September 14, 2010 | Updated: September 17, 2010

# No More Chewy Centers: Introducing The Zero Trust Model Of Information Security

by John Kindervag

for Security & Risk Professionals

FORRESTER® Making Leaders Successful Every Day

September 14, 2010 | Updated: September 17, 2010

# No More Chewy Centers: Introducing The Zero Trust Model Of Information Security

**by John Kindervag**
with Stephanie Balaouras and Lindsey Coit

## EXECUTIVE SUMMARY

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, the first in a series, will introduce the necessity and key concepts of the Zero Trust Model.

## TABLE OF CONTENTS

## NOTES & RESOURCES

In developing this report, Forrester drew from a wealth of analyst experience, insight, and research through advisory and inquiry discussions with end users, vendors, and regulators across industry sectors.

### Related Research Documents

"SOC 2.0: Virtualizing Security Operations"
April 20, 2010

"PCI Unleashed"
January 11, 2010

"TechRadar™ For Security & Risk Professionals: Network Threat Mitigation, Q3 2009"
July 22, 2009

## FORRESTER'S ZERO TRUST NETWORK SECURITY REPORT SERIES

This is the first in a series of reports that describe the concept, architecture, and benefits of Forrester's Zero Trust Model of information security. There is a simple philosophy at the core of Zero Trust: Security 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. Thus, security professionals must verify and secure all resources, limit and strictly enforce access control, and inspect and log all network traffic.

The Zero Trust network security report series will consist of the following reports:

- **Concept.** This report will introduce the necessity and essential concepts of the Zero Trust Model of information security.

- **Architecture.** This report will outline the key architectural components, capabilities, and required technologies of the Zero Trust Model.

- **Case studies.** In a series of case studies, Forrester will highlight security organizations that have adopted or applied concepts of the Zero Trust Model in their environment. Included in the case studies will be a discussion of best practices and benefits.

## THE CHANGING THREAT LANDSCAPE: THINGS ARE NOT ALWAYS WHAT THEY SEEM

On July 9, 2010, 10 seemingly ordinary people boarded a plane at New York's LaGuardia Airport bound for Vienna.[1] They weren't tourists heading for the historic old city. They were, in fact, confessed Russian spies expelled from the US for espionage. Unlike James Bond or Jason Bourne, these individuals were not obvious spies — in fact, they were by my most accounts, extraordinarily ordinary. They were travel agents, consultants, newspaper columnists, and real estate brokers.[2] One spy even tested software for Microsoft.[3] They were so ordinary that one neighbor commented, "They couldn't have been spies. Look what she did with the hydrangeas."[4] There are some important lessons that security professionals can learn from this case:

- **The spies went undetected for years.** They may have looked like ordinary middle-class individuals, but they really worked for the Russian Foreign Intelligence Service known as the SVR.[5] According to the US Justice Department, the spies were in the US on long-term, deep-cover assignments and they worked to hide all connections between themselves and the SVR. Similarly, today's hackers go to extreme measures to avoid detection and suspicion. And they're patient: Their security breaches are no longer audacious but "low and slow," meaning they collect valuable information from the network over long periods — weeks, months, or even years.

- **The spies targeted specific organizations and individuals.** Press reports indicate that the spies were working to gain access to individuals in influential positions in the US government, including a former legislative counsel for the US Congress and a former high-ranking US government official in national security.[6] One of the agents even applied for work at prominent Washington, D.C. think tanks.[7] The agents had a clear mission: to search and develop ties in policymaking circles in the US and to send intelligence reports home.[8] Similarly, security attacks are no longer indiscriminate. Hackers often target specific companies and organizations and even target the systems with the information they want — systems that contain personal and financial information or intellectual property.

## "THE PHILIP CUMMINGS PROBLEM": CYBERCRIME MOVES INSIDE

To further understand this changing threat landscape, let's look at something we'll call "The Philip Cummings Problem." Perhaps you've never heard of Philip Cummings before, but you'll remember Philip Cummings from now on. In fact it's very important that you begin to think about The Philip Cummings Problem.

