FORRESTER®

For: Security &
Risk Professionals

The Future Of Data Security: A Zero Trust Approach

by John Kindervag, Heidi Shey, and Kelley Mak, June 5, 2014

KEY TAKEAWAYS

As The Business Becomes Digital, Security Must Become Data-Centric

S&R leaders of enterprises undergoing a digital transformation will soon realize that in order to adequately ensure customer protection and enable a digital workforce, S&R pros must abandon traditional perimeter-based security and put the focus on the data by embracing Forrester's Zero Trust Model.

Forrester's Data Security And Control Framework Puts Security Closer To The Data

Forrester has created a framework to help S&R professionals embark on the data security journey. Forrester's data security and control framework breaks the problem of controlling and securing data down into three areas: 1) defining the data; 2) dissecting and analyzing the data; and 3) defending and protecting the data.

Data Holds Powerful Potential, But It Can Also Be Dangerous

The promise of big data and digital businesses has just started to be realized. However, the erosion of trust that can occur when customers lose confidence in an enterprise's commitment and ability to protect their privacy and personal data can be devastating. Take the necessary steps to prepare for the digital revolution today.

The Future Of Data Security: A Zero Trust Approach

Vision: The Data Security And Privacy Playbook

by John Kindervag, Heidi Shey, and Kelley Mak
with Stephanie Balaouras and Katherine Williamson

WHY READ THIS REPORT

Data is the lifeblood of today's digital businesses, and protecting it from theft, misuse, and abuse is the No. 1 responsibility of every S&R leader. Hacked customer data can erase millions in profits within weeks, stolen intellectual property can erase competitive advantage in less than a year, and unnecessary privacy abuses can bring unwanted scrutiny and fines from regulators while inflicting reputational damage that can last months, even years. Achieving a certain level of data security and protecting customer privacy is no easy feat. Almost every enterprise, from an online retailer to a hospital to a government agency, rarely works in isolation and can rarely confine data to within the four walls of the organization. The walls don't exist. They must work in a complex ecosystem of powerful customers increasingly concerned about their privacy, digitally native employees, and potentially hundreds of demanding partners and suppliers — all perpetually connected by new systems of engagement and cloud services. In this new reality, traditional perimeter-based approaches to security are insufficient. S&R pros must take a data-centric approach that ensures security travels with the data regardless of user population, location, or even hosting 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 industry experts.

