Software Management: Security Imperative, Business Opportunity

BSA
GLOBAL
SOFTWARE
SURVEY

JUNE 2018

CONTENTS

Introduction

Around the world, software has become one of the most ubiquitous and essential tools businesses use to perform their most fundamental everyday tasks — from tracking sales, maintaining books, targeting markets, communicating with customers, collaborating with partners, to boosting productivity. With breakthrough advances making software even more capable, organizations are increasingly using it as a catalyst for improving the way they do business, growing their bottom lines, reaching new markets, and obtaining competitive advantages.

Too often today however, users are seeing their efforts to harness innovative technologies hampered by crippling security threats, including exposure to malware. It is increasingly clear that malware infections are tightly linked to the use of unlicensed software. As a result, many CIOs are coming to understand the true costs of unlicensed software and taking pragmatic steps to improve their software management.

To better understand these impacts and opportunities, BSA's Global Software Survey, conducted in partnership with IDC, set out to quantify the volume and value of unlicensed software installed on personal computers across more than 110 national and regional economies. The results show that, although CIOs are aware that using unlicensed software creates security risks, 37 percent of software installed on personal computers is still unlicensed.

KEY TRENDS AND FINDINGS

- Use of unlicensed software, while down slightly, is still widespread.
- CIOs are finding unlicensed software is increasingly risky and expensive.
- Improving software compliance is now an economic enabler and security imperative.
- Organizations can take meaningful steps today to improve software management and achieve important gains.

The report thus makes clear that in this era of heightened cybersecurity risk, organizations need to take the critical first step of assessing what is in their network and eliminating unlicensed software. In doing so, they can reduce the risk of harmful cyber attacks and boost the bottom line.

This in-depth analysis of the use of unlicensed software shows that companies that implement strong measures to improve the way they manage software now have a powerful new tool for reducing security risks, boosting their bottom line, decreasing downtime, and growing opportunity.

KEY FINDINGS

Use of unlicensed software, while down slightly, is still widespread. Despite a global two-point drop in unlicensed software installation rates during the last two years, unlicensed software is still being used around the globe at alarming rates, accounting for 37 percent of software installed on personal computers. Although the overall commercial value of unlicensed software has also been declining, the majority of all countries in the survey still have unlicensed rates of 50 percent or higher. These high rates don't just delay the local economic benefits that are associated with thriving technology use, they impede growth in a company's bottom line and induce unprecedented security risks.

CIOs are finding unlicensed software is increasingly risky and expensive. Organizations now face a one-in-three chance of encountering malware when they obtain or install an unlicensed software package or buy a computer with unlicensed software on it. Each malware attack can cost a company $2.4 million on average and can take up to 50 days to resolve. To the extent that the infection leads to company downtime, or lost business data, it can also seriously affect the company's brand and reputation. The cost for dealing with malware that is associated with unlicensed software is growing too. It can now cost a company more than $10,000 per infected computer, and cost companies worldwide nearly $359 billion a year. Avoiding the security threats from malware is now the number one reason CIOs cite for ensuring the software on their network is fully licensed.

Improving software compliance is now an economic enabler and security imperative. With growing costs from malware, business leaders are increasingly turning to fully licensed software that can be patched with the latest updates as a key line of defense against crippling malware incursions, data breaches, and other security risks. More and more leaders are also realizing that improving their ability to manage software across an entire organization can be a powerful new tool to help them decrease downtime, and significantly boost their bottom line. In fact, IDC estimates that when companies take pragmatic steps to improve their software management, they can boost their bottom line by as much as 11 percent.

Organizations can take meaningful steps today to improve software management and achieve important gains. To access these benefits, organizations can implement proven software asset management (SAM) best practices to improve their software asset management and get more out of their technology. SAM not only helps CIOs ensure that software running on their network is legitimate and fully licensed, it can also help decrease debilitating cyber-risks, improve productivity, reduce downtime, centralize license management, and reduce costs. Studies show that organizations can achieve as much as 30 percent savings in annual software costs by implementing a robust SAM and software license optimization program.[1]

Malware Is Increasingly Pervasive, Costly, and Debilitating

Around the globe, consumers, companies, and countries are increasingly finding that that their efforts to harness the power and potential of new technologies is being hampered by the potentially serious threats caused by malware. These malware threats are now at an all-time high — with eight new threats appearing every second of every day.[2] As they grow in frequency, they also grown in impact; they are increasingly expensive and debilitating.

The number of malware attacks continues to grow exponentially both in number and in sophistication.[3] In 2016, for example, there were 15 data breaches with more than 10 million IDs exposed — almost double the number in 2013.[4] The attacks are not only aimed at large enterprises — consumers and enterprises of all sizes are affected. In fact, in 2015 43 percent of cyber-attacks worldwide were against small businesses with less than 250 workers.[5] And cybercriminals are now targeting mobile networks as well. Malware variants on mobile devices increased by 54 percent last year, with 24,000 malicious mobile apps blocked every day.[6]

These attacks are also becoming increasingly expensive. The average malware attack costs a company $2.4 million.[7] Each infection can lead to costly downtime, lost productivity, lost business opportunities, and additional IT labor costs to help mitigate the attack. To the extent that the infection leads to company downtime or lost business data, it can also seriously affect the brand and reputation of a business. Making matters worse, the economic cost of these infections continues to grow — up 20 percent since 2014. Malware-related activity now costs the global economy a startling $600 billion annually, or 0.8 percent of the global GDP.[8]

Complicating efforts, these attacks are often difficult to detect and resolve. It takes an organization an average of 243 days to detect a malware attack[9] and can take up to 50 days to resolve.[10]

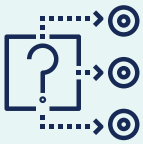
(continued on page 5)

Malware threats are now at an all-time high — with eight new threats appearing every second of every day.

MALWARE IMPACTS

Organizations now face a nearly one-in-three chance of encountering malware when they obtain or install unlicensed software.

Dealing with the malware associated with unlicensed software can cost more than $10,000 per infected computer for a worldwide total of more than $359 billion.



