failure.***

It's not a question of if — but when — your organization will experience a serious security breach. Cybercriminals are using more sophisticated and targeted attacks to steal everything from valuable intellectual property to the sensitive personal and financial information of your customers, partners, and employees. Their motivations run the gamut from financial to political to retaliatory. With enough time and money, they can breach the security defenses of even the largest enterprises. You can't stop every cyberattack. However, your key stakeholders, clients, and other observers do expect you to take reasonable measures to prevent breaches in the first place, and when that fails, to respond quickly and appropriately. A poorly contained breach and botched response have the potential to cost you millions in lost business and opportunity, ruin your reputation, and perhaps even drive you out of business.

Holland, R. (January 12, 2012). ***The CISO's Guide To Virtualization Security*****.**

In today's data centers, IT often virtualizes new applications and workloads by default. Virtualization is the norm; deploying a physical server is the exception. The technology is mature and enterprise adoption is high, yet information security does not have a significant focus on virtual security. Given the converged nature of virtual environments, security incidents can result in significant damage; therefore, it is critical that security professionals redouble their efforts and make securing their virtual infrastructure a priority. This guide describes the security challenges within virtualized environments and shows how to apply the concepts of Forrester's Zero Trust Model of information security to secure the virtual environment effectively.

Ferrara, E. (December 6, 2012). ***Measure The Effectiveness Of Your Security Architecture And Operations.***

Information security programs have struggled with legitimacy with senior leaders for a long time. There are many reasons for this, but they all can be traced back to the historical inability of chief information security officers (CISOs) to explain the business impact of information security, the risks facing the organization in business terms, and the business value of the information security organization. Senior leaders ask CISOs three questions: 1) Are we any more secure this year as compared to last year? 2) are we spending the right amount on information security? and 3) do we have the right people on the security team? If you have the right metrics, answering these questions is easy. This report proposes a practical set of information security metrics to address these questions as well as demonstrate information security effectiveness. Forrester designed this report to help you develop an information security metrics program that highlights information security's business and operational value.

Kindervag, J. (July 12, 2012). ***Control And Protect Sensitive Information In The Era Of Big Data.***

This report outlines the future look of Forrester's solution for security and risk (S&R) executives seeking to develop a holistic strategy to protect and manage sensitive data. In the never-ending race to stay ahead of the competition, companies are developing advanced capabilities to store, process, and analyze vast amounts of data from social networks, sensors, IT systems, and other sources to improve business intelligence and decisioning capabilities. "Big data processing" refers to the tools and techniques that handle the extreme data volumes and velocities and wide variety of data formats resulting from implementing these capabilities. As organizations aggregate more and more data, they need to be aware that much of it could be financial, personal, and other types of sensitive data that are subject to global laws and regulations. S&R professionals need to be aware of the security issues surrounding big data so they can take an active role early in these initiatives. This report will help S&R pros understand how to control and properly protect sensitive information in the era of big data.

Shey, H. and Kindervag, J. (November 1, 2012). ***Simplify Cybersecurity With PCI.***

US federal law, specifically the Federal Information Security Management Act (FISMA), requires US federal government agencies to adhere to National Institute of Standards and Technology (NIST) security standards and guidelines (specifically NIST 800-53). That's easier said than done. NIST 800-53 leaves a lot of room for interpretation, and many security and risk (S&R) pros in government turn to other standards such as the ISO 27000 family or the US Department of Defense's Information Assurance Certification and Accreditation Process (DIACAP) standard to find the specifics they need. However, neither standard fits the bill for a civilian agency, as ISO can be too high-level while the DoD standard is overkill. Forrester contends that the Payment Card Industry (PCI) data security standard (PCI DSS) holds promise as an additional baseline that can augment NIST 800-53. In this report, we map NIST 800-53 to PCI to provide prescriptive guidance for meeting NIST 800-53 requirements

Shey, H. and Kindervag, J. (August 9, 2012). ***Dissect Data To Gain Actionable INTEL*****.**

Forrester segments the problem of securing and controlling data into three areas: 1) defining the data; 2) dissecting and analyzing the data; and 3) defending and protecting the data. We refer to this as our Data Security And Control Framework. In this report, we offer more vision and detail for dissecting and analyzing data. Business executives demand data for decision-making. Security professionals want situational awareness. Security information management (SIM) tools are seen as a solution to fulfill both needs, but today's reality is that SIM creates more fog than clarity, doing little more than providing compliance reporting. Big data and network analysis and visibility (NAV) tools for security analytics will provide the necessary additional ingredients to overhaul SIM and move it from merely compliance reporting to providing situational awareness for both the business and IT security. This security analytics will provide "INTEL," a term we've coined that stands for "information, notification, threats, evaluation, and leadership." The intersection of big data, data warehousing, NAV tools, and business intelligence will be necessary to help stop not just network intrusions but also the exfiltration of data from organizations.

Kindervag, J. (November 15, 2012). ***No More Chewy Centers: Introducing The Zero Trust Model Of Information Security*****.**

There's an old saying in information security: "We want our network to be like an M&M, with a hard crunchy outside and a soft chewy center." For a generation of information security professionals, this was the motto we grew up with. It was a motto based on trust and the assumption that malicious individuals wouldn't get past the "hard crunchy outside." In today's new threat landscape, this is no longer an effective way of enforcing security. Once an attacker gets past the shell, he has access to all the resources in our network. We've built strong perimeters, but well-organized cybercriminals have recruited insiders and developed new attack methods that easily pierce our current security protections. To confront these new threats, information security professionals must eliminate the soft chewy center by making security ubiquitous throughout the network, not just at the perimeter. To help security professionals do this effectively, Forrester has developed a new model for information security, called Zero Trust. This report will explain the vision and introduce the necessity and key concepts of the Zero Trust Model to security and risk (S&R) leaders responsible for their organization's security architecture and operations.

