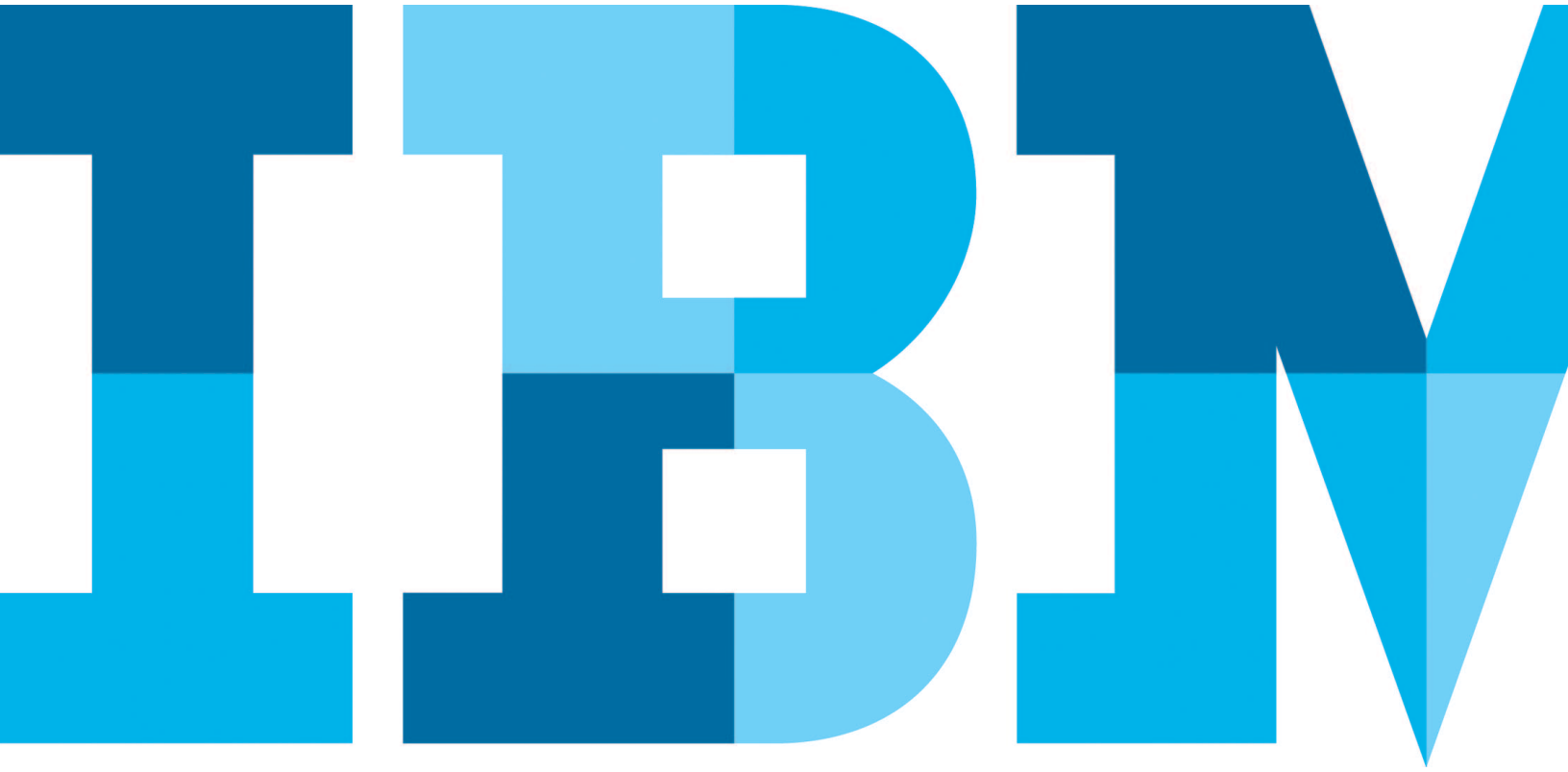
IBM Security Services 2014 Cyber Security Intelligence Index for Financial Services



