

Fighting a growing threat



49%

Nearly half of retail and consumer goods respondents say their company has experienced economic crime over the past two years.

76%

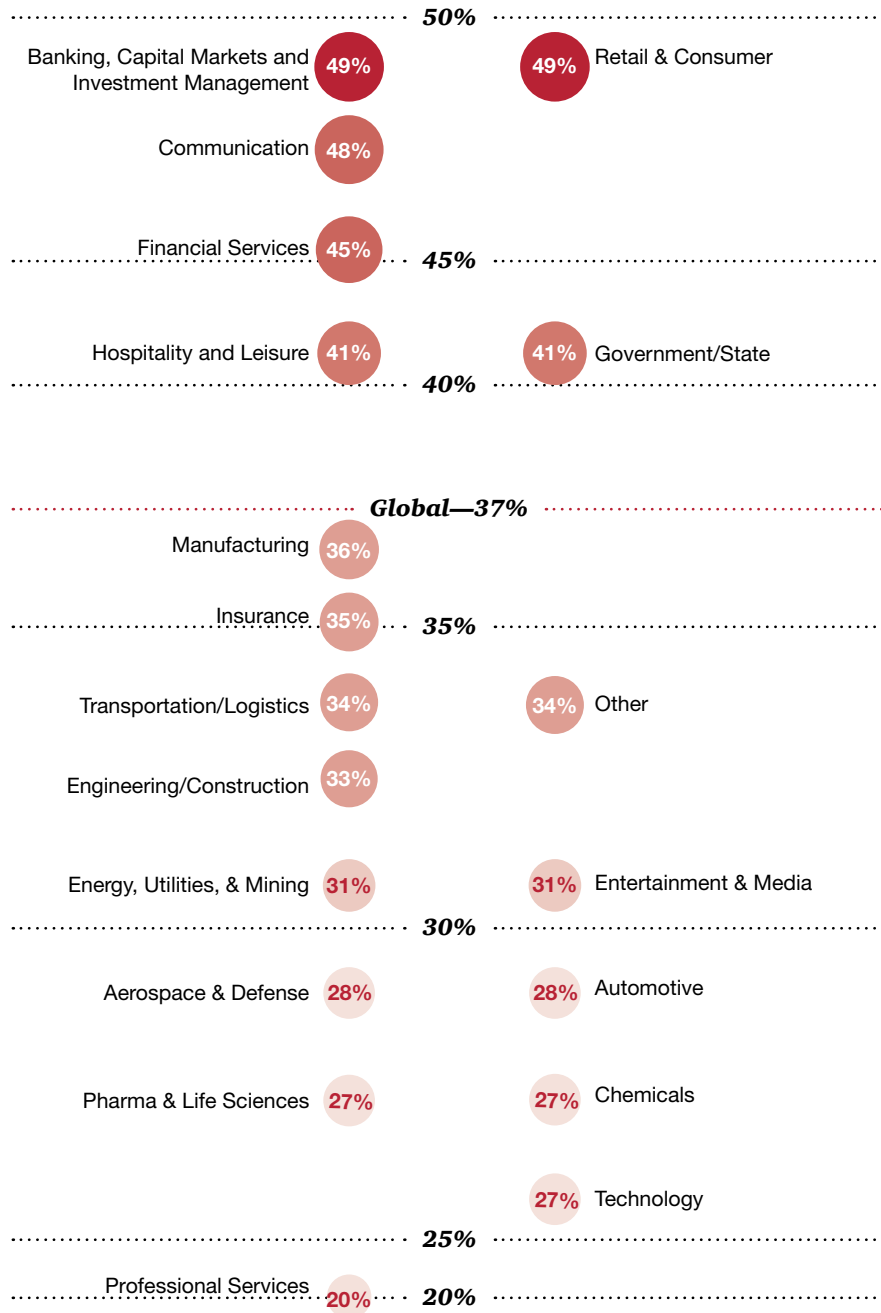
Asset misappropriation tops the list of types of economic crime experienced by retail and consumer goods companies.

67%

Two-thirds of the most serious economic crime incidents were perpetrated by insiders.