Kindervag, J. (November 15, 2012). ***Build Security Into Your Network's DNA: The Zero Trust Network Architecture*****.**

One of our goals with Zero Trust is to optimize the security architectures and technologies for future flexibility. As we move toward a data-centric world with shifting threats and perimeters, we look at new network designs that integrate connectivity, transport, and security around potentially toxic data. We call this "designing from the inside out." If we begin to do all those things together we can have a much more strategic infrastructure. If we look at everything from a data-centric perspective, we can design networks from the inside out and make them more efficient, more elegant, simpler, and more cost-effective. We designed this report so that security and risk (S&R) leaders can apply concepts of the Zero Trust Model to develop their security architecture and operations strategy.

Ferrara, E. (January 10, 2013). ***Measure The Effectiveness of Your Data Privacy Program*****.**

Privacy is one of the most important and emotional issues in information security. Privacy, or the lack thereof, affects a company's management, employees, and most importantly, customers. With the rise of social networking and the use of the Web for banking, insurance, and medical enrollments, more and more of a person's life is online. We all know this, but security and risk (S&R) professionals have the responsibility to make sure that the applications that manage this information also keep it private. At the same time, politicians around the world have taken on privacy as an important issue for their constituents and have passed myriad laws to protect an individual's privacy. This report proposes a practical set of information security metrics to measure privacy compliance and demonstrate the effectiveness of the privacy program. Forrester designed this report to help you, the S&R leader, develop an information security metrics program that highlights the importance of privacy to management, employees, and customers.

Shey, H. and Kindervag, J. (January 15, 2013). ***Know Your Data To Create Actionable Policy.***

Data defense is the fundamental purpose of information security. To defend your data, there are only four levers you can pull — controlling access, inspecting data usage patterns for abuse, disposing of data when the organization no longer needs it, or killing data to devalue it in the event that it is stolen. Policy addresses when and how much to pull the levers. Too often, organizations create data policies without a clear understanding of feasibility and purpose within their business because they themselves are in the dark about their data — from what data they have to where it resides. As a result, many data security policies are ineffective and can even hinder business processes. Data classification via traditional frameworks such as Bell-LaPadula and Biba can be too academic in nature and not enforceable in the modern world of big data and advanced threats. In today's evolving data economy, data identity is the missing link that security and risk (S&R) leaders must define in order to create actionable data security and control policy. We designed this report to help S&R leaders develop effective policies using our Data Security Control And Control Framework as a guideline.

Holland, R. (January 15, 2013). ***Five Steps To Build An Effective Threat Intelligence Capability.***

Against today's mutating threat landscape and sophisticated cybercriminals, security and risk (S&R) professionals are outgunned and outmatched. The traditional strategy of waiting for an alert and then responding to a compromise is futile against 21st century threat actors. Delayed responses when cybercriminals have already begun exfiltrating intellectual property aren't acceptable. Something must change, and S&R professionals must proactively defend their networks and data. In this report, we draw from the principles of military intelligence and guide S&R pros through a five-step process to build and leverage threat intelligence capabilities.

Shey, H. and Kindervag, J. (April 5, 2013). ***Strategy Deep Dive: Define Your Data.***

Defining data via data discovery and classification is an often overlooked, yet critical, component of data security and control. Security and risk (S&R) pros can't expect to adequately protect data if they don't have knowledge about what data exists, where it resides, its value to the organization, and who can use it. Data classification also helps to create data identity (data-ID), the missing link for creating actionable data security and control policies. Yet, organizations that attempt to classify their data are thwarted by their own efforts with overly complex classification schemes and haphazard approaches. As a result, many see data discovery and classification as a Sisyphean task. This report aims to help S&R pros rethink and simplify their strategy to define their data.

Appendix B: Relevant Team Biographies

John Kindervag

PRINCIPAL ANALYST SERVING **SECURITY & RISK PROFESSIONALS**

John serves Security & Risk Professionals. He is a leading expert on wireless security, network security, security information management, and PCI data security. John leads research efforts for Forrester's Data Security And Privacy and Security Architecture and Operations playbooks.

Previous Work Experience

John is a 25-year veteran of the high-tech world. He holds numerous industry certifications, including CISSP, CEH, QSA, and CCNA. Prior to joining Forrester, John was the senior security architect with security consultancy Vigilar, and he started the security practice for a Cisco Gold VAR, Flair Data Systems, where he was a principal security consultant. He has particular expertise in the areas of wireless security, intrusion detection and prevention, and voice over IP hacking. He has been interviewed and published in numerous magazines, including Hospitality Technology Magazine, SecurityFocus.com, and Techtarget.com. John has spoken at many security conferences and events, including ToorCon, ShmoCon, and InfoSec World.

Education

John has a Bachelor of Arts degree in communications from the University of Iowa.

Ed Ferrara

PRINCIPAL ANALYST SERVING **SECURITY & RISK PROFESSIONALS**

Ed serves Security & Risk Professionals, leading Forrester's coverage of security metrics, security program effectiveness, security awareness, and enterprise security information architecture. Ed's research builds on his work as a highly experienced in-program manager for the design and delivery of secure information technology solutions, including strategy, process, applications, and infrastructure. He has consulted with Fortune 50 companies in the area of solution determination based on understanding the needs and the skills required to create a successful security posture for large complex organizations.

Previous Work Experience

Before coming to Forrester, Ed's background was in information security consulting, leading a global information security practice for financial services, commercial, and chemical clients. Ed is an expert in the design and delivery of secure, cost-effective, high-performance information security solutions, methodology, and standards to address complex business and security problems. Ed holds a US patent in the area of software development, specifically in the area of software requirements traceability using UML and software patterns to align business requirements with IT implementation. He has successfully developed and implemented technology and organizational change programs globally for Fortune 100 companies. Ed has strong program and project management skills, as well as, demonstrated competence in multidivision matrix management, technical management, relationship building, and projecting influence at the C-level.

Education

Ed holds two master's degrees, in education technology and computer science from the University of Delaware and information assurance (cum laude) from Norwich University, as well as a bachelor's degree in economics from Franklin & Marshall College. Ed holds the CISSP certification.

Rick Holland

SENIOR ANALYST SERVING **SECURITY & RISK PROFESSIONALS**

Rick serves Security & Risk Professionals. He works with senior information security leadership providing strategic guidance on security architecture, security operations, and data privacy. His research focuses on incident response, threat intelligence, and email and web content security, as well as virtualization security. He is regularly quoted in the media and is a frequent guest lecturer at the University of Texas at Dallas.

