IBM Global Technology Services
Security Services

July 2013

IBM Security Services Cyber Security Intelligence Index

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

About this report

IBM Managed Security Services continuously monitors tens of billions of events per day for more than 3,700 clients in over 130 countries. This report is based on the cyber security event data we collected between 1 April 2012 and 31 March 2013 in the course of monitoring client security devices as well as data derived from responding to and performing forensics on cyber security incidents. It is complementary to the IBM X-Force 2012 Trend and Risk Report. 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, with approximately 500 security devices deployed within its network.

In a world where a week rarely goes by without reports of at least one serious cyber attack against a major organization, it's important to ask 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?

At the same time, an ever-increasing number of devices and growing volumes of data can make it difficult to develop and deploy effective cyber security measures. So it's easy to understand why a medium- to large-sized company is likely to have some 500 security devices deployed within its network. And thanks to all those security devices, it's possible to access vast quantities of data on security events across an enterprise. But what's not so easy is determining what all that data means and what to do about it.

Of course not all threats are created equal, and no threat should be overlooked for its significance to any organization. When thinking about security, it's also imperative to take a global view of the threat landscape.

That's where security intelligence comes in. It allows us to see what's happening, with a critical eye toward understanding the threat landscape as it really exists. By taking advantage of advanced analytics to help tackle the massive amount of information collected across our monitored platforms, we can develop real insight 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 analysts and incident response teams who interpret that data. Our aim is to help you gain important insights into the current threat landscape—with a close look at the volume of attacks, the industries most impacted, the most prevalent types of attacks and attackers, and the key factors enabling them.

Finding the threats inside the numbers

Security intelligence operations and services make it possible for us to narrow down the millions of security events detected annually in any one of our clients' systems to an average of 73,400 attacks in a single organization over the course of a year (see Figure 1). That's 73,400 attacks that have been identified by correlation and analytic tools as malicious activity attempting to collect, disrupt, deny, degrade, or destroy information systems resources or the information itself.

And while netting tens of millions of events down to roughly 73,400 attacks is an impressive reduction by any account, we're still talking about a sizable number of attacks. How would you even begin to know which ones might pose a real threat? By stepping up our security intelligence efforts to include the work of experts (i.e., human security analysts), we're able to identify those specific attacks that qualify as security incidents and therefore merit further investigation. As a result, we found an annual average of 90.2 security incidents per our mid- to large-sized clients—all of which call for action.

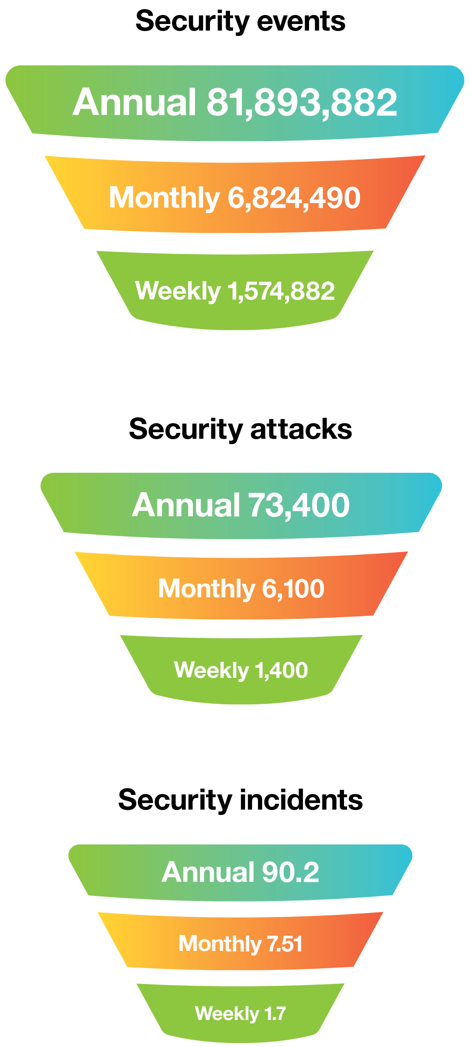


Figure 1. Security intelligence makes it possible to reduce the millions of security events detected annually in any one of our clients' systems to an average of 73,400 attacks—and under 100 incidents—in a single organization over the course of a year .

