Communiqués de presse

IBM poursuit sa lutte contre les cyber menaces grâce à un système global de protection et des services dédiés aux données critiques

IBM aide ses clients à détecter, prévenir et répondre au mieux aux attaques dans un contexte d'augmentation du coût lié aux violations des données et des menaces persistantes avancées (Advanced Persistant Threats)

Paris, France - 05 mai 2014: IBM (NYSE: IBM) présente un nouveau système de sécurité incluant des logiciels et des services qui aident les entreprises à protéger leurs données critiques dans un contexte d'augmentation des menaces persistantes avancées, des vulnérabilités informatiques « zéro jour », des infractions et des coûts qui en résultent. Grâce à une analyse généralisée des comportements et une expertise de recherche approfondie, IBM peut aider les entreprises à arrêter les personnes qui exploitent ces vulnérabilités.

Selon deux enquêtes commandées par IBM auprès de l'institut Ponemon, le coût moyen de la violation des données a augmenté de 15%, pour atteindre une moyenne de 3,5 millions de dollars. Les études indiquent également que les attaques ciblées sont considérées comme la plus grande menace par la majorité des entreprises. Leur coût est estimé à $ 9,4 millions de perte en valeur intrinsèque pour la marque.

L'arrivée d'**IBM Threat Protection System** et de **Critical Data Protection Program** représente deux années d'investissements significatifs en matière de croissance organique et d'acquisitions d'entreprises telles que Q1 Labs, Trusteer, Guardium, Ounce Labs, Watchfire et Fiberlink/MaaS360. Depuis la mise en place, fin 2011, d'un business dédié à la cyber-sécurité, IBM s'est développé pour devenir l'un des plus grands acteurs en matière de sécurité pour l'entreprise et est fort de six trimestres consécutifs de croissance à deux chiffres dans ce domaine. Selon l'indicateur de référence de la mesure du revenu logiciel par éditeur, IBM a distancé de façon significative le marché du logiciel de sécurité, et est passé en 2013 de la 4 à la 3ème place des plus grands fournisseurs de sécurité.

IBM Threat Protection System peut prévenir les attaques - avant qu'elles n'arrivent

Le nouveau système de protection Threat Protection System contre les menaces d'IBM exploite les renseignements liés à la sécurité afin d'aller au-delà des défenses et des pare-feu traditionnels, ceci pour perturber les attaques à travers l'ensemble de la chaîne d'attaque, de l'infiltration à l'exfiltration.

IBM Threat Protection System comprend une architecture de logiciels d'analyse et d'enquête (forensics) de bout en bout. Ces derniers aident les organismes à prévenir en continu, détecter et répondre aux cyber attaques complexes, en cours, et, dans certains cas, à éliminer la menace avant que le dommage ne se soit produit.

- Pour la prévention, IBM annonce une nouvelle solution, **Trusteer Apex,** destinée à bloquer les logiciels malveillants, d'importantes améliorations pour **IBM Network Protection** afin de mettre en quarantaine les attaques, ainsi que de nouvelles intégrations avec les partenaires clés bénéficiant des capacités du réseau des

« bacs à sable » testant les logiciels/programmes douteux (sandbox).

- Pour la détection, IBM a amélioré sa plateforme **QRadar Security Intelligence** en la dotant de nouvelles fonctionnalités - permettant aux entreprises de détecter les attaques à grande échelle et de les bloquer en un clic.

- Pour répondre aux attaques, IBM a introduit **IBM sécurité QRadar Incident Forensics**. IBM continue également à étendre ses services d'intervention d'urgence à l'échelle mondiale.

Les clients qui ont testé IBM Threat Protection System ont vu des résultats rapides. Par exemple, un fournisseur de soins de santé avec des milliers de terminaux a immédiatement détecté la présence de dizaines de cas de logiciels malveillants, malgré l'utilisation habituelle de nombreux outils de sécurité traditionnels. Ce code malveillant peut être utilisé pour contrôler à distance les terminaux ou exfiltrer des données, mais il a été immédiatement désactivé. De même, une grande banque européenne a récemment essayé ce système et a été en mesure de désactiver les logiciels malveillants détectés dans l'entreprise.