IBM

About this report

IBM Managed Security Services continuously monitors billions of events per year, as reported by a sample of nearly 1,000 of our clients in 133 countries. Information is based on the cyber attack event data that IBM collected between 1 January 2013 and 31 December 2013 in the course of monitoring client security devices as well as data derived from responding to and performing forensics on cyber attack incidents. It is complementary to the IBM® X-Force® 1Q 2014 Threat Intelligence Quarterly.[1]

Since our client profiles can differ significantly across industries and company size, we have normalized the data for this report to describe an average client organization as having between 1,000 and 5,000 employees (although IBM typically serves larger client organizations), with an average of 500 security devices deployed within its network. The annual cyber security intelligence index report offers a high-level overview of the major threats trending across businesses worldwide over the past year. This report has been developed to provide insights into your current threat landscape for the financial services industry and to offer solutions that can help you better protect your organization. Where noted, additional information comes from industry analysts and publicly available data.

The problem that isn't going away

In today's world, the continued existence of a financial services institution depends on reputation and trust. A strong reputation generates stakeholder trust. If a financial institution is trusted, customers feel confident about entrusting sensitive personal data and using online services. Should that trust be compromised, there can be serious consequences.

The unfortunate reality, however, is that each year it becomes more challenging to protect against cyber security threats. The challenge is particularly significant for the financial services industry, which attracts significantly more incidents than many other industries. To would-be attackers, the financial services industry offers the allure of a significant potential payoff. A single breach can result in both a major business disruption and big paydays for successful cyber criminals. As a result, cyber attacks against financial services firms have become more frequent and sophisticated over the years. Some attacks are aimed at critical information, others are aimed at critical infrastructures and still others are hostile government and terrorist-sponsored attacks intended to cripple a country's financial system.

Diverse as their intent may be, all of these attacks can significantly impact financial services companies, not only in terms of monetary losses but also in terms of credibility and reputation. If consumers lose faith in a company's ability to keep their personal data safe, the company can ultimately lose customers. Most certainly financial services providers stand to lose money in the event of a data breach. In its most recent analysis, the Ponemon Institute found that in 2013 each lost data record cost companies participating in the research an average of US$145 per record, with companies in the United States losing the most per record for each data breach (US$201), followed by Germany (US$195),

and companies in India the least at US$51. Ponemon also found that heavily regulated industries such as finance had a per record data breach cost ranging from US$177 to US$359—placing them well above the average of US$145.[2]

With more data comes more vulnerability—and more insight

Looking back at 2013, we asked a few key questions:

- What's happening across the threat landscape for the financial services industry?
- What kinds of attacks are being launched?
- How many of those attacks result in incidents requiring investigation?

Companies within the financial services industry often have a complex back-office IT architecture, consisting of diverse platforms and interfaces. They employ multiple front-office channels, including the Internet, mobile networks, automated teller machines (ATMs) and kiosks. At the same time, many financial services organizations rely on IT resources outside of their firewalls and distribute their applications and data across multiple devices. As a result, their endpoints, networks and applications are becoming vulnerable points for security breaches and data theft.

These new systems are also generating massive volumes of data, which require around-the-clock monitoring. Yet, it also creates enormous quantities of data on security events and the challenges of interpreting what that data means, and deciding what to do with it.

IBM employs proprietary advanced analytics to tackle the massive amount of information collected across our monitored platforms and to develop useful insights into the kinds of attacks that are taking place, who may be launching them and how their techniques are evolving.

This report reflects the data we've gathered through our monitoring operations, the security intelligence generated by our analysis, and the interpretations of our experienced security analysts and security response teams.

The impact of security incidents

What is the impact of a security incident? As we look through the data reported here, we see that the astronomical number of security events (see Figure 1) can be ultimately whittled down to a much more manageable number of incidents requiring action. However, of those incidents, how many are actually "noteworthy," which means they have the potential to result in a significant or material impact to the business? According to the IBM Computer Security Incident Response Team, of all the security incidents it works through and analyzes, only three percent actually reach a level of severity high enough to consider them "noteworthy"—with the most common impact being data disclosure or theft.