Previous Work Experience

Prior to joining Forrester, Rick was a solutions engineer with a national information security reseller and service provider. He advised Fortune 500 clients on security strategy and architected enterprise security solutions. Before that, he worked in both higher education and the home building industry, where he focused on intrusion detection, incident handling, and forensics. Rick also served as an intelligence analyst in the US Army stationed in the US, Europe, and the Middle East.

Education

Rick holds a B.S. in business administration with an MIS concentration (cum laude) from the University of Texas at Dallas. Rick is also a Certified Information Systems Security Professional (CISSP), a Certified Information Systems Auditor (CISA), and a GIAC Certified Incident Handler (GCIH).

Heidi Shey

ANALYST SERVING **SECURITY & RISK PROFESSIONALS**

Heidi serves Security & Risk Professionals. Her research focus is on intellectual property protection, data privacy, biometrics, cybersecurity topics such as policy and regulatory concerns, and consumer security. She also focuses on data-driven topics such as budgeting, spending, and the economics of security. She is a team lead for survey design, methodology development, data analysis, and building of forecasting models in consulting engagements.

Previous Work Experience

Heidi has been with Forrester since 2006. Her previous focus was on conducting quantitative analysis of B2B technology adoption and IT spending and budgeting trends for technology vendors. In her previous role, she also worked closely with Forrester's Forrsights team on survey development and data quality initiatives, in addition to leading companywide data use and quantitative analysis training for new research associate hires.

Education

Heidi holds a B.A. in economics and studio art with honors from Wellesley College and an M.S. in cybersecurity policy from the University of Maryland. She has also studied at the Chinese University of Hong Kong.

Securing Sensitive Documents

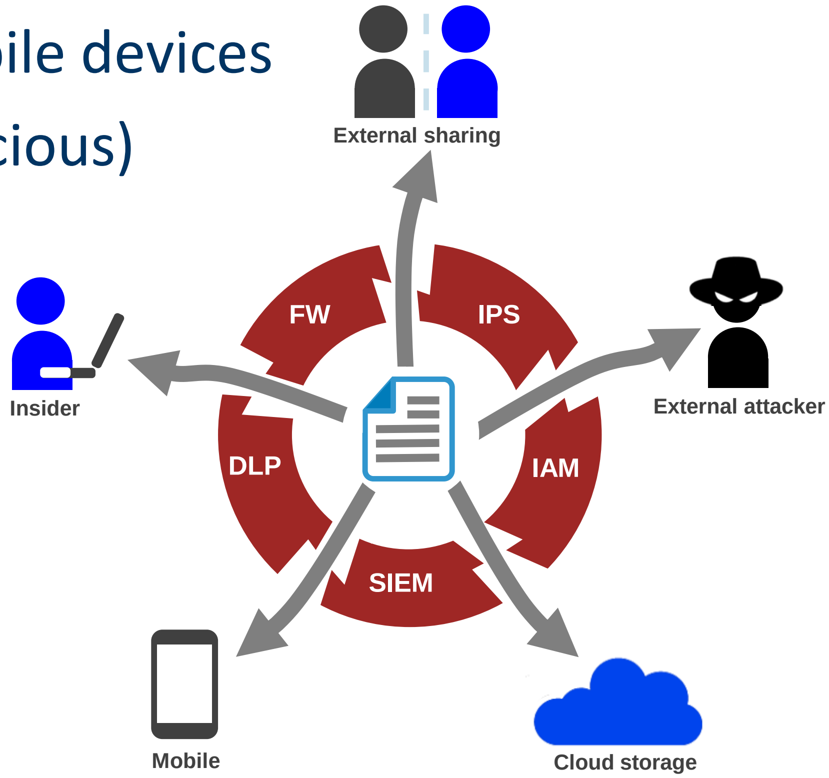
A Cyber Security Perspective

July 24, 2015

Why Do Data Leaks Happen?

Despite all perimeter security, data leaks still happen because of:

- Sharing documents with external agencies and parties
- The use of cloud storage
- Accessing data or storing it on mobile devices
- Action of insiders (careless or malicious)
- External attackers



Document Security Issues

Two issues that need to be addressed in parallel:

- Sensitive data, such as PII, needs to be shared with authorized parties, yet protected so it does not get into the wrong hands.
- As a user accesses sensitive agency data the user's identity must be validated.

The Challenges are:

- Government employees have access to free file sync sites, which often go un-scanned by DLP systems.
- The use of mobile devices for data access introduces new threats.
- There is a lack of visibility as to who accesses agency data.
- Lack of persistent data protection allows data exfiltration by an insider or an attacker who has penetrated the network perimeter.
- As government shares with external entities it can be a challenge to verify and authenticate the individual because CAC/PIV cards are not widely used.

Document Security Requirements

Data Dissemination:

- Using a secure EFSS tool that encrypts data in transit is an easy way to ingest data such as visitor request without sending plaintext PII over the wire.
- By using a secure EFSS tool that can apply data-centric security to files that leave the agency, it is possible to control the files' distribution without relying on trust (restrict copy, print, forward), track them and wipe them – even after they have been shared.
- By integrating EFSS with DLP, protection policies are made content aware.

Verify & Authenticate:

- Using a strong authentication tool that can federate disparate decentralized Auth servers will allow agency to protect files with strong authentication when sharing data externally.
- By adding biometric authentication to the authentication strategy, the adversary will not be able to spoof credentials to gain access to data.

Adhere to Compliance as Files Leave

- Agencies may require all outbound communication be scanned by the DLP engine.
- Currently, if content is allowed to be sent that is later determined to contain sensitive information, there may be no recourse.
- In addition, DLP policy cannot prevent additional dissemination or protect from device loss or theft.
- A secure EFSS solution can protect content enabling agencies to persistently control files and revoke access if it is later determined that the content should not have been sent.