Related Research Documents

TechRadar™: Data Security, Q2 2014
April 22, 2014

Strategy Deep Dive: Define Your Data
April 5, 2013

Know Your Data To Create Actionable Policy
January 15, 2013

Kill Your Data To Protect It From Cybercriminals
July 12, 2012

DIGITAL BUSINESSES REQUIRE A DATA-CENTRIC SECURITY APPROACH

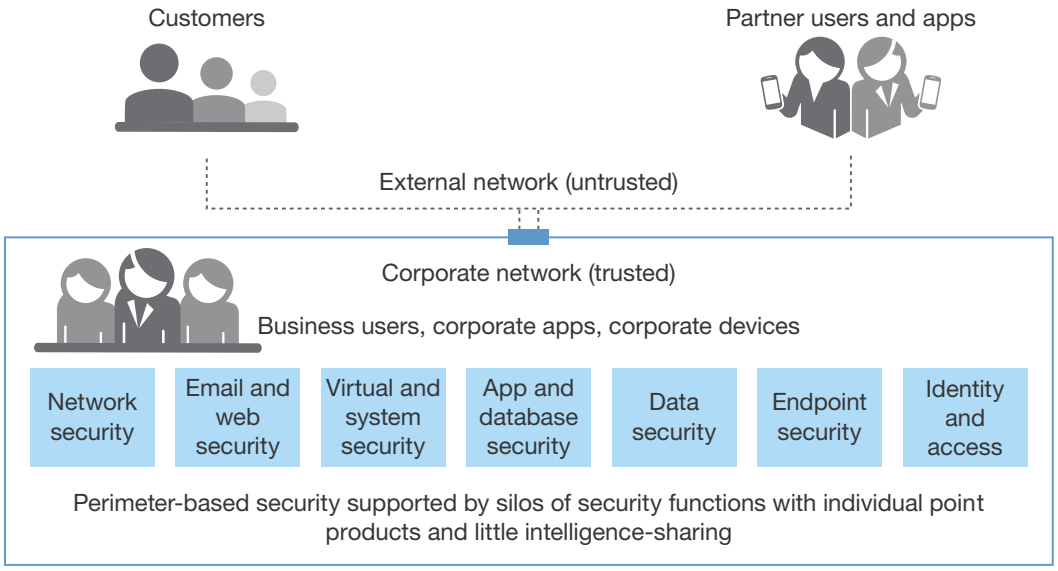
When you're trying to protect your organization's intellectual property (IP) and sensitive data assets, security and risk (S&R) leaders of enterprises undergoing a digital transformation will soon realize that there is fatal flaw in the main assumption underpinning perimeter-based security — the assumption that there is a "trusted" internal network where data is safe and an "untrusted" external network where data is unsafe (see Figure 1). This implicit trust assumption is both incredibly naive and untenable in a digital enterprise because it fails to:

- **Adequately protect customers' data security and privacy.** You must protect customers' data not only from cybercriminals but also from individuals operating inside the "trusted" network: malicious insiders cooperating with cybercriminals or driven by other motivations, whether political, social, or retaliatory; unwitting employees that accidentally leak sensitive data through email, file sharing, social networks, and other channels; and even well-intentioned employees who unintentionally violate privacy laws and/or tenets of good taste while processing and using customer data in efforts to personalize advertising, products, and services. In Verizon's 2014 Data Breach Investigations Report, researchers found that more than a quarter of incidents were caused by miscellaneous errors like accidental online publishing or sending an email to the wrong recipient.[1]

- **Enable a digital workforce while simultaneously guarding sensitive data.** The scale and diversity of personal devices are exploding, as is the spread of enterprise and consumer mobile apps and cloud services that employees can access from any browser. At most enterprises, bring-your-own-device (BYOD) is a foregone conclusion. On average, 15% of employees are accessing sensitive data such as customer information, nonpublic financial data, intellectual property, and corporate strategy from devices other than work laptops and desktops.[2] So it's now far less important to focus on protecting individual devices the organization no longer owns, or attempting to lock down the devices that connect to the network, and far more important to protect the organization's sensitive data regardless of device type or location.

- **Securely integrate partners and suppliers into business operations.** A business function is rarely, if ever, a self-contained workflow within the infrastructure confines of the company. Something as simple as onboarding a new customer and fulfilling an order could potentially include the services of a global payment processor; your own eCommerce, CRM, and ERP platforms (hosted in the cloud or on-premises); and warehouse and other logistics partners that deliver your products. These partners often need access to your network or specific data to do their jobs, but too much access can lead gaping holes in security. Retailer Target Brands was breached in late 2013 as a result of attackers compromising its HVAC provider's access to Target's systems.[3]

Figure 1 Yesterday's Traditional Perimeter-Based Security



Source: September 12, 2013, "Transform Your Security Architecture And Operations For The Zero Trust Ecosystem" Forrester report

