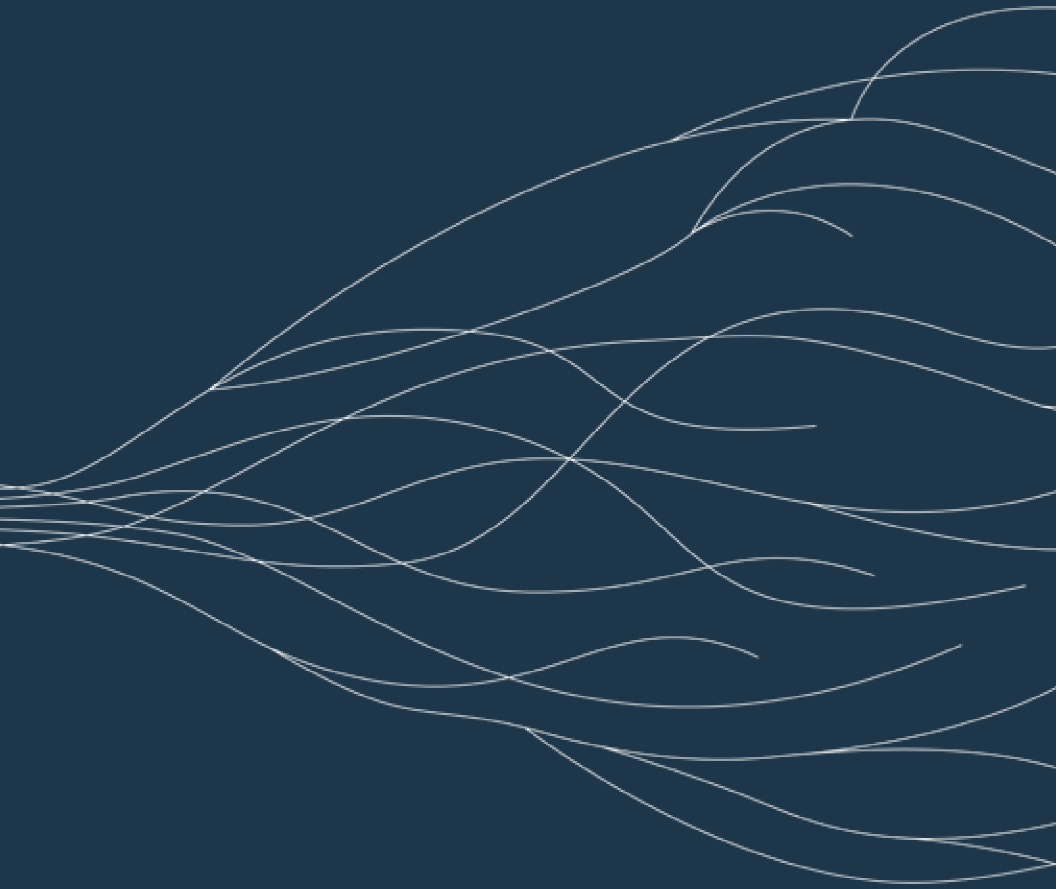
IBM Security



Security trends in the manufacturing industry

Intellectual property and operating information are the crown jewels

IBM X-Force® Research

Click here to start ►

◄ Previous Next ►

Contents

Executive overview

The good news? In 2016, the manufacturing sector clients monitored by IBM® Security Services experienced fewer attacks than our clients across all industries. The bad news? In manufacturing, the proportion of “security incidents”—those attacks to which we give our most serious classification—was almost 40 percent higher than the average across all industries (see Figure 1). Overall, the 2017 IBM X-Force Threat Intelligence Index reveals that manufacturing was the third most-attacked sector in 2016.

Despite the higher than cross-industry average security incidents in the manufacturing sector, 2016 actually saw a **significant decrease in both attacks and security incidents** year-over-year. Across all industries, figures fell sharply from 2015 to 2016, with attacks declining by 12 percent and security incidents by 48 percent. The data from the manufacturing sector is not surprising, then, but it’s still noteworthy: attacks down by 38 percent, security incidents down by 53 percent.