Le système de protection contre les menaces IBM dépend de 11 centres d'opérations de sécurité (SOC) qui peuvent surveiller le système une fois ce dernier déployé chez les clients.

« Les menaces persistantes avancées ont fondamentalement modifié la manière dont les entreprises doivent aborder la question de la sécurité des données. » Déclare Brendan Hanigan, Directeur Général de IBM Security Systems. *« Aujourd'hui, se défendre contre les cyber attaques nécessite plus d'une approche basée sur la signature ou le périmètre. Des capacités d'analyse approfondies et les forensics sont indispensables et doivent inclure la prévention au niveau des terminaux (les terminaux fixes, mobiles utilisés par les employés, les partenaires et mêmes les clients), la protection du périmètre et la capacité à se prémunir contre les attaques avant qu'elles ne causent des dégâts ».*

IBM Security Services protège les « Joyaux de la Couronne » d'une entreprise et la marque

Le nouveau **Critical Data Protection Program** permet de protéger les données critiques d'une organisation, ou notamment « Joyaux de la Couronne ». La richesse d'une entreprise est souvent générée par moins de 2% de ses données, ce qui a un impact majeur sur la réputation de la marque, sa valeur de marché et sa croissance.

« Les inquiétudes sur la capacité à protéger les données critiques contre les cyber attaques sont un préoccupation du Board », a déclaré Kris Lovejoy, Directeur Général de IBM Security Systems. *« Les cyber-attaques et la perte de données jouent un rôle sur la réputation de marque, peuvent réduire sa valeur en actions et confronter une entreprise à des litiges. Les nouveaux logiciels et services d'IBM sont conçus pour fournir à ces responsables une solution unique qui leur permet de focaliser leur attention sur les besoins de leurs clients et les revenus de l'entreprise au jour le jour ».*

Les organisations font de plus en plus appel à IBM pour les aider à construire une approche véritablement globale et intelligente pour identifier rapidement et bloquer les menaces avancées avant qu'elles ne fassent des dégâts. Récemment, IBM a commencé à fournir des services de soutien hotline par des experts et un

déchiffrage des vulnérabilités à ses assurés CyberEdge d'AIG.

« Nous nous réjouissons qu'IBM continue de miser sur sa capacité unique à combiner logiciel leader sur le marché, services, capacités de recherche et partenariats avec l'industrie pour contrer l'augmentation des attaques sophistiquées », a déclaré Tracie Grella , Head of Professional Liability, Global Financial à AIG.

Les nouveaux services de conseil en sécurité sont basés sur le **Data Centric Security Model d'IBM**. Ce qui permet de protéger les informations critiques ou business les plus sensibles pour une entreprise en utilisant les fonctionnalités de Guardium, StoredIQ et IBM Research.

Ces données critiques sont à forte valeur ajoutée comme les plans d'acquisition et de cession, les délibérations du Conseil exécutif et de la propriété intellectuelle. Ces données critiques correspondent à 70 % de la valeur d'une société cotée en bourse et s'avèrent extrêmement précieuses pour les forces hostiles – que sont les initiés de la société ou les attaquants sophistiqués.

Malgré l'importance et la valeur des données critiques, de nombreuses organisations ne sont pas conscientes de ce qu'elles représentent, d'où elles se trouvent, de qui y a accès, ou de comment elles sont protégées, ce qui les rend plus difficiles à surveiller et à protéger. En fait, la découverte de la perte de données peut prendre des jours ou plus dans plus de 95 % des cas, et il faut des semaines ou plus pour les contrôler dans plus de 90% des cas, un décalage qui peut avoir un impact catastrophique pour une entreprise.

Le nouveau programme de protection des données critiques d'IBM propose une approche itérative multi-étapes : Définir, Découvrir, Comparer, Sécuriser et Surveiller. Ceci pour un cycle de vie complet en matière de sécurité des données pour protéger la rentabilité, la position concurrentielle et la réputation.