Two industries are targeted in nearly 50 percent of all incidents

Here's a look at the five industries where we've seen most of these incidents taking place over the past year. Not surprisingly, the top two—which account for nearly half of the year's security incidents among our data sets (see Figure 2)—are the ones that offer attackers significant potential payoff. Think about what could be gained by uncovering proprietary manufacturing processes or product formulas. And it's easy to imagine how accessing financial data or blocking online banking services could result in massive cash losses and major business disruption.

The rise of manufacturing to the top of this list also appears to reflect a growing trend, where we're seeing more cyber attacks focused on sabotage than espionage. These attacks are often aimed at causing physical damage, disruption and safety issues—rather than accessing information. And they're raising new concerns about shifts across the threat landscape.

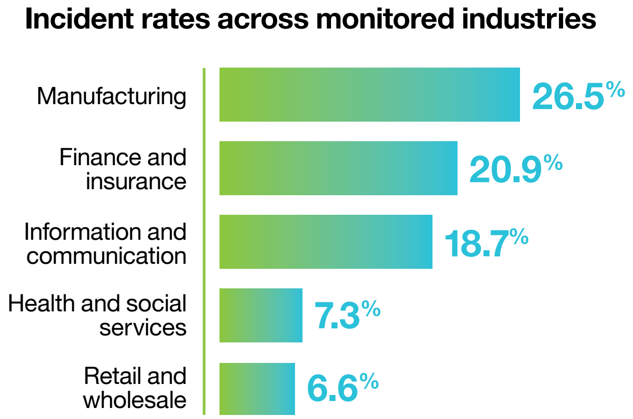


Figure 2. The manufacturing and finance and insurance industries tend to offer attackers the most significant potential payoff.

Spear phishing compromises two company networks

Industry: Financial

Incident: Spear phishing attack used against a smaller, less secure financial institution in order to gain access to a larger one through trusted access. Spear phishing targets specific individuals who can provide inadvertant access to very specific devices or data.

Why it happened: Hackers took advantage of social networking and known PDF exploits in order to plant malware on the targeted user's machine. This was accomplished by conducting a social engineering campaign against the specific target. Over time, the attacker was able to learn the victim's position within the company, office location and work schedule. Eventually the attacker knew enough about the victim to create a spear phishing message that would not be viewed as suspicious. Once the victim opened the attached malicious PDF, the attacker gained access to the user's workstation and the user's network as well as the network of the company's larger partner. Once a foothold was gained, covert communication channels were established for use in sneaking data out of the company's networks.

Damage done: Both financial institutions had personal information about their clients stolen.

Lessons learned: The lessons learned in disrupting and remediating this situation led to the development of new policies and guidelines—including new correlation rules and approaches to anomaly detection—that could be used to block this type of incident in the future.

Malicious code and sustained probes or scans dominate the landscape

Two types of incidents dominate the cyber security landscape. As Figure 3 shows, malicious code and sustained probes or scans account for over 60 percent of the security incidents impacting our clients. That's largely because 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).

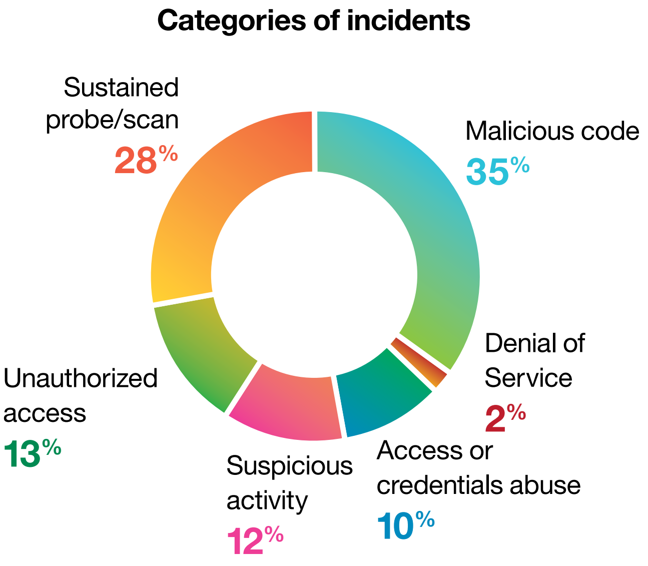


Figure 3. Malicious code and sustained probes or scans top the list of incident categories impacting every industry covered in this report.