### Cybercriminals And Malicious Insiders Team Up

Philip Cummings worked on the help desk of a company called TeleData Communications, Inc. (TCI) in 1999 and 2000. TCI provided software for credit bureaus like Equifax, TransUnion, and Experian. He had access to all of the client passwords and subscription codes because he supported software on all three credit bureau networks. During his TCI employment, members of a Nigerian organized crime syndicate contacted Philip Cummings and offered him $60 for each credit report he could provide them. This, of course, was illegal. There are several important aspects of this crime that security and risk professionals should be aware of:

- **The crime continued for years after Cummings was no longer an employee.** Cummings was technically savvy enough to preprogram a laptop that enabled his crime partners to automatically download credit reports from the three credit bureaus. One of the most astonishing aspects of this crime is that it took place between 2000 and 2002 — despite the fact that Cummings had left his job in 2000. It's astonishing that neither TCI nor the credit bureaus detected the breach, but it's also astonishing that it continued for two years. Information security breaches, like national security breaches, are "low and slow."

- **The victims were not aware that cybercriminals had infiltrated their network.** The credit bureaus never discovered the crime. In fact, it was a credit bureau customer, Ford Motor Credit Company, that discovered it in 2002. According to the FBI, "Ford discovered the scheme after reviewing bills sent by Experian for those credit histories and receiving numerous complaints from consumers who had been the subject of identity theft and fraud." Like the Russian spies, Cummings and his associates went to great lengths to cover their tracks.

- **The financial impact was enormous.** The US government estimates that Cummings and his criminal counterparts stole approximately 30,000 identities, resulting in a direct financial loss of at least $2.7 million. In the end, Cummings was sentenced to 14 years in prison and $1 million in fines, and his crime remains the biggest identity theft in US history.[9] It's clear that Cummings and his associates were targeting specific systems that contained personally identifiable information, not just any random IT system with vulnerability. Similarly, the Russian spies targeted high-ranking individuals in government with access to sensitive data.

Thinking about The Philip Cummings Problem should scare you. You need to ask yourself: "Do I have a Philip Cummings in my organization? Do I have somebody who is knowledgeable, who has access to data, and whose activities I don't follow — an employee who, if somebody came in and offered a lot of money, would jump at the chance to steal from me?"

## THE TRUST MODEL IS BROKEN

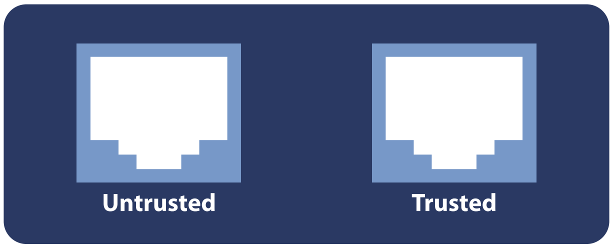
In light of Philip Cummings, clearly something is fundamentally broken in the world of information security. Even though we have a plethora of controls, attackers continually develop new threats that breach our defenses. Forrester's research shows that a new threat landscape is emerging in which organized crime and even nation-states are creating more significant, targeted attacks.

Forrester has identified 14 main controls in network threat mitigation alone. These controls include devices like firewalls, intrusion prevention systems (IPS), network access control (NAC), encrypted virtual private networks (VPNs), and Web application firewalls (WAFs).[10] With all this firepower protecting the network, it seems unimaginable that we continue to face new and more sophisticated attacks that our expensive security controls can't stop. However, there are four critical pitfalls with today's approach to network security.

### Pitfall No. 1: It's Impossible To Identify "Trusted" Interfaces

Almost every security device, such as a firewall, comes with at least one port labeled "untrusted" and another labeled "trusted" (see Figure 1). The assumption that security professionals can easily identify which network interfaces they can trust is built into the very design of the security device. However, as the Philip Cummings case illustrates, automatically assuming that you can "trust" anyone or any device inside your organization's network perimeter is a mistake. In today's threat environment, do you connect the Internet into the "untrusted" port or the "trusted" port? Do you connect the internal network into the "untrusted" port or the "trusted" port?

