J.P.Morgan

TREASURY SERVICES

Cybercrime: This Is War

EXECUTIVE SUMMARY

Drive-by downloads. Man in the Middle attacks. Fake installers. Rogue certificates. Bot zombies. Spyware, malware, Trojans. The list of cybercrime threats goes on. As the world becomes more connected, cybercriminals are becoming more adept, innovative and successful. How do organizations protect themselves in this high stakes game of corporate account takeovers, fraud and data and identity theft? Learn about best practices from the experts at the center of this escalating battle.

In the decade since the term "cybercrime" was first coined, it has quickly emerged as one of the top four economic crimes, just behind asset misappropriation, accounting fraud and bribery and corruption.[1] A faceless threat that affects individuals, organizations and governments worldwide, cybercrime is a multibillion-dollar industry whose perpetrators are increasingly well-organized, sophisticated and transnational.

Recent cyber attacks on corporations globally, combined with confirmed threats to critical infrastructure in the U.S. and other countries, had former Secretary of Defense Leon Panetta warning of a potential "cyber-PearlHarbor."[2] Today's increasing proliferation of mobile devices and the new frontiers of ecommerce and social networking are raising the ante for security experts: more is at risk than ever before in the war against cybercrime.

A Major Shift in Cybercrime Targets

The last several years have witnessed a dramatic shift in cybercrime targeting, as criminals move away from individual consumers and focus instead on enterprise opportunities. Recent breaches at large data warehouses have resulted in the theft of hundreds of millions of pieces of Personally Identifiable Information (PII). Due to its potentially high value and its use in facilitating fraud through additional channels, PII has become a valuable commodity in the world of cybercrime.

Enterprise attacks are also on the rise in the office, targeting individual employees attempting to get them to divulge sensitive information such as login credentials or to unknowingly trigger the download and installation of malicious software.

Perhaps even more worrisome, enterprise and executive level personnel with high-level authorities are not the only targets. Now, 58 percent of attacks are reaching sales, HR, executive assistants and even media relations staff, in other words, "lower-hanging fruit," who may offer more opportunity and, in many cases, be less well-protected than C-suite executives.[3]

The Cybercriminal Supply Chain

Cybercriminals can work independently or as members of a large group. Some are mercenaries doing the bidding of more sophisticated criminals. Others act on their own behalf, such as a disgruntled employee with access to high-level identity and password information. A most disturbing development is that highly organized crime syndicates are playing a leading role in the explosion of cybercrime. According to the FBI, these organizations operate like companies with specialists in each area of expertise:

- ORGANIZATION LEADERS assemble the team and choose targets
- CODERS write the exploits and malware
- DISTRIBUTORS trade and sell stolen data
- TECH EXPERTS maintain the criminal enterprise's IT infrastructure
- HACKERS search for and exploit vulnerabilities in applications, systems and networks
- FRAUDSTERS woo potential victims with social engineering schemes like phishing and spam
- HOSTED SYSTEM PROVIDERS offer illicit content servers
- CASHIERS control drop accounts and provide names and accounts to other criminals for a fee
- MONEY MULES complete wire transfers between bank accounts
- TELLERS who transfer and launder illicit earnings through digital currency services

THE CYBERCRIMINAL SUPPLY CHAIN

1. Information Collection: Fraudsters employ mechanisms such as phishing, spyware, crimeware, social networking sites and social engineering (e.g., rogue phone calls) to collect information.

2. Information Exchanges: Information is sold and traded to distributors. This information includes but is not limited to passwords, credit card numbers and personal information.

3. Attack: Hackers use information acquired from information exchanges for executing an attack. Compromised information allows stealthy execution of fraud as well as the ability to steal more information and botnets may be deployed to launch spam and Denial of Service attacks and distribute crimeware.

1 PricewaterhouseCoopers LLP. Global Economic Crime Survey. November 2011.
2 CIO Journal. The Wall Street Journal. "U.S. Defense Chief Warns of Digital 9/11." October 11, 2012.
3 Symantec Corporation. Internet Security Threat Report, 2011 Trends, Volume 17. April 2012.
4 Panda Security. The Cyber-Crime Black Market: Uncovered. 2011.