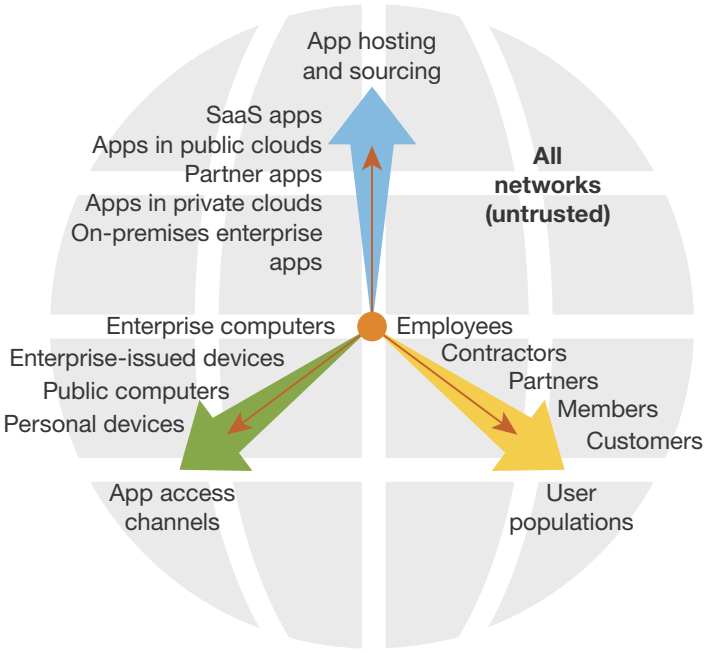
61244 Source: Forrester Research, Inc.

Apply A Zero Trust Lens To Data Security

Forrester's Zero Trust Model states that S&R pros must eliminate the idea of a trusted internal network and an untrusted external network. Three concepts underpin Zero Trust. S&R pros must: 1) verify and secure all resources regardless of location; 2) limit and strictly enforce access control across all user populations, devices/channels, and hosting models; and 3) log and inspect all traffic, both internal and external. To accomplish this, S&R pros need visibility into the interaction between users, apps, and data across a multitude of devices and the ability to set and enforce one set of policies irrespective of whether the user is connected to the corporate network (see Figure 2).

Unlike legacy, perimeter-based approaches to security, Zero Trust: 1) never assumes trust; "trust" is continuously assessed though a risk-based analysis of all available information; 2) fundamentally shifts the focus from the perimeter to the data itself; and 3) marshals the functions of many security domains (e.g., network, identity, application security, etc.) in a unified approach to data protection.

Figure 2 A Zero Trust Approach To Data Security



Data-centric security supported by integrated security functions and consolidated controls that form a security ecosystem

Data control and intelligence

Data control — the ability to apply universal security policies to protect sensitive data regardless of location, device type, hosting model, or user population. This requires the ability to:

- Inventory and classify data across networks, devices, and apps.
- Encrypt data in-flight-to and at-rest in any application, device, or network regardless of location.
- Enforce access control across user populations, apps, and devices.
- Apply and enforce declarative policy dynamically via APIs.

Intelligence — combining real-time analysis and visibility with contextual information to identify threats, address vulnerabilities, and uncover incidents in progress. This requires:

- Real-time analysis and visibility across networks, devices, apps, user, and data.
- Contextual information about the user, transaction risk, and overall security state such as traffic flows, device state, user identity and biometrics, behavior, app state, app classification, data classification, location, and time.

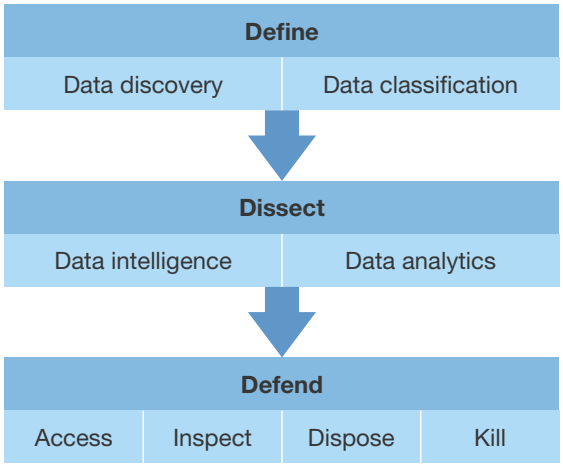
Source: September 12, 2013, "Transform Your Security Architecture And Operations For The Zero Trust Ecosystem" Forrester report

61244 Source: Forrester Research, Inc.

INTRODUCING FORRESTER'S DATA SECURITY AND CONTROL FRAMEWORK

Ideally, now is the time to bring together separate silos of data control and security such as archiving, DLP, and access management and move these controls closer to the data itself, instead of at the edges (perimeters) of networks. In organizations that are complex or that have huge amounts of data, S&R pros often don't know where to start. Forrester has created a framework to help S&R professionals embark on this journey. We break the problem of controlling and securing data down into three areas: 1) defining the data; 2) dissecting and analyzing the data; and 3) defending and protecting the data (see Figure 3).