**Figure 1** "Trusted" And "Untrusted" Interface Ports On Today's Security Appliances



56682 Source: Forrester Research, Inc.

## Pitfall No. 2: The Mantra "Trust But Verify" Is A Joke — Literally

Many security professionals have adopted the mantra "trust but verify." However, Forrester has found that most security professionals trust a lot but verify very little. By default we trust people, but it's hard to perform the verification, so we don't do to it. In addition, there's a fundamental misunderstanding of the meaning of the phrase.

"Trust but verify"comes to our vocabulary from a speech given by President Ronald Reagan to commemorate the signing of a historic nuclear weapons treaty between the United States and the Soviet Union. By looking at the transcript of the speech, we can get a correct understanding of what it meant and how our industry has misunderstood the context:

> "The President (Ronald Reagan): But the importance of this treaty transcends numbers. We have listened to the wisdom in an old Russian maxim. And I'm sure you're familiar with it, Mr. General Secretary, though my pronunciation may give you difficulty. The maxim is: Dovorey no provorey — trust, but verify.
>
> The General Secretary (Mikhail Gorbachev): You repeat that at every meeting. [Laughter]
>
> The President: I like it. [Laughter]"[11]

Note that both world leaders laugh as Reagan recites the old Russian proverb. The success of the treaty was not built on trust at all, but on verification. Reagan and Gorbachev clearly understood that each nation would watch the other very closely. There was no trust. In the security world, we have adopted the reverse as our actual security practice — we trust by default and never verify.

## Pitfall No. 3: Malicious Insiders Are Often In Positions Of "Trust"

Cynthia Whitehead had a position of trust that she exploited. In 2009, the US Justice Department sentenced Cynthia Whitehead of Atlanta to five years and one month in federal prison on charges of wire fraud and related identity theft. What did she do? According to the Justice Department:

> "Because of the position of trust WHITEHEAD held with the company, she had access to corporate records, including personal identifiers of former employees and the mechanism for paying wages. WHITEHEAD reactivated the employment status of more than a dozen former employees in the company's data system, made entries which falsely showed that these former employees were currently working for Randstad clients, arranged for the payment of their wages, and accessed the company's payroll accounts to collect those wages for herself. Over a 3-year period, WHITEHEAD embezzled approximately $300,000."[12]

Acting US Attorney Sally Quillian Yates identified trust as one of the root causes of this crime. According to records kept by DataLossDB, there is a considerable amount of malicious insider activity (see Figure 2). Each breach is an example of a person — a trusted user — who committed a crime or insidious act deliberately.[13] It's clear how easily malicious insiders can take advantage of the flawed "trust but verify" approach to security. "Trust but verify" has become a useless buzz phrase because corporate users are trusted by default and there is no verification.

### Pitfall No. 4: "Trust" Doesn't Apply To Packets

If we can't always trust the people we have hired or contracted, why would we ever trust data flowing across our network? If you look at a network — packets moving from point A to point B — why are we even talking about trust? Trust is not an idea that we should anthropomorphize for computing. When we do, it reveals several problems:

- **We don't know who is on our networks.** There is a flawed assumption that we know who is originating the traffic on our networks. We call this identity. In computer systems, identity is ultimately unknowable. Identities are IP addresses, MAC addresses, and how you were able to log in to the domain. But the IP and MAC are easy to discover if you look at the packets, and your domain password is knowable if somebody puts a gun to your head.

- **Network identity is limited to the information that can be derived from packets.** Identity at the network level is merely an assertion of certain attributes that may be true or false, forged or real. But all we can truly know about network traffic is what is contained in packets, and packets can't tell us about the veracity of the asserted identity, let alone the intentions or incentives of the entity generating the packets. Therefore, packets can't trust and we can't trust packets. This is the ontological problem that information security professionals must confront.