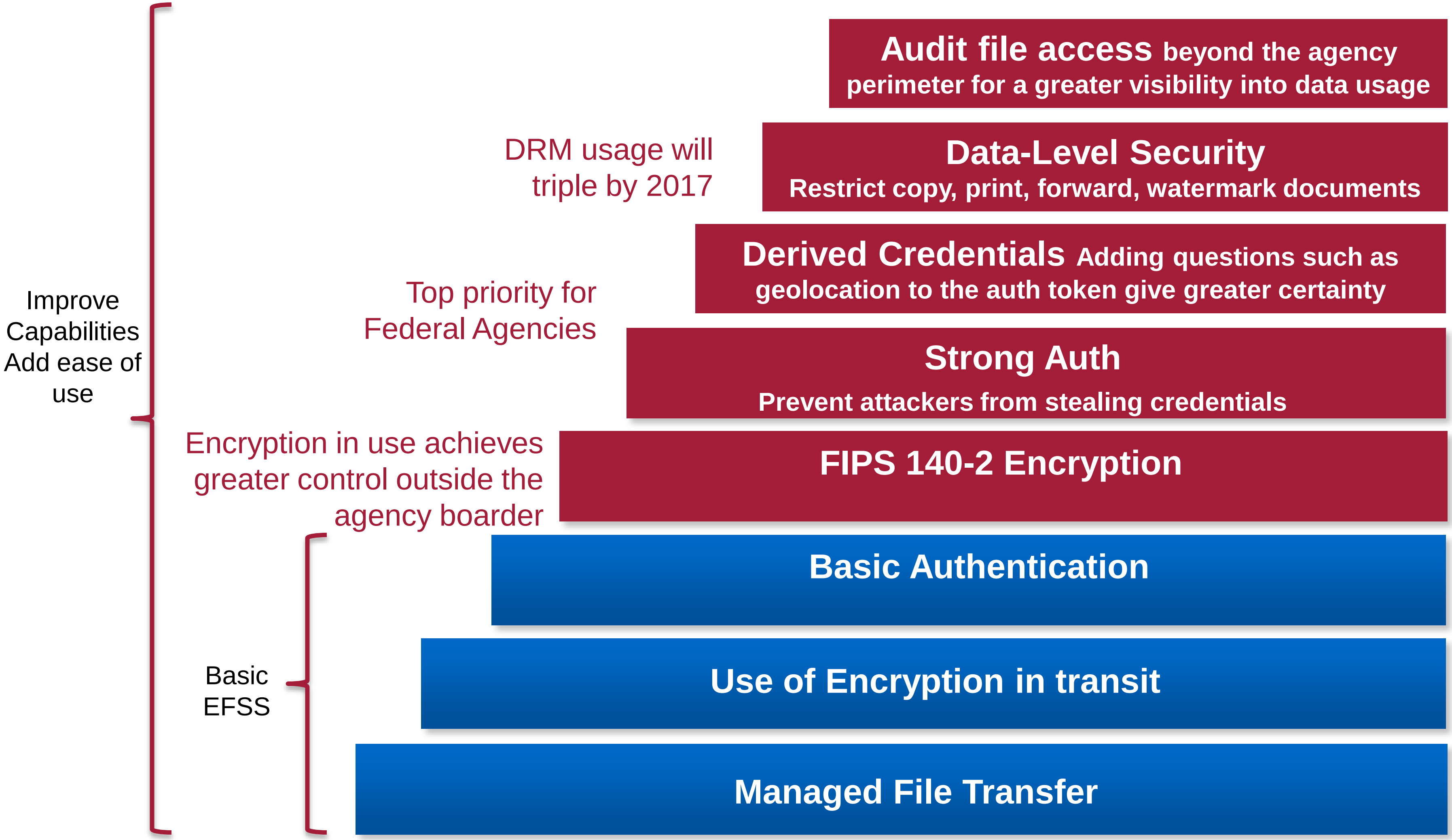
Reduce Risk by Discovery and Protection

- Many organizations would like to know where sensitive information (PII, PHI, PCI related, confidential data) is on their network and protect it to ensure it does not get into the hands of the wrong people.

- Trust, visibility are not sufficient – remediation is necessary to address exposure.

- By combining classification with EFSS data-centric controls, files become self-protecting and are not accessible by unauthorized users.

Secure EFSS Building Blocks



Audit file access beyond the agency perimeter for a greater visibility into data usage

Data-Level Security
Restrict copy, print, forward, watermark documents

DRM usage will triple by 2017

Derived Credentials Adding questions such as geolocation to the auth token give greater certainty

Strong Auth
Prevent attackers from stealing credentials

Top priority for Federal Agencies

FIPS 140-2 Encryption

Encryption in use achieves greater control outside the agency boarder

Basic Authentication

Use of Encryption in transit

Managed File Transfer

Improve Capabilities Add ease of use

Basic EFSS

Summary Checklist

- ✓ Do you have a secure, approved file sharing solution, or are personnel using consumer-grade services?
- ✓ Does your approved file sharing solution provide persistent data protection at-rest, in-transit and in-use, and maintains a granular audit trail?
- ✓ Are your identity management systems integrated with file sharing solution to allow easy federation of identities, and facilitate an easy way of receiving of sending data to other agencies?
- ✓ Do you have easy to use authentication systems that verify external parties that collaborate with the government?
- ✓ Are DLP and classification policies integrated with your file sharing tools and processes?
- ✓ Are you using strong, biometric authentication tools that increase security while easing the end user burden with credentials?

User – Based Encryption: Protect Information Independent of Storage and Transport

- When faced with data breaches, organizations turn to encryption methods. But, not all encryption methods are the same. For instance, turning on whole-disk encryption really only defends against physical theft of the drives. When hackers find their way into the system, the data is decrypted automatically on read, which can then be exfiltrated, and saved elsewhere in the clear. Moving up the stack to the application, like turning on transparent encryption in the database, helps, but is still prone to attackers employing SQL injection or application exploits to gain access to the information, which again can be automatically decrypted, exfiltrated, and saved elsewhere in the clear. In both cases, the information is **forever lost, and irretrievable.**

- A better approach is to leverage **user-based encryption**, like DRM (Digital Rights Management), which persistently protects sensitive information independent of storage and transport. While an attacker can try to steal the end-user¹s credentials to gain access to the encrypted information, the technology thwarts attempts to save the information in the clear. Furthermore, attempts at viewing the information can be detected and immediately revoked (remote shredding), providing powerful capabilities to defenders performing incident response.