What is fascinating—and disheartening—is that over 95 percent of all incidents investigated recognize "human error" as a contributing factor. The most commonly recorded form of human errors include system misconfiguration, poor patch management, use of default user names and passwords or "easy-to-guess" passwords, lost laptops or mobile devices, and disclosure of regulated information via use of an incorrect email address. The most prevalent contributing human error? "Double clicking" on an infected attachment or unsafe URL.

A more efficient approach to narrowing down the numbers

IBM's global monitoring operations and analysts have determined that the average financial services provider experienced more than 102 million security events in 2013 (see Figure 1), which reflects the continued worldwide growth of data, networks, applications, and the new technology and innovations they support.

Virtually no financial services provider is equipped to deal with the threat potential of 102 million events a year on its own. And because we know that only a fraction of a percent of those security events end up being identified as incidents, the real challenge is determining which of those events require additional investigation (see sidebar "Disruptions defined"). IBM security intelligence correlation and analytics tools filter through millions of events each year and determine which ones deserve further attention. In 2013, that meant identifying over 16,000 potentially critical attacks out of more than 102 million events. IBM security analysts went on to review those 16,000 security attacks and found 116 security incidents for the average financial services industry in 2013.

Disruptions defined

Security event: An event on a system or network detected by a security device or application.

Security attack: A security event that has been identified by correlation and analytics tools as malicious activity and is attempting to collect, disrupt, deny, degrade or destroy information system resources or the information itself.

Security incident: An attack or security event that has been reviewed by IBM security analysts and deemed worthy of deeper investigation.

Security breach: An incident that has successfully defeated security measures and accomplished its designated task.

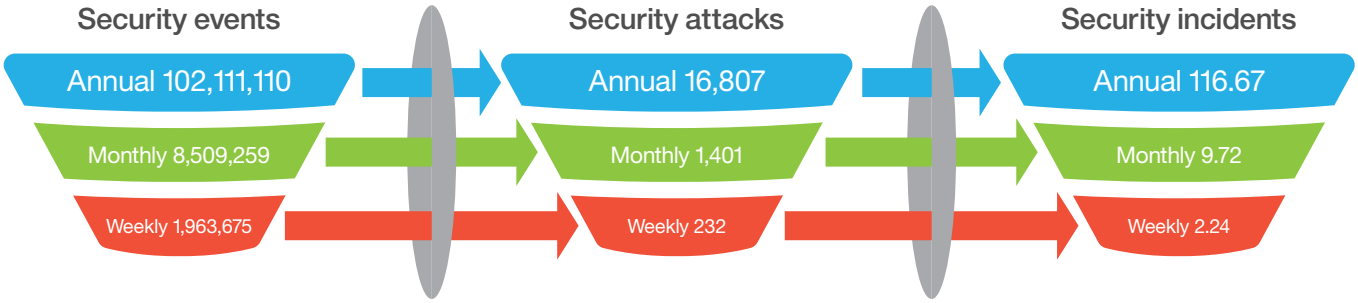


Figure 1. Security intelligence allows IBM to better identify which events are actual security incidents requiring action.

Malicious code and sustained probes or scans still dominate the landscape

There were two types of incidents dominating the cyber attack landscape in 2013. Together, malicious code and sustained probes or scans accounted for 59 percent of the security incidents affecting our clients (see Figure 2).

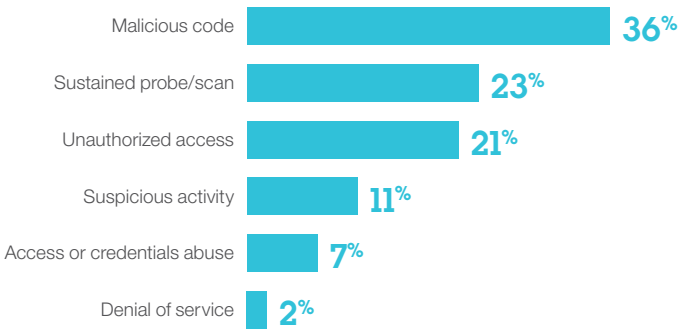


Figure 2. Sustained probes or scans and malicious code together are the primary types of incidents affecting financial services companies.

