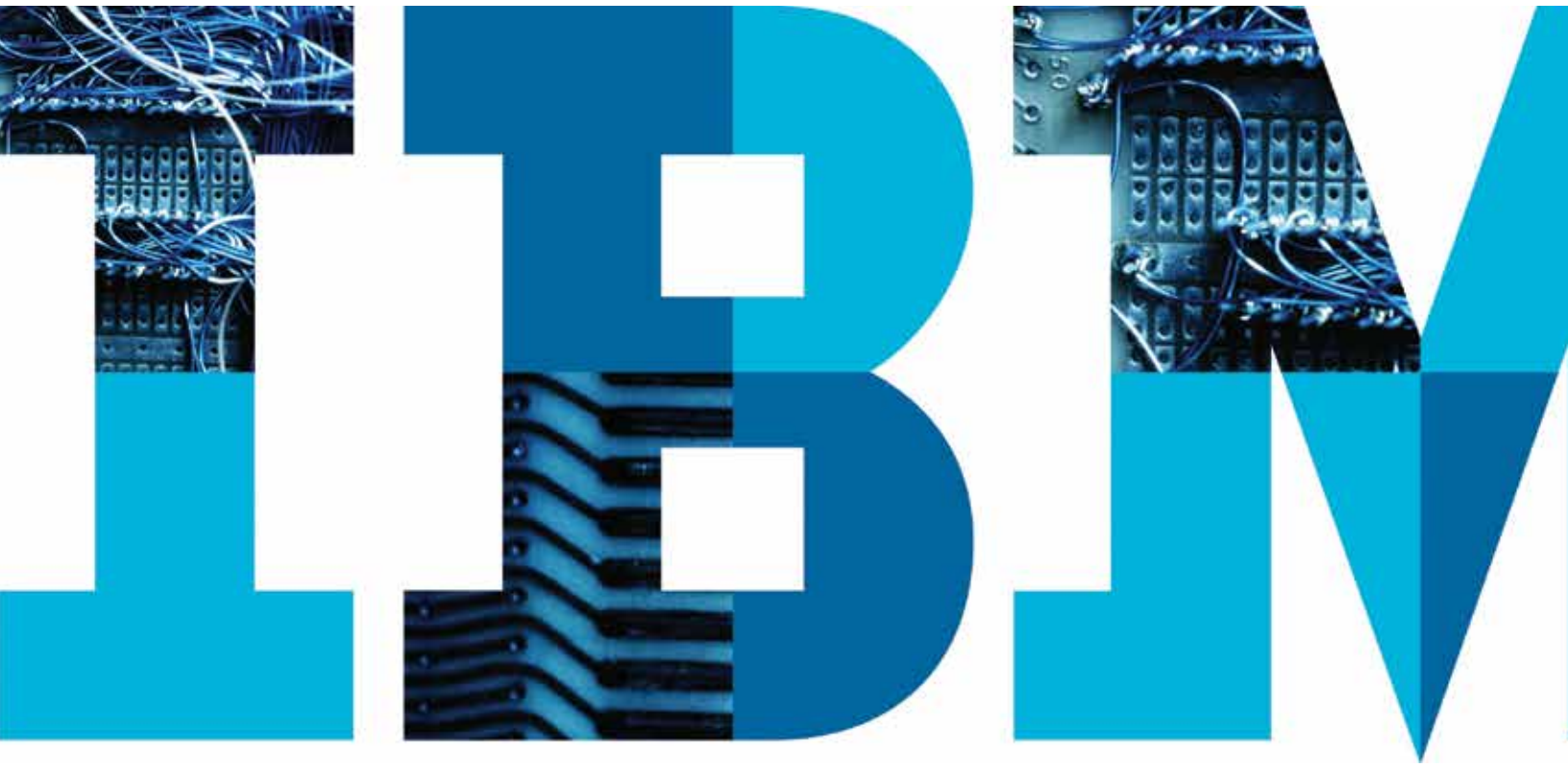
IBM Security Services 2014 Cyber Security Intelligence Index

Analysis of cyber attack and incident data from IBM's worldwide security operations



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. This report is based on the cyber attack event data 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. Our goal is to help you better understand the current threat landscape by offering a detailed look at the volume of attacks, the industries most affected, the most prevalent types of attacks and attackers, and the key factors enabling them. We provide insights into where and how successful attacks can impact today's technology-dependent organizations and discuss how the threat landscape is evolving from year to year as companies work to better detect and insulate themselves from future attacks.

The problem that isn't going away

After several years of continuing growth, data breaches literally hit home in 2013. In that one year, more than half a billion records of personally identifiable information—including names, emails, credit card numbers and passwords—were stolen. Heavy media coverage of several significant retail industry attacks pushed conversations about privacy and security straight from boardrooms into living rooms around the world.

