Cybercrime: The Growing Global Threat

Cybercrime is a faceless threat that affects individuals, organizations and governments worldwide. Learn about the latest tactics of these digital pirates and privateers – and how to protect your organization from attack.

A Global Phenomenon
Thanks to the Internet, the personal computer and other technological advances, cybercrime is becoming a truly global phenomenon. Online fraud and crimeware software development is a growing, multibillion dollar worldwide industry. Its perpetrators are well organized, sophisticated and transnational, often operating in rogue nations outside of developed countries’ established jurisdictions. Cybercriminals are brazen social engineers, skilled in duping targets into providing sensitive information and security credentials, such as passwords or user IDs. They attack corporations, governments and individuals, seeking the “softest” targets with the highest opportunity for gain.

Not only does cybercrime have no borders, it also requires no firearms and getaway cars. In this age of electronic banking, the prize is information – digital money. It is as lucrative as gold, diamonds or crude oil, and it’s traded internationally. It is estimated that businesses around the globe lose more than $1 trillion in intellectual property due to data theft and cybercrime per year.1 Companies may be grossly underestimating the value of their intellectual property as well as the serious economic impact if it is stolen.

---

Choose Your Partners Wisely in the Fight Against Cybercrime

Staying ahead of today’s increasingly insidious cybercrime trends demands that organizations understand the security priorities and capabilities of their key vendors, business partners and suppliers.

Effective crime prevention demands a constantly updated combination of internal controls such as segregation of duties, third-party audits and consistent policies across the enterprise. The best defense in the war against cybercrime is a team approach that includes all levels of management and staff in all departments and shares information freely and frequently with appropriate outside parties.
Cybercrime: The Growing Global Threat

Emerging Countries, Emerging Threats
Throughout the last few years, a pronounced shift in malicious activity to emerging countries has been noted. The annual Symantec Global Internet Security Threat Report has ranked malicious activity by country since 2006. The latest report published in April 2010 shows, for the first time, a country other than the United States, China or Germany that ranks in the top three: Brazil. The growing level of malicious code activity affecting Brazil is so severe that it has resulted in the proposal of a new cybercrime bill in the country.²

<table>
<thead>
<tr>
<th>MALICIOUS ACTIVITY BY COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall Rank</td>
</tr>
<tr>
<td>2009</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>8</td>
</tr>
<tr>
<td>9</td>
</tr>
<tr>
<td>10</td>
</tr>
</tbody>
</table>

Source: Symantec Corporation

Looking at the source of cyberthreats, a similar picture appears. The latest sourcing information from the tracking agency ThreatExpert.com reports the worldwide distribution of threat origination³ as follows:

<table>
<thead>
<tr>
<th>WORLDWIDE THREAT ORIGINATION DISTRIBUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
</tr>
<tr>
<td>China</td>
</tr>
<tr>
<td>Russian Federation</td>
</tr>
<tr>
<td>Brazil</td>
</tr>
<tr>
<td>United Kingdom</td>
</tr>
<tr>
<td>United States</td>
</tr>
<tr>
<td>Spain</td>
</tr>
<tr>
<td>Germany</td>
</tr>
<tr>
<td>Others*</td>
</tr>
</tbody>
</table>

* Includes Canada, India, Iran, Algeria, Egypt, Syria, Iraq, Saudi Arabia, South Korea and Turkey
Source: ThreatExpert.com

Though China is the threat leader, security software vendor Zscaler points a spotlight at South America as an emerging threat. Brazil is not alone; the continent is home to seven of the top 10 countries with a high saturation of malware-distributing servers.⁴ Worthy of mention as a growing threat is North Africa. Because of anti-cybercrime deficiencies in legal and political systems and a general lack of crime-fighting resources, cybercriminals in North Africa have flourished in the last several years, primarily targeting European organizations.⁵

The Cybercriminal Supply Chain

Cybercrime is a multilayered threat. So-called “pirates and privateers” can work independently or as members of a large group. Some are mercenaries; others act on their own behalf, such as a disgruntled employee with access to high-level identity and password information.