Cybercrime Knows No Borders

According to Akamai Technologies, the top ten countries from which cyber attacks originate have not changed significantly in the recent past. China remains the source of the largest recorded attack traffic. Aggregately, nearly 38 percent originated from the Asia Pacific/Oceania region, just over 36 percent in Europe, 23 percent in North and South America, and just under 3 percent from Africa. It should be noted, however, that due to the anonymity provided by the Internet, the point of attack origination is not necessarily the same as the location of the cybercriminal.[5]

Country	Q2 '12 % Traffic	Q1 '12 %
1 China	16%	16%
2 United States	12%	11%
3 Turkey	7.6%	5.7%
4 Russia	6.3%	7.0%
5 Taiwan	5.4%	5.3%
6 Brazil	4.6%	4.0%
7 Romania	3.5%	3.0%
8 India	2.9%	3.0%
9 Italy	2.1%	1.9%
10 South Korea	2.1%	4.3%
- Other	37%	39%

Source: Akamai Technologies

Old Threats Proliferate and New Technology Brings New Threats

Cybercriminals are brazen social engineers, skilled in duping targets into providing sensitive information and security credentials, such as passwords or user IDs.

According to the World Economic Forum, today, a relatively low-skilled individual can cause devastating consequences for governments and corporations remotely. Any device connected to a network of any sort, in any way, can be compromised by an external party.[6]

No review of current cybercrime trends would be complete without a mention of phishing, a type of cybercrime that has been studied for more than 16 years, and remains a global phenomenon. During the first half of 2012, phishing increased 19 percent over the last half of 2011, marking the fourth increase recorded since the second half of 2010.[7]

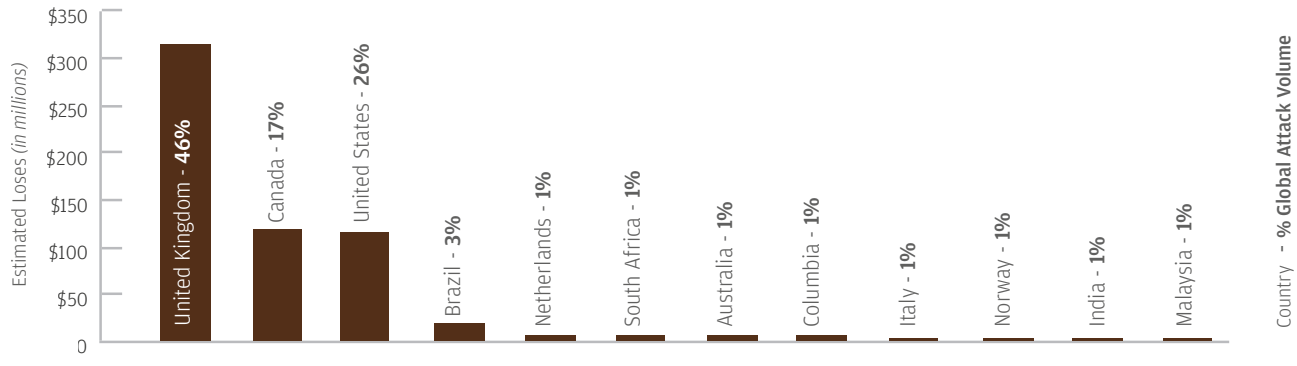
Why is this rather mundane cybercrime so effective? Security professionals insist it is because every phishing attack is built on an emotional trigger. Victims are convinced that they need to visit a fraudulent URL for a reason that is valid and credible to them.

According to RSA, the top ploys are[8]

- Rewards: such as tax refunds or prizes
- Greed: such as a promise of lottery winnings
- False accusations: tax fraud report from recognizable authority such as irs.gov
- Curiosity: a common "look who has been searching for you" scam
- Righting a wrong: fake order confirmations from a known online merchant
- Trust: fake emails from banks, service providers, social networking friend, etc.

Phishing is truly a global phenomenon, as the chart below demonstrates. The top five most attacked countries during the first half of 2012 were the U.K., U.S., Canada, Brazil and South Africa.[9]

TOTAL ESTIMATES LOSSES FROM PHISHING: FIRST HALF 2012



Source: RSA Global Phishing Map

5 Akamai Technologies, Inc., Volume 5, Number 2, The State of the Internet 2nd Quarter, 2012 Report
6 World Economic Forum. Global Risks 2012: Seventh Edition. January 2012.
7 RSA Blog. Speaking of Security. "Phishing in Season: A Look at Online Fraud in 2012."
8 Ibid.
9 Ibid.

