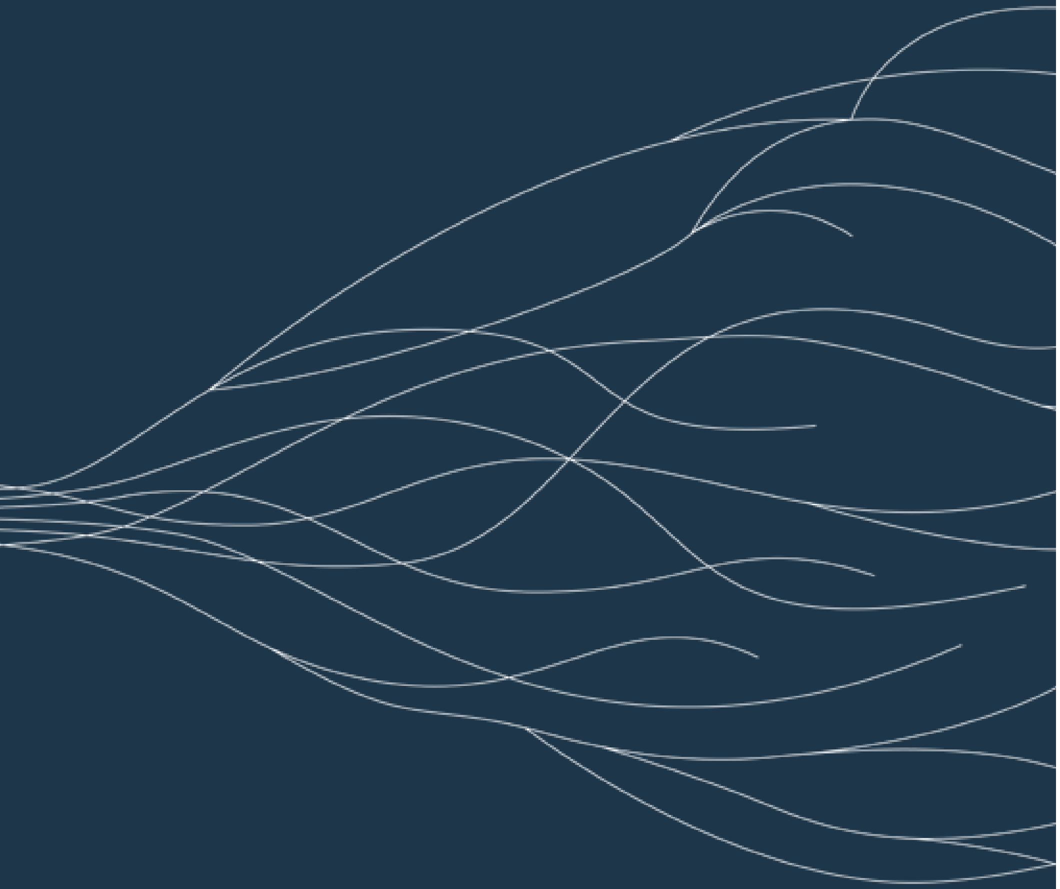


# Security trends in the information and communication technology industry

Attackers set their sights on the customer data in the care of these organizations

**IBM X-Force® Research**

Click here to start ►

◄ Previous Next ►

## Executive overview

The information and communication technology (ICT) industry has evolved greatly over the last several decades. The increasingly interconnected nature of ICT devices and systems, along with modern society's dependence on the technologies and services this sector provides, extend the risk of cyberattack. Furthermore, firms in this industry often act as a clearinghouse or storehouse for data gathered from other industries. In October 2016, for example, a misconfigured, publicly accessible NoSQL database at a data storage and web hosting company exposed millions of customer details—including email addresses, full names, home addresses, gender and job titles. A dump of the data was posted on Twitter before the company secured the database.[1]