**Figure 2** 2010 Breaches — Malicious Insider

| Date | Name | Data type | Total affected |
|---:|---|---|---:|
| 1/3/2010 | Transportation Security Administration (TSA) | SSN/NAA | 16 |
| 1/24/2010 | Ladbrokes | NAA/EMA/MISC/DOB | 10,000 |
| 1/29/2010 | Ameriquest Mortgage Company | SSN/NAA/FIN | 100 |
| 2/15/2010 | West Memphis Arkansas Police Department | SSN/NAA | 0 |
| 2/13/2010 | Eclipse Property Solutions | SSN/NAA | 0 |
| 2/24/2010 | Citigroup | SSN/NAA | 600,000 |
| 3/2/2010 | University of Washington Medical Center | CCN/SSN | 210 |
| 3/12/2010 | NHS Stoke on Trent | NAA/MED | 2,000 |
| 3/17/2010 | University of Calgary Medical Clinic-Sunridge | MED | 4,700 |
| 3/23/2010 | H&R Block | SSN/NAA/DOB | 60 |
| 3/25/2010 | Northwestern Medical Faculty Foundation | NAA/MED | 250 |
| 3/24/2010 | Washington School Information Processing Cooperative (WSIPC) | SSN/NAA/ACC/DOB/FIN | 5,000 |
| 1/4/2010 | Time | CCN/NAA | 0 |
| 1/22/2010 | Seattle Municipal Court | CCN | 0 |
| 1/19/2010 | Minnesota Department of Labor and Industry | ACC/FIN | 759 |
| 2/17/2010 | T.G.I. Friday's (Coon Rapids, Minn.) | CCN | 0 |
| 2/19/2010 | Group Health Cooperative Health Care System | CCN/NAA/MISC/MED/FIN | 1,700 |
| 1/6/2010 | Association for the Blind and Visually Impaired | MISC/ACC/FIN | 50 |
| 3/7/2010 | Diabetes Direct | SSN/NAA/MISC/MED/DOB | 0 |
| 3/30/2010 | Griffin Hospital | NAA/MED | 957 |
| 4/8/2010 | St. Francis Hospital | SSN/NAA/MED/DOB | 60 |
| 4/8/2010 | H&R Block | SSN/NAA/DOB | 20 |
| 4/26/2010 | Texas Child Protective Services Division | SSN/NAA | 70 |
| 5/26/2010 | Payless Travel & Cruises | CCN/NAA | 0 |
| 6/2/2010 | Bank of America | SSN/NAA/MISC/DOB | 0 |
| 6/17/2010 | Ocean Lakes High School | SSN/NAA/DOB | 0 |

Source: DataLossDB (http://datalossdb.org/)

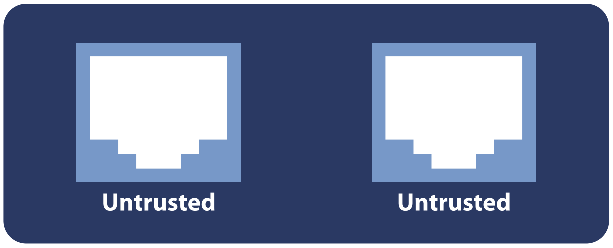
56682 Source: Forrester Research, Inc.

## NO MORE CHEWY CENTERS: INTRODUCING ZERO TRUST

If the current trust model is broken, how do we fix it? It requires a new way of thinking. The way we fix the old trust model is we begin at the beginning and look for a new trust model. Forrester calls this new model "Zero Trust." The Zero Trust Model is simple: Security 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 (see Figure 3).

Thus, security professionals must verify and secure all resources, limit and strictly enforce access control, and inspect and log all network traffic. Much of this can be automated so that it doesn't become burdensome. There are three fundamental concepts of our Zero Trust Model.