We see three keys to implementing user-based encryption:

1. Effectively matching people to content needs to happen early in the information lifecycle. By tagging assets coming into the content management system, DRM can be applied automatically and transparently to the documents required by end-users to get their jobs done.

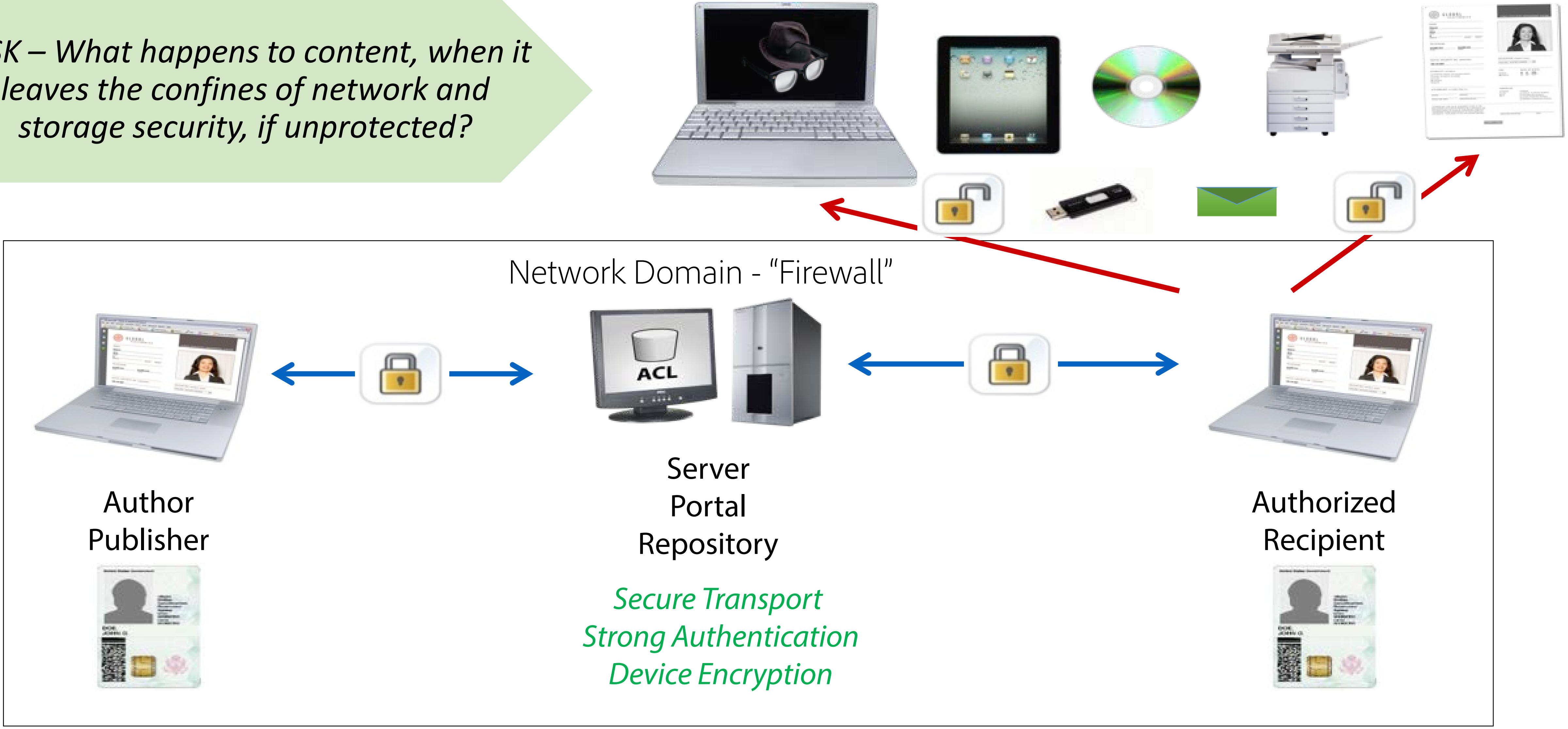
2. Persistently protecting content, independent of storage and transport. This includes dynamically controlling access, printing, copying and modification of content. Automatically auditing interactions with documents including valid/invalid access is also crucial to support detection and continuous monitoring.

3. Detecting potential breaches and immediately supporting incident response. Real time anomaly detection automatically alerts organizations to any unusual activity, while immediate revocation (^{3}Remote Shred^{2}) bolsters the incident response plan.

Context: Data Protection Challenges

RISK – What happens to content, when it leaves the confines of network and storage security, if unprotected?

Events: Accidents (Malicious or Unintentional), Insiders, Attacks)



Network Domain - “Firewall”