### 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.

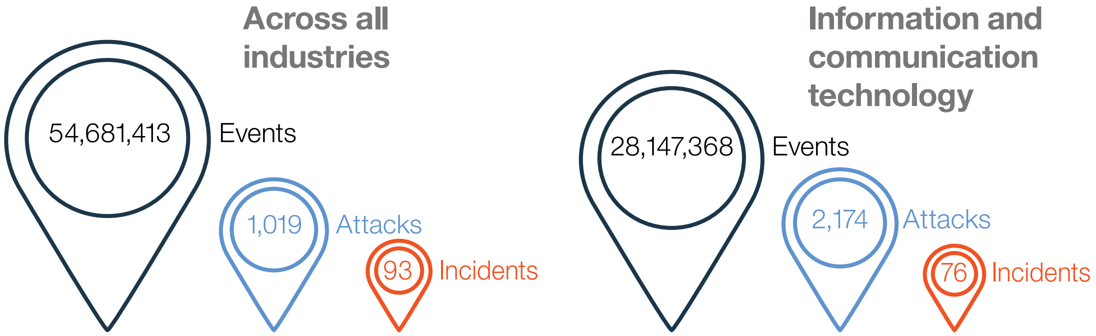


**Figure 1.** Comparison of organizations monitored by IBM for 2016, cross-industry clients versus information and communication sector clients. (See sidebar "Definition of terms" for definitions of event, attack and security incident.) Source: IBM Managed Security Services data, January 1 – December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

Not surprisingly, the 2017 IBM X-Force Threat Intelligence Index reveals that information and communication technology was the second most-attacked sector in 2016. The average IBM® X-Force®-monitored client in this sector experienced 133 percent more attacks than the average cross-industry client (see Figure 1), clearly contributing to this sector's higher placement among most attacked industries in 2016.

The information and communication technology sector saw a nearly 150 percent year-over-year increase in attacks. A rise in attacks or attempts to compromise target systems reveals attackers' increased focus on this industry. Fortunately, the proportion of "security incidents"—those attacks to which we give our most serious classification—was 18 percent lower than across all industries. In fact, there was a nearly 46 percent decrease in security incidents year-over-year.

## About this report

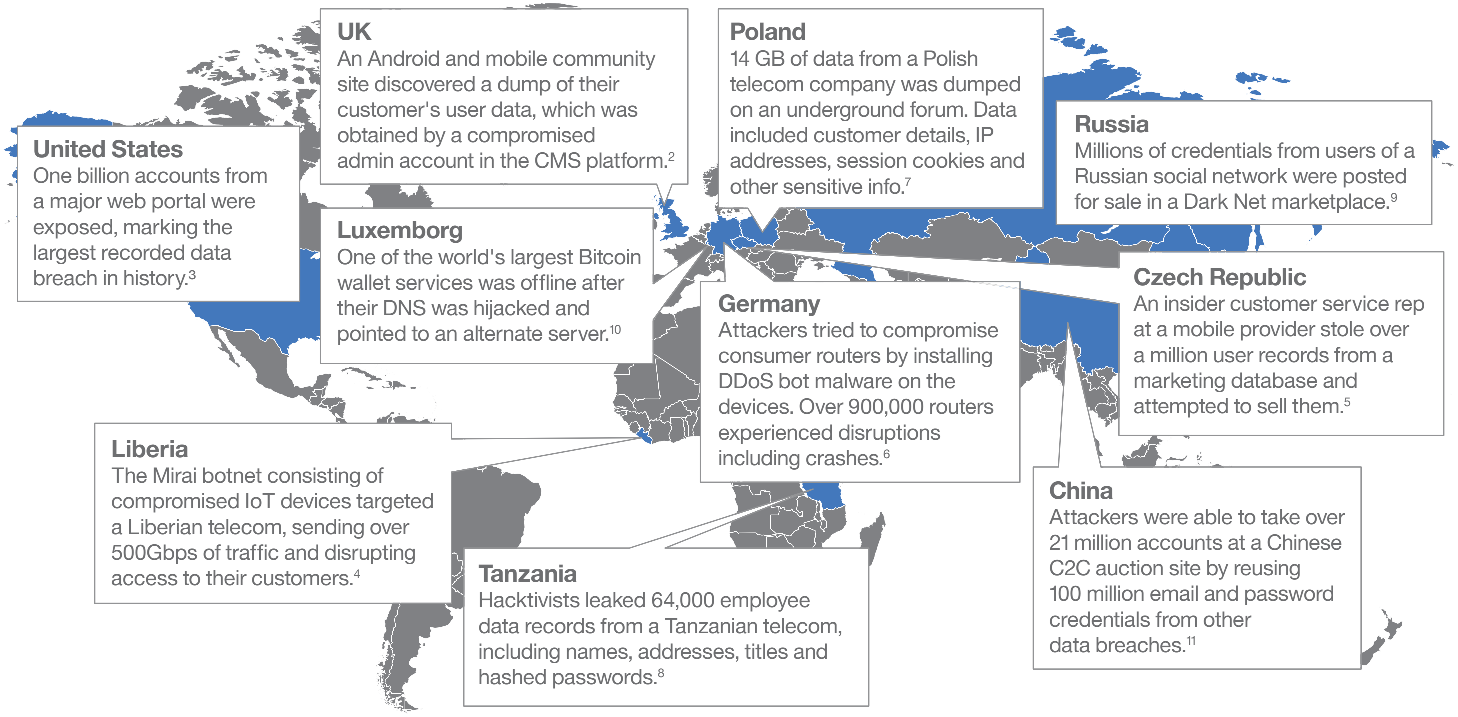
This IBM X-Force Research report was created by the IBM Managed Security Services Threat Research group, a team of experienced and skilled security analysts working diligently to keep IBM clients informed and prepared for the latest cybersecurity threats. This research team analyzes security data from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