The two types often go hand in hand. Sustained probes and scans are typically used to search for potential targets, enabling attackers to see where and when to unleash their malicious code or malware. Meanwhile, it might be surprising that denial-of-service attacks, which seem to run rampant across the threat landscape, make up only two percent of the incidents reported. But it turns out that many denial-of-service attacks lack the bandwidth necessary to make a significant impact on their targets. In addition, some clients employ denial-of-service protection services, which also blunt these attacks' effectiveness.

In fact, malicious code continues to be the primary mode of attack in cyber crime. And it can include third-party software, Trojan software, spear phishing, keyloggers and droppers (see the glossary for definitions). Over the past year, we've also continued to see greater sophistication in the creation of attack tools and the development and underground sale of tool kits (ready-to-use hacking applications). It appears that many of the tool kits that have been seen repeatedly over the years have been updated and "recycled" for use today.

Unauthorized access incidents were more prevalent in 2013—which fits with the apparently growing use of malware to elevate privilege levels after hacking into a network. After all, just because attackers are able to gain access to a network doesn't mean they can navigate it. The situation is similar to a trespasser who's able to "tailgate" into a building by following close behind someone with authorized access. Once inside, the trespasser still needs to figure out how to move around undetected. That activity in the cyber world is what comprises not only unauthorized access but also suspicious activity traffic as well.

How credit cards allow attackers to cash in

When it comes to consumers, attackers are going after valuable personal and financial information—including credit cards, which have become a hot commodity on the black market. The average credit card sells on the black market with higher prices depending on how much information is available with the card data—such as CSV security code, known limits and expiration date. But the story doesn't end there. Once the stolen cards are acquired, they then move into an elaborate laundering scheme where they're used to buy gift cards and prepaid credit cards. The shuffling of funds continues as these "untraceable" cards are used to purchase other items that can then be sold online with no ties back to the original stolen card data.

On the flip side, we know that in large-scale cases such as those disclosed late in 2013, the attackers' success can also be their demise. News about these massive breaches travels fast, and that means the stolen cards will often be deactivated by their owners before anyone can sell them. The United States is typically one of the largest targets in this underground market. That's at least partly due to its status as one of the last remaining countries using magnetic strip credit cards—which are the easiest to forge using stolen data, making them a highly attractive target.

Who's behind these attacks and where are they coming from?

As we continue to focus on determining who is carrying out these attacks, it's clear that the role played by both inadvertent actors and outsiders has become increasingly important (see Figure 3). Although inadvertent actors make up just five percent of the attacker population, they remain among the most dangerous. As members of your own organization who are unwittingly "recruited" to aid the cause of others with malicious intent, they can become key players in carrying out highly damaging, potentially prolonged attacks that fail to arouse suspicion. That said, outsiders will likely continue to play the largest role in cyber crime for some time to come, making it essential that we understand who those outsiders really are—and where they are located.

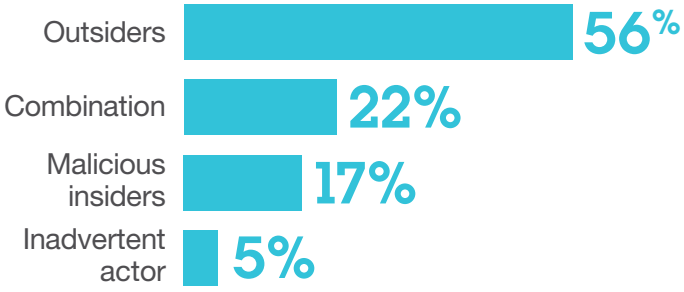


Figure 3. The vast majority of attacks on financial services organizations are instigated by outsiders.

The social life of the inadvertent actor

Today's organizations are made up of individuals who are more likely than ever to have vast networks of online relationships, each of which involves huge amounts of personal data. But how can that personal data pose a threat to your company?

Rather than seeing a particular enterprise as a single entity, attackers now also look at an enterprise as collections of individuals. That means they decide to target specific people instead of enterprise infrastructures or applications. In other words, the personal lives and business activities of employees can be used to target an enterprise.