# # #

IBM Advances Fight against Cyber Threats with Comprehensive Threat Protection System and Critical Data Protection Services

With the Cost of Data Breaches and Advanced Persistent Threats on the Rise, IBM Helps Clients Detect, Prevent and Respond to Attacks

ARMONK, N.Y. - 05, May 2014: IBM (NYSE: IBM <http://www.ibm.com/investor/>) today introduced comprehensive new security <http://www.ibm.com/security> software and services to help organizations protect their critical data in an environment where advanced persistent threats <http://www.ibm.com/security/threat-protection/> , zero day attacks, breaches and the financial impact on an organization continue to rise. Through pervasive behavioral analytics and deep research expertise, IBM can

help organizations stop attackers from exploiting these vulnerabilities.

According to two IBM-commissioned studies <http://www.ibm.com/services/costofbreach> announced today from the Ponemon Institute <http://www.ponemon.org/> , the average cost of a data breach increased by 15 percent globally, reaching an average of $3.5 million. The majority of companies surveyed say targeted attacks are the greatest threat, costing them on average $9.4 million in brand equity alone.

Today's introduction of the **IBM Threat Protection System** and **Critical Data Protection Program** represent two years of significant investment in organic development and the acquisition of companies, including Q1 Labs, Trusteer, Guardium, Ounce Labs, Watchfire and Fiberlink/MaaS360. Since forming a dedicated cyber security business in late 2011, IBM has risen to become one of the largest players in enterprise security and has achieved six straight quarters of double-digit growth. According to IDC's Software Tracker, IBM significantly outpaced the overall security software market, and has moved from the 4th largest security vendor to the 3rd for 2013.

IBM Threat Protection System Can Help Prevent Attacks — Before the Damage
IBM's new Threat Protection System <http://securityintelligence.com/advanced-threat-protection> leverages security intelligence and behavioral analytics to go beyond traditional signature-based defenses and firewalls to disrupt attacks across the entire attack chain — from break-in to exfiltrate.

The IBM Threat Protection System includes an end-to-end architecture of analytic and forensics software that helps organizations continuously prevent, detect and respond to ongoing and sophisticated cyber attacks, and in some cases, eliminate the threat before the damage has occurred. Among the highlights:

- For **prevention**, IBM is announcing a new Trusteer Apex solution for endpoint malware blocking, significant enhancements to the IBM Network Protection appliance for quarantining against attacks and new integrations with key partners' network sandbox capabilities.

- For **detection**, IBM is enhancing its QRadar Security Intelligence platform with new capabilities – allowing organizations to detect attacks at new scale and actively block exploits with a click.

- For **response**, IBM is introducing IBM Security QRadar Incident Forensics. IBM also continues to expand its emergency response services globally.

Clients testing the IBM Threat Protection System have seen quick results. For example, a health care provider with thousands of endpoints immediately found dozens of instances of malware present, despite their use of many more traditional security tools. This malicious code could be used to remote control endpoints or exfiltrate data, but instead was instantly disabled. Likewise a large European bank recently tried this capability and was able to disable undetected malware across the enterprise.

The IBM Threat Protection System is supported around the world by IBM's managed security operations centers (SOC), which can monitor the system once deployed by clients. IBM's SOC Optimization consultants can also

deploy and integrate them into customer SOCs.

“Advanced Persistent Threats have fundamentally changed the way organizations have to approach data security,” said Brendan Hannigan, General Manager, IBM Security Systems. “Today, defending against cyber attacks requires more than a signature-based or perimeter approach. Deep analytic capabilities and forensics are vital and need to include endpoint prevention, perimeter protection and the ability to guard against attacks before they can do damage.”

IBM Security Services Safeguard a Businesses’ “Crown Jewels” and Protect Their Brand

The new Critical Data Protection Program helps safeguard critical data — a corporation’s “Crown Jewels.” An organization’s fortune is often driven by less than two percent of its enterprise data, which has major impact on competitive advantage, brand reputation, market value and business growth.

“Concerns over the ability to protect critical data from cyber attacks have moved center stage in the board room,” said Kris Lovejoy, General Manager, IBM Security Services. “Cyber attacks and loss of data have the ability to impact brand reputation, reduce shareholder value and open an organization to litigation. IBM’s new software and services are designed to provide these executives with a unique solution that lets them keep their focus on the day-to-day needs of their customers and driving business revenue.”