Contents

# A global view: publicly disclosed information and communication technology incidents

IBM X-Force Interactive Security Incidents data is a sampling of notable publicly disclosed incidents. Included are breaches, which are incidents resulting in the exfiltration of data. As Figure 2 shows, there was no shortage of incidents affecting information and communication technology organizations globally.

With an unprecedented 3.3+ billion records compromised, the information and communication technology sector experienced the most records compromised out of all sectors in 2016 (see Figure 3). Almost half of those records were the result of two separate breaches from previous years (2013[12] and 2014[13]) that affected one major web portal company. With a billion accounts exposed, the first breach from 2013 marked the largest recorded data breach in history. The company suggested that forged cookies may have been used to access the data.[14]



**United States**
One billion accounts from a major web portal were exposed, marking the largest recorded data breach in history.[3]

**UK**
An Android and mobile community site discovered a dump of their customer's user data, which was obtained by a compromised admin account in the CMS platform.[2]

**Luxemborg**
One of the world's largest Bitcoin wallet services was offline after their DNS was hijacked and pointed to an alternate server.[10]

**Poland**
14 GB of data from a Polish telecom company was dumped on an underground forum. Data included customer details, IP addresses, session cookies and other sensitive info.[7]

**Russia**
Millions of credentials from users of a Russian social network were posted for sale in a Dark Net marketplace.[9]

**Germany**
Attackers tried to compromise consumer routers by installing DDoS bot malware on the devices. Over 900,000 routers experienced disruptions including crashes.[6]

**Czech Republic**
An insider customer service rep at a mobile provider stole over a million user records from a marketing database and attempted to sell them.[5]

**Liberia**
The Mirai botnet consisting of compromised IoT devices targeted a Liberian telecom, sending over 500Gbps of traffic and disrupting access to their customers.[4]

**Tanzania**
Hacktivists leaked 64,000 employee data records from a Tanzanian telecom, including names, addresses, titles and hashed passwords.[8]

**China**
Attackers were able to take over 21 million accounts at a Chinese C2C auction site by reusing 100 million email and password credentials from other data breaches.[11]

**Figure 2.** Notable 2016 publicly disclosed information and communication technology security incidents. Source: IBM X-Force Interactive Security Incidents data.