Figure 1: Economic crime percentage reported by industry



% of all respondents who experiences economic crime over the survey period

Highlights

- ***A serious threat***

49% of retail and consumer goods companies have suffered economic crime during the last two years, compared to only 37% across all other industries. That's up significantly from our last survey.

- ***More than one way to lose***

Asset misappropriation is the primary type of reported economic crime. Procurement fraud and bribery and corruption are also major issues.

- ***High growth markets can be high risk markets***

Expanding globally brings opportunities, but operating in markets with high risk of corruption brings additional challenges—especially during the market entry and expansion phases. Retail and consumer goods companies will need to be increasingly diligent.

- ***Some controls are working well***

Corporate controls are detecting a significant number of economic crimes, and suspicious transaction reporting is especially effective.

- ***Room for improvement***

The sector is lagging when it comes to implementing annual fraud risk assessments, which can be a valuable addition to an economic crime fighting toolkit.

- ***Retail and consumer companies face a threat from within***

By comparison to other industries, retail and consumer goods companies face more serious economic crimes from within the company.

- ***Getting tougher on criminals outside***

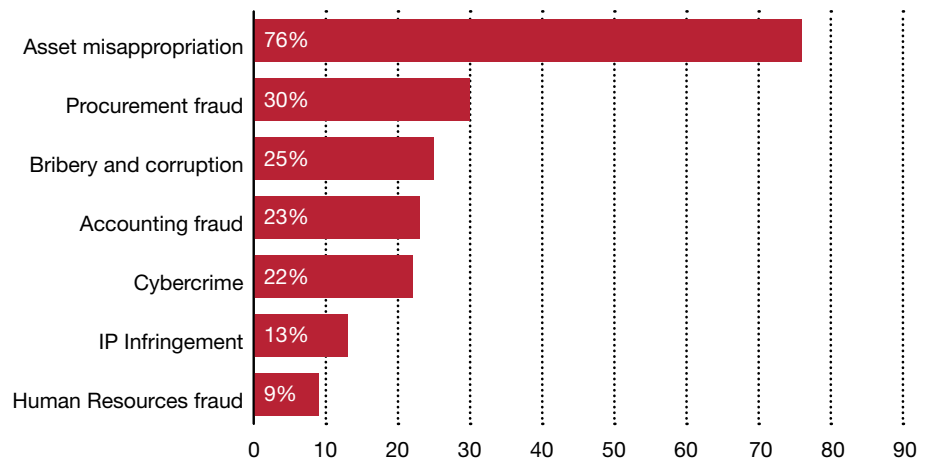
When the most serious economic crime faced was perpetrated by an external party, retail and consumer goods respondents were much less likely to say they had informed law enforcement, notified relevant regulatory authorities or ceased the business relationship.

Economic crime is on the rise

Retail and consumer goods companies are experiencing greater levels of economic crime. With nearly half of respondents saying their company has experienced this type of event in the past 24 months, the retail and consumer goods sector tied with financial services this year as the industries with the highest incidence of economic crime. Our most recent surveys have also shown a steady upward trend, with the rate of economic crime rising from 37% in the 2009 survey to 42% in 2011 and 49% in 2014.

By far the most commonly reported type of economic crime for the sector is asset misappropriation, with more than three-quarters of those executives reporting fraud saying their company has experienced it within the last 24 months. As was true across all industries surveyed, the other most common types of fraud included bribery and corruption, accounting fraud, and cybercrime (see Figure 2). Procurement fraud, a new category this year, ranked second with retail and consumer goods respondents. Those who experienced it highlighted vendor selection (59%) and vendor contracting/maintenance (39%) as the most common weak spots.

Figure 2: Top types of economic crime reported by retail and consumer goods companies that experienced economic crime during the survey period



% of 186 retail and consumer goods respondents who reported economic crime in the past 24 months

Asset misappropriation gets the most attention but other threats can be damaging too

Asset misappropriation is by far the most common economic crime experienced by organisations reporting any fraud, with 76% of respondents suffering from it. This amount is more than double the second-highest-occurring type of economic crime, procurement fraud (30%). While the individual impact of this fraud may be lower than that of cybercrime or government-enforced frauds, the magnitude of the threat requires organisations to be vigilant. For retail and consumer goods respondents the problem is very real; nearly half of them say it's likely they'll experience asset misappropriation in the next two years, more than across the sample overall.