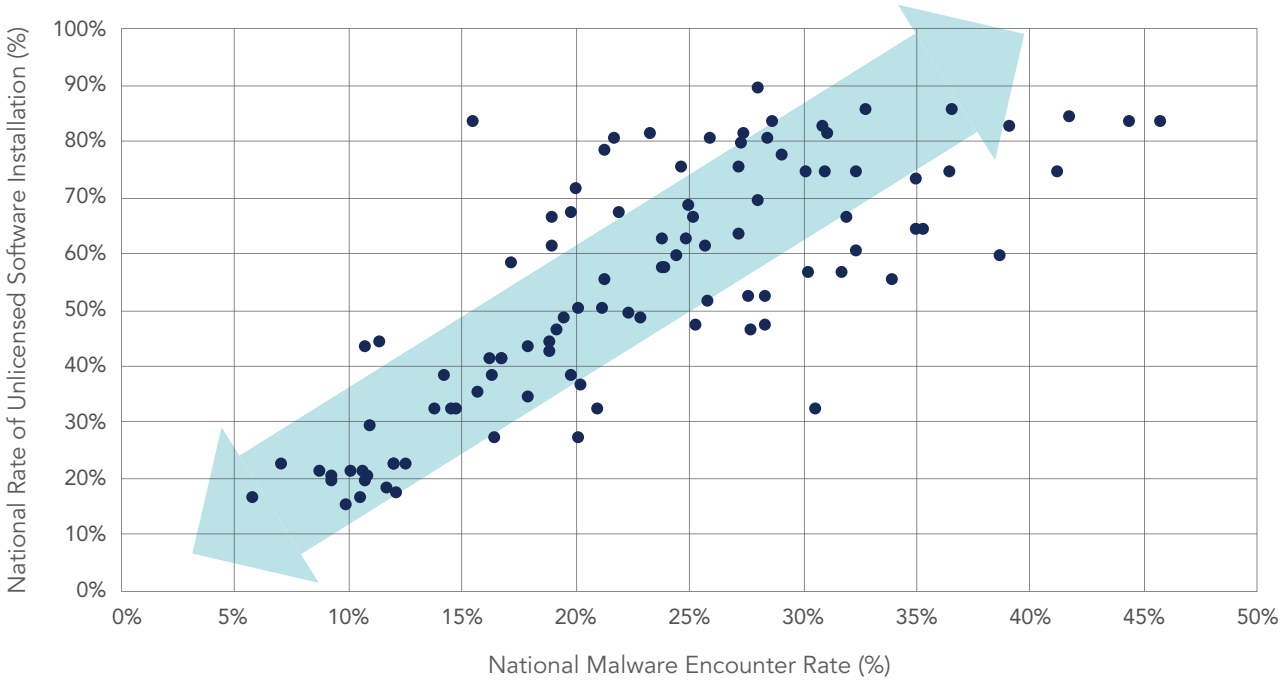
Users are taking note: 68 percent of computer users and 48 percent of CIOs rated malware among the top three reasons not to use unlicensed software.

CIOs top concerns from these unlicensed malware threats include the loss of corporate or personal data, system downtime, network outages, and the cost of disinfecting systems.

To help mitigate these impacts, the number of CIOs who have a formal written policy about the use of licensed software has jumped dramatically from 41 percent in 2015 to 54 percent this year. Yet only 35 percent of workers are aware of a formal written policy, suggesting a critical education gap.

Organizations taking proactive steps are finding that a 20 percent increase in software compliance can improve a company's profits by 11 percent — a boost of more than half a million dollars for the average-sized company in the survey.

Unlicensed Software and Malware Encounters Are Tightly Linked



Source: IDC

MALWARE INFECTIONS ARE ASSOCIATED WITH UNLICENSED SOFTWARE

It is increasingly clear that these malware infections are tightly linked to using unlicensed software — the higher the rate of unlicensed software use, the higher the likelihood of a debilitating malware infection.

Notwithstanding that link, however, unlicensed software continues to be deployed at an alarming rate. Around the globe a significant amount of software in use is unlicensed. Indeed, in four out of six regions — Asia-Pacific, Central and Eastern Europe, Middle East and Africa, and Latin America — the majority of software deployed on personal computers is unlicensed. (See pages 12–13).

Given the link between unlicensed software and malware infections, this creates enormous cyber-risk. IDC estimates that organizations that obtain or install an unlicensed software package or buy a computer with unlicensed software on it face a one-in-three chance (29 percent) of encountering malware.

Statistical analysis confirms this link. In countries around the globe, there is a strong and consistent correlation (r-0.78) between using unlicensed software and encountering malware. In fact, a country's unlicensed software rate is a reliable predictor of a country's malware infection rate.

CIOs understand this link. When asked to rank the top benefits of strong software license management and better software compliance, 54 percent of CIOs listed lower security risks as the primary reason to ensure their software was fully licensed.

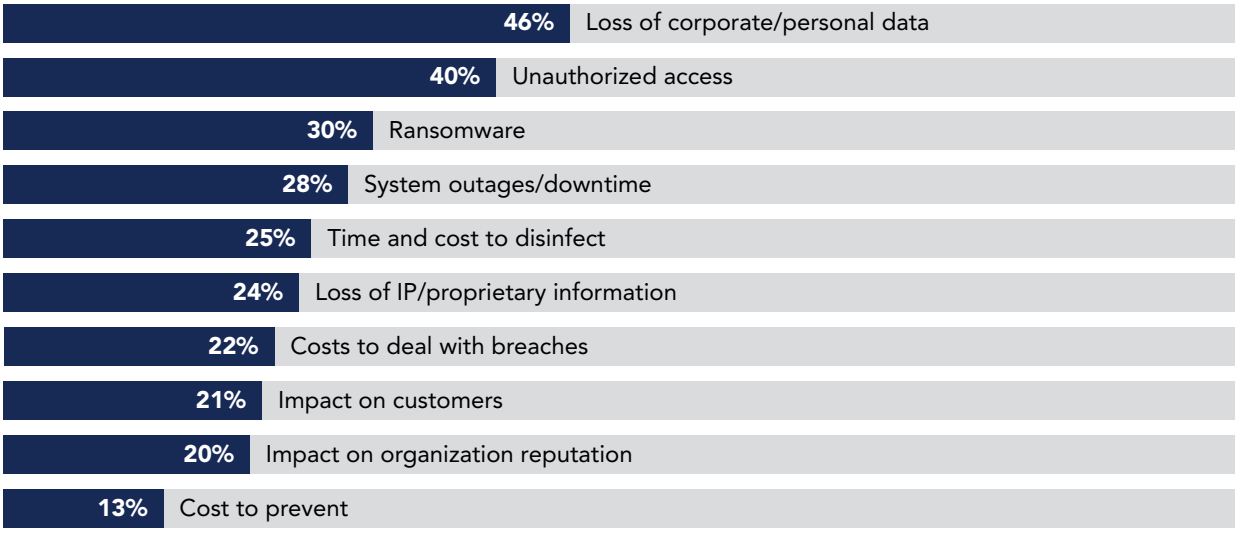
The link between malware and unlicensed software is top of mind for CIOs for good reason — CIOs know firsthand the debilitating consequences of a malware infection. CIOs surveyed noted their primary concern related to malware that can accompany unlicensed software is the theft of data (46 percent). They also reported significant concerns with unauthorized access to their network (40 percent), responding to potential ransomware (30 percent), system outages and downtime (28 percent), and the time and cost of disinfecting the network (25 percent). And they

CIOs Report the Top Benefits of Strong Software Compliance

recognize that these are not one-off experiences. In fact, one in five (19 percent) enterprises in our survey reported they have network, website, or computer outages every few months or more — and that the most common cause of security-related outages was from malware on end user computers (56 percent) — making unlicensed software a prominent vector of attack.

And, as noted above, these impacts can be devastating. Dealing with a cyber-attack and its aftermath can now cost a company more than $10,000 per infected computer — costing the company orders of magnitude more than what it would cost to obtain licensed versions of the software, and far more than the cost of the computer itself. IDC estimates that it costs companies nearly $360 billion a year to deal with malware associated with unlicensed software.