Cybercriminals are brazen social engineers, skilled in duping targets into providing sensitive information and security credentials, such as passwords or user IDs.

As online fraudsters broaden their attacks beyond their traditional targets, consumers and online banking sites, new tricks of the trade proliferate.

SMISHING is phishing by SMS (or Short Message Service). A text message is sent to an individual's mobile phone requesting personal information under false pretenses.

VISHING SCHEMES allow criminals to use the telephone to gain access to personal information. "War dialers" dial thousands of numbers at a time. When a call is answered, an automated recording claims that a credit card or bank account has been compromised and dupes account owners into supplying personal information. Many attacks combine vishing and phishing, using email to lure the individual to call a number manned by fraudsters and unwittingly supply confidential personal information.

TROJAN ATTACKS are playing a new role in real-time online theft. A Trojan is malicious software that appears to perform a desirable function for a user but instead facilitates unauthorized access of the user's computer system. A man-in-the-browser (MITB) attack intercepts data during a secure communication between a user and an online application. The Trojan embeds in the browser application and can intercept and manipulate any information that user submits. Trojans are also being used to attack instant messaging (IM) applications.

Cyberthreats also include viruses, ad-related spam email and keylogger robot or "bot" programs that record keyboard keystrokes to collect user access IDs and account information.

"Bring Your Own Device" (BYOD) Can Mean Bring Along a Hacker

Personally owned smartphones, laptops and, more recently, tablet computers present a brave new world of cybercrime opportunity.

Expert estimates contend that fully 10 percent of mobile applications leak logins and passwords, 25 percent expose PII and 40 percent communicate with third parties.[10] Though app stores have strict guidelines for developers and ad posters, security measures are not among them. Many widely downloaded apps lack any encryption and many insecurely share personal information with third parties, not the least of which are advertisers.[11]

According to Juniper Networks, mobile malware has reached a new level of maturity. In 2011, global mobile handset shipments reached 1.6 billion and tablet shipments reached 66.9 million. Now that these devices are firmly entrenched in day-to-day business experience, sheer volume makes for a "staggering range" of opportunities for hackers:[12]

- 30 percent of applications have the ability to obtain the device location without users' explicit consent
- 14.7 percent of applications request permissions that could lead to the initiation of phone calls without user knowledge
- 6 percent of applications request the ability to look up all the accounts on the device, including email and social networking sites
- 4.8 percent of applications are able to send an SMS message without users' involvement and knowledge

By operating system, Android takes the lead with nearly 47 percent of all malware samples detected. No surprise, since Android commands an equal market share of smartphone subscribers (see chart). In the last seven months of 2011 alone, Juniper found that malware targeting the Android platform rose 3,325 percent.[13]

Before Apple iOS advocates applaud the relatively limited number of malicious applications on the platform, Juniper points out that this does not necessarily mean iOS is fundamentally more secure. Since Apple does not provide developers the tools to create endpoint security products, users are left with little protection if cybercriminals ever succeed in passing Apple's vetting process (a concept that has already been proven). Juniper concludes, "In the long run, this could create a false sense of security for Apple users and prove to be an even bigger risk than Android's open model."[14]

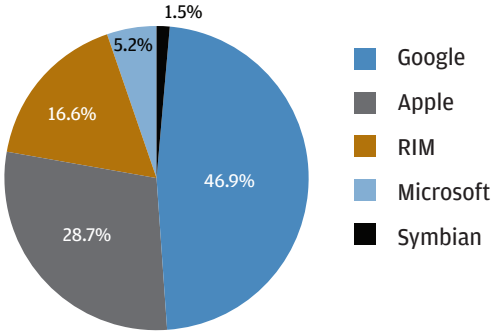
It should not go unnoted that mobile web browsers present threats, regardless of operating systems. Browser-based attacks can be triggered simply by visiting an infected website where a "drive-by download" begins automatically without the end user's knowledge.[15]

For this reason and others, app stores are beginning to be looked at as the enemy.