Asset misappropriation frequently involves thefts of cash—but not always. Schemes can include theft of cash receipts, fraudulent disbursements of cash, misappropriation of cash on hand and non-cash misappropriations such as stealing from a warehouse or storeroom. Schemes can be as complicated as covering up a theft by marking good inventory as “scrap”, removing it from the premises and reselling it. Besides the financial losses involved, such crimes often can tarnish a company's reputation and contribute to an operating environment that erodes the integrity of employees.

While they are not the most common form of crime reported, of all the types of fraud covered in our survey, bribery and corruption may pose the greatest threat to global businesses because of the number of business processes they threaten. Sales, marketing, distribution, payments, international expansion, expense reimbursement, tax compliance, and facilities operations are all vulnerable processes. For example, locating and acquiring land for stores and distribution centers and obtaining permits and utilities can provide significant challenges for companies entering new markets or expanding, while moving goods promptly through customs poses an on-going challenge to the retail and consumer goods supply chain. The risk of bribery and corruption is a threat to many different types of transactions, but it is of particular concern when companies are dealing with government agencies and state-owned businesses.

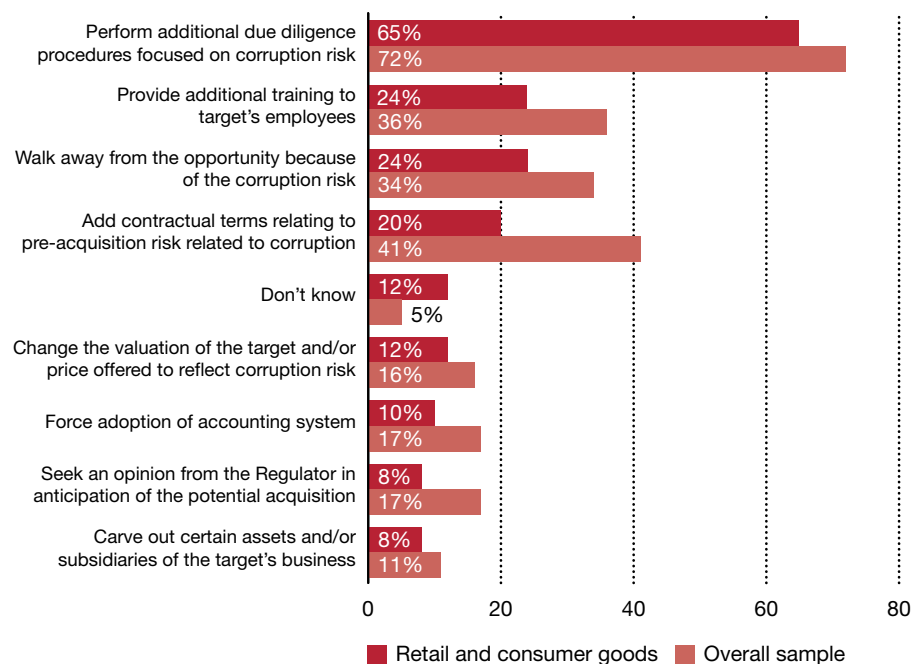
Every region in our main survey reported a significant number of incidences of bribery and corruption. About one quarter of retail and consumer goods companies experiencing economic crime reported that they have experienced bribery and corruption issues. One of the well-known perils of operating in certain international locations, clearly this is on the radar screens of management. In fact, 56% of retail and consumer goods executives see bribery and corruption as the highest risk of operating globally. More than one in five (23%) acknowledge that they've been asked to pay a bribe. And nearly as many say they've lost an opportunity to a competitor whom they suspect paid a bribe.

High growth markets are often high risk markets

More than half of retail and consumer goods companies have operations in markets with high corruption risk, as those markets represent some of the sector's biggest growth opportunities. Thirty-nine percent of retail and consumer goods respondents say they've pursued an opportunity in one of these markets in the past 24 months. But the challenges are changing how they operate; nearly a third pursuing growth opportunities in regions with high levels of corruption risk say they've needed to adapt their business strategies.

