Threat Control and Containment: New Strategies for a Changed Threat Landscape

Introduction

Network security threats have the potential to significantly impede productivity, disrupt business and operations, and result in loss of information—which can lead to financial losses and potential non-compliance. Hackers continue to develop new techniques to gain access to information, for their own financial gain.

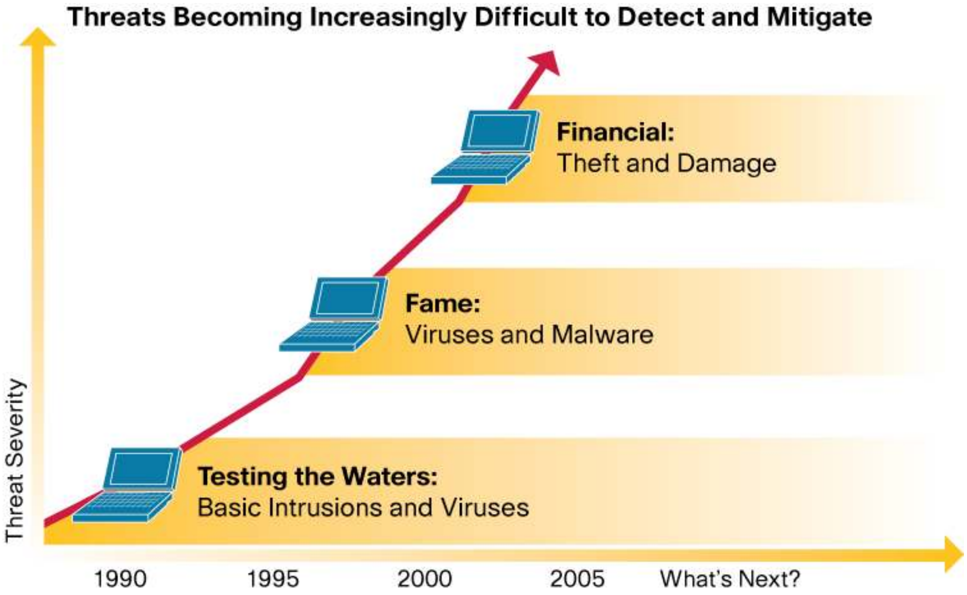
The evolution and complexity of threats must be addressed with proactive IT security strategies that maintain business continuity, provide infrastructure wide threat visibility and protection, and simplify day-to-day network management. The entire security infrastructure—network, systems, and management—must work in concert to proactively defend against a wide array of threats, and reduce the mean time to respond and mitigate during an event. Threat control solutions from Cisco® deliver comprehensive and proactive network defense, streamlined policy and system management, and business continuity.

The Changed Threat Landscape

At one time, fame was a primary incentive for hackers to take advantage of system and network vulnerabilities. Today, systems are increasingly exploited for financial gain. This change in motivation has resulted in a change in methods, which have made system exploits harder than ever to detect and mitigate (Figure 1).

Hackers are adapting more quickly than software and operating system vendors can develop patches and workarounds; often, their exploits are so targeted that there are no signatures to stop them. And in addition to broad-scale worm and virus outbreaks, IT organizations need to protect against network threats that are specifically designed to avoid detection and bypass traditional defenses.