A major development is that, in stark contrast to just a few years ago, highly organized crime syndicates are playing a leading role in the explosion of cybercrime.

The complexity of these syndicates can be byzantine as they employ sophisticated software, hardware and an army of fraudsters in varying roles:6

- **ORGANIZATION LEADERS** who assemble the team and choose targets
- **CODERS** who write the exploits and malware
- **DISTRIBUTORS** who trade and sell stolen data
- **TECH EXPERTS** who maintain the criminal enterprise’s IT infrastructure
- **HACKERS** who search for and exploit vulnerabilities in applications, systems and networks
- **FRAUDSTERS** who woo potential victims with social engineering schemes like phishing and spam
- **HOSTED SYSTEM PROVIDERS** who offer illicit content servers
- **BOTNETS**, also called zombie armies, a large number of compromised computers used to create and send spam or viruses or flood a network with messages as a Denial-of-Service (DOS) attack
- **CASHIERS** who control drop accounts and provide names and accounts to other criminals for a fee
- **MONEY MULES** who complete wire transfers between bank accounts
- **TELLERS** who transfer and launder illicit earnings through digital currency services

---

6 Ibid.

**INFORMATION COLLECTION:** The collector uses mechanisms such as phishing, spyware, crimeware, social networking sites and social engineering (e.g., rogue phone calls) to collect information.

**INFORMATION EXCHANGES:** The information collector sells information to the information warehouse, a wholesale distributor of stolen information. This information includes but is not limited to passwords, credit card numbers and personal information.

**ATTACK:** The attacker purchases information from the information warehouse for the purpose of executing an attack. Compromised information allows stealthy execution of fraud as well as the ability to steal more information. In addition, botnets are deployed to launch spam and Denial of Service attacks and distribute crimeware.
While most experts agree that cyberthreats are becoming increasingly more sophisticated, one of the more unsettling developments observed is the decreasing level of competence required to pose a cyberthreat. This, too, can be blamed on organized crime. These well-organized, highly mobile and extremely stealthy syndicates offer out-of-the-box hacking tools, packaged in such a way that even novice computer users can be in the cybercrime business overnight.

For example, VeriSign, the authentication company, recently uncovered that botnets are available to rent for as little as $8.94 (£5.99) per hour — the same price as a memory stick or a DVD.7 The syndicates also operate information warehouses that act as wholesale distributors of stolen data.

Advancing Technology and Techniques Bring New Threats

**Cyberthreats** come in all forms. As online fraudsters broaden their attacks beyond their traditional targets, consumers and online banking sites, new tricks of the trade proliferate.

**Phishing**, or bogus e-mails that trick users into supplying confidential information has evolved to smishing and even vishing — or combinations of the three. Smishing is phishing by SMS messaging. 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 e-mail 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.8

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

---

Concern Varies by Geography
There is no question that awareness of cyberthreats is growing across the globe. As shown in the table below, between 2007 and 2009, total awareness of phishing scams has doubled, from 38 percent to 76 percent, while awareness of Trojans has grown nearly 30 percent, from 63 percent to 81 percent.

Concerns about these forms of threat, however, show interesting differences in various regions. Trojans are of much greater concern in Latin America and Asia than in Europe and North America, because most organizations in the United States and Europe have already implemented strong access and authentication tools, alleviating customer concerns about Trojans. The difference in concern over phishing, however, may reflect a bit of overconfidence in the United States and Europe. RSA Security, the information security expert organization, reports that, although total awareness of phishing is high, the number of individuals falling victim to phishing schemes has risen nearly sixfold between 2007 and 2009, from 5 percent to 29 percent.9

Major Shifts in Cybercrime Targets
Individuals have been at risk of identity-related crimes long before the emergence of the Internet. What has changed in just the last two or three years is a dramatic shift in cybercrime targeting away from individual consumers and toward the enterprise.

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 commodity in the world of cybercrime.10

Enterprise attacks are also on the rise in the office. A form of phishing called spear phishing targets individual employees, attempting to get them to divulge sensitive information or to unknowingly trigger the download and installation of malicious software. Other popular scams are designed to steal login credentials, then initiate fake payroll payments or redirect deposit information on file to mule accounts.