Social networks intentionally make it easy for users to contact one another. It's a great way to wish a faraway friend a happy birthday. But it's also an easy way for an attacker to send a user to a malicious website or to send malware directly to that user—all of which renders enterprise email security countermeasures completely useless.

For example, a user can access social media using a device attached to a corporate network and thus open up a pathway for the malware. Or an attacker can take advantage of personal information available online to learn enough about the individual to implement a targeted phishing campaign via the corporate email account. In this scenario, the criminal sends what appears to be legitimate business correspondence and dupes the employee into opening an infected email attachment. Either way, the command and control malware gets into the enterprise systems.

A new security reality has taken hold

Organized criminals, hacktivists, governments and adversaries are motivated by financial gain, politics and notoriety to attack your most valuable assets. Their operations are well funded and businesslike. Attackers patiently evaluate targets based on potential effort and reward. Their methods are extremely targeted: they use social media and other entry points to track down people with access, take advantage of trust and exploit them as vulnerabilities. Meanwhile, negligent employees inadvertently put the business at risk via human error. Even worse, security investments of the past fail to protect against these new classes of attacks. The result is more severe security breaches more often. In fact, 61 percent of organizations say data theft and cybercrime are the greatest threats to their reputation.[3] And the costs are staggering.

Why act now?

Your business may be more vulnerable than you think. And that's just the first reason. Here are a few more:

- Criminals will not relent: Once you're a target, criminals will spend as much time trying to break into your enterprise as you spend on your core business. If you don't have visibility into attacks as they happen, the criminals will likely succeed.
- Today, diverse actors move with lightning speed to steal money, intellectual property, customer information and state secrets across all sectors.
- Your perimeter may already have been breached. Recent attacks demonstrate that victims were compromised for months before they discovered it. Assuming that you have already been breached is today's prudent security posture.

Why IBM Security for financial services?

Traditional security defenses are no match for today's unrelenting, well-funded attackers, while disruptive technologies introduce new vulnerabilities to exploit. Financial service providers must accelerate their ability to limit new risk and apply intelligence to stop attackers—regardless of how advanced or persistent they are. New analytics, innovation, and a systematic approach to security are necessary.

Applying analytics can allow organizations to discover, investigate and thwart suspicious activity before it becomes a full-fledged attack.

It starts with a phone call and ends with a major data breach

Social engineering techniques allow attackers to target a specific company and gain access to its valuable data. They steal internal phone directories and then call employees of interest. Their goal? To convince victims to willingly install remote administration software that the hackers can use to gain access into the victims' network. Posing as internal security or IT staff members, they direct their victims to download and install well-known remote administration software to help resolve a "critical systems problem." Or they instruct their unwitting victims to join a web conference and hand over control to the attackers.

Once the attackers gain control of the system, they download and install malware to maintain a persistent connection, then elevate privileges and penetrate the network. Because most companies don't have a system in place to verify calls, this has become a highly effective method for attackers to infiltrate internal systems—especially when those attackers are able to gain an understanding of the targets' processes and use it to convince victims that it's important to take immediate action.

The victims targeted for these attacks typically have easy access to the data that the attackers are after. So once a point of presence is solidified within the network, the attackers are able to steal just about any type of data—including financial and intellectual property.

Even those companies with strong security practices are still vulnerable to acts of social engineering. It's important to educate employees on an ongoing basis about identifying suspicious communications and potential risks to the organization.

At IBM, our IT security services can cover almost every corner of your network, from infrastructure to applications to devices. We monitor, in real time, some of the most complex corporate networks in the world. We develop some of the most sophisticated testing tools in the industry, many of which are used by our competitors. And our team of highly skilled security professionals is constantly identifying and analyzing new threats, often before they are even known by the world at large. In fact, we maintain one of the largest single databases of known cyber security threats in the world.

We constantly strive to help clients find the balance between necessary innovation and the need to control risk. Based on extensive experienced gained through client engagements, we have mapped out the ten essentials required to achieve security intelligence in the 21st century. These include:

1. **Build a risk-aware culture and management system.** Because attacks can come from anywhere, it is crucial to determine your security risks and goals and then communicate to all of your employees. This must come from the top down, and tools should be implemented to track progress.