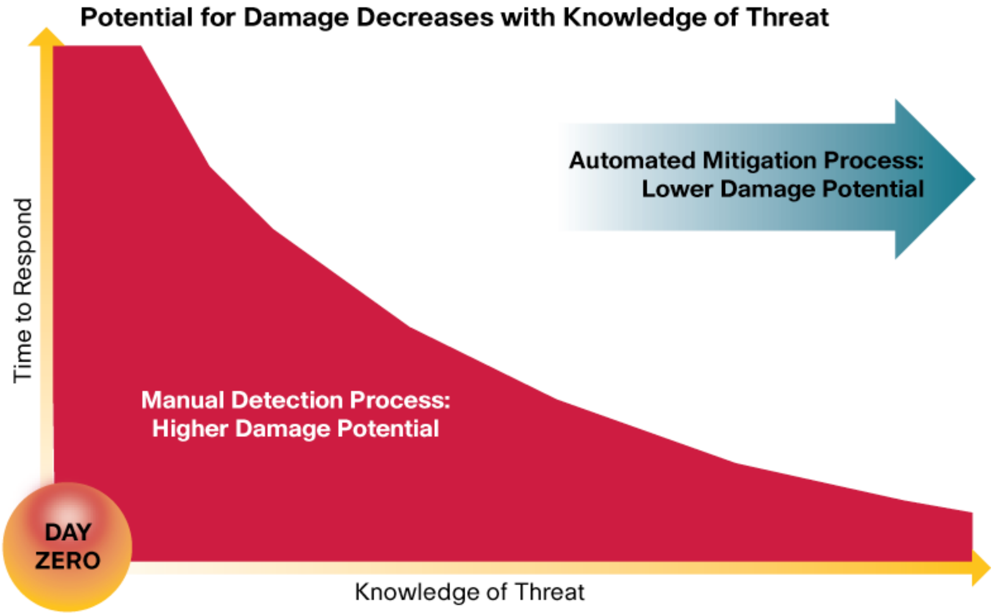
Figure 1. The Changed Threat Landscape



Adapting Policies and Technology to Combat Emerging Threats

New threats (often referred to as “day-zero” threats) can be more difficult to detect and mitigate, because of the lack of signatures or knowledge to prevent them. Unfortunately, many IT departments have few processes or tools available that can be automatically deployed to proactively prevent attacks, intrusions, or other system and application exploits. Additionally, the burden of daily system management, user calls and repairs, audit preparation, and a host of other details often impede an organization’s ability to focus on threats that are more difficult to detect.

Figure 2.


Potential for Damage Decreases with Knowledge of Threat
Automated Mitigation Process:
Lower Damage Potential
Time to Respond
Manual Detection Process:
Higher Damage Potential
DAY
ZERO
Knowledge of Threat

As a result of the increase in financially motivated, targeted system attacks, IT departments require full visibility across the infrastructure to help minimize the time to respond during an event. Tools to capture policy violations, vulnerability exploits, and anomalous behavior are required to discern between suspicious and harmful traffic.

360-Degree Threat Visibility and Protection

Increased visibility, deeper into systems and broader across the infrastructure, is required to combat both emerging and well-defined threats. By capturing policy violations, vulnerability exploits, and anomalous behavior across the infrastructure, organizations can more rapidly identify threats.

Simplified Threat Control

IT departments are continually expanding their tool portfolios to combat threats, generally resulting in a larger toolkit to work with: more systems, more processes, and more alarms. Managing security policies across heterogeneous networks helps assure control over new vulnerabilities. Tight linkage between the security intelligence system and security policy management system is required for minimal delay in deploying new policies to adapt to immediate threats.

Business Continuity

Hackers continue to find more entry points into the network. As a result, businesses need threat prevention strategies that are adaptable. Proactive threat defense requires not only defense in depth, but a strategy across all layers and elements of the infrastructure. Collaboration between endpoints, network, and management can enable faster response during events and can provide a far better level of security than discrete platforms.

Threat Vectors

Threats, both day-zero and well-defined, have numerous entry points into a network, all of which need to be considered for a comprehensive threat control policy and system management. Following is a brief overview of attack vectors, and some areas to consider as you continue to refine your threat control infrastructure.

Protecting Trusted Users from Internet Threats

Stopping the introduction, execution, and spread of threats from trusted users and computers can have dramatic positive effects on user and IT productivity. In many cases, processes can be automated to assure maximum protection from well-understood threats, such as viruses. When dealing with worms and spyware, proactive protection mechanisms must be employed to detect and mitigate those threats before they cause damage to the organization.

There are three primary entrance vehicles for a threat to enter a network: business communications, infected systems, and internal propagation.

Business Communications

E-mail, Websites, file transfers, instant messaging, and other standard forms of business and personal communications have the potential to introduce myriad threats to unsuspecting users. Because many users assume that these methods of communications are completely secure, they do not take extra measures to protect themselves. In many cases, threats are “nuisances” and are handled by standard antivirus software. Spyware and data leakage, however, can be more difficult to detect and monitor; this is often a targeted exploit of unsuspecting users.