Top Enterprise Concerns About Malware Effects From Unlicensed Software



MALWARE RISKS CAN TRANSLATE INTO SIGNIFICANT REAL-WORLD PROBLEMS

Lack of software asset management, and reliance on unlicensed software, is having huge security impacts around the globe, especially in countries with high rates of unlicensed software. For example:

- **China**, where a whopping 66 percent of software is unlicensed, has suffered from disproportionately devastating malware attacks that crippled an estimated 40,000 Chinese institutions. Just one malware attack traversed unpatched, unlicensed software so rapidly that it crippled prestigious research institutions like Tsinghua University, halted the electronic payment systems throughout the country at PetroChina's gas stations, shut down ATMs run by the Bank of China, and impacted the operations of major companies like China Telecom and Hainan Airlines. Finnish cybersecurity company F-Secure reports that the large number of computers running unlicensed software in China contributed to the breadth and depth of the devastating attack.[11] As a senior network engineer for a Beijing-based technology provider pointed out, "most of the victims in China are unlicensed users."[12]

- **Russia**, whose high 62 percent unlicensed software rate has a massive commercial value of $1.2 billion, also has experienced devastating impacts from recent malware attacks. In 2017, malware attacks crippled the Russian Health Ministry; the state-run Russian Railways; the Interior Ministry, which manages the police force; and the telecommunications company Megafon. A senior researcher at the Institute of International Relations in Prague indicated the broad scope of malware infection in Russia resulted from "using not just outdated software but pirated out-of-date software."[13]

The scope and impact of these threats should serve as a wake-up call for those who are relying on unlicensed software for critical business functions, don't have a software asset management system in place, or are relying on others who are at risk from unlicensed related malware.

Software compliance has now become an economic enabler and security imperative.

Software Asset Management Can Decrease These Cyber-Risks and Boost Bottom Lines

It is clear that there is an opportunity to reduce cyber-risk through ensuring that software is fully licensed. And there is an internationally recognized standard for doing so. Recent updates to the International Organization for Standardization's (ISO) SAM standard provide a framework for overall IT asset management (ITAM) including software.[14]

As one recent example demonstrates, implementing ISO-aligned SAM is a powerful tool to improve security. In the United States, Equifax was responsible for one of the most massive data breaches in history when the company failed to patch one of its servers for a vulnerability that had been known for months, costing the company an estimated $439 million, and forcing its CEO and CIO to resign.[15] Experts report that had the company used a SAM system to track all instances of the Apache software at issue, the breach could have been avoided.[16] Minimizing malware exposure by avoiding unlicensed use is critical but, as this example highlights, even when a company is using licensed software, having an adequate SAM system in place is still essential.

By ensuring that software is fully licensed and optimized to business needs, SAM brings additional benefits in the form of decreased downtime and bottom line savings. SAM also helps companies ensure they are getting the most value out of their software by ensuring that the software they are using best meets their business needs, and by taking advantage of new technology including, for example, cloud services. Taken together these make organizations more efficient and reduce costs. Studies show that organizations can achieve as much as 30 percent savings in annual software costs by implementing a robust SAM program.[17]

The survey also shows that SAM is a good investment. Based on information provided by respondents, IDC calculated that merely by increasing its software compliance rate by just 20 percent (for example, lowering an unlicensed software rate from 24 percent to 19 percent), an enterprise with annual revenue of $83 million — the average in our survey — could increase profits by an astounding 11 percent. These sizeable bottom-line benefits are estimated to be 29 times greater than the cost of replacing the unlicensed software needed to become 20 percent more compliant.[18]

ANECDOTAL EVIDENCE IN THE REAL WORLD

In Germany:

OSI International Foods, a company with more than 12,000 employees, reduced post-licensing costs by more than 30 percent by implementing a more effective software licensing model.[19]

In Russia:

Baltika Breweries is the leading Russian beer producer with eight separate breweries and a combination of both physical and cloud services. They launched a SAM program to optimize their IT infrastructure and saved $100,000 per year by moving business applications to the cloud.[20]

In the UK:

The University of Roehampt in London embarked on a SAM project to create a roadmap that identified both legacy software that was no longer used and over-licensed software. It enabled them to embark on a plan to reinvest savings into newer, more capable, and more secure technology. Over the project's lifetime, it is projected to save as much as $5 million.[21]

In the US:

Government agencies can benefit, too. For example, NASA has saved more than $100 million over the last six years by implementing SAM best practices across its divisions.[22] With a little work up front, NASA was able to achieve huge benefits from its digital transformation across its business, saving taxpayer dollars.

GOVERNMENTS CAN TAKE PRAGMATIC STEPS TO EXPAND THE BENEFITS FROM SOFTWARE

In addition to the steps organizations can and should be taking, governments also have within their reach a set of common sense and concrete steps they can take to reduce their unlicensed software rate and bring greater resiliency to their economic sector. These proactive government-led efforts (as described in more detail on page 15) include leading by example, improving governments' own software asset management, and ensuring that government contractors also use only authorized software.

To help governments make the move, BSA has developed a useful guide that they can use to improve their own software asset management.[23] By making clear that the government itself will only rely upon legitimate software and do business only with contractors that do the same, they send a strong and clear message that can catalyze action in both the public and private sectors.