Figure 3 Forrester's Data Security And Control Framework



61244 Source: Forrester Research, Inc.

Defining The Data Simplifies Its Control

Today, enterprises don't talk about terabytes of data; they talk about petabytes of data. Companies generate data every day, and in many cases, they're amassing vast amounts of data in "big data" stores. Few enterprises have proper data governance in place, and, as a result, they have data strewn across global data centers, computer rooms, remote offices, laptops, desktops, mobile devices, and now, even cloud storage. You can't protect it all: It's too operationally complex to encrypt *everything*, and it's too costly given that most security budgets have only grown by single digits in the past few years. Therefore, S&R professionals, together with their counterparts in legal and privacy, should define data classification levels based on toxicity.[4] This allows security to properly protect data based on its classification once security knows where that data is located in the enterprise. Discovery and classification are critical, because:

- **Data discovery locates and indexes data.** To protect data, you must first know where users have stored it. Unfortunately, data — especially toxic data — has proliferated throughout the enterprise and can be difficult to discover. This is one of the significant struggles when security professionals attempt to deploy a DLP technology — if you can't locate where the enterprise stores its sensitive information, you don't know where to deploy the DLP technology.[5] Without strong policies in place regarding data handling, storage, and records management, users have stored sensitive information on laptops and even mobile devices that are often outside the control of security teams. S&R professionals, together with legal and privacy teams, must undertake a data discovery project to locate and index existing data and develop a life-cycle approach that continuously discovers data as users create it throughout the extended enterprise network.

- **Data classification catalogs data to make it easier to control.** S&R pros can't properly protect data until it has been classified. Each data chunk must contain information that lets various users and tools understand the level of toxicity implicit in that data. Data classification can be an arduous process, and organizations will try to skip this step. Don't let your organization do that — proper data defense depends on accurate classification. Effective classification can indicate whether you must archive the data for regulatory compliance purposes (e.g., to comply with SOX or SEC Rule 17a-4) or whether it's subject to a regulation such as the Payment Card Industry Data Security Standard (PCI DSS). PCI mandates that security professionals protect cardholder data according to strict guidelines.[6]

Dissecting Data Helps Determine Its Value To The Business And To Security

Data classification is not a one-time event; S&R pros must continuously reassess classification as conditions change. In addition to the classification of the data, S&R pros also need to have continuous visibility into the changing threats to the data. Look for security information management (SIM) and network analysis and visibility (NAV) solutions to intersect with big data to enhance security decision-making. More specifically:

- **Data intelligence provides business and other contextual insights about data.** The classification of data (e.g., individual files, emails, database fields, etc.) can change as the value of the data changes over time. And some data such as acquisition plans or product road maps can be toxic one day and unimportant the next, after the deal completes or the successful launch of a new product. Classifications can also change because of changes in government or industry regulations. In addition to changing classification, it's important to understand the current state of data. Has someone compromised its integrity? Is there an exfiltration in process? How does data normally flow through the organization? For example, by linking SIM and NAV data, companies will be able to determine the state of their network in near real time, thereby finding potential breaches or insider abuse much more quickly.

- **Data analytics identifies changing threats to data and guides decision-making.** To have more insights into the changing threats to data, S&R pros must do a much better job of anticipating threats to their industry and enterprise, targeting efforts where it matters most, and limiting the damage of breaches that have already occurred. The promise of analytics, in some cases, married with big data processing, includes the ability to analyze more and more data in near real time to more proactively protect toxic data. Security pros should anticipate using this data more efficiently to prioritize security initiatives and more effectively place the proper security controls. For example, comparing vulnerability data with device configuration and real-time threat data will tell the organization where its most vulnerable assets lie and help it create defenses that are more targeted and proactive.