Just what are they doing? There's no one answer. As is true across the sample, additional due diligence is the most popular solution (see Figure 3). But compared to respondents overall, far fewer retail and consumer goods executives say they'll add contractual terms. And fewer are planning to provide additional training to staff. Will their efforts be enough? Only about a quarter say they walked away from an opportunity in response to corruption risk, less than across the overall sample (34%).

Figure 3: Changes to business plan or strategy in response to high corruption risks



% of respondents changing their business strategy while pursuing an opportunity in a high corruption risk market over the previous 24 months (overall sample, 757; retail and consumer goods, 49)

Cyber threats are building

More than a fifth of the retail and consumer goods companies that have experienced fraud say the incidents included cybercrime—in line with the overall results. But the industry is transforming, and many of the changes could increase the threat. Retailing has become multichannel, driven by evolving technologies and interactive, customer-focused applications. The acquisition of voluminous customer data and new security risks make retail touch points such as the web, mobile devices, and point of sale (POS) highly vulnerable and attractive targets for data security breaches. In the US, well-publicised thefts of POS information during December 2013 and January 2014 underscore the growing threat and increasing sophistication of these attacks.¹

Retail and consumer goods executives are taking note—45% of sector respondents say that the awareness of this type of economic crime in their organisation is increasing. And more than one in four (27%) says it's likely that their company will experience an incident of cybercrime in the coming 24 months. In our 17th Annual Global CEO Survey, 37% of retail and consumer goods CEOs said they're concerned that cyber threats, including lack of data security, could threaten growth, so the issue is starting to get C-suite attention. Now is the time to identify emerging threats and take action.

What can you do?

- Educate employees at all levels, from C-suite to junior management, about cyber threats. Cybercrime is not just the domain of the IT/network security department. Different types of cybercrime, from hacktivism to data theft, affect different functions of the company.
- For retailers, perform additional due diligence on all third party vendors that manage or store point-of-sale data. Make sure that every employee is aware of possible vulnerabilities in the point-of-sale system.
- Understand the potential culprits and their motivations to engage in a cyberattack on the organization.
- Ensure that key safeguards for effective cybersecurity are in place, including ongoing monitoring, up-to-date personal or sensitive data inventory, a back-up policy and business continuity plan.

Keeping an eye on IP

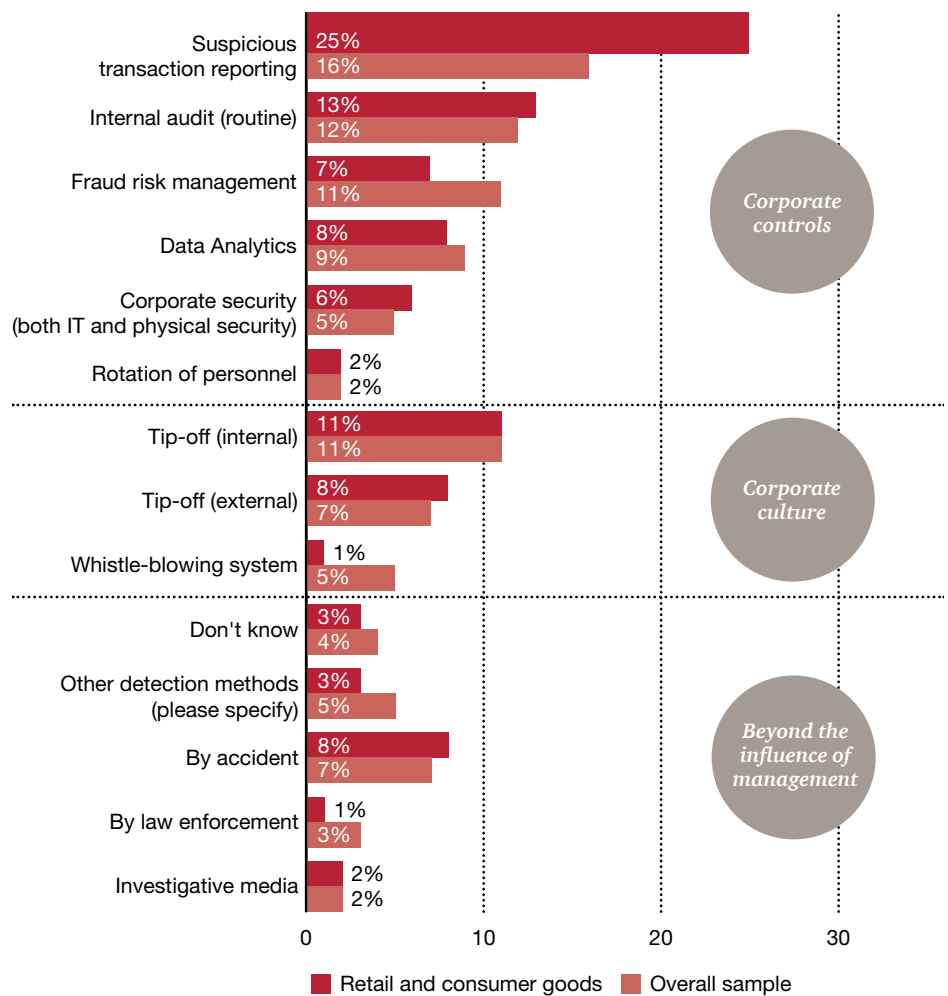
Loss of intellectual property (IP) is another worry, and it's more pronounced in emerging markets. While just 7% of all retail and consumer goods respondents have experienced IP infringement over the last 24 months, nearly three times as many (19%) believe it's likely they will face such an incident in the next 24 months. And in our 17th Annual Global CEO Survey, 39% of retail and consumer goods CEOs said they are concerned that an inability to protect IP could threaten growth.