Businesses require a comprehensive approach to combat well-known threats in the most efficient manner possible, and a process to help ensure visibility into emerging threats. By preventing threats such as spyware, viruses, and spam from entering through the gateway in the first place, administrators can reduce the burden of full endpoint scanning and the resulting performance effects this causes.

Infected Systems

Whether online or offline, mobile and desktop PCs have the potential to pick up infections from various sources, and introduce these infections to their networks. This could happen when a mobile PC connects to the Internet using public Wi-Fi access and then returns to a corporate office or remote site, or connects over a VPN. Mobile PCs are also a common target for theft; this is another way that they can become infected. These PCs are also at risk because they are often used by people other than the intended employee, such as family members.

Assuring that endpoints are compliant with corporate policies and have an acceptable security posture is important in making sure new threats do not enter the network from otherwise trusted users and devices. By validating endpoint security posture before allowing a system to access the network, administrators can broadly implement these controls in a “low-touch” fashion and dramatically reduce threat introduction.

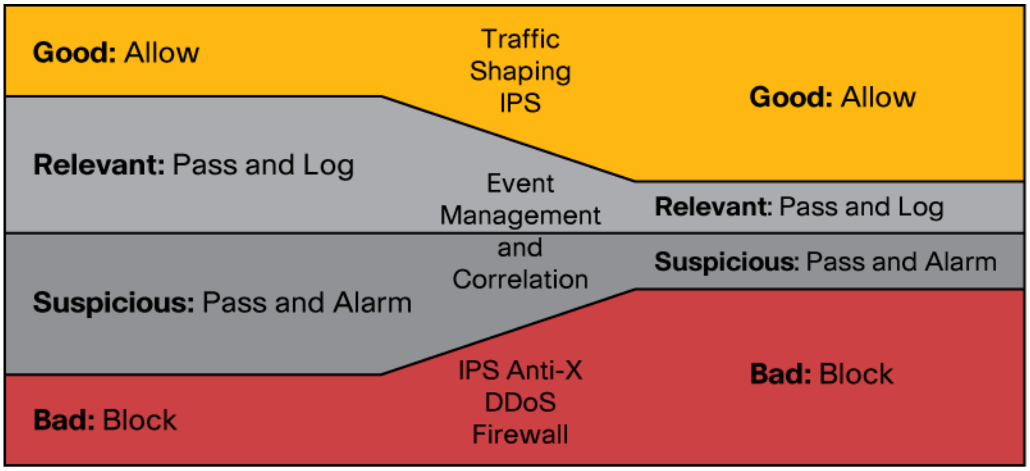
Internal Propagation

Despite best efforts at preventing the infection of an internal system, many malware programs still manage to bypass security controls and attempt to activate and distribute copies of themselves to other trusted systems. Proliferation from the “inside” is often much easier than penetrating systems from outside the network. The activation and distribution of threats can be prevented by controlling anomalous behavior and unwanted software installation and implementation on the host machines. Also, day-zero exploits can be prevented by validating system behavior, such as memory and network utilization.

Protecting Servers from Attacks and Intrusions

Critical information assets, such as HR records, financial data, user databases, and virtually all other electronic business information, must be classified by risk and protected as defined by corporate governance policies. New threats have emerged that have made detection and mitigation of infiltrations increasingly difficult. Tools and policies are available that proactively detect a potential threat before a vulnerability can be exploited, that provide broader visibility, and that improve detection and mitigation. These tools and policies can help minimize risk and reduce the time to respond during an attack or intrusion. Figure 3 shows some of the processes these tools use to determine what type of traffic can be safely allowed into the network

Figure 3.



Event Correlation and Reducing Information Overload

Security, network, and host devices often generate tremendous volumes of information during security events of any scale. Processing this information manually can overload IT groups, making standard tools ineffective and making it nearly impossible to find real threats in real time. Maximizing the efficacy of the security infrastructure can be achieved by looking for patterns in threats, correlating those events into risk categories, and determining a best course of action to mitigate them. In some cases, this can reduce the time to identify and respond by 95 percent. Many IT groups can now isolate a threat in less than two hours, that would have previously taken them two days.