◄ Previous Next ►

## Contents

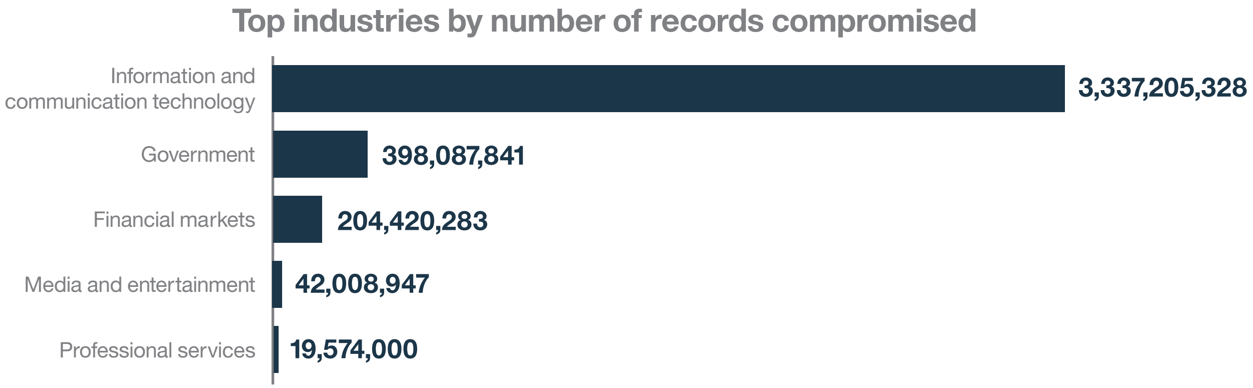


**Figure 3.** Top five industries by number of records compromised in 2016. Source: IBM X-Force Interactive Security Incidents data.

Aside from forged cookies, attackers used phishing techniques such as the Business Email Compromise (BEC) scam, SQL injection and account take-over via brute force to steal, expose and sell confidential and sensitive information. In one notable incident, attackers were able to take over 21 million accounts at a Chinese C2C auction site by reusing 100 million email and password credentials obtained from other data breaches.[15] The criminals used the hacked accounts for fake reviews and bid fraud.

Not only did this industry rank number one in terms of records compromised in 2016, but IBM X-Force Interactive Security Incidents data also shows the information and communication technology industry ranking number one in terms of total number of incidents disclosed (see Figure 4).

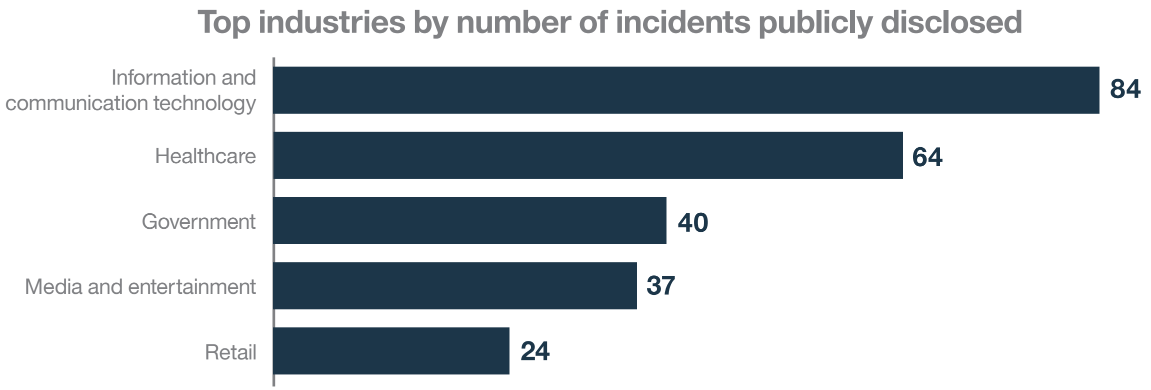


**Figure 4.** Top five industries by number of incidents publicly disclosed in 2016. Source: IBM X-Force Interactive Security Incidents data.