1. We discuss these threats in more detail in our January 2014 publication "Answering your cybersecurity questions".

Controls top the list of fraud detection measures

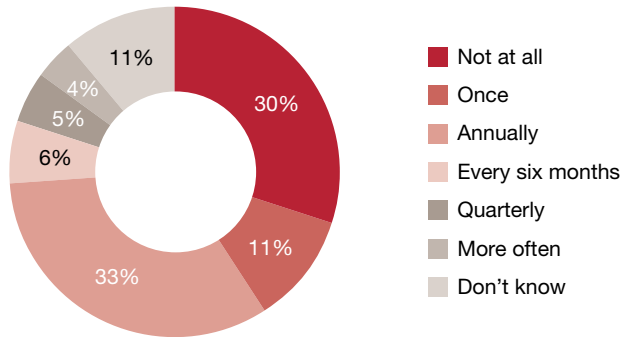
When it comes to detection, in this sector corporate controls are more successful than corporate culture. Suspicious transaction reporting in particular was responsible for the detection of 25% of the most serious incidents of economic crime in the retail and consumer goods sector—a notable success for the industry’s investments in better information technology such as more sophisticated point-of-sale inventory systems (see Figure 4). Internal audits are detecting a sizeable number of economic crimes too. But the industry is lagging slightly when it comes to fraud risk management systems. They detected just 7% of the sector’s most serious offences, compared to 11% of crimes across the total sample.

Figure 4: Economic crime detection methods in retail and consumer goods organisations



% of respondents who experienced economic crime over the previous 24 months

Figure 5: Two in five retail and consumer goods respondents say their companies haven't conducted a fraud risk assessment in the past 24 months or don't know whether they have or not