Vulnerability and Attack Protection

In order to increase security visibility and reduce the time to respond, technology must be deployed to detect intrusion and vulnerability exploitation attempts at various points in the network. Preventing threats from compromising critical systems by rapidly detecting anomalous behavior and known threat signatures can be achieved by implementing intrusion detection and prevention at all points of entry to the network, and at various internal demarcation points within the intranet. Intrusion detection and prevention can identify different types of exploit attempts and can notify administrators immediately of an attempt to improperly access a system. Intrusion prevention can stop those attempts before they cause damage.

System Intrusion Prevention

Operating system and application vulnerabilities can be exploited by various means, particularly when other network-layer defenses have been bypassed. After a system has been accessed, it is important to minimize any potential damage or loss. This means rapidly notifying administrators of a system breach, putting appropriate countermeasures along the attack path, and preventing the improper viewing or removal of information and potential damage caused to the system itself. Administrators can better protect server resources by employing endpoint intrusion prevention, helping minimize the effect of day-zero threats, and preventing further attack propagation. Endpoint intrusion prevention can prevent certain types of behavior, including binary manipulation, keystroke logging, improper network utilization, and other system behaviors.

Where to Begin

Most organizations have tools in place that can be used as a starting point to develop a robust threat prevention architecture. Technology can be introduced in phases as the security strategy for the company is revised. Security processes should be periodically reviewed to assure the organization is adopting best practices. A comprehensive, proactive security strategy is a constantly evolving process; identifying the crucial points is an important first step.

Maximize the Efficacy of Your Existing Security Infrastructure

Most organizations have already deployed firewalls and antivirus solutions. These products help in the first and last lines of defense and can provide invaluable information to administrators as to the status of the network at any given time.

- **Recommendation 1:** Deploy a threat correlation and alarm management system to maximize the effectiveness of alarms, policy violations, and logs. This will help minimize the amount of time IT staff must spend manually parsing log entries, and provides significant improvements into threat visibility.

  Cisco solution: The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS). For more information, visit http://www.cisco.com/go/mars.

- **Recommendation 2:** Revisit your perimeter security technology and policies to assure that new attack vectors are being addressed, such as protocol anomalies, application-based attacks, and intrusions. This will not only help in addressing current needs based on the changed threat landscape, but will also help position the infrastructure for the inevitable changes that will come as new vulnerabilities, and the methods to exploit them, are discovered.

  Cisco solution: Cisco ASA 5500 Series Adaptive Security Appliances. For more information, visit http://www.cisco.com/go/asa.

- **Recommendation 3:** Consider obtaining services that can help distill the numerous security advisories and customize them to your business and organizational needs. This can help minimize the time the IT department spends on reviewing new threat alerts from groups such as CERT or SANS, so they can focus in on the threats that are directly relevant to your organization.

  Cisco solution: Cisco IntelliShield Alert Manager. For more information, visit http://www.cisco.com/go/intellishield.

Fortify the Remote Sites of the Organization

Remote sites, including branch and satellite offices, partner locations, and remote users, increase the chances that threats will be introduced into an organization. Wireless networks, proper access control (including into the facilities), and unmanaged devices can pose challenges when trying to protect critical information and end systems.

- **Recommendation 1:** Deploy wireless authentication and rogue wireless detection to help assure that unauthorized users are not gaining unrestricted access to the infrastructure.

  Cisco solution: Cisco wireless security solutions. For more information, visit: http://www.cisco.com/go/wirelesssecurity.

- **Recommendation 2:** Consider performing a wireless vulnerability assessment that can identify exposure in your wireless infrastructure and can recommend solutions.

  Cisco solution: Cisco Wireless Security Posture Assessments. For more information, visit: http://www.cisco.com/go/securityconsulting.

- **Recommendation 3:** Make sure that endpoints are properly secured and are not propagating threats into the network, infecting other users, and potentially providing launching points for attacks and intrusions. Endpoints can be infected by threats that might not be recognized by antivirus and anti-spyware software. It is important to prevent endpoints from inadvertently implementing malicious code, gathering information and sending it to a hacker, or performing other behaviors that can be a threat to both the endpoint and the infrastructure at large.