Author
Publisher

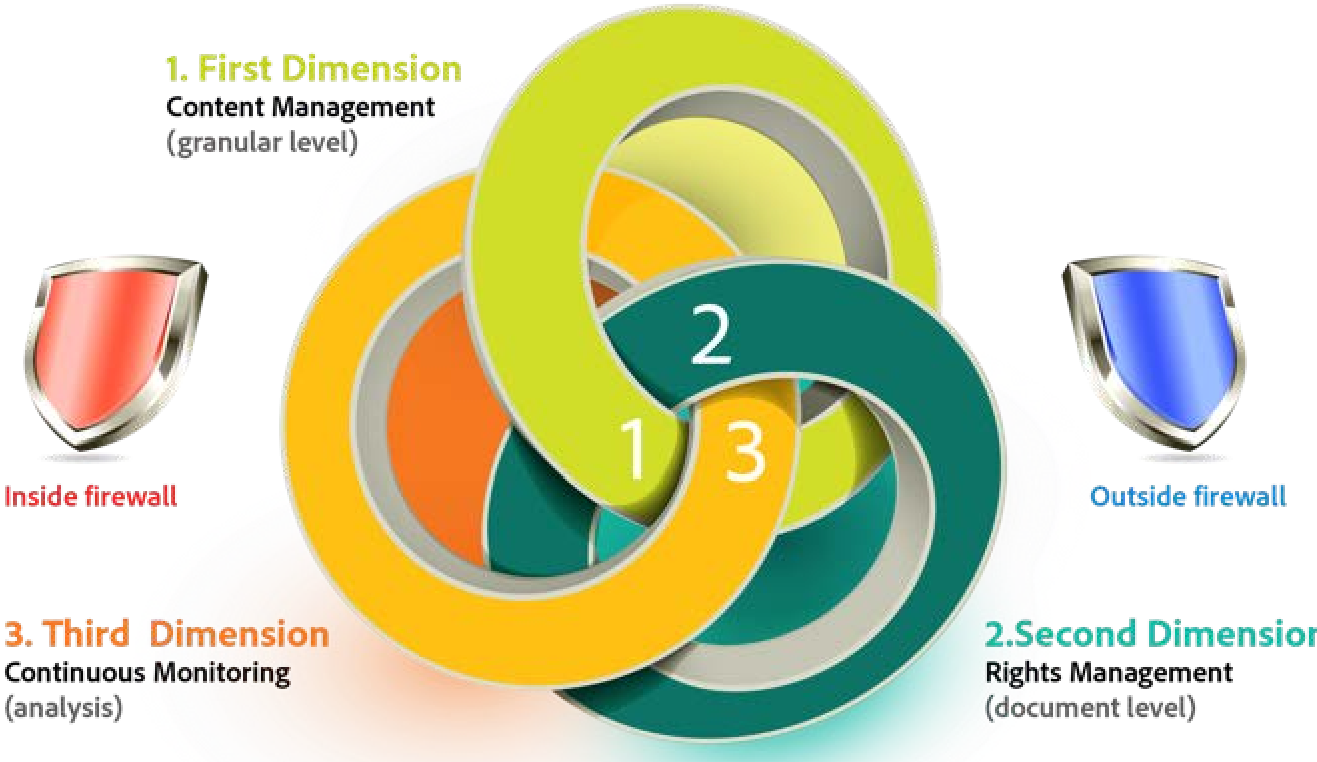
Server
Portal
Repository

Authorized
Recipient

Secure Transport
Strong Authentication
Device Encryption

Three Dimensions of User – Based Encryption with DRM (Authentication, Authorization, Auditing)

1. **Authentication:**
   - Who is trying to open/view the content based on login, PKI, SSO, IP address



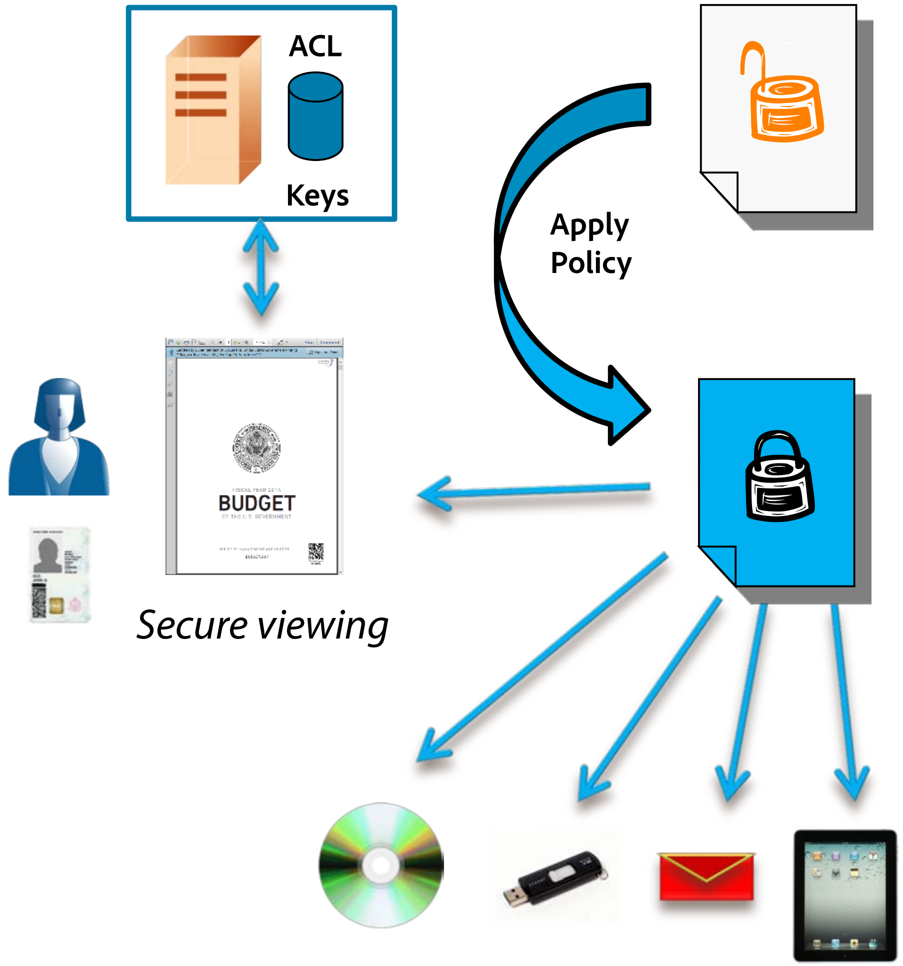
2. **Authorization:**
   - What can they do with the document (e.g. read, print, modify, offline access)?
   - Additional: Expiration, Revocation, Versioning, Watermarking

3. **Auditing:**
   - Track what’s been done or attempted with the document
     - Who?
     - What?
     - When?
     - Where?

User – Based Encryption *with rights management*

1. Author adds protection by picking an access “policy” from the management server.
2. The policy defines users and groups with *role based access* to content
3. Document does not touch the key server; you still control where it is stored and how it is distributed.

- Resulting document is protected:
  - Recipient authenticates on each access, server authorizes and audits
  - Always stays encrypted when distributed, even after authorized users open it.
  - Integrated with desktop apps for multiple file formats.
  - Also restricts printing, clipboard, modifying
  - Can expire, revoke, and watermark content



ACL

Keys

Apply Policy

BUDGET

Secure viewing

Document still protected independent of storage and transport

CIO’s Perspective on Cyber Security

Cyber Security Perspective – Risk Management

Internal Focus -

- Lock down the "Fort" and protect what is inside the "Moat".
- Security concerns are focused on infrastructure.
- Use existing Firmware, SOC, NOC, sniffers, contractors.
- Need to quickly remediate issue found with hardware, software and firmware already in place.