Additionally, look for more precise threat intelligence offerings as these vendors take advantage of big data. Ingesting threat intelligence that's specifically about attackers targeting your organization and aligning that data with your internal big data analytics platform will provide a powerful defensive advantage against new threats.

Defending Data Protects It From The Vast Array Of Modern Threats

As the number of attacks increases and their sophistication improves, it's clear that S&R professionals must do a better job of defending data. Our data security and control framework provides basic ways to defend and protect data:

- **Access control ensures that the right user gets access to the right data at the right time.** One of the tenets of Forrester's Zero Trust Model of information security is that you should limit access to all resources according to the principle of least privilege and strictly enforce this access control.[7] Amassing greater data volumes increases the risk that a cybercriminal or insider (malicious or otherwise) can readily compromise sensitive information. Therefore, to secure data throughout your ecosystem, you should strictly limit the number of people that can access data and continuously monitor those users' access levels throughout their employment. Security professionals don't always recertify access when an employee shifts roles within the company. Employees often accumulate access and privileges as they are promoted or transferred within the organization.[8] Even more alarming, they often don't have much insight into the access privileges of third-party users with whom data is shared.[9]

- **Inspecting data usage patterns can alert security teams to potential abuses.** It's impossible to protect against attacks you can't see. Both external cybercriminals and malicious internal users will leave artifacts of their attempts to breach your data security controls. Our Zero Trust Model mandates that you inspect and log all traffic on both your internal and external networks. You can accomplish this by deploying NAV tools such as metadata analysis, packet capture analysis, or flow analysis tools and integrating them with your SIM solution to give you the unparalleled network visibility you need to proactively protect toxic data.[10]

- **Disposing of data when the enterprise no longer needs it is a powerful defensive tactic.** Cybercriminals and malicious insiders can't steal or breach data that no longer resides in your ecosystem. Through day-to-day business processing and big data efforts, the enterprise will collect significant amounts of garbage data, and data typically loses its value to the business as it ages. Corporate policy will also specify the length of time that technology management pros must retain data for regulatory compliance or broader information governance purposes. With proper classification and supporting controls, you can defensively dispose of any toxic data no longer required by real business interests, compliance mandates, or data preservation obligations for investigations or litigation.[11] Resist the temptation to keep every byte of data just because you can. Remember, defensibly disposing of data in accordance with your retention policies mitigates legal risks, cuts storage and other IT costs, and reduces the risk of a data breach.

- **"Killing" data devalues it so that cybercriminals can't use or sell it.** Cybercriminals use underground markets on the Internet to buy and sell toxic data such as credit card numbers, credit reports, and even intellectual property. This underground market operates according to the economic principles of supply and demand. If we can take away the value of data, we can eliminate incentives to steal it. You can devalue or "kill" data using data abstraction techniques such as encryption, tokenization, and masking.[12] Generally, cybercriminals can't easily decrypt or recover data that one has encrypted or otherwise abstracted — and then that data no longer has any value on a black market. Look for an increase in the deployment of data-killing technologies like encryption as big data needs grow.

RECOMMENDATIONS

DON'T SHY AWAY FROM DATA SECURITY

As enterprises embark on digital transformation and big data initiatives become more important, S&R leaders must work to create awareness and understanding of the associated responsibilities and risks at the highest levels of the organization. These radical new changes will create new challenges and responsibilities for already overburdened security organizations. However, there are several things you can do to prepare for the digital revolution today:

- **Move your controls closer to the data itself.** 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. By placing controls as close as possible to the data store and the data itself, you can create a more effective line of defense.

- **Leverage existing technologies to control and protect data.** Most security organizations have already deployed numerous data security technologies, such as database activity monitoring and database encryption. As data volumes explode and data formats and types proliferate, vendors of these technologies will quickly upgrade their products to deal with the vast array of unstructured data types and even new platforms specifically for big data environments.