  Cisco solution: Cisco Security Agent Desktop. For more information, visit: http://www.cisco.com/go/csa.

- **Recommendation 4:** Deploy branch intrusion prevention to prevent hackers from gaining entry to the corporate network through a remote site. Intrusion prevention systems (IPSs) can be deployed on branch routers and can help prevent against unauthorized entry and help protect the branch server infrastructure from being compromised.

  Cisco solution: Cisco IOS® Software IPS. For more information, visit: http://www.cisco.com/go/ips. Cisco Services for IPS provide ongoing signature file updates, operating system and application software updates, and hardware and software support to keep Cisco IPS solutions continually up to date. For more information, visit: [[add URL]].

- **Recommendation 5:** Deploy remote gateway antivirus, anti-spam, and anti-spyware software to protect the network’s endpoints and infrastructure, particularly on devices that are unmanaged or where security controls have been turned off by the user. “Scrubbing” transmissions for infected code, such as viruses, spyware, and spam, can dramatically improve system security and network performance.

  Cisco solution: Cisco ASA 5500 Series Anti-X Edition. For more information, visit: http://www.cisco.com/go/asa.

Day-Zero Protection and Enhanced Threat Visibility

Server, system, and application infrastructure protection should be fortified to protect against day-zero exploits and assure conformance to governance policies and regulations. Incremental changes to an organization’s existing security technology can dramatically improve the security posture of the organization. These changes can also help increase the visibility into attack types and help IT groups reduce the time required to detect and respond to an event.

- **Recommendation 1:** Review and update intrusion and attack protection mechanisms, accounting for both signature and traffic pattern anomaly detection. IPS signatures should be evaluated regularly; in many cases, these can be aided by third-party IPS signature services. Best practices should be followed with industry peers on preventing exploitation of system vulnerabilities. Both signature and anomaly detection should be employed to assure maximum coverage and detection accuracy.

  Cisco solution: Cisco IPS 4200 Series Sensors, Cisco Catalyst 6500 Series Intrusion Detection System Module (IDSM-2), and Cisco ASA 5500 Series IPS Edition. For more information, visit:

  - Cisco IPS 4200 Series: http://www.cisco.com/go/ips
  - Cisco Catalyst IDSM-2: http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5058/index.html
  - Cisco ASA 5500 Series IPS Edition: http://www.cisco.com/go/asa

- **Recommendation 2:** Deploy endpoint protection on servers and user computers to protect systems and provide threat details to administrators. Anomalous behavior at the endpoint, including inadvertent code implementation, keystroke logging, and information farming and transit, can be detected, accounted for, and stopped. Systems can use the same tools to report these threats back to central management consoles and can help refine signatures, dramatically improving signature fidelity and further reducing response times.

Cisco solution: Cisco Security Agent. For more information, visit: http://www.cisco.com/go/csa.

- **Recommendation 3:** Examine policy management and threat correlation techniques to help minimize response times during an event. By reducing the amount of information to review and the steps needed to mitigate an attack or intrusion, IT administrators can reduce the time to respond—in some cases by 90 percent. Coordinated policy management and threat management tools are important in achieving that goal.

  Cisco solutions: Cisco Security Manager and Cisco Security MARS. For more information, visit:

  ◦ Cisco Security Manager: http://www.cisco.com/go/csmanager

  ◦ Cisco Security MARS: http://www.cisco.com/go/mars

Control Network Access and Endpoint Policy

Access to internal systems, networks, and applications should be limited to trusted users, and care should be taken to validate the security posture of endpoints before access is granted. This can dramatically reduce the introduction, accidental or intentional, of threats to the infrastructure.

- **Recommendation 1:** Deploy Network Admission Control (NAC) at wireless and public aggregation points. NAC helps prevent inadvertent admission over trusted links and allows greater flexibility in admissions for all users. Provisions should initially be made for wireless security from mobile PCs; next steps include moving to more comprehensive admission control of the device and user.

  Cisco solution: Cisco NAC. For more information, visit: http://www.cisco.com/go/nac.