RATES AND COMMERCIAL VALUES OF UNLICENSED PC SOFTWARE INSTALLATIONS

	RATES OF UNLICENSED SOFTWARE INSTALLATION				COMMERCIAL VALUE OF UNLICENSED SOFTWARE ($M)			
	2017	2015	2013	2011	2017	2015	2013	2011
ASIA PACIFIC								
Australia	18%	20%	21%	23%	$540	$579	$743	$763
Bangladesh	84%	86%	87%	90%	$226	$236	$197	$147
Brunei	64%	66%	66%	67%	$18	$19	$13	$25
China	66%	70%	74%	77%	$6,842	$8,657	$8,767	$8,902
Hong Kong	38%	41%	43%	43%	$277	$320	$316	$232
India	56%	58%	60%	63%	$2,474	$2,684	$2,911	$2,930
Indonesia	83%	84%	84%	86%	$1,095	$1,145	$1,463	$1,467
Japan	16%	18%	19%	21%	$982	$994	$1,349	$1,875
Malaysia	51%	53%	54%	55%	$395	$456	$616	$657
New Zealand	16%	18%	20%	22%	$62	$66	$78	$99
Pakistan	83%	84%	85%	86%	$267	$276	$344	$278
Philippines	64%	67%	69%	70%	$388	$431	$444	$338
Singapore	27%	30%	32%	33%	$235	$290	$344	$255
South Korea	32%	35%	38%	40%	$598	$657	$712	$815
Sri Lanka	77%	79%	83%	84%	$138	$163	$187	$86
Taiwan	34%	36%	38%	37%	$254	$264	$305	$293
Thailand	66%	69%	71%	72%	$714	$738	$869	$852
Vietnam	74%	78%	81%	81%	$492	$598	$620	$395
Other AP	87%	87%	91%	91%	$442	$491	$763	$589
TOTAL AP	57%	61%	62%	60%	$16,439	$19,064	$21,041	$20,998
CENTRAL AND EASTERN EUROPE								
Albania	74%	73%	75%	75%	$10	$10	$10	$6
Armenia	85%	86%	86%	88%	$17	$18	$26	$26
Azerbaijan	81%	84%	85%	87%	$50	$90	$103	$67
Belarus	82%	85%	86%	87%	$59	$76	$173	$87
Bosnia	61%	63%	65%	66%	$24	$24	$21	$15
Bulgaria	57%	60%	63%	64%	$72	$78	$101	$102
Croatia	50%	51%	52%	53%	$48	$49	$64	$74
Czech Republic	32%	33%	34%	35%	$149	$150	$182	$214
Estonia	41%	42%	47%	48%	$16	$16	$20	$25
FYROM	63%	64%	65%	66%	$15	$15	$19	$22
Georgia	81%	84%	90%	91%	$22	$25	$40	$52
Hungary	36%	38%	39%	41%	$104	$107	$127	$143
Kazakhstan	74%	73%	74%	76%	$62	$89	$136	$123
Latvia	48%	49%	53%	54%	$22	$23	$29	$32
Lithuania	50%	51%	53%	54%	$35	$37	$47	$44
Moldova	83%	86%	90%	90%	$35	$36	$57	$45
Montenegro	74%	76%	78%	79%	$6	$6	$7	$7
Poland	46%	48%	51%	53%	$415	$447	$563	$618
Romania	59%	60%	62%	63%	$151	$161	$208	$207
Russia	62%	64%	62%	63%	$1,291	$1,341	$2,658	$3,227
Serbia	66%	67%	69%	72%	$51	$54	$70	$104
Slovakia	35%	36%	37%	40%	$51	$55	$67	$68
Slovenia	41%	43%	45%	46%	$28	$30	$41	$51
Ukraine	80%	82%	83%	84%	$108	$129	$444	$647
Rest of CEE	86%	87%	89%	90%	$69	$70	$105	$127
TOTAL CEE	57%	58%	61%	62%	$2,910	$3,136	$5,318	$6,133
LATIN AMERICA								
Argentina	67%	69%	69%	69%	$308	$554	$950	$657
Bolivia	79%	79%	79%	79%	$94	$98	$95	$59
Brazil	46%	47%	50%	53%	$1,665	$1,770	$2,851	$2,848
Chile	55%	57%	59%	61%	$283	$296	$378	$382
Colombia	48%	50%	52%	53%	$241	$281	$396	$295
Costa Rica	58%	59%	59%	58%	$80	$90	$98	$62
Dominican Republic	75%	76%	75%	76%	$74	$84	$73	$93
Ecuador	68%	68%	68%	68%	$132	$137	$130	$92
El Salvador	80%	81%	80%	80%	$61	$63	$72	$58
Guatemala	78%	79%	79%	79%	$165	$169	$167	$116
Honduras	75%	75%	74%	73%	$32	$36	$38	$24
Mexico	49%	52%	54%	57%	$760	$980	$1,211	$1,249
Nicaragua	81%	82%	82%	79%	$20	$23	$23	$9
Panama	71%	72%	72%	72%	$112	$117	$120	$74
Paraguay	83%	84%	84%	83%	$76	$89	$115	$73
Peru	62%	63%	65%	67%	$190	$210	$249	$209
Uruguay	67%	68%	68%	68%	$51	$57	$74	$85
Venezuela	89%	88%	88%	88%	$317	$402	$1,030	$668
Other LA	82%	83%	84%	84%	$296	$331	$352	$406
TOTAL LA	52%	55%	59%	61%	$4,957	$5,787	$8,422	$7,459

	RATES OF UNLICENSED SOFTWARE INSTALLATION				COMMERCIAL VALUE OF UNLICENSED SOFTWARE ($M)			
	2017	2015	2013	2011	2017	2015	2013	2011
MIDDLE EAST AND AFRICA								
Algeria	82%	83%	85%	84%	$70	$84	$102	$83
Bahrain	52%	54%	53%	54%	$32	$34	$27	$23
Botswana	80%	79%	79%	80%	$22	$23	$20	$16
Cameroon	80%	82%	82%	83%	$20	$21	$9	$9
Egypt	59%	61%	62%	61%	$64	$157	$198	$172
Iraq	85%	85%	86%	86%	$107	$120	$116	$172
Israel	27%	29%	30%	31%	$165	$161	$177	$192
Ivory Coast	79%	80%	80%	81%	$21	$22	$24	$16
Jordan	55%	56%	57%	58%	$32	$34	$35	$31
Kenya	74%	76%	78%	78%	$99	$113	$128	$85
Kuwait	57%	58%	58%	59%	$86	$94	$97	$72
Lebanon	69%	70%	71%	71%	$61	$65	$65	$52
Libya	90%	90%	89%	90%	$66	$65	$50	$60
Mauritius	52%	54%	55%	57%	$6	$7	$7	$7
Morocco	64%	65%	66%	66%	$52	$57	$69	$91
Nigeria	80%	80%	81%	82%	$123	$232	$287	$251
Oman	60%	60%	60%	61%	$56	$59	$65	$36
Qatar	47%	48%	49%	50%	$64	$72	$77	$62
Reunion	38%	39%	39%	40%	$2	$2	$1	$1
Saudi Arabia	47%	49%	50%	51%	$356	$412	$421	$449
Senegal	74%	75%	77%	78%	$12	$12	$9	$9
South Africa	32%	33%	34%	35%	$241	$274	$385	$564
Tunisia	73%	74%	75%	74%	$39	$49	$66	$51
Turkey	56%	58%	60%	62%	$208	$291	$504	$526
UAE	32%	34%	36%	37%	$210	$226	$230	$208
Yemen	88%	87%	87%	89%	$10	$11	$9	$15
Zambia	80%	81%	81%	82%	$4	$4	$3	$3
Zimbabwe	89%	90%	91%	92%	$7	$7	$4	$4
Other Africa	83%	84%	85%	86%	$364	$419	$484	$363
Other ME	85%	84%	85%	87%	$478	$569	$640	$536
TOTAL MEA	56%	57%	59%	58%	$3,077	$3,696	$4,309	$4,159
NORTH AMERICA								
Canada	22%	24%	25%	27%	$819	$893	$1,089	$1,141
Puerto Rico	41%	41%	42%	42%	$27	$28	$27	$44
United States	15%	17%	18%	19%	$8,612	$9,095	$9,737	$9,773
TOTAL NA	16%	17%	19%	19%	$9,458	$10,016	$10,853	$10,958
WESTERN EUROPE								
Austria	19%	21%	22%	23%	$121	$131	$173	$226
Belgium	22%	23%	24%	24%	$182	$190	$237	$252
Cyprus	44%	45%	47%	48%	$14	$14	$19	$19
Denmark	20%	22%	23%	24%	$167	$176	$224	$222
Finland	22%	24%	24%	25%	$166	$171	$208	$210
France	32%	34%	36%	37%	$1,996	$2,101	$2,685	$2,754
Germany	20%	22%	24%	26%	$1,566	$1,720	$2,158	$2,265
Greece	61%	63%	62%	61%	$173	$189	$220	$343
Iceland	44%	46%	48%	48%	$12	$10	$12	$17
Ireland	29%	32%	33%	34%	$79	$87	$107	$144
Italy	43%	45%	47%	48%	$1,278	$1,341	$1,747	$1,945
Luxembourg	17%	19%	20%	20%	$20	$21	$30	$33
Malta	43%	44%	44%	43%	$4	$4	$5	$7
Netherlands	22%	24%	25%	27%	$448	$481	$584	$644
Norway	21%	23%	25%	27%	$159	$178	$248	$289
Portugal	38%	39%	40%	40%	$137	$145	$180	$245
Spain	42%	44%	45%	44%	$859	$913	$1,044	$1,216
Sweden	19%	21%	23%	24%	$260	$288	$397	$461
Switzerland	21%	23%	24%	25%	$399	$448	$469	$514
United Kingdom	21%	22%	24%	26%	$1,421	$1,935	$2,019	$1,943
TOTAL WE	26%	28%	29%	32%	$9,461	$10,543	$12,766	$13,749
TOTAL WORLDWIDE	37%	39%	43%	42%	$46,302	$52,242	$62,709	$63,456
European Union	28%	29%	31%	33%	$9,982	$11,060	$13,486	$14,433
BRIC Countries*	60%	64%	67%	70%	$12,272	$14,452	$17,187	$17,907

*BRIC Countries are Brazil, Russia, India, and China.