And during a year where ransomware wreaked havoc on almost every industry, information and communication technology companies were no exception. One French company shut down for five days due to a ransomware infection, nearly resulting in a loss of four months' worth of work due to impacts on critical systems such as payroll.[16] With 2017's onslaught of the now infamous WannaCry, a massive international ransomware campaign, there is no indication that the ransomware threat is slowing. WannaCry has infected over 200,000 endpoints in more than 150 countries, including disrupting services at Spanish and Portuguese telecommunication companies as well as several other businesses in the computer services sector.[17]

Like virtually every other industry, information and communications technology organizations were targets of ransomware attacks in 2016.

## Where are the “bad guys”? Insiders versus outsiders

Dealing with multiple attacks year in and year out, security executives and their teams must 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.

Source of attacks against information and communication technology security clients

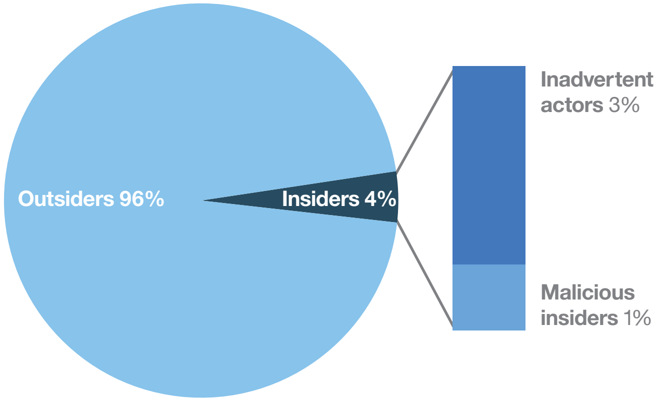


**Figure 5.** In 2016, outsiders were responsible for more information and communication technology sector attacks than insiders. Source: IBM Managed Security Services data, January 1 – December 31, 2016.

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 information and communication technology sector, IBM Managed Security Services 2016 data (see Figure 5) reveals considerably more outsider than insider attacks—96 percent outsiders to 4 percent insiders. Within the insider group, there were slightly more inadvertent actors (3 percent) than malicious insiders acting against the organization (1 percent).

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 manufacturing. Despite the overwhelming percentage of outside attacks, information and communication organizations need to realize that the threat from insiders is still very real. One notable example, as illustrated in Figure 2, involved the attempted sale of over a million user records by a customer service representative at a mobile provider in the Czech Republic.[18]

## Prevalent methods of attack in monitored information and communications technology clients

To classify and better understand the types of threats affecting the information and communications technology industry, 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 6). 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.