**Figure 3** In Zero Trust, All Interfaces Are Untrusted



56682 Source: Forrester Research, Inc.

### Concept No. 1: Ensure That All Resources Are Accessed Securely Regardless Of Location

When you eliminate the concept of trust from the network, it becomes natural to ensure that all resources are securely accessed — no matter who creates the traffic or where it originates from. In the Zero Trust Model, security professionals must assume that all traffic is threat traffic until it is verified 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 sniff 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.[14]

### Concept No. 2: Adopt A Least Privilege Strategy And Strictly Enforce Access Control

The next concept in Zero Trust is access control. When we properly implement and enforce access control, by default we help eliminate the human temptation for people to access restricted resources. For example, in 2008, officials caught several US State Department employees accessing the passport records of several presidential candidates.[15] The employees were subsequently fired, and some were criminally prosecuted successfully.[16] One defendant, Gerald Lueders, admitted that he accessed the passport applications out of "idle curiosity."[17] This case illustrates why access control is so important. Not only can it help protect against malicious attacks but it will keep embarrassing and life-destroying incidents like the US State Department passport scandal from happening.

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. With RBAC, security professionals place users into a role and based upon that role they are allowed access to certain specific resources. Zero Trust does not explicitly define RBAC as *the* preferred access control methodology. Other technologies and methodologies will evolve over time. What's important is the concept of minimal privileges and strict access control.

### Concept No. 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. But Zero Trust does not stop there. Instead of trusting users to do the right thing, we verify that they are doing the right thing. To do this we simply flip 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 doesn't 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. Based on our experiences and evidenced by such data breaches as Heartland Payment Systems and the recently announced US Military Central Command attack, Forrester believes that there is very little inspection of internal network traffic.[18]

## ZERO TRUST REQUIRES NETWORK ANALYSIS AND VISIBILITY

In Zero Trust, we inspect and log all traffic internally as well as externally. We've been so worried about the perimeter, we forgot about the malicious user on our internal network. In today's network, companies have focused their controls on the perimeter, and now is the time to add controls on the internal network as well as the external network. Once there are appropriate controls deployed throughout the entire network, security professionals must then log that data so we see all the traffic that is traversing our network.

To do this Forrester recommends deploying network analysis and visibility (NAV) tools in conjunction with your traditional security information management (SIM) system. NAV is a space we have defined to bring together a diverse set of tools that have a similar functionality. These include network discovery tools, tools that analyze flow data, tools that dissect packet captures, tools that look at network metadata, and tools used for network forensic examination.[19] The purpose of NAV products is twofold; it:

- **Gives security professionals insight into the network.** One purpose of NAV is to give security professionals insight into what is actually going on in their network and verify access and behavior on the network. There is an assumption that we need to monitor all applications individually in order to know who is accessing each application and what actions users have taken on the application. However, implementing various controls and agents on each application in a large organization is not scalable. Luckily, in order for an application to work, traffic must traverse the network. It is much easier and more efficient to reconstruct and review what is happening on the application level by analyzing network traffic than it is to try and monitor hundreds or even thousands of individual applications.

- **Sends a message to potential malicious insiders.** Once NAV is deployed, tell people that you're going to be watching what they do. This will change behaviors. If individuals know that security is monitoring their actions, they will be less tempted to do things that are questionable. If the convicted US State Department employees had known that IT was tracking their activities, they might not have gone and looked at the presidential candidates' passport information.

## ZERO TRUST WILL ENABLE THE EMPOWERED ENTERPRISE

The Empowered Enterprise gives employees access to new social tools to enhance business efficiency and serve their customers better. With this empowerment comes the potential for misuse and abuse of these technologies. Clearly, security professionals can no longer fight the rising tide of consumerization of the enterprise; Facebook and Twitter have become integral business tools that will not be banned. The task for IT security, therefore, is to establish oversight, mitigate risks, and consequently provide consistent, long-term support for these otherwise fragmented, ad hoc adoption initiatives. Zero Trust is an essential component to this strategy. The Zero Trust framework provides a secure foundation for the Empowered Enterprise — if you can inspect and log every user, every device, and every access point, you can create more granular and informative policies and controls that discover and mitigate the misuse and abuse of these consumer technologies. This, in turn, will further empower and energize your business.