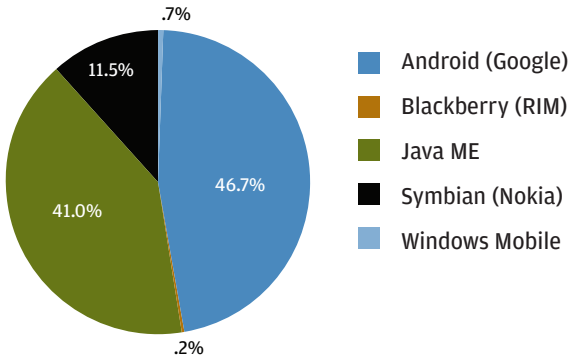
In October 2011, Juniper started to find large numbers of malicious applications called "fake installers" in several third-party application stores. These fake installers trick users into agreeing to automatically send

10 Zscaler. ThreatLabZ report. http://www.zscaler.com/20121008-press-release-zscaler-threatlabz-launches-free-mobile-app-profiler.html. Accessed October 5, 2012.
11 Ibid.
12Juniper Networks. 2011 Mobile Threats Report. February 2012.
13 Ibid.
14 Ibid.
15 Ibid.
16 Ibid.

MARKET SHARE OF SMARTPHONE SUBSCRIBERS BY PLATFORM



UNIQUE MOBILE MALWARE SAMPLES DETECTED BY OPERATING SYSTEM



premium text messages to attackers when they download either pirated or legitimate versions of paid applications. This type of malware presents a low barrier to entry for even novice cybercriminals and is especially dangerous for consumers who have no way of knowing they are not dealing with a legitimate entity.[16]

Add to these threats the ubiquity of wifi environments where hackers can use man-in-the-middle techniques to infiltrate an unprotected network, and the propensity for mobile devices to be lost or stolen—and the scale of potential data breach becomes very clear indeed.

No Business Segment Is Exempt

Though media reports would lead many to believe that cybercriminals target only large organizations, the truth is that no entity is immune.

In 2011, more than half of the targeted attacks measured by Symantec were directed at small and midsized businesses (fewer than 2,500 employees). And 17.8 percent were directed at companies with fewer than 250 employees.[17]

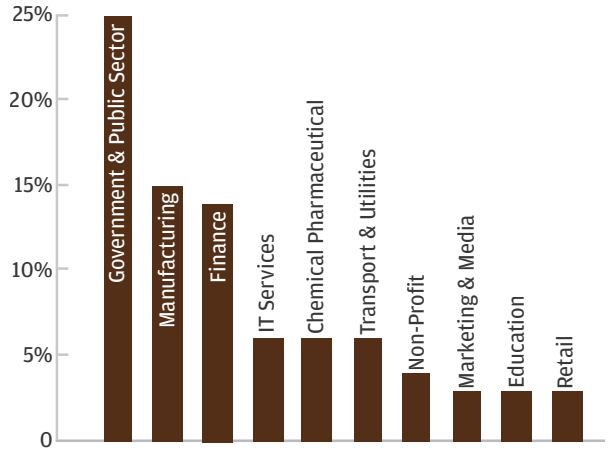
Customer data, industrial espionage and supply chain disruption are becoming common among targeted attacks, as cybercriminals continue to find new ways to monetize non-financial data.

For example, consumer utility account records can provide access to certain PII that facilitates opening fraudulent bank accounts. Medical records can be cashed out to shady law firms or used to commit insurance fraud. And courier service accounts can allow fraud perpetrators to get merchandise reshipped to their country of residence. Further, a search of the cybermarket reveals that date of birth and social security numbers are among the most widely demanded commodities in the underground, commanding prices of $1 to $3 USD per record.[18]

When it comes to targeted email attacks, government, manufacturing and finance lead as the most attacked industries. Interestingly, it is estimated that more than two-thirds of attack campaigns focus on a single organization or a very small number of companies in a given sector, sometimes attacking that company in different countries at the same time.