The damage from such data breaches can be severe. If consumers lose faith in a company's ability to keep their personal data safe, the company can ultimately lose customers. Most certainly they stand to lose money, and in some cases, intellectual property. In its most recent analysis, the Ponemon Institute found that in 2013 each lost data record cost companies an average of $145 per record, with companies in Germany losing the most per record for each data breach ($201), followed by the United States ($195), and companies in India the least at $51.[2] Based on the global average cost per record, that means:

- A major retailer with millions of leaked credit cards could face more than $100 million in direct costs, including fines.
- A university that leaked 40,000 records could suffer over $5.4 million in losses.

Ponemon also found that heavily regulated industries such as healthcare, finance, pharmaceuticals and communications had a per record data breach cost ranging from $177 to $359—placing them well above the mean of $145. Meanwhile, retailers and public sector organizations had a per record cost of $105 and $100, considerably below the mean value.[3]

The U.S. experienced the highest total average cost at more than $5.9 million, followed by Germany at $4.7 million. At the other end of the scale, Brazilian and Indian companies experienced the lowest total average cost at $1.6 million and $1.4 million respectively.[4]

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?
- What kinds of attacks are being launched?
- How many of those attacks result in incidents requiring investigation?

As companies around the world continue to expand their businesses and IT infrastructure—adding more devices and increasing connectivity across their organizations—their volumes of data requiring 24x7 monitoring also continue to grow. That can increase an organization's vulnerability by making it even more difficult to develop and deploy effective measures to fend off cyber attacks, but at the same time, such growth creates enormous quantities of data on security events. It also presents us with the challenge of understanding what all that data means and deciding what to do about it.

IBM employs proprietary advanced analytics to tackle the massive amount of information collected across our monitored platforms and 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 both the data we've gathered through our monitoring operations and 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) is ultimately whittled down to a much more manageable number of incidents. However, of those incidents, how many are actually "noteworthy," with 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 they work through and analyze, 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 company experienced more than 91 million security events in 2013 (see Figure 1)—a 12 percent increase over 2012. That reflects the continued worldwide growth of data, networks, applications and the new technology and innovations they support. It also reflects a growing number of targets for potential attacks.

Virtually no company is equipped to deal with the threat potential of 91 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 deserve further attention (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 nearly 17,000 potentially critical attacks out of over 91 million events.

While the number of security events grows, so does our ability to analyze and manage them more efficiently. As a result, the annual number of security attacks seen by the average IBM client in 2013 dropped to an average of 16,900, down from 73,000 in 2012. IBM security analysts went on to review those 16,900 security attacks and found 109 security incidents for the average company in 2013, which is 19 more than the year before.[5]

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 that 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.

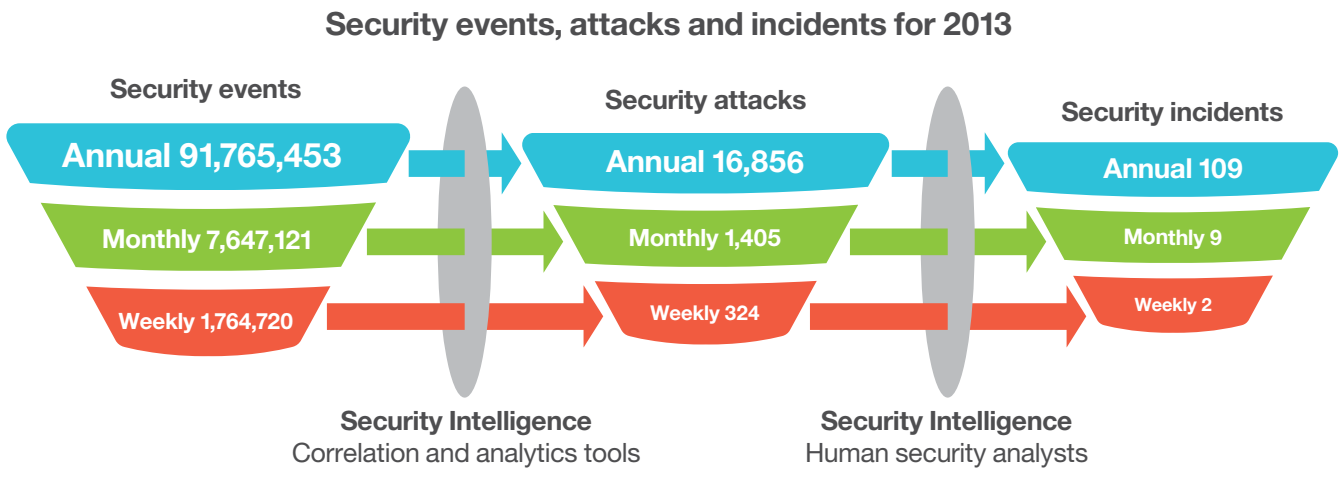


Figure 1. Security intelligence makes it possible to reduce the millions of security events detected annually in any one of our clients' systems to an average of 16,900 attacks—and under 110 incidents—in a single organization over the course of a year.