## RECOMMENDATIONS

### ZERO TRUST IS NOT A ONE-TIME PROJECT

Zero Trust is designed to provide a new conceptual model for information security that includes modern threats and anticipates the need for changes in the future. It is designed to be incremental and nondogmatic. Its purpose is to help create a new dialogue about the future of information security that can lead to actionable and effective solutions. But to do this we must first attack the fundamental flaw in information security — trust. Thus, Zero Trust is not a project but a new way of thinking about information security. By adopting the concepts of Zero Trust and the architectural components that Forrester will detail in upcoming reports, we believe that organizations can become more secure in an efficient way that eases compliance burdens and ultimately reduces costs. As you embark on the Zero Trust journey, there are two steps that you can take now, both of which are free.

- **Step 1: Change how you think about trust.** This involves changing your thinking about trust models and becoming aware of the misuse of the word "trust" in relation to networking and security. Once attuned to how inappropriate trust is in the infosec realm, you can socialize the Zero Trust concept throughout the organization. The basic idea is simple and resonates with both infrastructure and operations and security and risk professionals. Use Zero Trust to begin dialogues among teams about how the core concepts can be added to existing networks.

- **Step 2: Integrate Zero Trust into future planning.** Forrester's clients are looking at issues such as network segmentation, virtualization security, and compliance issues that can all benefit from the ideas implicit in Zero Trust. Budgets intended for traditional security upgrades may well be more attractive and effective if done within the concept of Zero Trust. The network is at an inflection point, where compliance pressures and new technologies are creating a need to rethink current network and security deployments. Throw Zero Trust into the mix and begin to ask if these concepts can be leveraged to ease your compliance and technological burdens.

## ENDNOTES

[1] Source: Jim Heintz, Veronika Oleksyn, and Vanessa Gera, "US and Russia Swap Spies in Vienna," *The Boston Globe,* July 9, 2010 (http://timelines.boston.com/timelines/russian-spy-ring/2010/7/9/us-and-russia-swap-spies-in-vienna).

[2] Source: David Voreacos and David Glovin, "'Deep Cover' Spies Worked Day Jobs to Glean Data for Russia," Bloomberg, July 1, 2010 (http://www.bloomberg.com/news/2010-06-29/-deep-cover-russian-spies-had-day-jobs-including-consultant-columnist.html).

[3] Source: Charles Arthur, "Russian spy worked for Microsoft," *The Guardian*, July 14, 2010 (http://www.guardian.co.uk/technology/2010/jul/14/russian-spy-worked-for-microsoft).

[4] Source: Scott Shane and Charlie Savage, "In Ordinary Lives, U.S. Sees the Work of Russian Agents," *The New York Times*, June 28, 2010 (http://www.nytimes.com/2010/06/29/world/europe/29spy.html).

[5] In Russian: Sluzhba Vneshney Razvedki.

[6] "According to the FBI, some of the people the accused spies met with include a former legislative counsel for U.S. Congress, a former high ranking U.S. government national security official, a person working on bunker busting nuclear warheads, and a New York financier who is prominent in politics and a major fundraiser for an un-named political party." Source: Jason Ryan and Megan Chuchmach, "Russian Spy Ring Suspects Busted! 10 Alleged Secret Agents Arrested in U.S.," ABC News, June 28, 2010 (http://abcnews.go.com/Blotter/russian-spy-ring-10-accused-russian-spies-arrested/story?id=11037360&page=1).

[7] Source: Toby Harnden and Michele Walk, "Russian spy applied for jobs at think tanks with links to Obama," *The Daily Telegraph*, July 8, 2010 (http://www.telegraph.co.uk/news/worldnews/northamerica/usa/7879850/Russian-spy-applied-for-jobs-at-think-tanks-with-links-to-Obama.html).

[8] Source: "UNITED STATES OF AMERICA -v- ANNA CHAPMAN, and MIKHAIL SEMENKO, Defendants," US Department of Justice, June 27, 2010 (http://www.justice.gov/opa/documents/062810complaint1.pdf).

[9] Source: "UNITED STATES OF AMERICA -v- PHILIP CUMMINGS, Defendant," FindLaw, November 22, 2002 (http://news.findlaw.com/wsj/docs/crim/uscummings112202cmp.pdf) and "U.S. Announces What Is Believed The Largest Identity Theft Case In American History; Losses Are In The Millions," US Department of Justice, November 25, 2002 (http://www.justice.gov/criminal/cybercrime/cummingsIndict.htm).