Definition of terms

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

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.

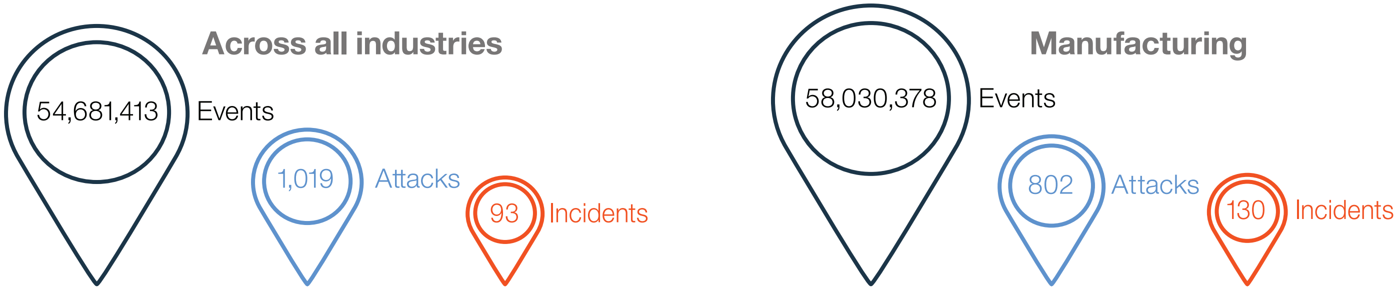


Figure 1. Comparison of organizations monitored by IBM for 2016, cross-industry clients versus manufacturing sector clients. (See sidebar “Definition of terms” for definitions of event, attack and security incident.) Source: IBM Managed Security Services data, January 1 – December 31, 2016.

Notable publicly disclosed manufacturing incidents

The fact that very few manufacturing sector incidents were disclosed publicly in 2016 leads IBM X-Force researchers to suspect some underreporting, perhaps because manufacturing is not as tightly regulated or subject to scrutiny as industries like financial services, healthcare and retail. Several notable incidents were disclosed, however, for instance the cyber theft of trade secrets from one of the world's largest steel makers.[1] A manufacturer’s crown jewels, intellectual property (IP) and internal operational information (OI), may not be as readily negotiable as cash or personally identifiable information, but cyber criminals and traders in business espionage still value them highly.

Attackers are opportunistic, employing tactics already proven successful against targets in other industries. One is the use of business email compromise (BEC) scams, including a global wire transfer scam designed to compromise the legitimate business email accounts of company executives in order to have their employees perform unauthorized wire transfers.[2]

About this report

This IBM X-Force Research report was created by the IBM Managed Security Services Threat Research group, a team of experienced and skilled security analysts working diligently to keep IBM clients informed and prepared for the latest cybersecurity threats. This research team analyzes security data from many internal and external sources, including event data, activity and trends sourced from endpoints managed and monitored by IBM.

BEC scams have also been known to target employee tax data for use in fraudulent returns and sale in Dark Web markets. In April 2016, a boat motor and supply company disclosed that it had been the victim of a BEC scam in which an employee unwittingly provided all its employees' W-2 forms to an unauthorized third party.[3] Considering the high cost of such incidents—an average of $156 for each lost or stolen record containing sensitive and confidential information—manufacturers should be making every effort to thwart threats that could result in data compromise.

The manufacturing sector did not emerge unscathed from a year in which ransomware and digital extortion got a foothold in nearly every industry and region.[4] In one incident, a precast concrete and construction services company with contractual ties to the US Navy was targeted by an attacker who threatened to sell stolen data unless a ransom was paid.[5] Another attacker made the same threat against a manufacturer of polyurethane and epoxy products: pay up, or we'll sell your stolen data.[6]

The threat is serious. Given the momentum and pace at which ransomware is spreading, and especially the advent of ransomware-as-a-service (RaaS)[7], manufacturers must do what they can to prepare an effective response.

Opportunistic attackers employed email scams, ransomware and extortion to make money off of manufacturers.