% of all retail and consumer goods respondents

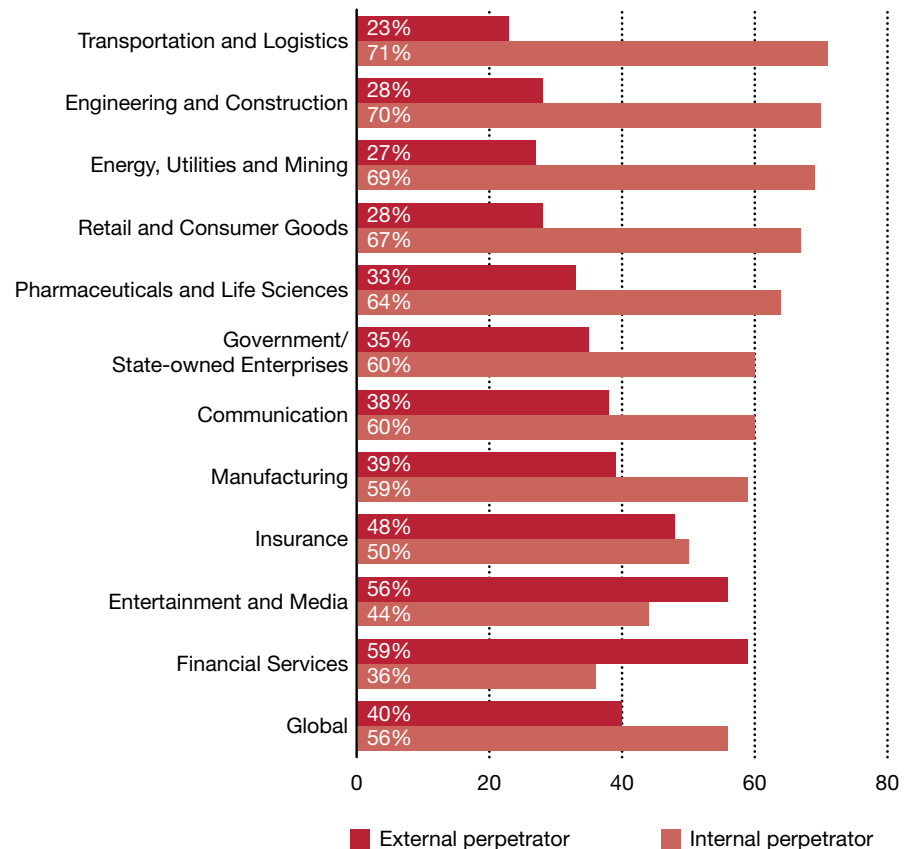
About a third of retail and consumer goods companies conduct fraud risk assessments each year; another 15% conduct them more frequently (see Figure 5). But 30% of sector respondents say their companies don't perform assessments at all, and 11% don't know whether their companies do or not. For those who don't perform fraud risk assessments, nearly half say they either aren't sure what a fraud risk assessment is or don't know why their company has chosen not to perform one. Only 17% say cost is the primary issue. Enhancing such systems can be a valuable tool in a company's economic-crime-fighting toolkit.

Retail and consumer goods companies face threats from within

Retail and consumer goods respondents reported that more than two-thirds of the most serious incidents of economic crime they experience were actually perpetrated by insiders. That's a higher rate than across the sample overall (56%) and higher than most other industries (see Figure 6). Nearly half of the culprits came from middle management.

Dishonesty in the ranks can erode employee trust. Thirty-one percent of retail and consumer goods executives describe the impact their most serious incident of economic crime had on employee morale as "significant".

Figure 6: Internal vs. external perpetrator



% of respondents, selected industries

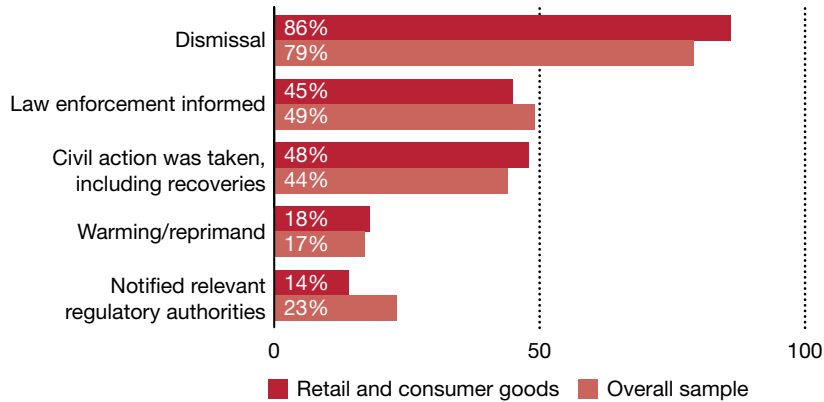
Is the sector too soft on external perpetrators?

Once a perpetrator has been identified, what should companies do? To deter future crime and improve employee morale it's important to take action. For internal perpetrators of serious economic crime, the most likely result is dismissal; many retail and consumer goods respondents also say they are taking civil action or reporting perpetrators to the authorities.