External Focus -

- What do you "Trust" that's an add-on to the Network infrastructure
- CIO's accept a certain level of "Risk" in their appliances
- Affects both Hardware and Software appliances
- Security in the Supply Chain is a critical part of Risk Management
- The Supply Chain can react much more quickly than the Federal Government – need to take advantage of this.

Comparison view of 3 Gartner Magic Quadrant PC Suppliers

Hardware Component Sourcing Analysis of equivalent 14”Laptops based upon suppliers and locations of suppliers

Component	Supplier “A”	Supplier “B”	Supplier “C”
CPU/ Chipset / vPro	Intel	Intel	Intel
LCD Display	Multiple; Asia	LG; China	LG; China
Finger Print sensor	Validity; China	Validity; China	Broadcom/China
Smart Card reader	Alcor; China	Alcor; China	O2Micro; China
Touchpad	Synaptics; China	Synaptics; China	Alps; China
Memory	Multiple; Asia	Ramaxel; China	Micron; Korea
Hard Drive	Multiple; Asia	Hitachi; Thailand	Seagate; Korea
WLAN card	Intel; China	Intel; China	Atheros; China
Ethernet	Intel; China	Intel; China	Intel; China
TPM IC	ST Micro; China	Infineon; Asia	Atmel; Asia
Super I/O IC	Toshiba; China	SMSC; Taiwan	SMSC; Taiwan
Embedded Controller IC	Microchip; Taiwan	N/A	SMSC; Taiwan

- Assumption: These suppliers have multiple sources

Supply Chain Security Checklist – General Security

- Get to know your Supplier – Who owns, where designed, where made?
- What is your Suppliers Company Security Policy?
- How does your Supplier manage hardware and IP assets?
- How well does your Supplier screen their personnel?
- How good is the security at the Supplier's offices and factories?
- How does your Supplier handle security with their suppliers?
- How well does your Supplier manage their internal Information systems?
- Who (inside or outside their company) has access to the Suppliers IT Network?
- How does your Supplier handle security incidents?
- Does your Supplier have contingencies for disasters?

Supply Chain Security Checklist – Software/ Firmware Security

- Does your Supplier follow security practices in their software or firmware development?
- Is the developed software or firmware code being evaluated and tested for security vulnerabilities?
- Does the developed software or firmware code use any 3rd party or open source code?
- How does your Supplier respond to discovered vulnerabilities in product that have already been delivered to you?
- Does your Supplier support periodic updates?
- Are the updates delivered over secure communications?

Supply Chain Security Checklist – Hardware Security

- Are all of the components and subassemblies in the Suppliers product under source control?
- How does the Supplier prevent the introduction of counterfeit parts?
- Is their traceability between the components and subassemblies and the final product delivered?
- Are there security vulnerabilities in Manufacturing Test that can affect the product security?
- How does your Supplier respond to discovered problems found in product that have already been delivered to you?
- Does your Supplier participate in C-TPAT, CIP, SCIP or BASC programs?
- What are your Suppliers security requirements for warehouses and freight forwarders that handle the product before delivery?

Backup Material »

Supply Chain Security Checklist – General Security

Company Information

- Contact and Responder Information
- Basic Company Information
- Identify all hardware, software and firmware products received
- Identify foreign government or entities with >10% ownership, influence or influence
- Identify all design, product test, and/or manufacturing facilities (owned or 3rd party)
- Identify name and residence of company directors and executives

Company Security Policy

- Is Security Policy supported by top Management?
- Are Security responsibilities defined throughout the company?
- Is Information Security part of your business and planning process?
- Share the results of internal and external Security reviews performed in the past 12 months?

Supply Chain Security Checklist – General Security

Asset Management

- Are there documented policies and procedures governing Asset Management?
- Is there an inventory of all information, software and hardware assets?
- Have information assets been classified in any way, for example according to their importance to the business and/or their sensitivity?
- What is the process to dispose of secure documents and devices?

Human Resource Security

- Are Security responsibilities defined and documented within employee job responsibilities?
- Are verification and background checks performed at recruitment?
- Are regular security awareness training activities conducted?
- Is there a written code of conduct that addresses security violations?
- Are employees required to sign confidentiality or Non Disclosure Agreements?
- Do you have an employee termination procedure that includes removing access rights, recovering keys, identification badges, and other access devices?

Supply Chain Security Checklist – General Security

Physical & Environmental Security

- Do the facilities have physical entry controls for all personnel?
- Are visitors required to wear ID badges that show their status
- Are visitors required to be escorted?
- Are there documented procedures for maintaining a safe work environment?
- What security controls been implemented for the removal of equipment and media taken off-site?
- How do you ensure the sensitive data and licensed software removed or securely overwritten from the equipment containing storage media prior to disposal / re-use?

Supplier Relationships

- Have the security requirements for mitigating the risks associated with supplier's access to your assets been identified and documented ?
- Are the supplier service deliveries monitored with regular review or audit ?

Supply Chain Security Checklist – General Security

Communications & Operations Management

- Are there documented operating procedures for all key information systems, and maintained control of who has access?
- Are duties segregated to reduce opportunities for unauthorized or unintentional modification or misuse of your company's assets?
- Are any information security services outsourced to other parties?
- Are controls implemented for detection, prevention, and recovery against malicious code and appropriate user awareness procedures?
- Do you have back-up policy and procedures?
- Are controls implemented for networks and services to be protected from threats and to maintain security for the systems and applications using the network, including information in transit?
- Are policies and procedures implemented regarding the management of removable media, and the secure and safe disposal of all media (electronic, paper, voice, etc.)?

Supply Chain Security Checklist – General Security

Communications & Operations Management (con’t.)

- Are employees, contractors or visitors permitted to bring any digital storage media such as USB drives into any of your facilities?
- Are formal exchange policies, procedures, and controls in place to protect the exchange of information through communication means?
- Are on-line transactions protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, disclosure, or replay?
- Do you record and log user activities, exceptions, and information security events?
- Are procedures to monitor use of Information Processing Facilities?