Note that malicious code can include third party software, Trojan software, spear phishing, keyloggers and droppers (see the glossary on page 11 for definitions). Unauthorized access incidents listed here include suspicious activity on a system or failed attempts to access a system by a user or users who do not have access, while access or credentials abuse refers to activity that violates the known use policy of that network or falls outside of what is considered authorized, typical usage.

What's more, although news of denial of service attacks regularly seems to dominate security-focused media, our data shows only a small percentage of incidents falling in that category. That's because it accounts only for those denial of service attacks deemed severe enough to actually impact the targeted environment.

The job of securing an enterprise's network continues to grow infinitely more complex as information pours in from thousands of devices and through scores of public web-based services.

Who's behind these attacks and how much of a threat do they pose?

Although this index data and report are not focused on who specifically is responsible for all these attacks, it can provide some insight into the types of attackers behind them (see Figure 4). Although most attacks originate outside a company's network, it's important not to dismiss the role played by inadvertent actors, despite the fact that they comprise such a small percentage of the attacker population. As members of your own company who are unwittingly "recruited" to aid the cause of others with malicious intent, they can become key players in carrying out a highly damaging—and potentially prolonged—attack without arousing any suspicion.

Opportunistic attacks are those that take advantage of existing vulnerabilities without any specific motivation. They're simply aimed at damage or disruption. In our experience—through service engagements and attack investigations—we've seen that nearly half of attackers are typically motivated by sheer opportunity (see Figure 5). Due to their typical lack of sophistication, they're generally easy to detect, which means that those organizations able to reduce opportunistic threats can potentially make better use of their time and resources to detect and respond to targeted and sophisticated attacks. Nonetheless, because opportunistic attacks occur so frequently, it's important to not let down your guard against them.

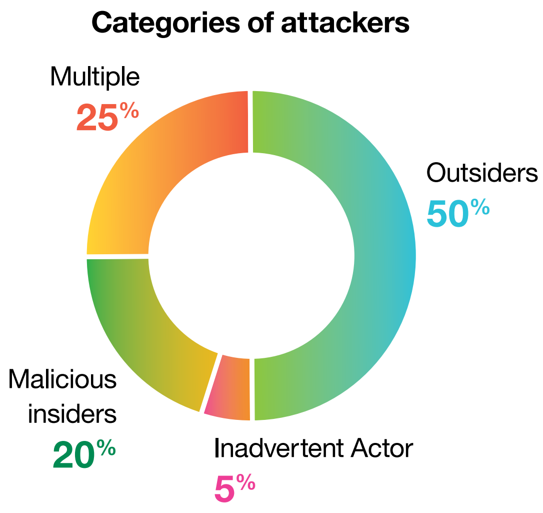


Figure 4. Half of all attacks are most likely to be instigated by outsiders.

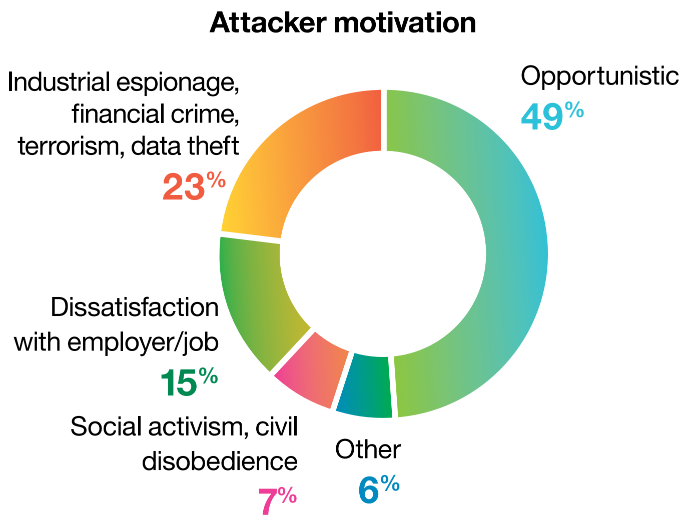


Figure 5. Opportunity served as the prime motivator for nearly half of the attackers we identified and investigated.