Spear phishing and money mules played a significant role in U.S. payments fraud in 2009. This type of fraud is estimated to have cost U.S. businesses close to $100 million in attempted losses, and the FBI has issued a statement warning the public of the threat.11

No Business Segment Is Exempt
As businesses become the prime target for increasingly well-resourced online criminals, it is clear that no industry category or individual organization size is immune to the threat. Retail and financial enterprises may capture the most headlines, but evidence proves that all sectors are vulnerable to malware attacks in pursuit of intellectual and corporate assets and government intelligence. And, small and mid-sized commercial, educational, and state and local government entities in the United States are estimated to lose on average $100,000 to $200,000 per day to cybercrime, undoubtedly because they lack appropriate IT services and resources.12

---

MALICIOUS ACTIVITY BY COUNTRY

<table>
<thead>
<tr>
<th></th>
<th>% TOTALLY AWARE</th>
<th>% VERY CONCERNED BY REGION 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2007</td>
<td>2009</td>
</tr>
<tr>
<td>Phishing</td>
<td>38</td>
<td>76</td>
</tr>
<tr>
<td>Smishing</td>
<td>N/A</td>
<td>33</td>
</tr>
<tr>
<td>Trojans</td>
<td>63</td>
<td>81</td>
</tr>
</tbody>
</table>

Source: RSA Security, Inc.

---

9 Ibid.
11 Ibid.
Organizations are at increased risk due to the proliferation of mobile and other connected devices across the enterprise, the virtualization of business operations and the demographic shift toward online collaboration and social networking. These forces are dramatically changing the way business works, communicates, shares information and conducts transactions. And they underscore the need for new security models that acknowledge those changes.

In their 2010 Data Breach Investigations Report, the Verizon RISK Team and the United States Secret Service give insights into the who, what and how of data breaches. In 2009, fully 98 percent of all breaches were the work of criminals outside the victim organization, and 85 percent of stolen data records could be traced to organized crime. Interestingly, privilege misuse topped the list of threat actions leading to breaches (48 percent), followed by hacking and malware (40 and 38 percent, respectively). An alarming find showed that cases involving the use of social attacks more than doubled year over year, from 12 percent in 2008 to 28 percent in 2009. If there is good news to be gained from this major annual investigation, it is that most breaches could have been avoided without complex or expensive controls.13

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. They must develop and enforce policies and practices to protect their networks and systems from cyberattacks. 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 enterprisewide awareness of cybercrime threats. Make all employees, contract staff and business partners aware of the seriousness of cybercrime and potential attacks on the enterprise. Make sure they know your firm’s policies, practices and incident processes and syndicate any updates as they occur in this ever-changing landscape of threats. Should evidence of an attack be found, be prepared to respond quickly and effectively and to use your firm’s resources for forensic and incident response, investigation, and disaster and document recovery.

Ensure security policy enforcement with comprehensive employee training. The increasing sophistication of cybercrime techniques demands that organizations step up the level and consistency of employee security training. Application developers, system administrators and all staff who handle sensitive information are priorities, but understanding how to identify and report suspicious activity should be considered basic training for all employees. Given the growing expertise of criminals to target high-level executives, especially those with access to important intellectual property and trade secrets, organizations should consider specialized training for these individuals on the latest cybercriminal breach tactics such as phishing and other social engineering schemes.

---

Set strict controls for data access. In this newly mobile world, devices and applications adopted by users outside of work are increasingly being used within day-to-day business. The impact of such unsupported technology could have a devastating effect on enterprise security. Limit borderless access to information to the extent possible. Be sure to have standards, acceptable-use and approval policies in place for laptops, smartphones and any other IP-addressing wireless devices. Also establish a lifecycle management program for those devices the company controls so you can have a record of who is accessing what information and the ability to lock and/or wipe the device clean remotely after employment termination or if the device is lost or stolen. Talk with your IT staff and security vendors about solutions to protect your network and data regardless of the access device. Be sure to communicate and enforce your policies throughout the enterprise.