Organizations are increasingly turning to IBM to help them build a truly comprehensive and intelligent approach to quickly identify and stop advanced threats before they do damage. Recently, IBM began providing external vulnerability scanning and expert hotline support services to AIG’s CyberEdge insureds.

“We look forward to IBM continuing to build on its unique ability to combine market-leading software, services, research capabilities and industry partnerships to counter the momentum of sophisticated attacks,” said Tracie Grella, Head of Professional Liability, Global Financial Lines at AIG.

The new security consulting services announced today are based on IBM’s unique Data Centric Security Model, under which IBM deploys assets from Guardium, StoredIQ and IBM Research to help protect this business critical information.

This critical data — which may include such high value data assets as acquisition and divestiture plans, executive and board deliberations and intellectual property — accounts for an estimated 70 percent of the value of a publicly traded corporation. As a result, this type of data is extremely valuable to hostile forces – whether company insiders or sophisticated attackers.

Despite the importance and value of critical enterprise data, many organizations are not aware of what their Crown Jewel information is, where it resides, who has access to it, or how it is protected, making it more difficult to monitor and protect. In fact, data loss can take days or more to discover in more than 95 percent of cases, and weeks or more to contain in more than 90 percent of cases, a lag that can have a catastrophic impact on a business.

IBM's new Critical Data Protection Program offers an iterative multi-phased approach of Define, Discover, Baseline, Secure and Monitor for a full lifecycle of data security to protect profitability, competitive position and reputation.

About IBM Security

IBM's security portfolio provides the security intelligence to help organizations holistically protect their people, data, applications and infrastructure. IBM offers solutions for identity and access management, security information and event management, database security, application development, risk management, endpoint management, next-generation intrusion protection and more. IBM operates one of the world's broadest security research and development, and delivery organizations. IBM monitors 15 billion security events per day in more than 130 countries and holds more than 3,000 security patents. For more information, please visit www.ibm.com/security <http://www.ibm.com/security> , follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog <http://securityintelligence.com/> .

###

Global Cost of Data Breach Increases by 15 percent, According to Ponemon Institute

Traverse City, MI—May 5, 2014—Today Ponemon Institute released its ninth annual *Cost of Data Breach Study: Global Study,* sponsored by IBM*.* According to the study of 314 companies spanning 10 countries, the average total cost of a data breach increased 15 percent in the last year to $3.5 million Local currencies were converted to U.S. dollars for comparison purposes.. The study also found that the cost incurred for each lost or stolen record containing sensitive and confidential information increased more than nine percent to $145.

The ninth annual study involved the collection of detailed information about the financial consequences of a data breach. For purposes of this research, a data breach occurs when sensitive, protected or confidential data is lost or stolen and put at risk. Ponemon Institute conducted 1,690 interviews with IT, compliance and information security practitioners representing 314 organizations in the following 10 countries: United States, United Kingdom, Germany, Australia, France, Brazil, Japan, Italy, India and, for the first time, the Arabian region (a consolidation of organizations in the United Arab Emirates and Saudi Arabia).

"The goal of this research is to not just help companies understand the types of data breaches that could impact their business, but also the potential costs and how best to allocate resources to the prevention, detection and resolution of such an incident," said Dr. Larry Ponemon, Chairman and Founder of Ponemon Institute. "This

year's *Cost of Data Breach Study* also provides guidance on the likelihood an organization will have a data breach and what can be done to reduce the financial consequences."

All those interviewed are knowledgable about their organization's data breach and the costs associated with resolving the breach. All participating organizations experienced a data breach ranging from a low of approximately 2,400 to slightly more than 100,000 compromised records, which identifies the individual whose information has been lost or stolen in a data breach.

"Clearly, cybersecurity threats are a growing concern for businesses, especially when we consider how persistent data has become in the age of cloud and mobility," said Kris Lovejoy, General Manager, IBM Security Services Division. "A data breach can result in enormous damage to a business that goes way beyond the financials. At stake is customer loyalty and brand reputation."