Targeted attacks are one of the most watched developments in the war against cybercrime. They are increasingly sophisticated and present the greatest danger of the greatest loss to a victim organization.[19]

TARGETED EMAIL ATTACKS BY SECTOR



Source: Symantec Corporation. Internet Security Threat Report, 2011 Trends

17 Symantec Corporation. Internet Security Threat Report, 2011 Trends.
18 RSA. RSA 2012 Cybercrime Trends Report, "The Current State of Cybercrime and What to Expect in 2012." January 2012.
19 Symantec Internet Security Threat Report, 2011 Trends.

The Frequency and Cost of Cyber Attacks are on the Rise

The growing frequency of cyber attacks is unsettling to say the least. Symantec Corporation, whose Global Intelligence Network represents one of the most comprehensive sources of Internet threat data in the world, blocked more than 5.5 billion malicious attacks in 2011, an increase of 81 percent over 2010.[20]

Estimates of the costs of cybercrime to a victim organization vary, but all agree they are substantial—and growing. According to a recent Ponemon Institute report, the cost of cybercrime to the large companies studied ranged from $1.4 million to $46 million in 2011, with an average annualized cost of $8.9 million, an increase of 6 percent, year over year.[21]

The highest *external* cost claimed was information theft, followed by the cost of business disruption. Recovery and detection combined (including cash outlays and labor) accounted for 47 percent of the *internal* activity cost.

No matter the size of the victim organization, the costs of cybercrime cannot be firmly measured in dollars and cents alone. It is nearly impossible to put a price tag on the loss of reputation and of the public trust in general, not to mention loss of customer loyalty that often results from major data breaches.

Online Fraud Follows the Money

Worldwide e-retail sales are projected to reach nearly one trillion dollars by 2013.[22] It's no wonder then that the cost of managing online fraud continues to grow for merchants of all sizes. In 2011, an estimated $3.4 billion was lost to online fraud in North America alone, a $700 million increase over 2010.[23] The majority of fraud loss is due to reverse of charges after the buyer claims fraudulent account use. And, fraud on international orders is more than three times higher than fraud on domestic orders.[24]

It is also no surprise that, given the continuing shift to electronic payments, card-not-present fraud losses have increased at twice the rate of counterfeit card losses.[25] Further, debit card fraud now outpaces credit card fraud. According to a recent FICO analysis, the top three sources for debit card fraud were ATMs, grocery stores and fuel dispensers where criminals install skimming devices to collect personal data. Top merchant categories for credit card fraud included grocery stores, restaurants and online retailers.

Online fraud impacts merchant profits in several ways. In addition to revenue losses, there is loss from the cost of stolen goods or services, delivery and fulfillment costs, customer experience costs and staffing costs for the review and administration of fraudulent claims. These "profit leaks" are forcing an increase in fraud detection tools, such as automated screening and decision tools, new manual review techniques and new approaches to fraud claims management.[26]

What's Ahead?

As hackers learn to crack codes on any and all devices, via both hardware and software, the threat of cybercrime will only grow. A review of a few top cybercrime watchdogs offers this list of several fraud trends to watch:[27]

- Mobile threats will pass threats to PCs
- Targeted attacks will increase
- Malware authors will increase their use of social networking sites
- Cloud computing will evolve and with it the way IT departments must adapt and protect corporate end users
- Hacktivism will rise, spurred on by Wikileaks and other highly-publicized hacking incidents
- Mac users will see increased attacks as they are exposed to websites that are able to drop Trojans
- New botnets will thrive, presenting major threats to all networks, public and private
- Embedded hardware (function control systems in cars, medical devices, digital camera and other items) will be on hackers' radar
- Increased industrial attacks
- "Fraud as a Service" will thrive, making it easier for cybercriminals to buy, find and pay for off-the-shelf services such as the latest Trojan codes and plug-ins, setup, instructions and support

Conclusion

There is no sign that the growth of cybercrime is slowing. Managing fraud risk requires nothing less than constant vigilance. Organizations of all types and sizes must understand the security priorities and capabilities of key vendors, business partners and suppliers.

20 Symantec. Internet Security Threat Report, 2011 Trends.
21 Ponemon Institute LLC. 2012 Cost of Cyber Crime Study: United States. October 2012.
22 Retail Decisions. Fight Fraud: Finding the right combination of solutions to stay one step ahead. 2011.
23 CyberSource Corporation. 2012 Online Fraud Report. 2012.
24 Ibid.
25 The Paypers. "US: card-not-present fraud losses higher than counterfeit fraud." August 24, 2012.
26 CyberSource. 2012 Online Fraud Report.
27 Symantec Internet Security Threat Report; RSA 2012 Cybercrime Trends Report; Pursuit Wire "Top 10 Security Threats for 2012. January 4, 2012.

