



July 2, 2009

IT Security's Critical Role During Layoffs

by Andrew Jaquith
for Security & Risk Professionals



July 2, 2009

IT Security's Critical Role During Layoffs

How To Safeguard Company Data In Difficult Times

by **Andrew Jaquith**

with Robert Whiteley and Margaret Ryan

EXECUTIVE SUMMARY

The Gateway Recession of 2009 has brought the prospect of slowing sales and profits — and job losses. Although layoffs are never desirable, they are often necessary. Much of the responsibility for keeping company data safe during layoffs falls to security and risk professionals. When enterprises must think the unthinkable, Forrester recommends a four-step action plan to safeguard sensitive data and secrets. Enterprises should: 1) Prepare a comprehensive plan by creating a team composed of IT, HR, PR, executives, and legal; 2) practice executing the plan by simulating deprovisioning activities and war-gaming failure scenarios; 3) execute the plan when day zero comes; and 4) evaluate the successes or failures of deprovisioning, information protection, and monitoring activities. Enterprises should supplement these tactical activities by implementing technologies like data leak prevention (DLP) and PC backups to create a sustainable, ongoing data protection program.

TABLE OF CONTENTS

2 **In Recessional Times, Protecting Innovation Becomes A Top Priority**

Job Losses In The US Are Increasing, And Employers Are Worried

Enterprises Possess Information That Could Be Valuable To Aggrieved Former Employees

IT Security's Critical Role In Keeping Secrets Safe

5 **Habits Of Highly Effective Security Organizations**

Four Steps To Take Before Layoffs Are Needed

Creating An Effective Plan For Day Zero

Lessons Learned: Sweating The Details

RECOMMENDATIONS

9 **IT Security Must Partner, Not Just Implement**

10 **Supplemental Material**

NOTES & RESOURCES

Forrester interviewed three user companies that have recently laid off workers.

Related Research Documents

["Inquiry Spotlight: Data Leak Prevention, Q1 2009"](#)
February 10, 2009

["Identity And Access Management Mitigates Risks During Economic Uncertainty"](#)
January 26, 2009

["Top Data Security Predictions For 2009"](#)
January 9, 2009

IN RECESSIONARY TIMES, PROTECTING INNOVATION BECOMES A TOP PRIORITY

The Gateway Recession of 2009 has brought the prospect of slowing sales and profits — and job losses.¹ Although layoffs are never desirable, they are often necessary. When layoffs come to enterprises of all sizes, the need to protect company secrets, customer data, and innovation becomes paramount.

Job Losses In The US Are Increasing, And Employers Are Worried

In the United States, few companies have escaped the impact of the recession. Job losses and the risk of information theft have risen steadily. Consider the evidence:

- **The recession has been much more severe than expected.** Last October, as the recession became official, the US Federal Reserve predicted that the US unemployment rate would hit an unheard-of 7.6% by the end of 2009. The reality has been far worse than even the Fed's most dire predictions. As of May 2009, the unemployment rate was nearly two percentage points higher, at 9.4%. The total number of unemployed workers since November 2008 now stands at 4.3 million.
- **The largest companies have cut deeply into their workforces.** As of June 2009, 40% of the 1,000 largest US companies have laid off workers since last fall. Each company let go an average of nearly 3,000 workers: more than 550,000 workers and about 7% of their workforces.² In the broader economy, the US Bureau of Labor Statistics reports that employers have initiated more than 15,000 layoff events since November 2008 — more than 1.5 million in total.

Enterprises Possess Information That Could Be Valuable To Aggrieved Former Employees

Enterprises keep two kinds of data valuable to determined or disgruntled ex-employees:

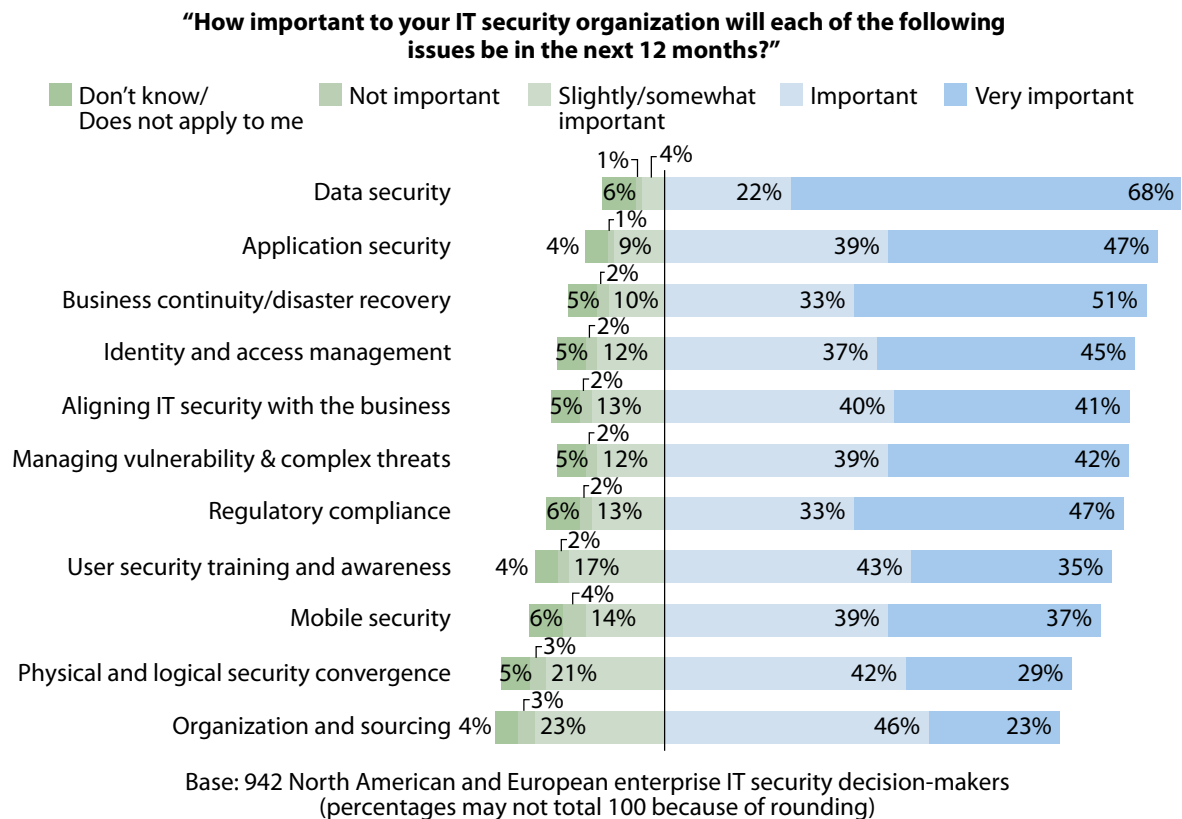
- **Toxic data: information protected by mandates.** Toxic data refers to information that could cause embarrassment, trigger fines, or cause a public relations fiasco if it were lost, stolen, or inadvertently exposed to the public. Regulations, statutes, or contractual agreements such as PCI forbid the movement of toxic data such as cardholder data, government identifiers, and health care records.
- **Secrets: data that is the source of competitive advantage.** By contrast, secrets are product plans, proprietary trade secrets, and other information that could cause irreparable competitive harm to an enterprise if it were released. Secrets have intrinsic value to the organization and are generally strategic.³

The risks to company secrets and confidential data are real. In 2007, whistleblower Gerald Eastman was arrested for secretly downloading more than 8,000 company documents from Boeing's internal servers onto USB thumb drives. Many of these documents were leaked to *The Seattle Times* in an

attempt to prove claims of corruption. Boeing valued the intellectual property Eastman took at \$15 billion.⁴ In a more serious incident, Countrywide Financial employee Rene Rebollo downloaded 2 million loan customer records in batches of 20,000 to USB drives. He sold these records to outside loan agents for \$70,000. Rebollo was arrested in August 2008 but has not yet been to trial.

The Rebollo and Eastman cases illustrate what chief information security officers (CISOs) know to be true: Even in the best of times, valuable company data is difficult to safeguard. But in a recessionary climate, poor security practices could have more serious consequences. As a result of these and other factors, in 2009 CISOs have put data security at the top of their priority lists. Ninety percent of US and European security decision-makers rated it “important” or “very important,” higher than any other issue (see Figure 1).

Figure 1 Data Protection Becomes Top CISO Priority



Source: Enterprise And SMB Security Survey, North America And Europe, Q3 2008

48235

Source: Forrester Research, Inc.