Where are the "bad guys"? Insiders versus outsiders

Dealing with multiple attacks year in and year out, security executives and their teams continually keep tabs on where threats are coming from in order to prioritize their defenses and budgets. A security investigation team's first step is to identify the source and destination IPs as internal or external, then further investigate the associated attack pattern to determine malicious or inadvertent intent.

What are they finding these days? Are most attackers outsiders, or do insiders make up a larger part of their organizations' overall attack surface?

In the manufacturing sector, IBM Managed Security Services 2016 data (see Figure 2) reveals considerably more outsider than insider attacks—91 percent outsiders to 9 percent insiders. Within the insider group, there were slightly more inadvertent actors (5 percent) than malicious insiders acting against the organization (4 percent).

Source of attacks against manufacturing industry security clients

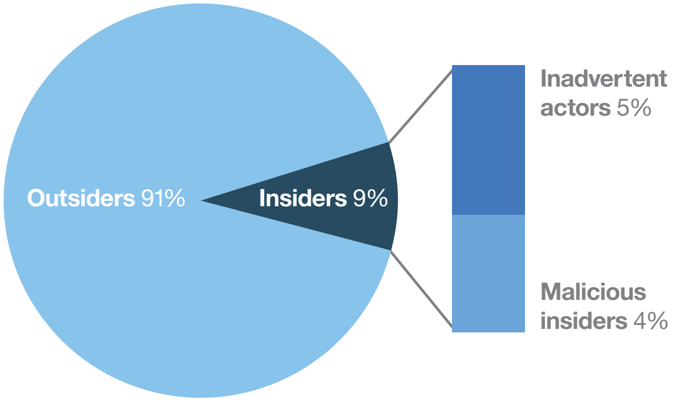


Figure 2. In 2016, outsiders were responsible for more manufacturing sector attacks than insiders.
Source: IBM Managed Security Services data, January 1 – December 31, 2016.

Among the top five targeted industries, the 2017 IBM X-Force Threat Intelligence Index reveals two other sectors experiencing more outsider than insider attacks, retail and information/communications.

The outsiders could include well-funded hackers, organized crime groups, and nation-state actors. Most outsider attacks in the manufacturing sector were initiated using injection-type attack mechanisms such as SQLi and CMDi.

Prevalent methods of attack in monitored manufacturer clients

To classify and better understand the types of threats affecting manufacturers, IBM X-Force has grouped 2016 observed attack types according to the standard set by the MITRE Corporation's CAPEC™ (Common Attack Pattern Enumeration and Classification) effort (see Figure 3). As described by MITRE, their system “organizes attack patterns hierarchically based on mechanisms that are frequently employed in exploiting a vulnerability.” The only exception is the “Indicator” category, which describes conditions and context of threats and attack patterns.