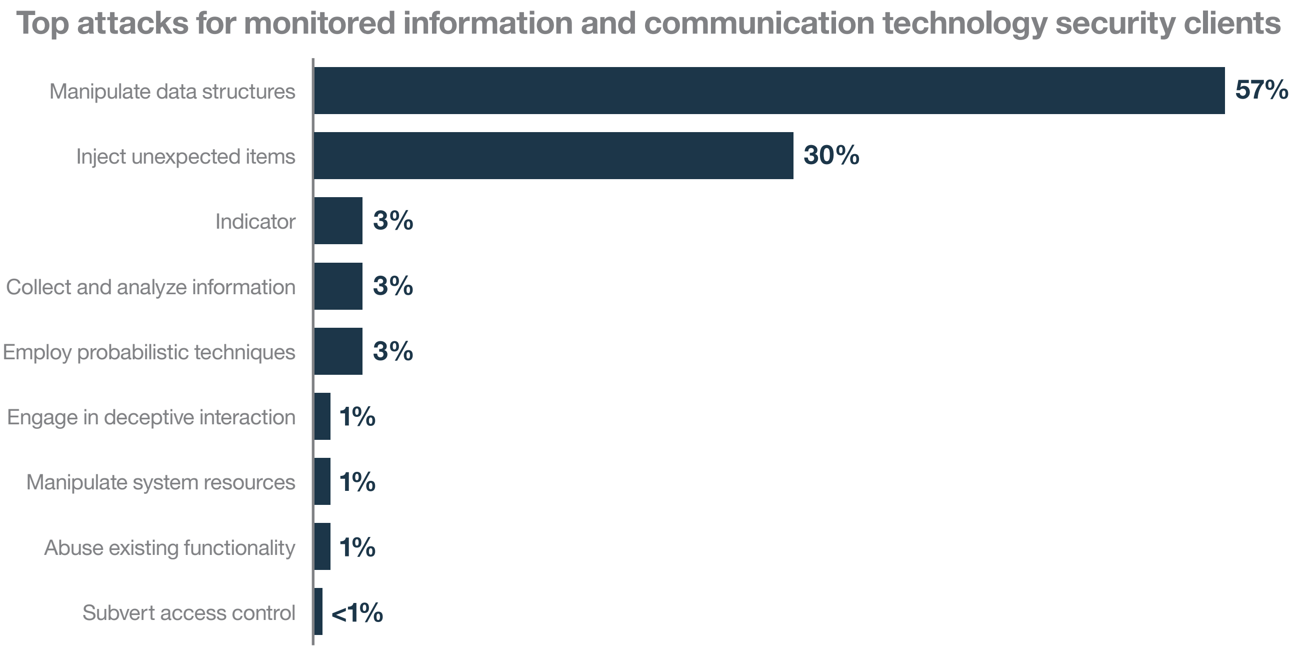


**Figure 6.** Incidents involving attempts to gain unauthorized access by manipulating system data structures made up more than half of the attacks on the information and communication technology sector in 2016. Source: IBM Managed Security Services data, January 1 – December 31, 2016.

The following sections present further details on each attack type.

## Manipulate data structures

Of the top five most targeted industries in the 2017 IBM X-Force Threat Intelligence Index, information and communication technology was the only sector to experience the category “manipulate data structures” as the number one attack vector. Information and communication technology, at 57 percent, is substantially higher than the cross-industry client average of 32 percent.

That might be because attackers view this attack vector—involving attempts to gain unauthorized access by manipulating system data structures—as potentially more successful against ICT targets. 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.”[19]

## Inject unexpected items

According to IBM Managed Security Services analysis of 2016 data, the number two attack vector, involving the use of malicious input data to attempt to control or disrupt a system, targeted 30 percent of the information and communication technology clients monitored by IBM X-Force. That figure was notably lower than the cross-industry average of 42 percent.

Command injections, which include operating system command injection (OS CMDi) and SQL injections (SQLi), belong in this category. SQLi made up 11 percent of these attacks. OS CMDi, also known as “shell command injection”—after which the now infamous and widely prevalent Shellshock vulnerability is named—made up 16 percent.[20] Another 3 percent of the attacks involved other types of injection methods.

These results indicate that attackers are banking on information and communication technology organizations running outdated SQL servers. For instance, in one publicly disclosed incident in 2016, exploitation of an SQL vulnerability resulted in a dump of the user table of a popular Linux distribution’s official forum. Exposed data included email addresses and IP addresses of forum members.[21]

### Indicator

Note that "Indicator" is not a CAPEC™ mechanism of attack but rather a cyber threat indicator consisting 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.

### Collect and analyze information

Attacks focused on the collection and theft of information made up three percent of attacks targeting client devices, lower than the cross-industry average of nine percent. 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 an application. Attackers can use the information to identify known vulnerabilities in the target organization's IT infrastructure and better prepare their tactical plans.

### Employ probabilistic techniques

Three percent of attacks involved an attacker using what CAPEC™ describes as "probabilistic techniques to explore and overcome security properties of the target."[22] 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.