IT Security's Critical Role In Keeping Secrets Safe

The challenges to locating, monitoring, and protecting sensitive corporate data during layoffs are vast. Much of the responsibility for keeping company data safe falls to security and risk professionals: 79% of European and US security managers tell Forrester they are primarily or completely responsible for endpoint and network security, with 61% saying the same for physical security.⁵

During normal times, IT security's role is central to protecting innovation. Security and risk professionals are expected to:

- **Identify what must be protected.** The intrinsic amorphousness of digital data makes it hard to understand the scope of the problem: what it is, where it's kept, who has it, and what the consequences might be if it's lost. IT security has traditionally driven this discussion by helping to identify the kind and location of sensitive assets, develop security classifications, and assess risks. The information that security teams are charged with protecting generally falls in either the toxic data or secrets categories as described earlier.
- **Implement processes and tools to protect data on an ongoing basis.** Security teams use a plethora of tools from their bag to protect data on an ongoing basis. The technologies enterprises can marshal include proactive controls like enterprise risk management (ERM); reactive controls like email filtering, security information management (SIM), device-kill software, and forensics technologies; and dual-use (both reactive and proactive) controls like data leak prevention (DLP) and database monitoring and protection (DMP) (see Figure 2).

Thanks to the IT security spending boom since 2002, many IT security teams have already taken steps to identify the data that must be protected and have put reactive, proactive, and dual-use data protection technologies in place. By the end of 2009, Forrester expects that 59% of enterprises will have deployed some form of data leak prevention on the network or desktop; 52% will have deployed unified monitoring of users' rights and activities; and 47% will have deployed automated user account provisioning.⁶ These organizations are well positioned to be effective, even before layoffs happen.

Figure 2 IT Security Uses Proactive, Reactive, And Dual-Use Technologies To Protect Data

Usage	Technology	Vendors
Proactive	Enterprise rights management (ERM)	Adobe Systems, Liquid Machines, Microsoft, Workshare
	Device control	DeviceLock, Lumension, Symantec
Dual-use	Database monitoring and protection (DMP)	Guardium, HP, Imperva, Microsoft, Oracle
	Data leak prevention (DLP)	CA, McAfee, RSA Security, Symantec, Verdasys, Websense
Reactive	Email filtering (DLP Lite)	Clearswift, Google (Postini), Proofpoint, Symantec, Trend Micro
	Web and URL filtering	McAfee, Symantec, Websense
	Security information management (SIM)	ArcSight, LogLogic, RSA Security
	System integrity	Tripwire
	Device kill	Absolute Software, Beachhead Solutions
	Forensics	Guidance Software, Mandiant

48235

Source: Forrester Research, Inc.

HABITS OF HIGHLY EFFECTIVE SECURITY ORGANIZATIONS

IT security practices take on special importance in recessionary times. To understand how enterprises handle security during layoffs, Forrester spoke with three companies, off the record, about the experiences of their security teams.⁷ The three companies Forrester spoke with underscored the difficulty of securing sensitive information, even when the security team was well prepared. However, these firms also disclosed a range of processes and practices that were effective at stopping information leaks during layoffs.

Four Steps To Take Before Layoffs Are Needed

Highly effective security groups use all of the technological tools at their disposal in tough times. But keeping secrets safe during layoffs doesn't just depend on the tools and security widgets they have bought. Success doesn't depend much, either, on the actions enterprises take on "day zero," when management announces layoffs and executes its plans. Success depends even more on specific process steps firms have taken *beforehand*. Forrester recommends enterprises implement the following data protection practices as standard operating procedure — well before layoffs are needed:

- **Screen employees at time of hire.** The most important predictor of theft of intellectual property is whether employees are predisposed toward it. In business as in sports, character matters. As one CISO put it: "Above all, hire honest people." Firms that are serious about preventing theft perform criminal background checks. For employees who have access to sensitive information or bulk quantities of fungible customer information, credit checks are essential to verify that prospective employees won't be tempted by financial gain.⁸
- **Review entitlements regularly.** As Forrester has written elsewhere, leading enterprises regularly review the access privileges their employees have. Why? To make sure that they access the minimum number of applications and resources they need to do their jobs effectively and no more. Periodic reviews of employee entitlements also ensure that employees do not remain over-privileged when they change roles within the enterprise.⁹
- **Centralize authentication and provisioning.** Most employees require access to dozens of enterprise systems, applications, and networked resources, many of which maintain their own identity stores. Leading enterprises try to reduce the need to create separate credentials for each system by delegating their authentication responsibilities to IT-managed LDAP directories or Active Directory (AD). In addition to simplifying the user experience, centralized authentication and associated provisioning processes make it easier to shut off access during layoffs.¹⁰
- **Eliminate sensitive data on endpoint devices.** Also called data minimization, elimination of sensitive data on employee devices is a priority for leading enterprises. They believe that data can't be stolen if an employee doesn't have it. As such, reducing the need for employees to carry sensitive data or secrets on their laptops and mobile devices is a leading preventive practice. Increasingly, security teams are investigating advancements that allow thin clients instead of thick ones and Webified applications instead of the locally installed variety.

These four proactive steps — employee screening, regular entitlement reviews, centralized authentication and provisioning, and data elimination — set the foundation for effective security organization performance, if and when management identifies the need to lay off staff.

Creating An Effective Plan For Day Zero

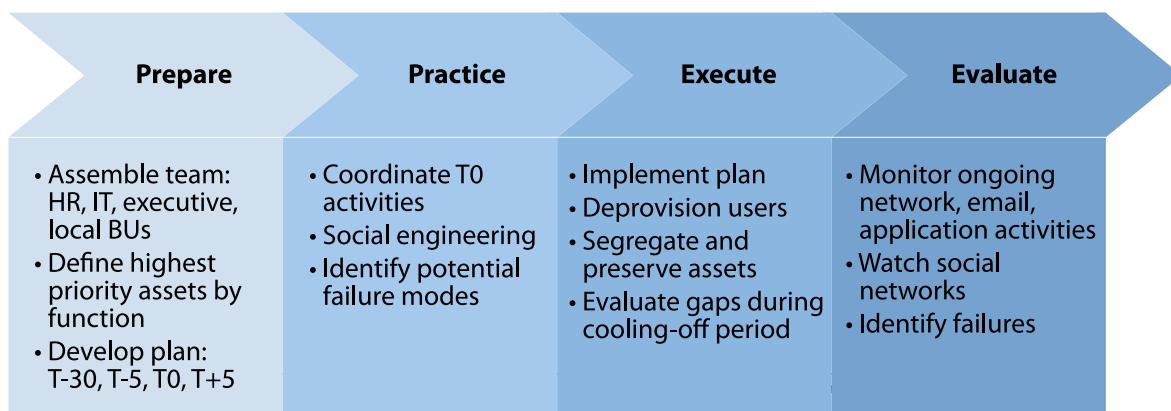
The implementation of proactive data protection processes sets the stage for an effective response if and when layoffs must be considered. Once management identifies the need for layoffs, it must work hand-in-hand with IT security to protect the enterprise's sensitive data and secrets. Forrester recommends a four-step plan for enterprises that must take these drastic actions (see Figure 3):

- **Prepare.** When layoffs are being planned, IT security coordinates its day zero activities with HR, finance, legal, corporate communications, and the executive team. The group collectively identifies key employees and assets to be safeguarded. It plans activities for before, during, and

after day zero. Actions typically include: verifying that endpoint backup systems work 30 days before day zero; stepping up network and email surveillance five days before; deprovisioning on day zero itself; and enhancing internal and external network monitoring for a week or more thereafter. To develop deprovisioning checklists, IT security documents the privileges granted to knowledge workers, developers, IT security, system administrators, and other key roles. To understand what is “typical,” IT security interviews known “power users” within each role.

- **Practice.** After the plan is developed, IT security practices executing it. To do this, IT security simulates deprovisioning processes using a member of the IT security group as a test subject. The test subject is then systematically locked out per the plan. To evaluate effectiveness, the subject attempts to regain access by exploiting gaps in the deprovisioning process or through social engineering. Enterprises may also find it helpful to retain an outside security testing firm to assist; they can often identify holes the IT security group misses.
- **Execute.** During layoffs, security implements its plan to lock down systems and networks. IT security deprovisions affected user accounts, temporarily shuts down VPNs and companywide Internet access, retrieves company devices, watches networks for signs of intrusions, monitors security information management (SIM) consoles and logs, and responds to security events. Deprovisioning is done as quickly as possible for all affected employees. During the execution phase, IT security helps corporate communications monitor outside blogs and social media like Twitter for adverse publicity.
- **Evaluate.** IT security’s job is not done after day zero is complete. Shortly after completion of lockout activities, the extended team — IT security, HR, legal, et al. — evaluates the relative success of the plan. Did IT security fail to identify user accounts? Allow privileged users to access sensitive databases? Fail to account for external or outsourced Web sites? Understanding failure modes helps the security team spot opportunities to improve efficiencies or close process gaps.