Supply Chain Security Checklist – General Security

Access Control

- Is there a documented access control policy based on business and security requirements for access?
- Does management review users' access rights at regular intervals?
- Are there password management systems used to ensure the use of quality passwords?
- Are users only provided access to network services that they are authorized for?
- Are authentication methods implemented for external connections to control access by remote users?
- Are all users required to have a unique logon ID and authentication method to substantiate identity?
- Are mobile devices allowed to access your networks and information systems?
- Are there any policies to address security for teleworking activities?

Supply Chain Security Checklist – General Security

Information Systems Acquisition, Development and Maintenance

- Do the business requirements specify the requirements for security controls for new information systems, or enhancements?
- Do processes include input data validation, control of internal processing, message integrity, and output data validation to prevent errors, loss, unauthorized modification, or misuse of information in applications?
- Is there a policy and documented procedures on the use of cryptographic controls for protection of information?
- Are There procedures in place to control the installation of software on operational systems, and restrict access to program source code?
- When operating systems are changed, are business critical applications reviewed and tested to ensure there is no adverse impact on organizational operations or security?
- Do you conduct security functionality testing during development?

Supply Chain Security Checklist – General Security

Information Security Incident Management

- Is there a documented security incident response plan that complies with industry standards?
- Is there Root Cause Analysis of every security investigation to understand process deficiencies and to protect against reoccurrence?

Business Continuity

- Is there a formal business continuity plan to operate in extraordinary circumstances?
- Are business continuity plans tested at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?

Compliance

- Have relevant statutory, regulatory and contractual requirements been identified and documented for each information system?
- Are there internal assessments to ensure that all security procedures are carried out to achieve compliance with security policies?
- Have any external or internal security reviews been performed in the past 12 months?

Supply Chain Security Checklist – Software, Firmware & Test Code

Company Information

- Number of code developers?
- Name of software products provided or used?

Secure Software Development Practices

- Is any part of the code being provided being developed by 3rd parties?
- How is the security of 3rd party code developers assessed?
- How is development IT system security different from general IT system security?
- At any time, is CLOUD storage used for the development or deployment of Software, Firmware code or Test Software?
- Does the product developed go through a formal threat modeling exercise?
- Please provide a list of all interfaces to the product(s) offered (e.g. attack surface). These may include any API's or external access to the hardware, software, or firmware provided (e.g. external web interfaces, API's for UEFI or OS).

Supply Chain Security Checklist – Software, Firmware & Test Code

Secure Software Development Practices (con't.)

- Describe the process in which security testing such as Penetration Tests, Vulnerability Assessments, "fuzzing", business logic tests, functional edge, and boundary condition tests are performed?
- Are either the firmware or software binaries signed with a company private key for authenticity?
- What verification mechanisms are in place that prevent the unauthorized modification of code?
- Are source code reviews performed? Manual or Automatic?
- Is there a Product Security Incident Response Team (PSIRT)?
- What is the SLA on providing code fixes to security issues identified?
- What is the support policy for providing code updates?

Supply Chain Security Checklist – Software, Firmware & Test Code

3rd Party Provided Software or Firmware Code Security

- What 3rd party software or firmware code is received and used in product provided?
- How is the received software or firmware stored to prevent unauthorized access?
- After the 3rd party software or firmware code has been incorporated into the final product, how is that code verified that it was loaded correctly and matches the code delivered from the 3rd party?

Manufacturing Test Software

- What manufacturing tests of the product are performed that require test software to complete?
- Is any part of the test software provided by a 3rd party?
- Is the test software maintained in a secure data storage and issued to the manufacturing test computers only when needed?
- Is the test software delivered to the manufacturing test computers over a secure connection?
- How is the software on the manufacturing test computer validated to be unmodified from the original in secure storage?

Supply Chain Security Checklist – Software, Firmware & Test Code

Manufacturing Test Software (con’t.)

- Are the USB ports on the manufacturing test computers disabled to prevent unauthorized access to those computers?
- Are the manufacturing test computers isolated from public internet access?
- Has a threat analysis been performed on the manufacturing test computers to determine if unauthorized access or MiM attacks can be detected?

HARDWARE

Company Information

- Does the company participate in any US Government Security programs (C-TPAT, CIP, SCIP, BASC or other)?

Supply Chain Security Checklist – Hardware Security

Component, Sub-Assemblies, or Box Assembly

- Are the intelligent components and sub-assemblies in the hardware under source control for the supplier and supplier part numbers?
- Are Incoming Inspection procedures in place to verify the correct parts received and prevent receipt of counterfeit parts?
- How is inventory managed to prevent theft, mixed stock or wrong stock on the manufacturing line?
- Are parts or sub-assemblies stored in a secure area with restricted access?
- Are the people that have access to the secure restricted access area required to sign in or badge in and out?
- Is there lot traceability between the parts and sub-assemblies received and the final product delivered?
- Are there documented procedures for dealing with damaged inventory, scrap inventory or excess/obsolete inventory?

Supply Chain Security Checklist – Hardware Security

Shipping Container

- Is there a written policy to ensure containers are stored in a secure place to prevent unauthorized access and/or manipulation?
- Is U.S. Customs' seven-point inspection of container integrity conducted prior to stuffing the container?
- Do container seals meet or exceed the current PAS ISO 17712 standards for high security seals?
- Is all outgoing/finished product properly marked, weighed, counted, and verified against manifest documents, delivery orders, and purchase orders?
- Is the entrance and exit time of people receiving and delivering goods recorded along with the assets picked up or delivered?
- Are the people receiving and delivering goods denied access to the outgoing or incoming product inventory areas?

Supply Chain Security Checklist – Hardware Security

Freight Handlers

- Are there standards for selection of freight forwarders, carriers, and consolidators at 3rd party warehouses?

Incident Management and Investigation

- Is there a written policy or process for the timely reporting of lost and missing assets as well as anomalies in the packaging/shipping process?
- Are Investigations initiated in a timely manner?
- Is Root Cause Analysis performed as part of every investigation to understand any process deficiencies and to prevent reoccurrence?
- How is Law Enforcement involved in the investigation?

THANK YOU GRAZIE MERCI DANKE GRAZIAS 謝謝 СПАСИБО
GRACIAS OBRIGADO ありがとう DANK TAKK BEDANKT DAKUJEM