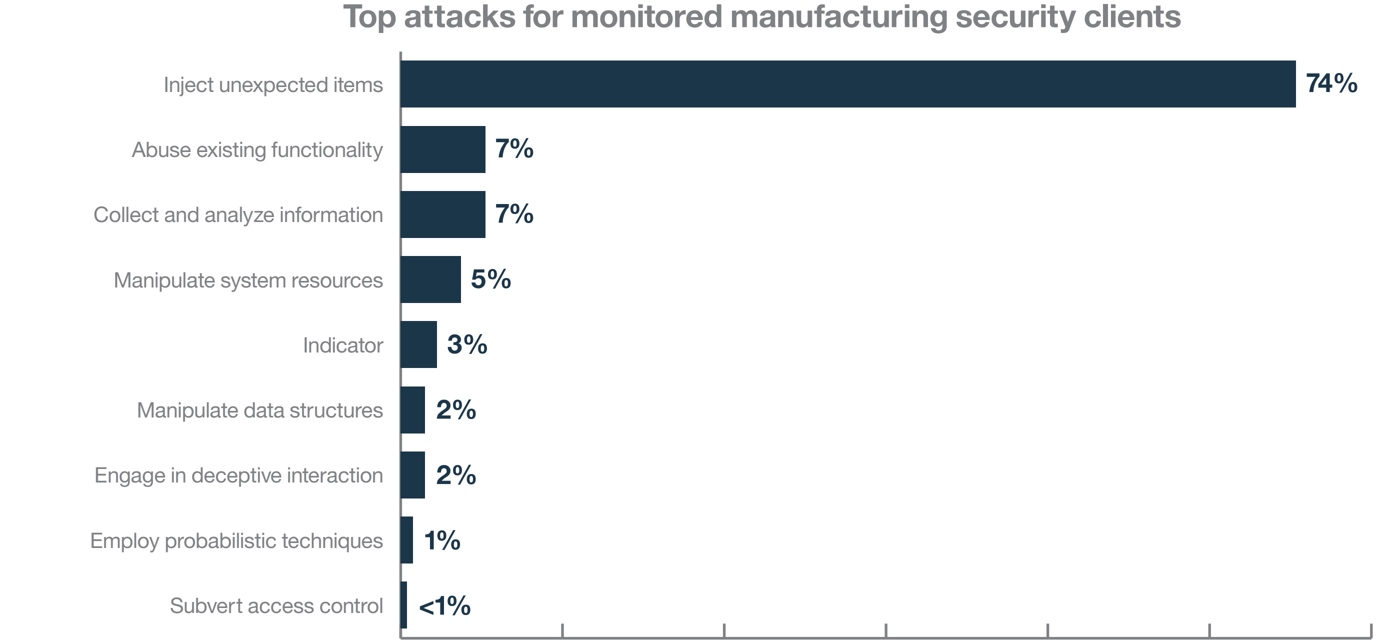


Figure 3. Injection-type incidents made up nearly three quarters of the attacks on the manufacturing sector in 2016. Source: IBM Managed Security Services data, January 1 – December 31, 2016.

The following sections present further details on each attack type.

Inject unexpected items

According to IBM Managed Security Services analysis of 2016 data, the number one attack vector, involving the use of malicious input data to attempt to control or disrupt a system, targeted 74 percent of the manufacturing clients monitored by IBM X-Force. That figure was notably higher than the cross-industry average of 42 percent.

Command injections, which include operating system command injection (OS CMDi) and SQLi, belong in this category. SQLi attacks made up 45 percent of these attacks. OS CMDi made up 18 percent and is also known as "shell command injection," after which the now infamous and widely prevalent Shellshock vulnerability is named.[8] Another 11 percent of the attacks involved other types of injection methods.

These results indicate that attackers are banking on manufacturers running outdated SQL servers. For instance, support for SQL Server 2005 ended in April 2016.[9] Enterprises still running SQL 2005 face potentially serious security vulnerabilities if they don't upgrade.

Abuse existing functionality

The number two attack vector involved attempts to abuse or manipulate "one or more functions of an application to deplete a resource to the point that the target's functionality is affected."[10] At seven percent, attacks for this category were substantially higher than the cross-industry client average of two percent.

Three out of four attacks on monitored manufacturing firms were injection-type attacks that targeted both databases (SQLi) and operating systems (OS CMDi).

Collect and analyze information

Attacks focused on the collection and theft of information made up seven percent of attacks targeting client devices. Most of these involved fingerprinting, often viewed as a kind of reconnaissance that gathers information on potential targets to discover their existing weaknesses. Essentially, an attacker compares output from a target system to known “fingerprints” that uniquely identify specific details about the target, such as the type or version of its operating system or that of an application. Attackers can use the information to identify known vulnerabilities in the target organization’s IT infrastructure and better prepare their tactical plans.

Manipulate system resources

Attacks attempting to manipulate some aspect of a system’s resource state or availability accounted for five percent of all attacks. Resources include files, applications, libraries and configuration information. Successful attacks in this category could allow the attacker to cause a denial of service, infect a machine to become part of a botnet, grant the attacker access to the company’s network, or execute arbitrary code on the target.