What makes these incidents possible?

Among the many factors that allowed these incidents to take place (see Figure 6), more than 70 percent can be attributed to end-user error and misconfigured systems or applications.

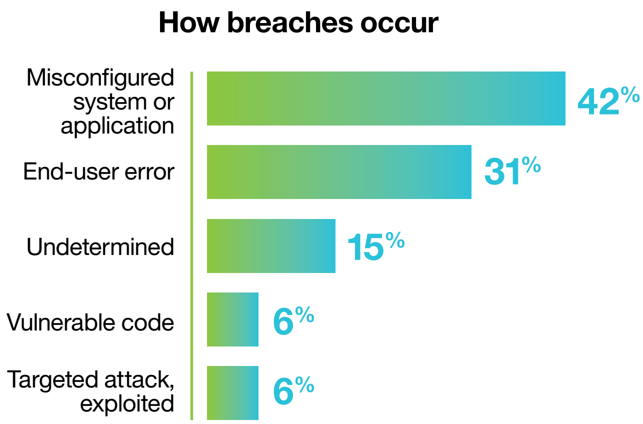


Figure 6. Although preventable errors are often to blame for security incidents, it was impossible to identify the culprit in nearly 20 percent of the cases we examined.

Online sales lost for lack of a routine software patch

Industry: Retail and wholesale

Incident: An individual or group with no specific target in mind discovers a vulnerability in a large retail outlet's website days after a patch for the specific vulnerability is released. The individual or group exploits this weakness, making the targeted website unavailable to the victim company's clients. This is a classic denial of service incident—which 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.

How it happened: When security patches for software are released to the public, this also notifies opportunistic hackers that the vulnerability exists. In response, they start scanning the internet for vulnerable systems. Due to change control protocols, the victim company in this incident did not apply the released security patch to their website. This left the web server vulnerable to a denial of service attack. Once discovered through scanning, the attacker took advantage of this simply because it was possible.

Damage done: The retail outlet lost any sales that would have taken place during the downtime. Additionally, customers may now choose not to do business through that website due to concerns about lack of security.

Lessons learned: While change control is extremely important, exceptions to the control procedures should be worked into the process in order to override change freezes when the risks of not patching exceed the risk of an out-of-process change. Once vulnerabilities in software are made public, it's usually only a matter of days and in some cases hours before reconnaissance software is updated to detect the vulnerability. An intrusion prevention system (IPS) device in protection mode also could have negated this risk or at least detected the reconnaissance activity before the attack took place.

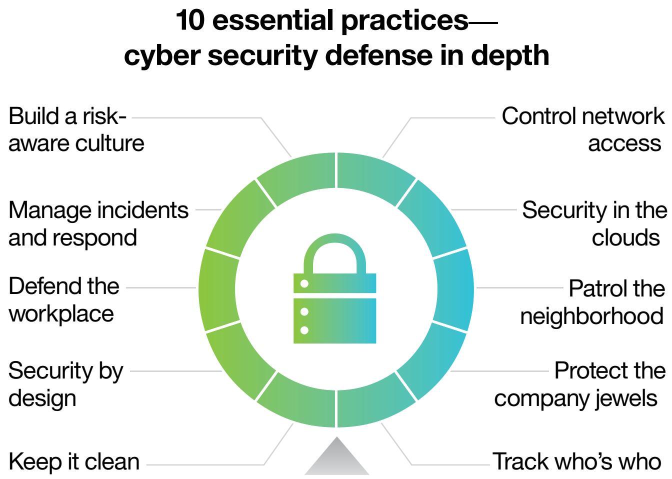
Are you ready?