Figure 3 Forrester’s Four-Step Plan For Day Zero (T0)



Lessons Learned: Sweating The Details

The four-step action plan for protecting innovation during layoffs — prepare, practice, execute, and evaluate — provides an outline for what must be done. But even the best plans go awry. In discussions with affected firms, Forrester identified key lessons learned during the layoff process:

- **Involve IT security early.** Cautions one security manager: “Don’t involve IT security at the last minute.” Cutting IT security out of the communication chain is a recipe for disaster, because critical contextual information about employees’ roles, entitlements, and sensitive information they possess can be lost in the crush. It may seem obvious, but it’s still overlooked by far too many companies.
- **Remember employee-owned devices.** While many IT organizations would like to believe that only IT-sanctioned gear is used to access company resources, reality is messier than that ideal. When employees leave, IT security groups should ask affected employees if they own phones or PCs that contain sensitive company information and require the employees to scrub them before they leave the premises.¹¹ This may require that IT familiarize itself with how to wipe data on the more popular devices like iPhones and BlackBerrys, even nonsanctioned gear.
- **Consider a cooling-off period to ease transitions and monitor networks.** One enterprise we spoke with announced layoffs on Thursday. Affected employees received a four-day cooling-off period, then returned on Tuesday after the weekend to collect personal effects and say their goodbyes. The security manager Forrester spoke with “thought this was a nice balance. We reduced the volatile period and gave people a chance to cool off. It also gave us a chance to make sure we were protecting everything appropriately.”
- **Deprovision all affected employees, without exception.** Many enterprises retain selected employees after the layoff as consultants. It’s tempting to leave their privileges largely intact so that they can continue their work. But this opens up potential security holes. Instead, IT security should follow the same steps used for employees who are leaving for good. Remove prospective contractors’ logins, accounts, and privileges completely, *then* reprovision them with only the access privileges they need.
- **Block access, but don’t forget to monitor.** After IT security deprovisions access to AD accounts, VPNs, and email, the real work of monitoring begins. As important as blocking is, monitoring external connections and social networks such as Twitter and Facebook gives IT security valuable situational awareness.
- **Preserve assets to transfer knowledge.** During layoffs, IT security’s job is to do as much as possible, as quickly as possible. High priorities include retrieving and reconditioning IT-issued PCs. But IT shouldn’t wipe PC assets too quickly, because it risks losing tacit knowledge and documents that should be retained. Before sanitizing and repurposing retrieved PCs, IT

security should back up former employees' document folders to a central location, making them available to their respective former bosses for review.

- **Pay special attention to outside vendors.** Outside Web sites that aren't managed by the company directly pose specific security risks. It's easy to forget about company blog sites managed by Six Apart or Blogger — terrific bully pulpits in the wrong hands. Travel agent sites are also problematic, especially if company credit cards are used for air or hotel travel. IT security should make special deprovisioning arrangements with these outside entities.
- **Be courteous with employees' personal data requests.** No matter what the IT policy states, it's impossible in the modern age for employees to keep their PCs completely free of personal documents, like photographs of their weddings or their kids. For many employees, the IT-issued PC is their only computer. Time permitting, fulfilling limited requests for personal documents doesn't cost much time and buys goodwill.¹² "People will behave like criminals if you treat them that way," notes one manager.
- **Deal firmly with theft or deletions.** Most employees who are laid off are upset, but won't take active steps to damage their employers. Aggrieved employees who are caught deleting or stealing information, however, should be firmly reminded of the seriousness of their transgressions. One security manager described his company's deterrent strategy this way: "We isolate the problem, contain the individual, and walk him out of the building. Then we have our attorneys contact him and explain how screwed he is."