### Engage in deceptive interaction

One 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.

Contents

### Manipulate system resources

Attacks attempting to manipulate some aspect of a system’s resource state or availability accounted for one 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.

### Abuse existing functionality

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”[23] made up one percent of the activity. Attacks for this category were just slightly lower than the cross-industry client average of two percent.

### 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.”[24]

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 or steal the information going back and forth, or insert malicious code into the connection.

Attackers attempting to manipulate system resources may have any number of motives, including causing a denial of service, creating a new bot, gaining access to a network or executing code.

◄ Previous Next ►

## Recommendations and mitigation

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

### Test applications throughout the lifecycle

The number one attack vector targeting the information and communication technology sector involved attackers attempting to gain unauthorized access through the manipulation of system data structures, such as an application's interaction with a buffer. Deploying a security testing solution, such as IBM® Security AppScan®, can help prevent potential vulnerabilities such as buffer overflow vulnerabilities. By scanning web and mobile applications prior to deployment, organizations are better able to identify security vulnerabilities and generate reports and fix recommendations.

### Centralized patching and data input sanitization

The number two attack vector targeting the information and communication technology 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 that managing and deploying patches for multiple operating systems and applications across hundreds of thousands of endpoints can be challenging for administrators. Fortunately, information and communication technology enterprises can rely on solutions such as IBM BigFix® Patch Management to help 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.

◄ Previous Next ►

## 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 help contain and remediate the attack.

## Incident response services

According to the 2017 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 $19.30 per record, from $141 to $121.70. In 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 Services, are key to helping reduce the overall cost of a data breach.

## 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 information and communications technology companies 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™, helps augment 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 help 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.

## 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.

◄ Previous Next ►

## Contributors

Michelle Alvarez - Threat Researcher, IBM Security
Scott Craig - Threat Researcher, IBM Security
Jason Kravitz - IBM X-Force Research,
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://arstechnica.com/security/2016/10/breach-exposes-at-least-58-million-accounts-includes-names-jobs-and-more/

[2] https://haveibeenpwned.com/PwnedWebsites#MoDaCo

[3] https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached

[4] http://thehackernews.com/2016/11/ddos-attack-mirai-liberia.html

[5] http://www.theregister.co.uk/2016/06/20/tmobile_czech_breach/

[6] http://www.securityweek.com/german-isp-confirms-malware-attacks-caused-disruptions

[7] https://www.hackread.com/ukranian-hacker-hacks-polish-telecom-netia/

[8] https://www.hackread.com/anonymous-opafrica-tanzanian-telecom-firm-hacked/

[9] http://thehackernews.com/2016/06/vk-com-data-breach.html

[10] http://thehackernews.com/2016/10/blockchain-bitcoin-website.html

[11] https://nakedsecurity.sophos.com/2016/02/05/data-breach-in-china-100-million-records-used-to-hack-20-million-taobao-users/

[12] https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached

[13] http://www.bbc.com/news/world-us-canada-37447016

[14] https://www.usatoday.com/story/tech/news/2017/02/15/yahoo-notifies-users-forged-cookie-breach/97955438/

[15] https://nakedsecurity.sophos.com/2016/02/05/data-breach-in-china-100-million-records-used-to-hack-20-million-taobao-users/

[16] http://www.larepubliquedespyrenees.fr/2016/04/20/une-entreprise-ranconnee-par-un-pirate-informatique,2019097.php

[17] https://www.nytimes.com/2017/05/14/world/europe/cyberattacks-hack-computers-monday.html?_r=3

[18] http://www.theregister.co.uk/2016/06/20/tmobile_czech_breach/

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

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

[21] http://www.cio.co.nz/article/603600/flaw-vbulletin-add-on-leads-ubuntu-forums-database-breach/

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

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

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

◄ Previous Next ►

Contents

IBM Security
75 Binney Street
Cambridge MA 02142

Produced in the United States of America
July 2017

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.