- **Look to new solutions for cloud visibility and data protection.** Gain visibility into the types of cloud services in use within the enterprise and monitor services' use with help from vendors like Aladom, CipherCloud, CloudPassage, illumio, JumpCloud, and Skyhigh Networks.[13] Cloud encryption solutions like those from CipherCloud, nCrypted Cloud, Perspecsys, Skyhigh Networks, Vaultive, and Voltage Security can help to encrypt data before it goes into the cloud.

- **Always seek to control your encryption keys.** Bring your own encryption, or hold the keys to your kingdom. The Snowden/NSA leaks have raised questions and concerns about government surveillance and access to data, sparking discussions between service providers and customers about the security and privacy of their data. For example, in the case of many file-sharing and

collaboration solutions, there are currently few service providers that provide customers with the native capability and option to hold their own keys; some fill the gap by integrating with a third-party partner for encryption that allows the customer to hold the key.[14] However, given market demand for this feature, many are working to offer this capability natively.

- **Ask legal to define clear policies for data archiving and data disposal.** As data volumes grow into the petabytes, protecting sensitive information becomes an almost Herculean task for the security organization. Data security becomes more manageable and realistic when you reduce data volumes. Imagine that your organization no longer stores every terabyte of information it collects or generates, but follows defensible disposal practices to archive information and then delete it when its value to the business declines or its retention policy expires (provided that the information in question isn't subject to eDiscovery or investigative preservation obligations). In this scenario, discovering, dissecting, and defending your sensitive information is much easier.

- **Diligently control access to data resources and watch user behavior.** Always remember that every byte of data could contain information about people — customers, employees, and business partners. Remember that global privacy laws mandate that you protect their personal information and that no one deserves to have their finances and credit destroyed by a cybercriminal. Also remember that intellectual property such as trademarks, formulas, and product designs is the key to your organization's global competitive advantage. To protect personal data and intellectual property, your first line of defense is to limit data access to only those individuals whose job function requires it. It is no longer acceptable to allow unfettered data access to the vast majority of your employees. You must then monitor those users for proper data access behavior.

WHAT IT MEANS

PROTECT CUSTOMER DATA LIKE IT WAS YOUR OWN

Data is powerful — but data is also dangerous. The wrong data falling into the wrong hands can have devastating consequences. Sony's 2011 PSN breach cost the company $170 million in hard costs and potentially more than $1 billion in lost opportunities. Target's 2013 breach contributed to a 46% decline in profits; publicly, Target reported breach expenses totaling $61 million in the fourth quarter of 2013 alone.[15] While the cost of breach remediation and IP theft remain unacceptably high, the prevailing concern is the erosion of trust that can occur when customers lose confidence in an enterprise's commitment and ability to protect their privacy and personal data. Today's empowered customers don't have to do business with you — they have to want to do business with you. And if you don't live up to the trust they place in you, those customers will take their business elsewhere.

ENDNOTES

[1] Source: "2014 Data Breach Investigations Report," Verizon (http://www.verizonenterprise.com/DBIR/2014/).

[2] To increase the productivity for information workers on the go and customer-facing employees, technology management leaders must provide employees with access to business apps, collaboration tools, and data. To be a business enabler, S&R pros must understand how mobile strategies for management and security are shifting from devices to apps and data. For more information, see the February 3, 2014, "The State Of Enterprise Mobile Security, Q1 2014: Strategies Shift From Devices To Apps" report.

[3] Source: Jon Oltsik, "Lessons Learned from the Target Breach," Networking Nuggets and Security Snippets, March 27, 2014 (http://www.networkworld.com/community/blog/lessons-learned-target-breach).

[4] 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. For more information on defining data, see the April 5, 2013, "Strategy Deep Dive: Define Your Data"report.

[5] Data loss prevention or protection (DLP) — depending upon your usage — is both one of the hottest topics and most difficult challenges among information security professionals today. However, failed projects and continued challenges have smashed the hope of a DLP technology as a silver bullet that can provide total data security. Forrester looked at DLP with a different lens and realized that security pros needed to approach DLP as an ongoing process, not a product or even a one-time project. For more information, see the January 3, 2012, "Rethinking DLP: Introducing The Forrester DLP Maturity Grid" report.