[10] The news is filled with reports of networks attacks and stolen data. Consumers routinely undergo the stress of fraudulent charges or compromised credit cards. Terms such as "botnet" have become part of our vocabulary. As a result, security and risk professionals find themselves on a never-ending quest to maintain the integrity of their networks. To provide some insight into the vast array of options available to meet today's threats, Forrester investigated 14 threat mitigation technologies, including encryption, wireless IDS/IPS, unified threat management, and Web content filtering. Compliance-driven products, such as Web application firewalls and network firewalls, continue to remain strong in the enterprise. Network IDS and IPS continue to play in both the best practice and compliance arenas, with IPS poised to replace IDS in most organizations. Also, recent data breaches will benefit the adoption of emerging technologies such as network encryption and firewall auditing tools. See the July 22, 2009, "TechRadar™ For Security & Risk Professionals: Network Threat Mitigation, Q3 2009" report.

[11] Source: "Remarks on Signing the Intermediate-Range Nuclear Forces Treaty," Ronald Reagan Presidential Library, December 8, 1987 (http://www.reagan.utexas.edu/archives/speeches/1987/120887c.htm).

[12] Source: "Former Randstad Branch Manager Sentenced to Federal Prison for Embezzlement," US Department of Justice, September 16, 2009 (http://www.justice.gov/usao/gan/press/2009/09-16-09c.pdf).

[13] Source: DataLossDB (http://datalossdb.org/).

[14] Zero Trust builds upon the deperimeter ideas first socialized by the Jericho Forum. For more information, go to The Open Group Web site. Source: The Open Group (https://www.opengroup.org/jericho/index.htm).

[15] Source: "Passport files of candidates breached," MSNBC, March 21, 2008 (http://www.msnbc.msn.com/id/23736254/).

[16] Source: "Third Individual Pleads Guilty to Illegally Accessing Confidential Passport Files," US Department of Justice, January 27, 2009 (http://www.justice.gov/opa/pr/2009/January/09-crm-066.html).

[17] Source: "Former State Department Employee Sentenced for Illegally Accessing Confidential Passport Files," US Department of Justice, July 8, 2009 (http://www.justice.gov/opa/pr/2009/July/09-crm-666.html).

[18] A recent article in *The Washington Post* reports that the US Military's Central Command network was infected by "malicious code placed on the [flash] drive by a foreign intelligence agency [that] uploaded itself

onto a network run by the US Military's Central Command." The story quotes a US Defense Department official saying the "code spread undetected on both classified and unclassified systems." Source: Ellen Nakashima, "Defense official discloses cyberattack," *The Washington Post,* August 24, 2010 (http://www.washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406154.html?hpid=topnews).

[19] The Zero Trust concept of NAV shares similarities with, and is indebted to, the idea of network security monitoring (NSM) as advocated by Richard Bejtlich in his book *The Tao of Network Security Monitoring: Beyond Intrusion Detection*. In the book, Bejtlich defines NSM as "the collection, analysis, and escalation of indications and warnings (I&W) to detect and respond to intrusions." Zero Trust adds packet inspection of all internal traffic to NSM and looks beyond intrusion alerting to proactive discovery of all types of network abuse. Source: "Network Security Monitoring History," *TaoSecurity*, April 11, 2007 (http://taosecurity.blogspot.com/2007/04/network-security-monitoring-history.html).

FORRESTER®

Making Leaders Successful Every Day

## Headquarters

Forrester Research, Inc.
400 Technology Square
Cambridge, MA 02139 USA
Tel: +1 617.613.6000
Fax: +1 617.613.5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

## Research and Sales Offices

Forrester has research centers and sales offices in more than 27 cities internationally, including Amsterdam; Cambridge, Mass.; Dallas; Dubai; Foster City, Calif.; Frankfurt; London; Madrid; Sydney; Tel Aviv; and Toronto.

*For a complete list of worldwide locations visit www.forrester.com/about.*

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com.
We offer quantity discounts and special pricing for academic and nonprofit institutions.