Global Trends

Around the world, years of education and enforcement, and a growing understanding of the benefits of properly managing software assets, have led to a modest decrease in unlicensed software use. From 2015 to 2017, the worldwide unlicensed software rate declined 2 percentage points from 39 percent to 37 percent and the commercial value of unlicensed software dropped 8 percent in constant currency to $46.3 billion globally.

Although some of the decline in the unlicensed software rate comes from declining PC shipments, IDC estimates that roughly 60 percent of the drop comes from increased software compliance, suggesting that many are now coming to understand that improving software compliance can make sense for business. Despite this progress, the majority of software in more than half of the markets surveyed is unlicensed — demonstrating the need for continued progress.

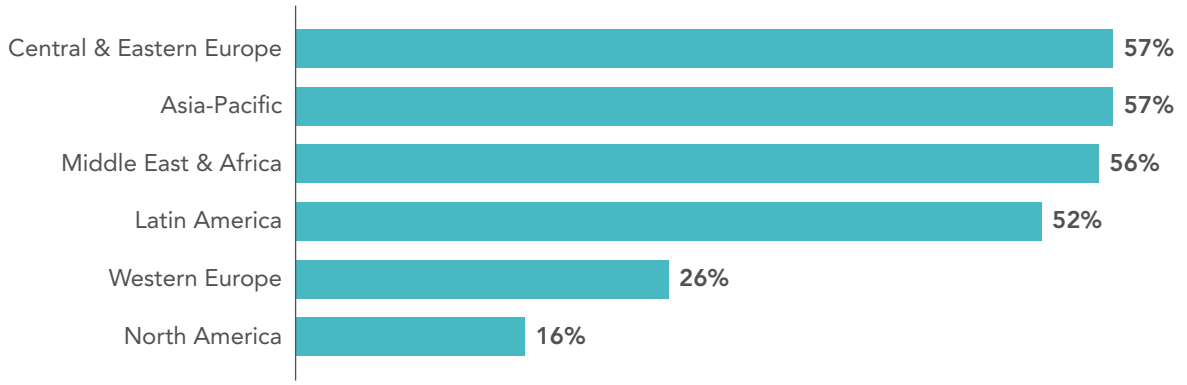
Although the unlicensed software rate dropped across all regions, it would have dropped significantly more except for emerging markets, which have a higher than normal unlicensed use rate of 61 percent, and account for a larger share of unlicensed software (75 percent) in 2017 than in 2015 (70 percent).

Around the globe, unlicensed rates dropped in 101 markets and rose in only six. Twelve countries saw their rates decline by 3 percentage points in 2017,[24] while China and Vietnam saw four-point drops — largely reflecting the fact that they started with high rates to begin with. On a percentage basis — the 2017 rate divided by the 2015 rate — the biggest drops were in developed counties, with the US, Australia, Austria, Japan, Luxembourg, New Zealand, Singapore, and Sweden all dropping 10 percent or more — helping them achieve both economic and cybersecurity gains.

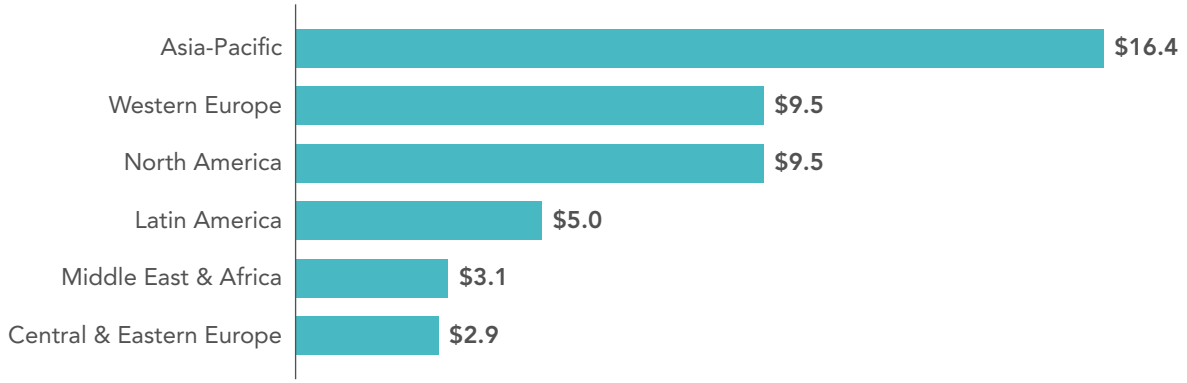
EVERY REGION BENEFITS WHEN UNLICENSED SOFTWARE RATES DECLINE

- **Asia-Pacific:** With 57 percent of its software unlicensed, the Asia-Pacific region is tied with the highest overall rate in the world despite a four-point decline from 2015. As a result, the region's unlicensed software has a staggering commercial value of $16.4 billion — far beyond any other region in the world and representing more than one-third of global commercial value of unlicensed software. Within the region, $6.8 billion worth of the unlicensed commercial value comes from China alone.
- **Central and Eastern Europe:** The Central and Eastern Europe region is tied with the Asia-Pacific region for the highest overall rate of unlicensed software at 57 percent — down just 1 percent from 2015. Within the region, there are vast differences in how extensively unlicensed software is used. At 85 percent, Armenia has the highest rate of unlicensed software in the region followed by Moldova at 83 percent, and Belarus at 82 percent. In contrast, the Czech Republic has the lowest rate in the region at 32 percent followed by Slovakia at 35 percent. However, with a commercial value of $1.3 billion, Russia continues to account for the largest dollar share of unlicensed software in the region.
- **Middle East and Africa:** In the Middle East and Africa, the overall rate fell one point to 56 percent despite having rates in two markets increase by one point and four markets that didn't change. The region is still just one percentage point lower than the highest rate in the world. Within the region, several countries are among the highest users of unlicensed software in the world including Libya at 90 percent, and Zimbabwe at 89 percent. By contrast the United Arab Emirates (32 percent), South Africa (32 percent), and Israel (27 percent) are enjoying greater benefits from licensed software.

Average Rate of Unlicensed Software Use



Commercial Value of Unlicensed Software Use (in Billions)



- **Latin America:** Within the Latin America region, 52 percent of software is unlicensed, a three-point reduction since the 2015 survey. This unlicensed software has a commercial value of nearly $5 billion. The countries with the highest rates include Venezuela at 89 percent (second highest rate in the world), Nicaragua at 81 percent, and El Salvador at 80 percent. By contrast, Brazil at 46 percent, Columbia at 48 percent, and Mexico at 49 percent now can take advantage of the benefits of a lower unlicensed rate. In fact, Mexico achieved a three-point drop in its unlicensed rate since 2015. Even though Brazil now has the lowest rate in the region, as the biggest country it accounts for $1.7 billion in commercial value of unlicensed software — the largest in the region.
- **Western Europe:** In Western Europe, the overall unlicensed rate dropped two points to 26 percent. Ireland achieved the largest drop — down three points — to obtain a 29 percent unlicensed rate. Greece continues to be the outlier in the region with an outsized 61 percent unlicensed rate. Several countries in the region have been able to maximize their value from commercial software and reduce their cybersecurity risks by working to keep their unlicensed software rates among some of the world's lowest — including Luxembourg at 17 percent, Sweden at 19 percent, Austria at 19 percent, Denmark and Germany at 20 percent, and Switzerland at 21 percent. Sixteen of the 20 countries studied dropped two or more points from 2015.
- **North America:** North America continues to have the lowest regional rate at 16 percent, although because of its size it still constitutes a significant commercial value of $9.5 billion.