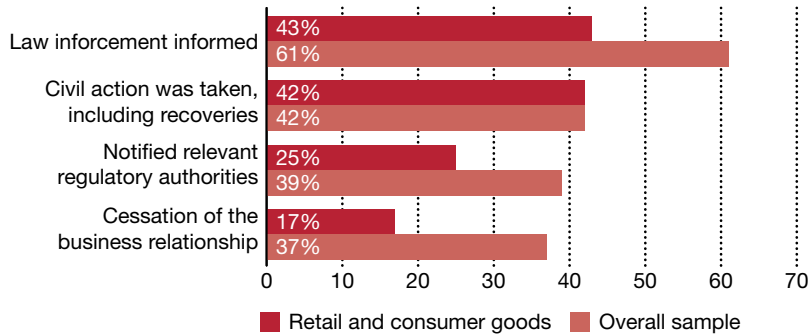
But what about external parties? Retail and consumer goods companies were less likely to take action against the main external perpetrator of the most serious incident of economic crime they experienced. Far fewer retail and consumer goods respondents say their companies informed law enforcement, notified relevant regulatory authorities, or ceased the business relationship. And 13% say their company took no action at all against the main external perpetrator.

Figure 7: The retail and consumer goods sector is taking less action against external perpetrators of the most serious economic crimes

7a: Internal perpetrators (not all choices listed)



7b: External perpetrators (not all choices listed)



% of respondents who experienced economic crime over the previous 24 months

Economic crime is a serious threat to organisations of all kinds, with one in three being impacted over the last 24 months—and the retail and consumer goods sector has the highest incidence of the sectors surveyed. With the likelihood of continued issues arising from our increasingly networked world, it's critical that retail and consumer goods companies continue to step up policies and programs to combat these practices and take appropriate action against perpetrators.

Contacts

For more information on the 2014 Global Economic Crime Survey and the survey methodology, please refer to Economic crime: A threat to business globally at www.pwc.com/crimesurvey.

If you would like to find out more about the information contained within this report, or to discuss any issues around economic crime and how our team can help you, please contact your local PwC office or one of the people named below.

Editorial team

John Maxwell
Global R&C Leader
+1 646 471 2738

Susan Eggleton
+1 206 398 3257
susan.eggleton@us.pwc.com

Michael Brewster
+1 646 471 1705
michael.brewster@us.pwc.com

Forensic Service Leaders

Andrew Gordon
Partner, United Kingdom,
Global Leader
+44 20 780 44187
andrew.gordon@us.pwc.com

Andrew Palmer
Partner, United Kingdom,
Central Cluster Leader
+44 20 7212 8656
andrew.palmer@uk.pwc.com

John Donker
Partner, Hong Kong,
East Cluster Leader
+852 2289 2411
john.donker@hk.pwc.com

Erik Skramstad
Partner, USA,
West Cluster Leader
+1 617 530 6156
erik.skramstad@us.pwc.com

Retail and Consumer Forensic Specialists

Matthew Shelhorse
+1 646 471 5749
matthew.j.shelhorse@us.pwc.com

Sulaksh Shah
+1 703 918 4477
sulaksh.r.shah@us.pwc.com

About the survey

The 2014 Global Economic Crime Survey was completed by 5,128 respondents (compared to 3,877 respondents in 2011) from 99 countries (compared to 78 countries in 2011). Of the total number of respondents, 50% were senior executives of their respective organisations, 35% represented listed companies and 54% represented organisations with more than 1,000 employees. This report looks at responses from 383 retail and consumer goods companies. For more information about our methodology and definitions of terminology used, please see our 2013 Global Economic Crime Survey report: “Economic crime: A threat to business globally.”

Editorial team acknowledgements

Thank you to Elizabeth Montgomery and Matthew Hameline for their assistance in the production of this document.

PwC firms help organisations and individuals create the value they're looking for. We're a network of firms in 158 countries with close to 169,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2014 PwC. All rights reserved. Not for further distribution without the permission of PwC. "PwC" refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm's professional judgment or bind another member firm or PwCIL in any way.