2. **Build an intelligent threat protection and response center.** A company-wide effort to implement intelligent analytics and automated response capabilities is essential. Creating an automated and unified system that implements intelligent analytics can better monitor your operations and respond more quickly.

3. **Create a security-rich, collaborative workplace environment.** Each workstation, laptop or smartphone provides a potential opening for malicious attacks. Better securing the workforce means vanquishing chaos and replacing it with confidence.

4. **Build security inside services, by design.** One of the biggest vulnerabilities in information systems—and wastes of money—comes from implementing services first, and then adding security on as an afterthought. Build in security from the beginning, and carry out regular automated tests to track compliance.

5. **Manage IT hygienically.** A robust, security-rich system helps you keep track of programs that are running and makes it possible to install updates and patches as they are released. This "hygiene" process should be routine and embedded in the foundation of your system's administration.

6. **Create a security-rich and resilient network.** Companies that channel registered data through monitored access points may have a far easier time spotting and isolating malware.

7. **Address unique security requirements of cloud.** Cloud computing promises enormous efficiencies, but it can come with some risk. To thrive in this environment, you must have the tools and procedures to isolate your assets and to monitor possible threats.

8. **Manage third-party compliance.** An enterprise's culture of security must extend beyond company walls, and establish best practices among its contractors and suppliers. Security, like excellence, should be infused into the entire ecosystem.

9. **Provide data security and privacy.** Each enterprise should carry out an inventory, with the critical data getting special treatment. Each priority item should be guarded, tracked and encrypted as if the company's survival hinged on it—and in some cases it may.

10. **Manage the digital identity lifecycle.** Controlling who has access to critical data is an essential aspect of cyber security. Doing this effectively requires development of an optimized identity and access management strategy that includes standard, policy-based control mechanisms and more intelligent monitoring across the identity lifecycle.

IBM Security Services consultants help you plan, implement and manage virtually all aspects of your security strategy. Our senior security professionals have honed their skills through years of engagements with the financial services industry. We can optimize your level of control by providing consulting services to establish your security strategy. We can also provide implementation and integration services using market-leading technologies to help protect your applications, prevent data loss and employ sophisticated encryption

In addition to offering consulting services since 1995, IBM has helped to set the standard for accountability, reliability and protection in managed security services. IBM Managed Security Services can provide the security intelligence, expertise, tools and infrastructure you need to help secure your information assets from Internet attacks. When you engage with IBM for managed security services, you gain access to a full suite of capabilities that can help you extend protection from the back office to the front office. And we help integrate and coordinate the full suite across your enterprise. Should you experience a security breach, you can call on IBM's emergency response team to help speed your response to and recovery from a computer security incident.

The need

A major bank needed to better manage regulatory compliance and increase control and visibility of its security posture. Its top priorities included enhancing the logging and monitoring capabilities of its intrusion-prevention system and providing truly effective system investments. But with limited resources, the bank required additional expertise to implement the necessary security capabilities.

The IBM solution

Working closely with the IBM security team, the bank implemented several IBM Security Systems that implement logging and monitoring tasks and help manage compliance with regulations by providing daily reviews of its security-compliance posture. And on an ongoing basis, IBM provides Managed Security Services for the security system, including web services that provide a single holistic view on compliance, intrusion protection and web defense, including Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks.

Among the benefits, the solution offers:

- **The ability to better manage compliance with security policies and regulatory requirements**
- **Increased control and visibility over the security posture by outsourcing logging and monitoring tasks**
- **Ability to supplement security areas that may be lacking in resources**

The need

A major bank needed an overhaul of its IT security in a short amount of time. With millions of security events occurring each day, the bank wanted a more efficient way to monitor and report on these events.

