



CYBER SECURITY AND FRAUD PROTECTION

# Cybersecurity Is a Top Focus for JPMorgan Chase

## Technology and Architecture

Adaptive security embedded throughout all parts of the technology infrastructure

## Security Operations

Proactive, risk-based and intelligence-led operations

## Data Security

Differential protection of critical information assets at every level

## Enabling the Business

Robust programs to ensure cybersecurity awareness and preparedness

Dear Fellow Shareholders,



Jamie Dimon,  
Chairman and  
Chief Executive Officer

### CYBERSECURITY UPDATE

In last year's letter, I gave a frank assessment about cybersecurity and why it is such a critical priority for the entire company. We outlined how JPMorgan Chase had spent approximately \$200 million in 2012 to protect ourselves from cyberwarfare and to make sure our data were safe and secure, and we dedicated more than 600 employees across the firm to the task. Despite these intense efforts, we acknowledged that the issue of cybersecurity worried us – and, today, that worry only has continued to intensify.

By the end of 2014, we will have spent more than \$250 million annually with approximately 1,000 people focused on the effort. This effort will continue to grow exponentially over the years.

In our existing environment and at our company, cybersecurity attacks are becoming increasingly complex and more dangerous. The threats are coming in not just from computer hackers trying to take over our systems and steal our data but also from highly coordinated external attacks both directly and via third-party systems (e.g., suppliers, vendors, partners, exchanges, etc.). It appears that a large, successful attack on a major retailer last year was the result of a third-party system breach.

“We will do whatever it takes to protect the company and its clients...It is critical that government and business and regulators collaborate effectively and in real time. Cybersecurity is an area where government and business have been working well together, but there is much more to be done.” *Jamie Dimon, Chairman & CEO*

“We spent more than \$250 million in 2014 on our cyber capabilities. We established three global Security Operations Centers to monitor, detect and defend the firm...We doubled the number of cybersecurity personnel over the past two years...Over the next two years, we will increase our cybersecurity spend by nearly 80%...” *Matt Zames, COO*

Source: JPMorgan Chase & Co. 2014 Annual Report letters to shareholders

# Cybersecurity Threats Are Increasing Globally

- Criminals are aggressively trying to gain access to corporate information technology systems to steal money by obtaining information about banking security credentials and/or tricking employees into sending fraudulent wire transfers.
- Criminals frequently are using two types of fraud schemes to trick employees at companies into sending wire payments. There has been an increase in these schemes in the last six months:
  - Emails or other communications to clients that appear to be from legitimate contacts, but which actually direct clients to make funds transfers to accounts controlled by criminals
  - Malware attached to emails or website links that infect client computers and capture client security credentials, enabling criminals to issue payment instructions in the name of the client
- As incidents of cyberfraud increase globally, JPMorgan Chase reminds all clients of the precautions they can take and the controls it offers to help them avoid loss.