Software Asset Management: How to Protect Your Organization From Risk and Increase Value

Businesses have globally applicable best practices that they can apply today to continuously maximize the benefits they derive from their technology assets and reduce the malware risks associated with unlicensed software. Studies show that organizations can achieve as much as 30 percent savings in annual software costs by implementing a robust software asset management (SAM) program.[25]

The 2017 edition of the ISO/IEC 19770-1 standard provides a holistic approach to implementing an effective ISO-aligned system for SAM. Implementing the standard enables continuous process improvement across three progressive implementation tiers. This tiered approach enables organizations to stage their implementation as appropriate. The standard contemplates application of these tiers through an industry-standard process of (1) creating a comprehensive implementation plan tailored to the selected tier; (2) executing the plan in a controlled, disciplined manner; (3) evaluating progress against the plan; and (4) adjusting the plan as necessary to ensure continuous improvement.

TIER 1

TRUSTWORTHY DATA

The first stage involves gaining a thorough understanding of what you have so you can manage it comprehensively. It begins by assessing the software on the system to enable compliance with software license agreements. In addition to license management, this tier also enables organizations to develop the processes necessary for change management, data management, and security management.

TIER 2

LIFE CYCLE INTEGRATION

The second stage builds upon the first, and helps organizations achieve greater efficiency and cost-effectiveness by improving management across the entire IT asset life cycle — from specification, to acquisition, development, release, deployment, operation and retirement.

TIER 3

OPTIMIZATION

The third stage helps organizations achieve greater efficiency and cost effectiveness by focusing on functional areas like contracts and financial management.

STEPS GOVERNMENTS CAN TAKE

In order to unlock the vast new jobs, tax-base enhancements, and economic benefits that come from organizations that are able to take full advantage of the latest technology-driven advancements, governments have a set of common sense and concrete steps they can take to reduce their unlicensed software rate and bring greater resiliency to their economic sector.

1 LEAD BY EXAMPLE:

Governments are the largest users of software in the world. As with all organizations, they can benefit from reducing risks, improving their technology accountability, and adopting SAM practices. Governments can also promote SAM and use of fully licensed software in state-owned enterprises, and among contractors and suppliers.

2 INCREASE PUBLIC EDUCATION AND AWARENESS:

Governments, accounting and auditing professionals, industry consultants, trade associations, and business organizations should educate organizations about software license compliance and the dangers of unlicensed software installation and usage.

3 MODERNIZE LAWS TO ACCOUNT FOR NEW INNOVATIONS:

With the advent of cloud computing and the proliferation of networked mobile devices, software is being stored, delivered, and used in innovative new ways. Policymakers should ensure it is protected regardless of the format or means of delivery.

4 CREATE A CONDUCIVE ENVIRONMENT FOR ENFORCEMENT:

Governments should ensure that legal frameworks provide effective means for redress and promote collaboration among stakeholders to reduce software copyright infringement.

ACCELERATING OPPORTUNITIES IN TRANSITIONING TO THE CLOUD

The cloud is emerging as one of the most transformative technologies in a generation because it fundamentally revolutionizes the way computing resources are bought, sold, and delivered. It enables almost anyone — whether a small business or a growing company — to access technology once only available to large organizations. This cloud-enabled digital empowerment has led to an explosion in the quantity, quality, and variety of cloud-based services that companies use today. It is estimated that the number of cloud-based applications used by an average enterprise tripled over three years.[26] In many cases the cloud is delivering traditional and enhanced software functionality as a service accessed through the Internet. In fact, IDC estimates that the cloud now delivers 22 percent of software functionality worldwide.

Businesses are flocking to these cloud services because of their innate ability to cut costs, improve agility, reduce complexity, and boost security.

- **THE CLOUD IS COST EFFICIENT:** IT organizations that have successfully transitioned to the cloud enjoy 21 percent lower IT costs on average than industry peers who continue to operate large data centers and host most of their applications on premise.[27] These leaders are discovering that the cloud enables organizations to reduce their IT costs by avoiding the expensive capital investments necessary to upgrade and maintain their existing hardware infrastructure. Organizations are also lowering costs because the cloud gives them the ability to pay only for the resources they need, while at the same time gaining access to nearly infinite computing and storage capacity over the Internet.
- **THE CLOUD IS SECURE AND FLEXIBLE:** The cloud's unique architecture also provides unprecedented new flexibility not only by changing the way computing resources can be bought, sold, and delivered, but also by enabling applications to be accessed any time, from any device, from anywhere around the globe. For some, the cloud's greatest advantage is the major security improvements it offers over traditional models. Cloud providers can see across a broader threat landscape to identify risks earlier and deploy more sophisticated security technologies than an individual customers could afford on their own. They are also able to maximize security by deploying advanced threat protection technologies, encrypting data at rest and in transit, and automating updates to more quickly protect systems from newly discovered threats. Together these capabilities can improve the resiliency of data and strengthen an organization's security.
- **SAM CAN ENABLE OPPORTUNITIES TO MIGRATE TO THE CLOUD:** As the cloud offers businesses unparalleled potential to drive new digital opportunities throughout the enterprise, SAM has become a critical enabler for accelerating the transition to the cloud. SAM helps organizations improve their cloud readiness in several key ways. It helps organizations optimize their licensing strategy, gain new insights into the additional savings achievable by moving to the cloud, and develop the strategy needed to become cloud ready. Only with such a strategy in place can enterprises achieve the full potential from what cloud services can enable. For example, the University of Roehampton in southwest London took advantage of SAM by developing a comprehensive cloud migration strategy. By enabling a smooth migration of a majority of the university's IT infrastructure to the cloud, it was able to avoid major new investments in data center hardware, gain new flexibility and scalability, improve security, and achieve savings of as much as 40 percent over 10 years — or about $4.7 million.[28]

At a time when many organizations are turning to the cloud to give them a strategic advantage in the marketplace, they often are looking for the foundational steps necessary to make a smooth transition. Implementing SAM helps companies to accelerate the transformational benefits they can achieve by migrating to the cloud.

Methodology

The BSA Global Software Survey quantifies the volume and value of unlicensed software installed on PCs across more than 110 national and regional economies in a given year — in this case, 2017. It also includes a global survey — with more than 22,500 responses from consumers and employees in 32 countries who use PCs at home or at work — to provide key insights into the attitudes around software licensing and new insights on the direct economic impact of lowering unlicensed software use. To compile the report, BSA worked closely with IDC, one of the world's leading independent research firms, to measure, understand, and evaluate licensed and unlicensed software use globally.