[6] PCI is controversial and is here to stay. It's time to move beyond complaining and embrace PCI to extract value. For more information on PCI guidelines, see the January 11, 2010, "PCI Unleashed" report.

[7] Forrester has developed a new model for information security, called Zero Trust. Information security professionals must eliminate the soft chewy center by making security ubiquitous throughout the network, not just at the perimeter. For more information on the Zero Trust Model of information security, see the November 15, 2012, "No More Chewy Centers: Introducing The Zero Trust Model Of Information Security" report.

[8] Protecting against a breach is difficult because you have an enormous amount of data to protect stored in many silos and growing at an alarming rate. Security professionals often turn to technologies such as data leak prevention (DLP) and enterprise rights management (ERM), but these don't perform well alone without an identity context. You need to have a full understanding of how users join, move, and leave the enterprise so that you can assign and revoke access to sensitive data assets. For more information on access management and privileges, see the June 27, 2011, "Your Data Protection Strategy Will Fail Without Strong Identity Context" report.

[9] Human error, in addition to data security policy and data handling process failures, is a common cause of data breach and security incidents. In 2013, out of 1,460 publicly reported cyberevents, 325 were caused by a data governance failure, representing 22% of incidents overall. As employees engage in collaboration and file sharing, do so from various device types, or seek to sync files across devices for easy access on the go, they also risk losing or exposing information. For more information, see the February 4, 2014, "Market Trends: Secure File Sharing And Collaboration In The Enterprise, Q1 2014" report.

[10] Forrester's new Zero Trust Model of information security demands that organizations know what types of activities take place on their internal network as well as their external network. To provide this type of deep insight into internal and external networks, Forrester has defined a new functional space called network analysis and visibility (NAV). For more information, see the January 24, 2011, "Pull Your Head Out Of The Sand And Put It On A Swivel: Introducing Network Analysis And Visibility" report.

[11] Many enterprises report significant eDiscovery challenges, and awareness of key process elements varies greatly across IT, legal, records management, security, and other functional roles. For a review of eDiscovery concepts, see the December 15, 2010, "Q&A: eDiscovery Fundamentals For Content & Collaboration Professionals" report.

[12] To avoid the hype and take a holistic and long-lasting approach to data security that encompasses people, processes, and technology, we developed Forrester's data security and control framework. We developed a TechRadar that assesses 20 of the key traditional and emerging data security technologies that S&R leaders and their staff can use to underpin the best practices and recommendations of our framework. For more information, see the April 22, 2014, "TechRadar™: Data Security, Q2 2014" report.

[13] Complexity of cloud security will only expand as departments use more cloud services. A new breed of cloud security vendors has emerged that restores the ability to discover, analyze, and control corporate data in the cloud. For more information, see the March 13, 2014, "Protect Your Data In The Cloud" report.

[14] Most file sharing and collaboration solutions encrypt data at rest via 256-bit Advanced Encryption System (AES) and data in transit with secure socket layer (SSL) or transport layer security (TLS); few provide encryption for data in use. The key management component is where it gets interesting. Some providers will retain control over the keys, while others put the keys in the customer's hands. Some providers design solutions so that the application holds the keys, while others adopt an approach where the cloud partner (e.g., Amazon Web Services) holds the keys. For more information, see the May 5, 2014, "Market Overview: Secure File Sharing And Collaboration" report.

[15] Source: Elizabeth A. Harris, "Data Breach Hurts Profit at Target," The New York Times, February 26, 2014 (http://www.nytimes.com/2014/02/27/business/target-reports-on-fourth-quarter-earnings.html?_r=0).

FORRESTER®

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

CLIENT SUPPORT

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.

Forrester Focuses On Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

« **SEAN RHODES,** client persona representing Security & Risk Professionals