Security intelligence relies on data—and the analytics, tools and people who use them. And these days, most enterprises are generating more data about what's going on inside their businesses than they can put to good use. So the first thing you can do is give some serious thought to how you're using (or not using) the security data you have at hand. If you're like many of our clients, you're likely to find that the complexity of your environment is making it difficult to understand and analyze all that data in a way that will help you make smarter decisions about cyber security.

At IBM, we are constantly striving to find the balance between improving the way we do business and the need to control and mitigate risk. Our approach includes technology, process and policy measures. It involves 10 essential practices (see Figure 7).

1. **Build a risk-aware culture**—where there's simply zero tolerance, at a company level, when colleagues are careless about security. Management needs to push this change relentlessly from the very top down, while also implementing tools to track progress.

2. **Manage incidents and respond**—A company-wide effort to implement intelligent analytics and automated response capabilities is essential. Creating an automated and unified system will enable an enterprise to monitor its operations — and respond quickly.



Within each essential practice, move from manual and reactive to automated and proactive to achieve optimized security.

Figure 7. Ten essential practices: A successful security program strikes a balance that allows for flexibility and innovation while maintaining consistent safeguards that are understood and practiced throughout the organization.

3. **Defend the workplace**—Each work station, laptop or smart phone provides a potential opening for malicious attacks. The settings on each device must all be subject to centralized management and enforcement. And the streams of data within an enterprise have to be classified and routed solely to authorized users.

4. **Security by design**—One of the biggest vulnerabilities in information systems comes from implementing services first, and then adding security on afterwards. The only solution is to build in security from beginning, and to carry out regular tests to track compliance.

5. **Keep it clean**—Managing updates on a hodgepodge of software can be next to impossible. In a secure system, administrators can keep track of every program that's running, be confident that it's current, and have a system in place to install updates and patches as they're released.

6. **Control network access**—Companies that channel registered data through monitored access points will have a far easier time spotting and isolating malware.

7. **Security in the clouds**—If an enterprise is migrating certain IT services to a cloud environment, it will be in close quarters with lots of others — possibly including scam artists. So it's important to have the tools and procedures to isolate yourself from the others, and to monitor possible threats.

8. **Patrol the neighborhood**—An enterprise's culture of security must extend beyond company walls, and establish best practices among its contractors and suppliers. This is a similar process to the drive for quality control a generation ago.

In the end, success hinges upon promoting and supporting a risk-aware culture, where the importance of security informs every decision and procedure at every level of the company. That means secure procedures need to become second nature, much like locking the door behind you when you leave home.

9. **Protect the company jewels**—Each enterprise should carry out an inventory of its critical assets—whether it's scientific or technical data, confidential documents or clients' private information—and ensure it gets special treatment. Each priority item should be guarded, tracked, and encrypted as if the company's survival hinged on it.

10. **Track who's who**—Companies that mismanage the "identity lifecycle" are operating in the dark and could be vulnerable to intrusions. You can address this risk by implementing meticulous systems to identify people, manage their permissions, and revoke those permissions as soon as they depart.

Start a conversation

Ask yourself—and your colleagues—how well your organization is currently following the ten essential practices outlined above. But don't stop there. The complexity involved in making sound security decisions in today's environment means you'd probably benefit from talking to a security expert from outside your company. At IBM, we've been asked for both formal and informal assessments by numerous executives in virtually every industry. And we'd be happy to have a conversation with you, too.

IBM Security Services offers the industry-leading tools, technology and expertise to help you plan your approach to security intelligence and develop a security intelligence monitoring platform, and to provide security incident response services support.

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 learn more about IBM's 10 essential practices for building a successful cyber security program, visit this website:
ibm.co/EssentialPractices

To download the 2012 IBM CISO Study, visit this website:
ibm.co/CISOstudy

Follow us on Twitter
@ibmSecurity

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 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 event is 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 and/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.
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 comes 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, accounts, and/or steal their identity.
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).
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/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 who does not have access.
Wiper	Malicious software designed to erase data and destroy the capability to restore it.

IBM Global Technology Services
Route 100
Somers, NY 10589

Produced in the United States of America
July 2013

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Please Recycle