The following are key takeaways from the *Global Cost of Data Breach Study:*

§ The most costly breaches occurred in the U.S. and Germany at $201 and $195 per compromised record, respectively. The least expensive data breaches were in India and Brazil at $51 and $70, respectively.

§ Root causes of data breaches differ among countries and affect the cost of the breach. Countries in the Arabian region and Germany had more data breaches caused by malicious or criminal attacks. India had the most data breaches caused by a system glitch or business process failure. Human error was most often the cause in the UK and Brazil.

§ The most costly data breaches were those caused by malicious and criminal attacks. The U.S. and Germany paid the most at $246 and $215 per compromised record, respectively. These types of data breaches were least costly for companies in India and Brazil at $60 and $77 per compromised record, respectively.

§ A strong security posture was critical to decreasing the cost of data breach. On average, companies that self-reported they had a strong security posture were able to reduce the cost by as much as $14 per record.

§ The involvement of business continuity management reduced the cost of data breach by an average of almost $9 per record.

§ The appointment of a Chief Information Security Officer (CISO) to lead the data breach incident response team reduced the cost of a breach by more than $6.

§ Countries that lost the most customers following a data breach were France and Italy. Companies in the Arabian region and Brazil experienced the lowest loss of customers.

§ The probability of a company having a data breach involving 10,000 or more confidential records is 22 percent over a two-year period. Countries most likely to experience a data breach include India, Brazil and France.

Consistent with previous *Cost of Data Breach* studies, the most common cause of a data breach is a malicious insider or criminal attack. In this year's study, we asked companies represented in this research what worries them most about security incidents, what investments they are making in security and the existence of a security strategy. Following are some of the key findings:

§ The greatest threats to the companies in this study are malicious code and sustained probes. According to threats increased.

§ Only 38 percent of companies have a security strategy to protect its IT infrastructure. A higher percentage (45 percent) has a strategy to protect their information assets.

§ Malicious code and sustained probes have increased the most. Companies estimate that they will be dealing with an average of 17 malicious codes each month and 12 sustained probes each month. Unauthorized access incidents have mainly stayed the same and companies estimate they will be dealing with an average of 10 such incidents each month.

§ The majority of companies (50 percent) have low or no confidence that they are making the right investments in people, process and technologies to address potential and actual threats.

§ Ideally companies would like to invest $14 million over the next 12 months to execute their organization's security strategy. However, in the next 12-month period, companies anticipate having an average of about half that amount, or $7 million, to invest in their security strategy.

***The State of Advanced Persistent Threats* study**

Today Ponemon also released *The Economic Consequences of an APT Attack* study sponsored by Trusteer, an IBM company.This newly released report is part of a larger research study entitled, *The State of Advanced Persistent Threats*, published in December 2013. This original research of 755 U.S. IT security practitioners supports the findings of *The Cost of Data Breach* study, wherein targeted criminal attacks are considered by a majority of respondents to be their organizations' greatest threat. Another corroborating fact is a finding that

reputation damages represent the most costly component or consequence of criminal attacks, and especially those involving the theft or misuse of information assets. Respondents in this study estimate an average cost to restore reputation as much as $9.4 million.

About Ponemon Institute

Ponemon Institute is dedicated to independent research and education that advances information security, data protection, privacy and responsible information management practices within businesses and governments throughout the world. Our mission is to conduct high quality, empirical studies on critical issues that affect the protection of information assets and IT infrastructure. As a member of the Council of American Survey Research Organizations (CASRO), we uphold strict data confidentiality, privacy and ethical research standards. www.ponemon.org <http://www.ponemon.org> .

About IBM Security

IBM’s security portfolio provides the security intelligence to help organizations holistically protect their people, data, applications and infrastructure. IBM offers solutions for identity and access management, security information and event management, database security, application development, risk management, endpoint management, next-generation intrusion protection and more. IBM operates one of the world’s broadest security research and development, and delivery organizations. IBM monitors 15 billion security events per day in more than 130 countries and holds more than 3,000 security patents. For more information on IBM security, please visit: www.ibm.com/security <http://www.ibm.com/security> .