**Companies are responsible for the security of their own systems and compliance with their internal controls.**

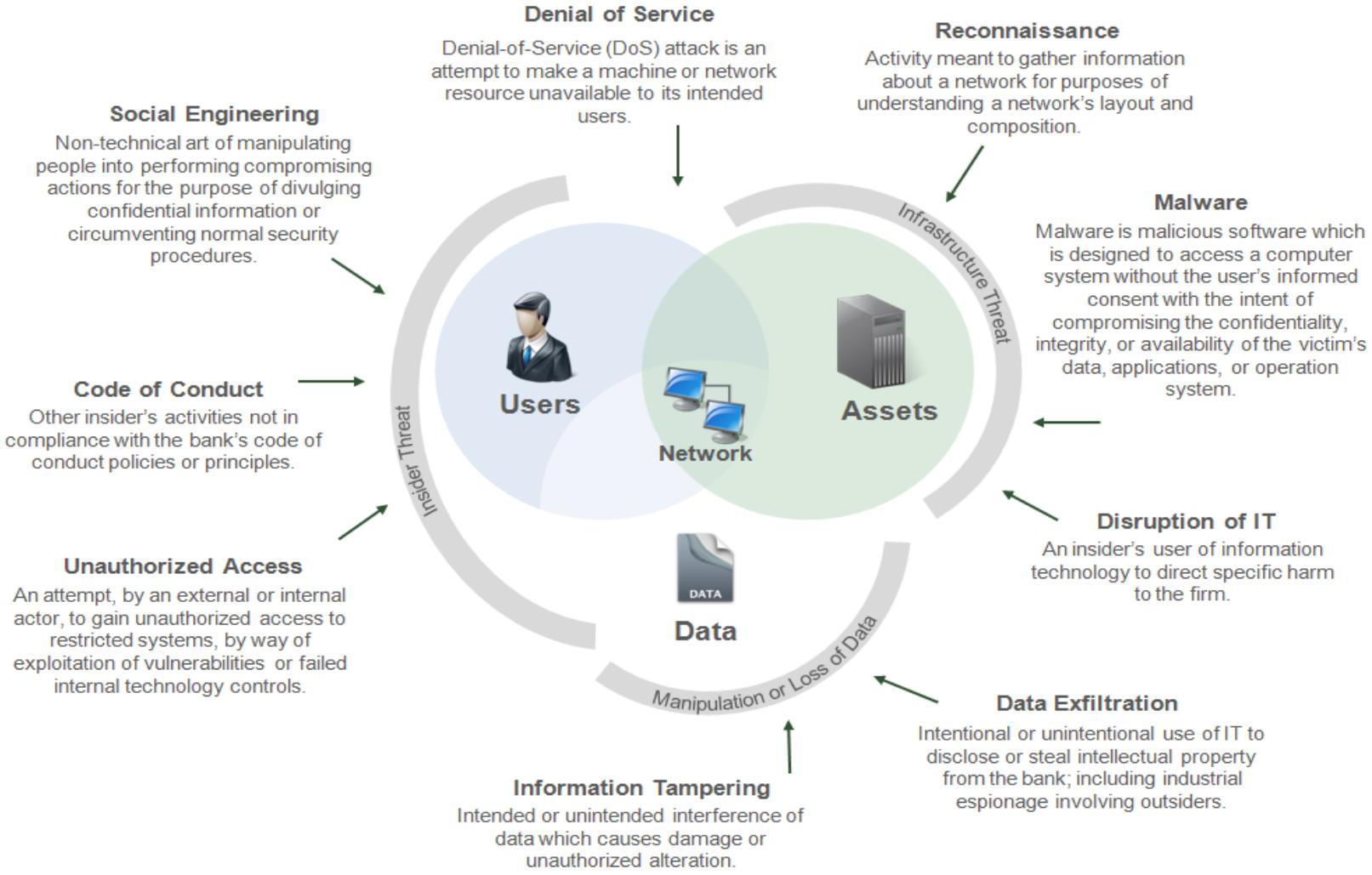
**Companies, not financial institutions, are responsible for wire transfers originated by their authorized representatives or with the use of authorized credentials, even if they are tricked into giving the funds transfer instructions.**