Measuring the scale and scope of unlicensed software use clearly has its challenges. Although this study is considered to be one of the most sophisticated appraisals of global copyright infringement, BSA and its partners continually look for new ways to improve the data reliability. In 2011, in partnership with two prominent IT economic researchers, BSA made several modifications designed to refine the inputs and ensure the most accurate estimation of unlicensed software use possible.

GLOBAL SURVEY OF SOFTWARE USERS

A key component of the BSA Global Software Survey is a global survey of more than 22,500 home and enterprise PC users, conducted by IDC in November 2017. The survey was conducted online or by phone in 32 markets that make up a globally representative sample of geographies, levels of IT sophistication, and geographic and cultural diversity. In addition, a parallel survey was carried out among 2,300 IT managers in 23 countries.

The surveys are used, in part, to determine the "software load" for each country — that is, a picture of the number of software programs installed per PC, including commercial, open-source, and mixed-source programs. Respondents are asked how many software packages, and what type, were installed on their PC in the previous year; what percentage were new or upgrades; whether they came with the computers or not; and whether they were installed on a new computer or one acquired prior to 2017. These questions are asked of both consumers and business users.

In addition, the surveys are used to assess key social attitudes and behaviors related to intellectual property, unlicensed software use, and other emerging technology issues. This insight provides fresh perspective each year on the dynamics underlying unlicensed software use around the world.

Survey countries are selected using a rotational strategy to maximize worldwide coverage year over year. Eleven priority markets are surveyed in concurrence with each study cycle and 52 countries are surveyed at least once every two to three cycles. The remaining countries are selected on an ad hoc basis. In any given study cycle, the total survey population accounts for more than 85 percent of total software units deployed and around 90 percent of paid-for units, while ensuring that most markets are surveyed at least once every three study years.

CALCULATING RATES OF UNLICENSED SOFTWARE INSTALLATION

Since 2003, BSA has worked with IDC, the leading provider of market statistics and forecasts to the IT industry, to determine rates of unlicensed software use and the commercial value of those unlicensed installations.

The basic method for coming up with the rate and commercial values in a country is as follows:

1. Determine how much PC software was deployed during the year by consumers and business users.
2. Determine how much was paid for or otherwise legally acquired during the year (such as through an open-source, free, or complementary license), again segmented by business and consumer usage.
3. Subtract one from the other to get the amount of unlicensed software. Once this amount is known, the unlicensed rate is computed as a percentage of total software installed.

Unlicensed Rate
=
Unlicensed Software Units /
Total Software Units Installed

Total Software Units Installed
=
 # PCs Getting Software X
Software Units per PC

To calculate the total number of software units installed — the denominator — IDC determines how many computers there are in a country and how many of those received software during the year. IDC tracks this information in quarterly research products called "PC Trackers" that cover 92 countries. The remaining few countries are researched annually for this study.

Once IDC has determined how many computers there are, both consumer PCs and business PCs, and using the software load data collected in the survey, it can determine the total software units installed — licensed and unlicensed — in each country.

To estimate the software load in countries not surveyed, IDC uses a cluster analysis technique to find like characteristics with countries with varying software loads and uses these characteristics to assign loads to countries not surveyed. IDC validates this by looking at correlations between the known software loads from surveyed countries and their scores on an emerging market measure published by the International Telecommunications Union, called the ICT Development Index, and dividing them into cohorts in order to compare them to unsurveyed countries.

To get the number of unlicensed software units — the numerator of the equation — IDC must determine the value of the legally acquired software market. IDC routinely publishes software market data from about 80 countries and studies roughly 20 more on a custom basis. For the few remaining countries, IDC conducts annual research for the purposes of this study. This research provides the value of the legally acquired software market. The value is broken down by consumer and business users.

To convert the software market value to number of units, IDC computes an average price per software unit for all of the consumer and business PC software in the country. This is done by developing a country-specific matrix of software prices — such as retail, volume-license, OEM, free, and open-source — across a matrix of products, including security, office automation, operating systems, and more.

IDC's pricing information comes from its pricing trackers and from local analysts' research. The weightings — OEM versus retail, consumer versus business — are taken from IDC surveys. IDC multiplies the two matrices to get a final, blended average software unit price.

To arrive at the total number of legitimate software units, IDC applies this formula:

Legitimate Software Units
=
Software Market Value /
Average Software Unit Price

In 2011, IDC implemented several measures to validate its calculations of average software unit price. Analyst teams in 25 countries have provided additional information on software price by category and user (consumer or business) and estimates of acquisition type (e.g., retail, volume license, free/

open-source) to serve as a cross-check against IDC's computed values. Rotating the countries for which information is collected each year allows IDC to recalibrate software prices periodically and provides a more accurate estimate of legitimate software units from industry revenues.

Finally, subtracting the number of legitimate software units from the total software units reveals the number of unlicensed software units installed during the year.

Unlicensed Software Units
=
Total Software Units Installed
–
Legitimate Software Units

This process provides the underlying data for the basic rate equation.

CALCULATING THE COMMERCIAL VALUE OF UNLICENSED SOFTWARE

The commercial value of unlicensed software provides another measure of the scale of unlicensed software use and allows for important year-over-year comparisons of changes in the software landscape.

It is calculated using the same blend of prices by which IDC determines the average software unit price, including retail, volume license, OEM, free, open-source, consumer or business, etc. The average software unit price is lower than retail prices one would find in stores.

Having calculated the total units of software installed, as well as the number of legitimate and unlicensed software units installed and the average price per software unit, IDC is able to calculate the commercial value of unlicensed software.

WHAT SOFTWARE IS INCLUDED

The BSA Global Software Survey calculates unlicensed installations of software that runs on PCs — including desktops, laptops, and ultra-portables, such as netbooks.

It includes operating systems, systems software such as databases and security packages, business applications, and consumer applications such as games, personal finance, and reference software. The study also takes into account the availability of legitimate, free software and open-source software, which is software licensed in a way that puts it into the public domain for common use. It is typically free but also can be used in commercial products.

It does NOT include software loaded onto tablets or smartphones. It also excludes software that runs on servers or mainframes and routine device drivers, as well as free downloadable utilities, such as screen savers, that would not displace paid-for software or normally be recognized by a user as a software program.

The study includes cloud computing services such as software-as-a-service (SaaS) and platform as-a-service (PaaS) that could replace software that would otherwise be installed on personal computers. Software sold as part of legalization programs — such as a bulk sale for a government to distribute to schools — also is included in the study.

THE EFFECT OF EXCHANGE RATES

Prior to 2009, dollar figures in the value tables were in current dollars from the year before. For example, the 2007 value of unlicensed software was published in 2006 dollars for easier year-on-year comparison. In 2009, BSA made a decision to publish value figures in the current dollars of the year being studied. Thus, 2009 values are in 2009 dollars, 2017 values in 2017 dollars, etc. We do not restate previous values in current dollars.

This is important when evaluating changes in the values over time. Some of the changes will be based on real market dynamics, some on exchange rate fluctuations from year to year.

ENDNOTES

[1] "Gartner Says Organizations Can Cut Software Costs by 30 Percent Using Three Best Practices," Gartner (July 19, 2016), available at www.gartner.com/newsroom/id/3382317 and "Demonstrating the Business Value of Software Asset Management and Software License Optimization," Gartner, available at http://imagesrv.gartner.com/media-products/pdf/flexera/flexera_issue1.pdf.