The solution

IBM Security Services helped the bank plan and build a transformative security operations center that includes a robust security information event management platform. Among the benefits, the solution offers:

- **The ability to monitor thousands of server and network devices**
- **User-friendly dashboards for line of business users**
- **Tracking and reporting capabilities**

Glossary

Term	Definition
Access or credentials abuse	Activity detected that violates the known use policy of that network or falls outside of what is considered typical usage.
Attacks	Security events that have been identified by correlation and analytics tools as malicious activity attempting to collect, disrupt, deny, degrade or destroy information system resources or the information itself. Security events such as Structured Query Language (SQL) injection, URL tampering, denial of service and phishing fall into this category.
Breach or compromise	An incident that has successfully defeated security measures and accomplished its designated task.
Denial of service	Attempts to flood a server or network with such a large amount of traffic or malicious traffic that it renders the device unable to perform its designed functions.
Droppers	Malicious software designed to install other malicious software on a target.
Event	An observable occurrence in a system or network.
Inadvertent actor	Any attack or suspicious activity coming from an IP address inside a customer network that is allegedly being executed without the knowledge of the user.
Incidents	Attacks or security events that have been reviewed by human security analysts and have been deemed a security incident worthy of deeper investigation.
Keyloggers	Software designed to record the keystrokes typed on a keyboard. This malicious software is primarily used to steal passwords.

Term	Definition
Malicious code	A term used to describe software created for malicious use. It is usually designed to disrupt systems, gain unauthorized access or gather information about the system or user being attacked. Third-party software, Trojan software, keyloggers and droppers can fall into this category.
Outsiders	Any attacks that come from an IP address external to a customer's network.
Phishing	A term used to describe when a user is tricked into browsing a malicious URL designed to pose as a website they trust, thus tricking them into providing information that can then be used to compromise their system or accounts and steal their identity.
Security device	Any device or software designed specifically to detect or protect a host or network from malicious activity. Such network-based devices are often referred to as intrusion detection and prevention systems (IDS, IPS or IDPS), while the host-based versions are often referred to as host-based intrusion detection or prevention systems (HIDS or HIPS).
Security event	An event on a system or network detected by a security device or application.
Spear phishing	Phishing attempts with specific targets. These targets are usually chosen strategically in order to gain access to very specific devices or victims.
SQL injection	An attack used that attempts to pass SQL commands through a website in order to elicit a desired response that the website is not designed to provide.
Suspicious activity	These are lower-priority attacks or instances of suspicious traffic that could not be classified into one single category. They are usually detected over time by analyzing data collected over an extended period.
Sustained probe or scan	Reconnaissance activity usually designed to gather information about the targeted systems, such as operating systems, open ports and running services.
Trojan software	Malicious software hidden inside another software package that appears safe.
Unauthorized access	This usually denotes suspicious activity on a system or failed attempts to access a system by a user who does not have access.
Wiper	Malicious software designed to erase data and destroy the capability to restore it.

For more information

To learn more about how IBM can help you protect your organization from cyber threats and strengthen your IT security, contact your IBM representative or IBM Business Partner, or visit this website: **ibm.com**/services/security

To more know about the current threat level, your cyber risk profile, global trends, the potential impact of attacks and essential practices for creating a world-class security culture in your organization, please contact your IBM account executive to arrange a session of the complementary **Cyber Security Executive Briefing**.

Additionally, IBM Global Financing can help you acquire the IT solutions that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize an IT financing solution to suit your business goals, enable effective cash management, and improve your total cost of ownership. IBM Global Financing is your smartest choice to fund critical IT investments and propel your business forward. For more information, visit: **ibm.com**/financing

[1] IBM Managed Security Services is responsible for monitoring exploits related to endpoints, servers (including web servers) and general network infrastructure. This team tracks exploits delivered over the web as well as via other vectors such as email and instant messaging. Meanwhile, the X-Force research and development team studies and monitors the latest threat trends including vulnerabilities, exploits and active attacks, viruses and other malware, spam, phishing, and malicious web content. In addition to advising customers and the general public about emerging and critical threats, X-Force also delivers security content to help protect IBM customers from these threats. As a result, these two groups issue reports that look at similar issues, but from a slightly different perspective and over different timeframes. Therefore, their findings are meant to complement one another, even though those findings are not always identical.

[2] Ponemon Institute, "2014 Cost of data breach study: Global analysis," May 2014.

[3] IBM 2012 Global Reputational Risk & IT Study.

IBM Corporation
IBM Global Technology Services
Route 100
Somers, NY 10589

Produced in the United States of America
November 2014

SEW03046-USEN-02