Keep basic hardware and software protections current. Often, organizations focus on fighting the latest threat at the expense of staying up to date with basic protections. Make sure all work PCs have robust and current antivirus, botnet checking and malware checking software. Utilize the security features built into operating systems and Web browsers, such as intrusion detection and firewalls. Also ensure that all software patches are loaded as they become available. Software development cycles have shortened for many vendors. For example, in the first three months of 2009, Microsoft announced 58 vulnerabilities; in the first three months of 2010, the company announced 77 vulnerabilities. Adobe announced an increase in vulnerabilities from nine to 26 in the same time periods for its Adobe Reader product. A good part of cybercriminals’ success is their constant vigilance, looking for new ways to hack a network or launch an executable malware file via an unpatched piece of software.14

Know your employees — before and after hiring. Today’s business environment demands greater emphasis on the need for effective background checks of job candidates and current employees. Organizations must have policies, practices and procedures that can minimize the probability of hiring an unqualified candidate or, in the instance of cybercrime, a dangerous one. Background checks, reference checking and drug testing are essential to the process of identifying, recruiting, attracting and retaining top employees with high integrity. Postemployment rechecking is an equally critical practice that helps organizations mitigate ongoing risk.

Establish employee guidance for the use of social media. Social networking is increasingly prevalent among today’s workforce. In fact, among Generation Y (or millennials) — those under 30 years of age — it is fast replacing e-mail as their preferred method of communication. We all know the names Facebook and Twitter, but social media also comprises countless blogs, wikis, photo-sharing sites and social news sites. While social media may be a groundbreaking collaboration tool, it is also a perfect conduit for attacks against individuals. Many IT security company experts agree: Social media will quickly become a primary path to the enterprise for cybercriminals. According to a recent Accenture report, 45 percent of employed millennials use social networking sites when they are at work, but only 32 percent say that use is supported by their IT departments.15 No organization can create policies to cover every incidence of social networking, but all can give employees guidance on acceptable use and establish decision-making protocols to deal with new and questionable uses as they arise.

15 Ibid.
Always require employees to connect to your work network via VPN, as opposed to connecting via the Internet. Virtual private network (VPN) links are key to improving the security of your employees’ wireless connectivity to the enterprise. They serve as a gateway for authorized users and a firewall for unauthorized users. The VPN setup mandates proper authentication for access to the network, then encrypts all data that passes through the link.

**Manage and monitor cloud computing.** Cloud computing, or sharing resources, software and information via the Internet, is transforming the way IT services are used and managed. It is revolutionizing business processes, saving time, money and resources, as it enables connectivity for far-flung employees and locations. In a recent report on security in cloud computing, PricewaterhouseCoopers quotes a Gartner Research finding that, by 2012, fully 80 percent of Fortune 1000 enterprises will be buying cloud computing service. As the practice reaches critical mass, it is destined to become the preferred choice for the majority of application development efforts among large enterprises. Trusted players, such as Amazon, Google, AT&T, Microsoft and IBM lead the way, fueling adoption.

IT administrators face new challenges surrounding the information that is exchanged via cloud computing. Among the issues to consider in this new, uncharted territory are:

- Does your cloud service provider have the technical capability to identify where, when and how data are used?
- What rights and recourse do you have for security breaches or incidents?
- Is there some form of accepted third-party review of security (ISO 27001 certification, for instance)?
- In the event of disaster, what are the recovery requirements?
- Can data be securely deleted once it is no longer needed?

**Monitor audit logs and inbound/outbound traffic.** Network log data can be invaluable in detecting potential threats or attacks in progress. Used and reviewed properly, logs can identify unusual or unauthorized events that may signal network compromise. For example, Web server log monitoring programs can track if and when company Web sites, logos and images have been completely downloaded, which may indicate that a cybercriminal is preparing to use your legitimate site to create a phony site for phishing. 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.