Over 75 percent of incidents target the same five industries

The not-so-big news is we're seeing the same five industries top the list of those struck by the most incidents over the past year. Some of them, however, have changed places within the group since 2012. Once again, the top two (see Figure 2) account for nearly half of the year's security incidents among our data sets. The only difference is that they swapped places in 2013. It's likely that these two industries will continue to battle for the number one target spot in the years to come, since a breach in either one can result in both major business disruption and big paydays for successful cyber criminals.

Moving down the list, the two industries occupying fourth and fifth place have also swapped places—although together they account for 12 percent of the incidents in 2013, compared to 14 percent in 2012. Because both the retail and health services industries deal directly with consumers, attackers there are going after valuable personal and financial information—including credit cards, which have become a hot commodity on the black market.

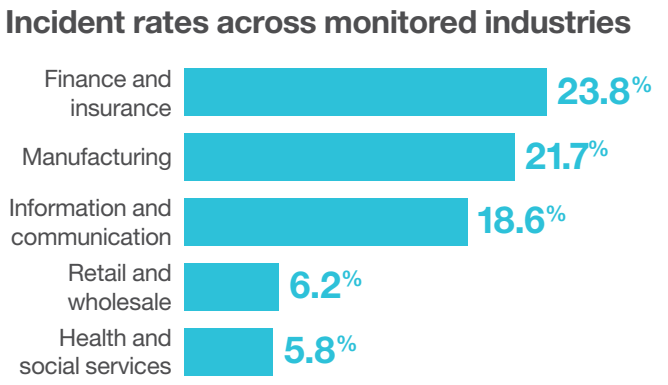


Figure 2. The finance and manufacturing industries continue to offer attackers the most significant potential payoff.

How credit cards allow attackers to cash in

The average credit card sells on the black market for anywhere from $25 to $100, depending on how much information is available with the card data—such as CSV security code, known limits, and expiration date. Since news accounts reported that more than 110 million credit records were stolen in recent retail breaches, it's easy to see how the sellers could have netted as much as $11 billion.

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 such large-scale cases 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. And although the retail industry is the primary target here, credit card theft is really a threat to many industries. That means we're likely to see a strong push for tighter credit card security in the very near future.

Malicious code and sustained probes or scans still dominate the landscape

As was the case for 2012, there were two types of incidents dominating the cyber attack landscape in 2013. Together, malicious code and sustained probes or scans accounted for 58 percent of the security incidents affecting our clients (see Figure 3). The two 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 seem 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.

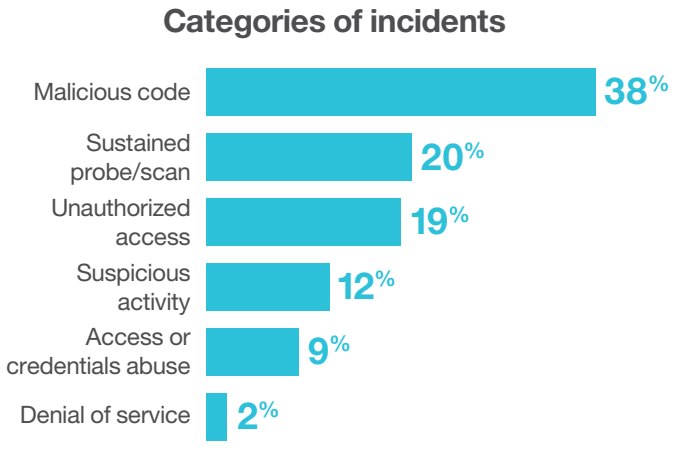


Figure 3. Malicious code and sustained probes or scans top the list of incident categories affecting every industry covered in this report.

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 on page 11 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—up six percent over the previous year—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 suspicious activity traffic as well.

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 4). While inadvertent actors make up just five percent of the attacker population, as they did in 2012, 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. A new addition to the threat index shows us where these attacks originate (see Figure 5). But let's be clear about what this information means. For example, when considering the list of the top 10 countries responsible for the attacks we detected in 2013, we need to take into account the size of each country and the availability of bandwidth within it. That goes a long way toward explaining why more than half of the attacks we saw in 2013 originated in the United States. And for many of the same reasons, the United States was also the most attacked country in 2013 (see Figure 6).