RECOMMENDATIONS

IT SECURITY MUST PARTNER, NOT JUST IMPLEMENT

IT security's role during layoffs is a difficult one. In addition to performing its normal duties of safeguarding the company perimeter, during layoffs it must also deprovision assets, monitor networks for intrusions, and work closely with counterparts in the organization to handle incidents. Although this is a tall order, as an IT security manager you can maximize your effectiveness if you:

- Involve IT security early and often.
- Test your plan before you need to act.
- Try to defeat the security controls yourself, before someone else does.
- Use cooling-off periods to watch for intrusions and transition knowledge.
- Use lessons learned to improve deprovisioning architectures and processes.

SUPPLEMENTAL MATERIAL

Methodology

To understand prevailing practices, Forrester spoke confidentially with three companies about their security practices during layoffs. These companies laid off substantial numbers of workers in the first and second quarters of 2009.

ENDNOTES

- ¹ We'll look back on this recession as much more than an ugly economic moment. History will view it as The Gateway — a portal connecting two very different eras. See Forrester CEO George Colony's blog post, "The Gateway Recession: What CEOs Will Face Next" (<http://blogs.forrester.com/colony/2009/06/the-gateway-recession-what-ceos-will-face-next.html>).
- ² Source: Forbes Layoff Tracker (<http://www.forbes.com/layofftracker>), plus additional Forrester analysis of the raw data.
- ³ *Toxic data* itself has little to no intrinsic strategic value, but becomes a valuable commodity when airborne. *Secrets* accrue intrinsic value. In addition to business secrets, enterprises must also protect, in the course of their normal business operations, technical secrets such as passwords and encryption keys. The technologies and processes needed to protect each kind of data are dramatically different.
- ⁴ The case was settled out of court after a mistrial. Boeing vs. Eastman indicates the difficulty in locking down large, complex enterprise networks. Eastman argued that because he had access to the files, he broke no laws. Source: Mike Carter and Steve Miletich, "Whistle-blower settles case," *The Seattle Times*, July 11, 2008.
- ⁵ Source: Enterprise And SMB Security Survey, North America And Europe, Q3 2008.
- ⁶ Source: Enterprise And SMB Security Survey, North America And Europe, Q3 2008.
- ⁷ Quantitative information about security practices during layoffs is difficult to find, because the topic is quite sensitive. One company was a small services firm forced to cut 30% of its workforce as a response to flagging demand for its products. Another was a large Fortune 100 manufacturer that cut 3,000 employees. A third was an outsourcing firm whose normal seasonal ebb in demand was exacerbated by the recession. The information Forrester presents in this report is by necessity a composite.
- ⁸ In our conversation, the CISO discussed the importance of having honest employees. In addition to lessening the risk of theft during time of layoffs, he stressed how having stringent screening processes helped lessen other types of exposure, too. Perhaps most interestingly, he noted that the *inbound* risks could also be substantially reduced: "... the risk of bringing someone else's IP in is at least as big of a problem as leakage."
- ⁹ The term "entitlements" originated in the financial services sector. It denotes the enumerated set of documents, databases, applications, hosts, and other networked resources that an employee's privileges enable him or her to access.

- ¹⁰ Even in normal times, deprovisioning is a key competency security organizations must master. Forrester has identified deprovisioning cycle times as a key security metric. See the January 26, 2009, "[Identity And Access Management Mitigates Risks During Economic Uncertainty](#)" report.
- ¹¹ Some organizations include language in the employee contracts that requires employees who use personal gear to access company resources to temporarily turn them over to the IT organization for sanitization during investigations, layoffs, or terminations.
- ¹² One of the CIOs Forrester spoke to said, candidly: "In some cases employees have files in their My Documents folder they want us to retrieve for them, for example, their wedding photos. Employees shouldn't really have that stuff on the PCs, but I've asked my staff to be courteous and helpful when we receive those kinds of requests."

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

Australia	Israel
Brazil	Japan
Canada	Korea
Denmark	The Netherlands
France	Switzerland
Germany	United Kingdom
Hong Kong	United States
India	

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.

Forrester Research, Inc. (Nasdaq: FORR) is an independent research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. Forrester works with professionals in 19 key roles at major companies providing proprietary research, consumer insight, consulting, events, and peer-to-peer executive programs. For more than 25 years, Forrester has been making IT, marketing, and technology industry leaders successful every day. For more information, visit www.forrester.com.