16 “Security Among the Clouds.” 2009. PricewaterhouseCoopers, LLC.
17 Ibid.
Banking-Specific Best Practices

- Segregate duties within your firm (initiate vs. approve), including payment activities with banking applications, making payments vs. reconciling accounts
- Use Positive Pay and/or Reverse Positive Pay for checks
- Use verified lines when possible
- Do not allow online banking from home PCs or public kiosks
- Segregate accounts by:
  - **Account type**: deposits or disbursements
  - **Payment method**: check, ACH, wire
  - **Payment type**: payroll, claims
  - **Payment amount and volume**: high or low
- Monitor and reconcile accounts daily

Best Practices in Online Channel Security

Organizations interact with customers across multiple touch points, but online communication, especially e-commerce and social networking, garners the most concern. Whether your customer is a business entity or a consumer — or both — you originally offered online services to reduce costs and provide additional convenience. Though the impact of strong security measures on customer usability is always a concern, research shows that security is a key driver to adoption.18

Balancing Protection and User Convenience

**Examples of J.P. Morgan ACCESS™ Security Elements**

J.P. Morgan incorporates sophisticated, multilayered security, including a patented, two-factor digital-signing authentication process for transaction processing to assure secure and reliable customer interaction.

**USER AUTHENTICATION**

Multifactor user authentication at logon and transaction time, incorporating both User Name and Passwords/SecurID and machine registration practices

**USER ENTITLEMENTS**

Client manages end-user access to products, product functions and accounts

**APPLICATION ENFORCEMENT**

Client manages end-user functionality for transaction processing (dual authority for creation, approval and release) and transaction limits

**CONSEQUENTIAL EVIDENCE AND CONFIDENTIALITY**

J.P. Morgan ACCESS enforces the use of digital signatures to ensure consequential evidence and industry-strength encryption for confidentiality as well as provides tools to track audit logs and online wire/ACH transaction inquiries

**CORE J.P. MORGAN INFRASTRUCTURE PROTECTIONS**

- Multilayered firewalls
- Internal education and training
- Secure onboarding with KYC program
- Quality control
- Intrusion detection and scanning
- Secured data centers
- Fraud analysis team
- Restricted product and account access by J.P. Morgan
- Rigorous Change Control program
- Server monitors and security scans

---

Here are some basic requirements:

• Conduct customer education programs and hone communications to address attacks
• Encourage the reporting of attacks and provide a mechanism for customers to do so easily
• Offer 100 percent SSL encrypted Web sites, with Federal Information Processing Standard (FIPS) 140-2 level 2 or better for storing the key (in other words, banks should store SSL key in hardware)
• Provide great security in customer onboarding and credential distribution
• Provide multifactor-based individual and machine authentication models with user-initiated deregistration
• Enforce the dual-authority model and/or “step-up authentication” for transactions
• Offer real hardware tokens for value-bearing transactions (software-based multifactor authentication is simply not good enough)
• Offer Digital Signing of transactions for after-the-fact evidence
• Utilize IP filtering solutions
• Put in place robust entitlements and application enforcement
• Display last login time for online applications

Support your organization’s strategies with a financial partner that takes cybercrime very seriously and has made reducing it a top priority. That partner is J.P. Morgan. We continue to invest in technology, support and the ongoing research necessary to keep you ahead of the curve — and help keep your business safe.
About J.P. Morgan Treasury Services
As one of the world's largest and most trusted full-service providers, J.P. Morgan's Treasury Services delivers cash management, trade, liquidity, commercial card and escrow services that resolve the working capital and efficiency challenges treasury professionals face today. We are committed to making it as easy as possible for clients to do business with us by providing streamlined documentation, fast-track implementations, online service tools and continuing to invest in the seamless global operating model that differentiates us in the market. More than 135,000 corporations, financial institutions, governments and municipalities in over 180 countries and territories entrust their cash business to J.P. Morgan.

About JPMorgan Chase
JPMorgan Chase & Co. (NYSE: JPM) is a leading global financial services firm with assets of more than $2 trillion and operations in more than 60 countries. The firm is a leader in investment banking, financial services for consumers, small business and commercial banking, financial transaction processing, asset management and private equity. A component of the Dow Jones Industrial Average, JPMorgan Chase serves millions of consumers in the United States and many of the world’s most prominent corporate, institutional and government clients under its J.P. Morgan and Chase brands. Information about the firm is available at jpmorganchase.com.