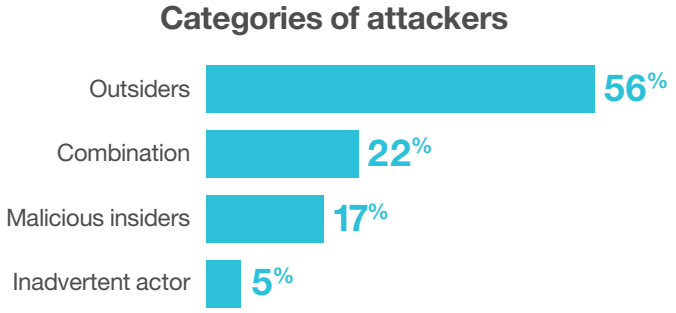


Figure 4. More than half of all attacks are most likely to be instigated by outsiders.

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 leveraged 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 execute a targeted phishing campaign via the corporate email account. In this scenario the bad guy 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.

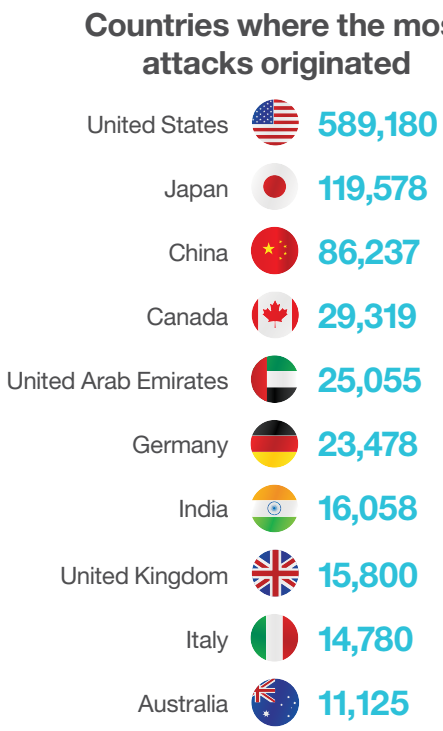


Figure 5. More than half of all attacks originated in the United States.

Figure 6. More than 45 percent of all attacks took place in the United States.

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.[6] 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 succeed.
- Every business is affected: Banks were once the primary targets of cyber criminals, but 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.

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 financials 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.

Why IBM Security?

Traditional security defenses are no match for today's unrelenting, well-funded attackers, while disruptive technologies introduce new vulnerabilities to exploit. Organizations 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. And there are very few companies able to meet those requirements on their own. That's why Forrester Research has noted: "[Managed security services providers] leverage impressive economies of scale to offer clients an enhanced security environment, cost-effective security, and a scalable and flexible security platform capable of handling future expansion."[7]

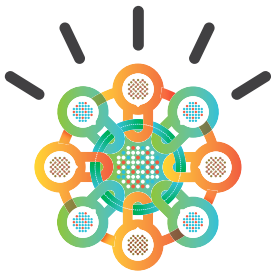
When you engage with IBM for managed security services, you gain access to a full suite of capabilities that can help you extend protection from the back office to the front office. And we help ensure that it's all integrated and coordinated across your enterprise. Should you experience a security breach, you can call on IBM's emergency response team to help speed your response to and recovery from a computer security incident.

At IBM, our IT security services can cover every corner of your network, from infrastructure to applications to devices. We monitor, in near 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 the largest single database of known cyber security threats in the world.

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

Follow us



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 SQL Injection, URL tampering, denial of service, and spear 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 malicious traffic that it renders the device unable to perform its designated functions.
Droppers	Malicious software designed to install other malicious software on a target.
Event	An event is an observable occurrence in a system or network.
Inadvertent actor	Any attack or suspicious activity sourcing from an IP address inside a customer network that is allegedly being executed without the knowledge of the user.
Incidents	Attacks and/or security events that have been reviewed by 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.
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 sourced from an IP address external to a customer's network.
Phishing	A term used to describe when users are lured 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, accounts, and/or steal their identity.
Security event	An event on a system or network detected by a security device or application.
Security device	Any device or software designed specifically to detect and/or protect a host or network from malicious activity. Such network-based devices are often referred to as intrusion detection and/or prevention systems (IDS, IPS or IDPS), while the host-based versions are often referred to as host-based intrusion detection and/or prevention systems (HIDS or HIPS).
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 that attempts to pass SQL commands through a website in order to elicit a desired response—one that the website is not designed to provide.
Suspicious activity	These are lower priority attacks or suspicious traffic that could not be classified into one single type of category. They are usually detected over time by analyzing extended periods of data.
Sustained probe/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 or users who does not have access.
Wiper	Malicious software designed to erase data and destroy the capability to restore it.

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

Produced in the United States of America
May 2014

[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.

[2,3,4] 2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute, May 2013.

[5] IBM Security Services 2013 Cyber Security Intelligence Index, June 2013.

[6] 2012 Global Reputational Risk & IT Study, IBM.

[7] The Forrester Wave: Managed Security Services: North America, Forrester Research, Inc., March 26, 2012.

SEW03039-USEN-01