# Changing threat landscape

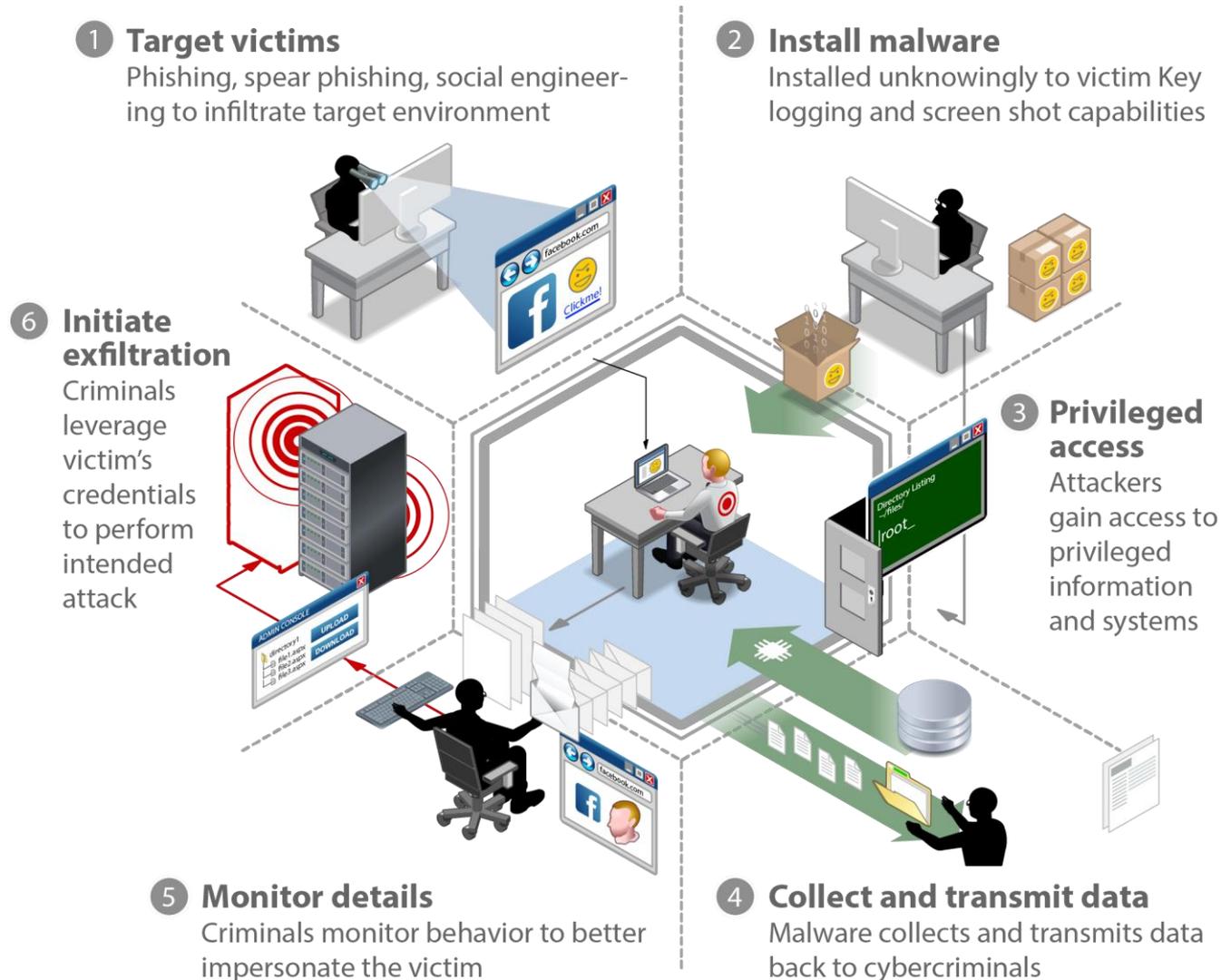
**Increasing Impact and Risk**

|                  | Disruption   | Fraud / Theft<br><small>(money, data, identity)</small>   | Destruction  | “Brand”   |
|------------------|--|---|--|---|
| External Threats | <p><i>Vulnerability</i></p> <p><b>New poll shows most internet users ignored merchant breaches</b></p>                    | <p><i>Data Theft</i></p> <p><b>Breach affected 110 million people</b></p>                                   | <p><i>Cyberwarfare</i></p> <p><b>Ukrainian authorities suffer new cyber attacks</b></p>         | <p><i>Reputational damage</i></p> <p><b>Cyber attacks expose online risks for brands</b></p>                           |
| Internal Threats | <p><i>Insider Threat</i></p> <p><b>Insiders suspected in attack that erased 30,000 hard drives at Saudi Aramco</b></p>  | <p><i>Unauthorized Access</i></p> <p><b>Direct access billing system leads to \$2.4 million scam</b></p>  | <p><i>Disgruntled Employee</i></p> <p><b>Disgruntled worker tried to destroy servers</b></p>  | <p><i>Data leakage</i></p> <p><b>Explosive data leaks have company’s and Governments in damage control mode</b></p>  |
|                  | <p><b>Increasing in pace, complexity and potential impact</b></p>  | <p><b>Motives moving from inconvenience to theft and espionage to destruction</b></p>   | <p><b>People are the targets</b></p>   |   |