Best Practices in Cybercrime Protection

Cybercrime begins and ends with individual computers and their users. Organizations need to take a risk-based and policy-driven approach to security. The following best practices have been culled from a number of knowledgeable sources that track, investigate and report on cybercrime and/or advise organizations on cybersafety protocols.

- FOSTER ENTERPRISE-WIDE AWARENESS OF CYBERCRIME THREATS. Make all employees, contract staff and business partners aware of the seriousness of cybercrime and any potential attacks on the enterprise and employ training as necessary.
- SET STRICT CONTROLS FOR DATA ACCESS. Limit borderless access to proprietary information on personally-owned devices as much as possible. Be sure to have standards, acceptable-use and approval policies in place for laptops, smartphones and any other IP-addressing wireless devices.
- ESTABLISH A LIFECYCLE MANAGEMENT PROGRAM FOR COMPANY-CONTROLLED DEVICES. Strict oversight allows you to have a record of who is accessing what information and provides the ability to remotely lock and/or wipe the device clean after employment termination or if the device is lost or stolen.
- SECURE YOUR NETWORK WITH A VPN REQUIREMENT. Always require employees to connect to your work network via VPN, as opposed to connecting via the Internet. The VPN setup mandates proper authentication for access to the network, then encrypts all data that passes through the link.
- ENFORCE CLEAR SOCIAL MEDIA GUIDELINES FOR EMPLOYEES. Employees must be clear on social media boundaries to avoid unwanted entry points.
- KEEP BASIC HARDWARE AND SOFTWARE PROTECTIONS CURRENT. Make sure all work PCs or other devices have robust and current antivirus, botnet checking and malware checking software and have software patches loaded as they become available.
- MANAGE AND MONITOR CLOUD COMPUTING. IT administrators face new challenges surrounding the information that is exchanged via cloud computing and must consider these issues:
  - » **Governance:** Can your Cloud Service Provider (CSP) assure you that the encryption software controls and other security mechanisms are permitted in a particular country or jurisdiction? Can they provide required evidence and reports to show compliance to regulations such as PCI and Sarbanes-Oxley?
  - » **Data:** Where does the data reside? How is it backed up? How is it deleted? Can privileged access be properly controlled in the cloud environment?
  - » **Architecture:** How do you protect against attack when you have a standardized infrastructure and the same vulnerabilities exist in many places across that infrastructure?
  - » **Applications:** How do you check and manage vulnerabilities in applications? How do you ensure patches are up-to-date?
  - » **Assurance:** How much experience does the provider have in audit/investigation procedures in a shared environment? What happens to the data if the cloud provider goes out of business?
- LOG INBOUND AND OUTBOUND NETWORK TRAFFIC. An abnormal increase—or decrease—in the amount of log data, or abnormal length of lines within logs, will sound alarms. Log data should also be checked to make sure users have not visited any known blacklisted sites.
- USE ENCRYPTION TO PROTECT SENSITIVE DATA. Restrict access as much as possible and use a data loss protection solution to identify, monitor and protect data from breaches.
- ENFORCE AN EFFECTIVE PASSWORD POLICY. Demand "strong" passwords with at least 8 to 10 characters with a mixture of letters, numbers and characters—and require employees to change them regularly.
- CONDUCT CUSTOMER EDUCATION PROGRAMS ALLOWING THEM TO TAKE INITIATIVE IN INCREASING SECURITY. Encourage the reporting of attacks, provide a mechanism for customers to do so easily and communicate attacks internally and externally.

For more information, please contact your J.P. Morgan Treasury Services Manager or visit www.jpmorgan.com/ts

J.P. Morgan

For more information, please contact your
J.P. Morgan Treasury Services representative
or visit us at **jpmorgan.com/ts**.

follow us on twitter

join us on linkedin

find us on facebook

see us on youtube

We are committed to making a difference by using paper with post-consumer fiber.

Produced by Treasury Services Global Marketing.

W5550413