[2] McAfee Labs Threat Report (March 2018), available at https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2018.pdf.

[3] "Cyber-Attacks Occurring More Frequently and With Greater Sophistication, NTT Security Report Finds," Security InfoWatch (August 9, 2017), available at www.securityinfowatch.com/press_release/12358487/cyber-attacks-occurring-more-frequently-and-with-greater-sophistication-ntt-security-report-finds.

[4] *Internet Security Threat Report*, Symantec (April 2017), available at www.symantec.com/security-center/threat-report.

[5] In 2015, 43 percent of cyber-attacks worldwide were against small businesses with less than 250 workers. Elizabeth MacDonald, "Cyber Attacks on Small Businesses on the Rise," *Fox Business* (April 26, 2016), available at www.foxbusiness.com/features/cyber-attacks-on-small-businesses-on-the-rise.

[6] *Internet Security Threat Report*, Symantec (April 2017), available at www.symantec.com/security-center/threat-report.

[7] Ponemon Institute, *2017 Cost of Cyber Crime Study*, available at www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf.

[8] "Global Cybercrime Costs Top $600 Billion," DarkReading (February 21, 2018), available at https://www.darkreading.com/attacks-breaches/global-cybercrime-costs-top-$600-billion-/d/d-id/1331106.

[9] M-Trends 2013: Attack the Security Gap, Mandiant (2013), available at https://www.fireeye.com/current-threats/annual-threat-report/mtrends/rpt-2013-mtrends.html.

[10] Ponemon Institute, *2017 Cost of Cyber Crime Study*, available at www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf.

[11] Paul Mozur, "China, Addicted to Bootleg Software, Reels From Ransomware Attack," *New York Times* (May 15, 2017), available at www.nytimes.com/2017/05/15/business/china-ransomware-wannacry-hacking.html.

[12] "China's Fondness for Pirated Software Raises Risks in Attack," *Phys Org* (May 16, 2017), available at https://phys.org/news/2017-05-china-fondness-pirated-software.html.

[13] "Jakub Kroustek, a malware researcher with Avast, a security software company in the Czech Republic, said in a blog post that Russia was the most-affected country so far [from a malware attack]."Elizabeth Dwoskin and Karla Adam, "More Than 150 Countries Affected by Massive Cyberattack, Europol Says," *Washington Post* (May 14, 2017), available at https://www.washingtonpost.com/business/economy/more-than-150-countries-affected-by-massive-cyberattack-europol-says/2017/05/14/5091465e-3899-11e7-9e48-c4f199710b69_story.html.

[14] International Organization for Standardization, *ISO/IEC 19770-1:2017 Information Technology—IT Asset Management*, available at www.iso.org/standard/68531.html.

[15] "Equifax Breach to Cost Total of $439M," PYMNTS (March 5, 2018), available at www.pymnts.com/news/security-and-risk/2018/equifax-cost-275m/.

[16] "How Could ITAM Have Helped the Equifax CIO?" *The ITAM Review* (October 19, 2017), available at www.itassetmanagement.net/2017/10/19/equifax-itam/.

[17] "Gartner Says Organizations Can Cut Software Costs by 30 Percent Using Three Best Practices," Gartner (July 19, 2016), available at www.gartner.com/newsroom/id/3382317 and "Demonstrating the Business Value of Software Asset Management and Software License Optimization," Gartner, available at http://imagesrv.gartner.com/media-products/pdf/flexera/flexera_issue1.pdf.

[18] These important benefits are derived from the combination of better security by reducing malware that may accompany unlicensed software, fewer disruptive audits that take precious time to respond to, reduced legal risks around license compliance violations, better IT productivity by eliminating outdated or unsupported software, more trusted brand identity by avoiding risky behavior, and better relationships with vendors.

[19] With a more effective licensing model in place, OSI reduced costs by more than 30 percent and achieved 100 percent compliance with Microsoft guidelines. See "OSI International Foods Increases Software License Visibility and Reduces Costs by 30 Percent," Microsoft Customer Solution Case Study, available at http://download.microsoft.com/download/7/F/1/7F18B556-BC4D-4B5C-BAB8-9386515BF1EB/Germany-OSI_International_Foods.doc.

[20] Baltika conducted a SAM project that now saves them $100,000 per year in the workstation, software, and servers. See "Baltika Breweries Unlocks the Power of Microsoft Technologies Through SAM," YouTube, available at www.youtube.com/watch?v=yocvI9nl8o0&feature=youtu.be; and "Software Asset Management Customer Evidence," Microsoft, available at www.microsoft.com/en-us/sam/customers.aspx.

[21] "University of Roehampton Benefits From Azure Migration Through Microsoft SAM," YouTube, available at https://www.youtube.com/watch?v=hAHHvZ_8zz4&feature=youtu.be; and "Software Asset Management Customer Evidence," Microsoft, available at https://www.microsoft.com/en-us/sam/customers.aspx.

[22] Using a specialized SAM tool and other strategies, the space agency uncovered software consolidation opportunities. For NASA, it meant eliminating duplicate software licenses and negotiating better prices for the software it already buys. "How NASA Saved $100 Million on Software Licenses," *FedTech* (February 23, 2017), available at https://fedtechmagazine.com/article/2017/02/how-nasa-saved-100-million-software-licenses.

[23] See BSA | The Software Alliance, *Government Guide for Software Asset Management*, available at www.bsa.org/~/media/Files/Tools_And_Resources/Guides/SoftwareManagementGuide/SoftwareManagementGuide_Government.pdf.

[24] Azerbaijan, Belarus, Bulgaria, Georgia, Hong Kong, Ireland, Mexico, Moldova, Philippines, Singapore, South Korea, and Thailand.

[25] "Gartner Says Organizations Can Cut Software Costs by 30 Percent Using Three Best Practices," Gartner (July 19, 2016), available at www.gartner.com/newsroom/id/3382317 and "Demonstrating the Business Value of Software Asset Management and Software License Optimization," Gartner, available at http://imagesrv.gartner.com/media-products/pdf/flexera/flexera_issue1.pdf.

[26] Ajmal Kohgadai, "12 Must-Know Statistics on Cloud Usage in the Enterprise," SkyHigh Networks, available at https://www.skyhighnetworks.com/cloud-security-blog/12-must-know-statistics-on-cloud-usage-in-the-enterprise/.

[27] "Cloud Users Enjoy Significant Savings," Computer Economics (April 2016), available at https://www.computereconomics.com/article.cfm?id=2185.

[28] Case Study: A Confident Move to the Cloud for the University of Roehampton," available at https://www.civica.com/globalassets/7.document-downloads/2.uk-docs/case-studies/roehampton-case-study.pdf.

ABOUT BSA | THE SOFTWARE ALLIANCE

BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life.

With headquarters in Washington, DC, and operations in more than 60 countries around the world, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

www.bsa.org

BSA Worldwide Headquarters

20 F Street, NW
Suite 800
Washington, DC 20001

+1.202.872.5500
@BSAnews
@BSATheSoftwareAlliance

BSA Asia-Pacific

300 Beach Road
#25-08 The Concourse
Singapore 199555

+65.6292.2072
@BSAnewsAPAC

BSA Europe, Middle East & Africa

65 Petty France
Ground Floor
London, SW1H 9EU
United Kingdom

+44.207.340.6080
@BSAnewsEU