- **Recommendation 2:** Review perimeter firewall infrastructure and account for new types of vulnerabilities. Firewall policies should be reviewed, taking into account new application-level and protocol-level exploits. Management should allow for the rapid deployment of new firewall policies and access lists to help contain day-zero threats.

  Cisco solution: Cisco Firewalls. For more information, visit: http://www.cisco.com/go/firewall.

- **Recommendation 3:** Review corporate LAN access policies and deploy intranet-wide NAC. With proper LAN-connected protection and perimeter controls in place, verify user access policies based on user role and access requirements by enforcing admission control policies for all intranet and extranet users.

  Cisco solution: Cisco NAC. For more information, visit: http://www.cisco.com/go/nac.

A Systems Approach to Threat Control and Containment

To effectively deploy a threat control solution, a lifecycle systems approach is recommended. The best way to manage network security risk and compliance requirements is through a systematic, architectural approach that addresses the entire lifecycle of the network, and that is built upon a standards-based network security infrastructure. The Cisco Lifecycle Services approach to security helps organizations realize the maximum benefits from network and security technologies, and helps them maintain comprehensive protection as their networks evolve.

Working with partners, Cisco provides a range of services based on proven methodologies and best practices to deploy threat control systems that are effectively designed, deployed, managed, and integrated into the infrastructure and business processes.

- **Recommendation 1:** Understand the network's current security strengths and vulnerabilities. Cisco Security Services employ a range of methodologies to evaluate the network's ability to prevent, detect, and mitigate threats. Vulnerability assessments and security architecture reviews are effective tools for identifying vulnerabilities at the system and network level.

  Cisco solution: Cisco Security Posture Assessments and Security Architecture Review Services. For more information, visit: http://www.cisco.com/go/securityconsulting.
- **Recommendation 2:** Plan and design a threat control system based on an in-depth, systemwide methodology and accepted industry standards. A strong design and integration plan can increase the effectiveness of threat control solutions, shorten deployment time, and reduce overall integration costs. Cisco can provide expert design assistance in developing a strong threat control design.

  Cisco solution: Cisco Security Design Services. For more information, visit: http://www.cisco.com/go/securityconsulting.
- **Recommendation 3:** Deploy, configure, and integrate new threat control systems into the network infrastructure, based on an understanding of the overall security architecture. Multilayer defenses are necessary, but may increase the complexity of managing network security and make it more difficult to identify and mitigate threats. Bringing sound network integration expertise, Cisco can accelerate the successful implementation of threat control solutions.

  Cisco solution: Cisco Security Deployment Services. For more information, visit: http://www.cisco.com/go/securityconsulting.
- **Recommendation 4:** Proactively manage your IT infrastructure by anticipating, identifying, and resolving issues quickly and accurately. A threat control system should include timely, accurate, and credible security intelligence combined with a threat correlation and alarm management system. Consider obtaining remote management services to proactively manage your threat control infrastructure.

  Cisco solutions: Cisco Security Intellishield Alert Manager, Cisco Services for IPS, Cisco Remote Management Services. For more information, visit:

  - Cisco Security IntelliShield Alert Manager: http://www.cisco.com/go/intellishield
  - Cisco Services for IPS: http://www.cisco.com/en/US/products/ps6076/serv_group_home.html
  - Cisco Remote Management Services: http://www.cisco.com/go/ros

Summary

The threat landscape has changed. IT and security operations teams must control a vast array of threats to the network infrastructure and must simultaneously assure network access for all who need it. Managing the volume of alarms and information and assuring minimal damage during an event are crucial; as a result, IT and security operations teams are pressured to reduce their time to respond in a crisis.

From viruses to phishing to hijacking to intrusions, the evolution and complexity of threats must be addressed in a way that helps IT departments make rapid decisions based on all intelligence available across the entire IT infrastructure. The network itself must provide accurate, detailed threat analysis and must prevent, detect, and mitigate both emerging and well-defined threats to help ease the burden of information overload to the IT department and enable a shorter time to respond and remediate. The Cisco Self-Defending Network and Cisco threat control solutions help IT departments deal with the ever-changing landscape of threats and mitigate the damage these threats aim to cause.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

C11-377861-00 01/07