Indicator

Note that “Indicator” is not a CAPEC™ mechanism of attack. A cyberthreat indicator consists of certain observable conditions as well as contextual information about the condition or pattern. These “Indicator” type events, which accounted for three percent of all attacks, could indicate either an attempted or a successful attack on the target system. A large percentage of the attacks involved targeted systems experiencing 100 or more external pings in a short time, which might indicate a compromised internal host. If compromised, a host could be inadvertently attacking other targets or communicating with other compromised hosts until detected and stopped.

Manipulate data structures

While the cross-industry client average for attacks in this category is 32 percent, the figure in the manufacturing services sector, two percent, is very substantially lower. That might be because attackers view this attack vector as potentially less successful against manufacturing targets. This vector involves attacks in which the attacker attempts to gain unauthorized access through the manipulation of system data structures. As CAPEC™ states, “Often, vulnerabilities [such as buffer overflow vulnerabilities], and therefore the exploitability of these data structures, exist due to ambiguity and assumption in their design and prescribed handling."[11]

Engage in deceptive interaction

Two percent of attacks attempted to convince a victim to perform an action through spoofing, such as in a clickjacking or user interface redress attack. In this type of attack, the attacker attempts to hijack the victim's click actions and possibly launch further attacks. Computers aren't the only target. A recent report highlighted how Android mobile devices were vulnerable to clickjacking attacks via Google Play apps.[12]

Employ probabilistic techniques

One percent of attacks involved an attacker using what CAPEC™ describes as "probabilistic techniques to explore and overcome security properties of the target."[13] Most of the activity involved brute-force password attacks, a tactic in which an intruder tries to guess a username and password combination to gain unauthorized access to a system or data. Most of the attacks observed by IBM X-Force targeted the Secure Shell (SSH) network protocol. Users favor SSH because it can provide secure remote access. The downside is that it can provide attackers with shell account access across the network.

Subvert access control

Less than one percent of activity involved attacks attempting to subvert access controls through the "exploitation of weaknesses, limitations and assumptions in the mechanisms a target utilizes to manage identity and authentication."[14]
Most of the attacks we observed in this category involved the exploitation of vulnerabilities in the target's client-server communication channel for authentication and data integrity by leveraging the implicit trust a server places in what it believes to be a valid client.

Man-in-the-middle (MITM) attacks, in which attackers attempt to intercept and relay messages between two parties (people or systems), fall under this category. This technique could allow an attacker to become privy to and/or steal the information going back and forth, or insert malicious code into the connection.

Recommendations and mitigation

Secure production environments and trusted supply chains are critical to the protection of proprietary information and products in the manufacturing industry. Based on the findings of this report, we present the following best practices guidelines for manufacturers.

Centralized patching and data input sanitization

The number one attack vector targeting the manufacturing sector involved the use of malicious input data such as SQLi or CMDi. To mitigate these attacks, patching and maintaining current software versions are essential. The dilemma is, managing and deploying patches for multiple operating systems and applications across hundreds of thousands of endpoints can be challenging for administrators. Fortunately, manufacturing enterprises can rely on solutions such as IBM BigFix® Patch Management to automate and simplify the patching process.

Aside from timely patching, input data control and sanitization is another important step to mitigating the number one attack vector. There are many ways attackers can exploit unsanitized input data, so data sanitization must be comprehensive. Filter all user input.

Endpoint detection and response

An effective endpoint detection and response solution allowing visibility into your network can help in quickly identifying SQL and command injection attacks. Solutions such IBM BigFix Detect use advanced behavioral analytics to detect new and evasive threats and give you the tools to contain and remediate the attack.

Incident response services

According to the 2016 Ponemon Cost of Data Breach Study, having an incident response team as part of your organization’s cyber defenses reduced the cost of data breach by $16 per record, from $158 to $142. During an incident, that could translate into cost savings in the millions. Solutions that allow your enterprise to effectively prepare for and respond to cyberattacks with a proven response strategy, such as IBM X-Force Incident Response and Intelligence Services, are key to helping reduce the overall cost of a data breach.

Manufacturing and cloud

With cloud technology revolutionizing the manufacturing industry[15], organizations considering cloud adoption should know that it requires a structured approach to security. Manage access, protect your data and gain visibility through cloud solutions such as IBM Cloud Security Services, which offers both consulting services and managed services.