# Cyber threats we face today



# Anatomy of a “typical” attack



# Information security best practices

## Protect

- Educate, raise awareness and enforce clear employee & third party policies
- Set strict controls for data access and protect sensitive data with encryption
- Establish lifecycle management program for company-controlled devices
- Build resiliency into systems and processes
- Join industry information sharing groups

## Detect

- Manage and monitor infrastructure, applications and endpoints
- Log inbound and outbound network traffic
- Establish alerts and reporting
- Data analytics for system and behavioral deviations

## Respond

- Define plan for incident handling
- Forensic investigations of known incidents and events
- Event correlation to determine impact and reach of attacks
- Prevent recurrence

# How Clients Can Protect Their Companies

## What executives can do:

- Require senior financial officer approval for any request for an immediate payment that is over a standard threshold amount or for any request that a payment be handled in secret.
- Establish and closely follow internal controls for the approvals required to change vendor remittance addresses or bank account information, and to pay invoices.
- Regularly check account activity for any suspicious transactions, and contact us immediately about any suspicious or erroneous wires.
- Immediately contact the Chase Commercial Online service center or J.P. Morgan ACCESS regional help desk if users become suspicious after sending a wire transfer.
- Use the security features that are available on J.P. Morgan ACCESS and Chase Commercial Online.

## What operations employees can do:

- Stop any online session that makes them uncomfortable, especially at log in, and call us.
- Always validate every payment request that has new or changed beneficiary information.
- Never provide sensitive confidential information in an email. This includes account numbers, log-in credentials and passwords, and SecurID® token information.
- Never respond to pop-ups or unsolicited phone calls asking them to resubmit log-in information, or the information of another user, especially on the same computer.
- Look for the personal verification image in reviewing any email that appears to be sent from us through the secure Voltage encryption system.
- Never share user IDs.
- Avoid multiple people using the same computer to process a transaction.
- Forward any suspicious emails to [abuse@chase.com](mailto:abuse@chase.com) or [abuse@jpmorgan.com](mailto:abuse@jpmorgan.com).

*J.P. Morgan* is a marketing name for certain businesses segments of JPMorgan Chase & Co. and its subsidiaries worldwide.

This document was prepared exclusively for the benefit and internal use of the party to whom it is directly addressed and delivered (the “Company”) in order to make a preliminary presentation to the Company regarding certain products or services provided by J.P. Morgan. This document and any related presentation are for discussion purposes only and are incomplete without reference to, and should be viewed solely in conjunction with, a related oral briefing provided by J.P. Morgan (collectively, the “briefing materials”). The briefing materials are: not intended as nor shall be deemed to constitute or contain advice on which the Company may rely; do not constitute in any way J.P. Morgan research, and should not be treated as such; and are confidential and proprietary to J.P. Morgan and may only be used by the Company in order to evaluate the products and services described therein, and may not be copied, published, disclosed or used, in whole or in part, for any purpose other than as expressly authorized by J.P. Morgan. The Company should consult with its own financial, legal, tax, accounting, compliance, treasury, technology or information system advisors prior to entering into any agreement for J.P. Morgan products or services, or with respect to its use of such products and services. All J.P. Morgan products, services, or arrangements are subject to applicable laws and regulations and service terms. Not all products and services are available in all geographic areas.

JPMorgan Chase Bank, N.A. Member FDIC © 2015 JPMorgan Chase & Co. All rights reserved.