Augment cyber security intelligence capabilities

Through security and threat intelligence, organizations come to understand the attack vectors to which they are most vulnerable. Having this knowledge can help manufacturers stay a step ahead of criminals and bolster internal and external detection and protection mechanisms.

But how can security operations teams keep pace with the fast-multiplying threats and ever-growing volume of attacks targeting their organizations? Staying current with threat intelligence is a vital part of risk awareness, but the speed of threat data far exceeds human capability. Even the most skilled security professionals have difficulty sifting through the sheer volume of security incidents and available threat data. A solution combining cognitive capabilities and analytics, such as IBM QRadar® Advisor with Watson™, augments a security analyst's ability to identify and understand sophisticated threats by tapping into unlimited amounts of unstructured data from blogs, websites, research papers and the like, and correlating it with relevant security incidents.

Protect your enterprise while reducing cost and complexity

From infrastructure, data and application protection to cloud and managed security services, IBM Security Services has the expertise to help safeguard your company’s critical assets. We protect some of the most sophisticated networks in the world and employ some of the best minds in the business.

IBM offers services to help you optimize your security program, stop advanced threats, protect data and safeguard cloud and mobile. Security Intelligence Operations and Consulting Services can assess your security posture and maturity against best practices in security. With IBM X-Force Incident Response and Intelligence Services, IBM experts proactively hunt and respond to threats, and apply the latest threat intelligence before breaches occur. With IBM Managed Security Services, you can take advantage of industry-leading tools, security intelligence and expertise that can help you improve your security posture—often at a fraction of the cost of in-house security resources.

◄ Previous Next ►

Contents

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force research, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. IBM operates one of the world’s broadest security research, development and delivery organizations, monitors billions of security events per day in more than 130 countries, and holds more than 3,500 security patents.

Contributors

Michelle Alvarez - Threat Researcher, IBM Security
Scott Craig - Threat Researcher, IBM Security

For more information

To learn more about the IBM Security portfolio, please contact your IBM representative or IBM Business Partner, or visit: ibm.com/security

For more information on security services, visit: ibm.com/security/services

Follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog

[1] http://www.reuters.com/article/us-thyssenkrupp-cyber-idUSKBN13X0VW

[2] https://www.scmagazine.com/two-tech-firms-swindled-out-of-100m-were-google-and-facebook/article/653712/

[3] http://www.scmagazine.com/brunswick-corps-13000-workers-w-2-data-compromised/article/494352/

[4] https://www-01.ibm.com/marketing/iwm/dre/signup?source=mrs-form-10908&S_KG=ov55738&ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US

[5] https://www.databreaches.net/thedarkoverlord-reveals-three-more-attacks-with-more-to-be-revealed/

[6] https://www.databreaches.net/thedarkoverlord-reveals-three-more-attacks-with-more-to-be-revealed/

[7] https://securityintelligence.com/news/files-with-that-ransomware-as-a-service-lets-would-be-fraudsters-order-on-demand/

[8] https://exchange.xforce.ibmcloud.com/collection/2016-Shellshock-Attack-Campaign-ca5ef17ba943d740605597fa0fb622ad

[9] https://www.microsoft.com/en-us/cloud-platform/sql-server-2005

[10] https://capec.mitre.org/data/definitions/210.html

[11] https://capec.mitre.org/data/definitions/255.html

[12] http://searchsecurity.techtarget.com/news/450418664/Android-clickjacking-attacks-possible-from-Google-Play-apps

[13] https://capec.mitre.org/data/definitions/223.html

[14] https://capec.mitre.org/data/definitions/225.html

[15] https://www.forbes.com/sites/louiscolumbus/2013/05/06/ten-ways-cloud-computing-is-revolutionizing-manufacturing/#7d028123859c

◄ Previous Next ►

IBM Security
75 Binney Street
Cambridge MA 02142

Produced in the United States of America
June 2017

IBM, the IBM logo, ibm.com, BigFix, QRadar, Watson and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml

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.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.