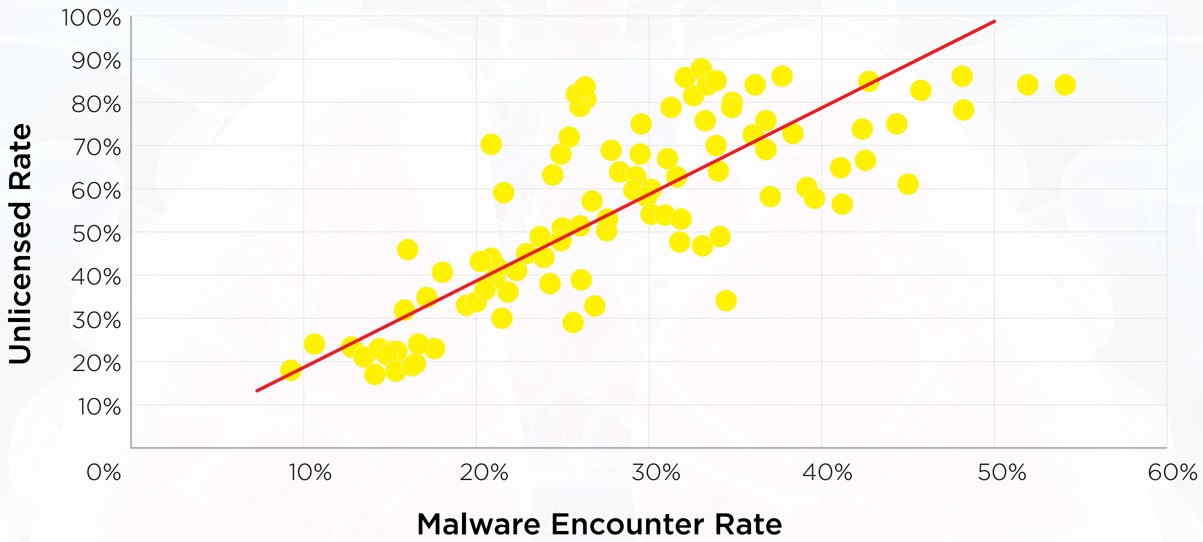
Causes and Costs of Security Threats from Pirated Software in Europe 2017

An IDC InfoBrief, sponsored by Microsoft | September 2017

The Strong Correlation Between Malware and Pirated Software

Malware Encounters and Unlicensed SW, 102 Countries



» **The correlation is strong (.77)**—stronger than that between smoking and lung cancer (.72)

» The R-squared is 0.60, which means that **60% of the malware encounter rate can be predicted by the unlicensed rate.**

» While correlation does not prove causation, the research supporting this report **does** prove it.

Data based on 2015 unlicensed SW Rates (BSA) and average quarterly malware encounter rates (2H 2015 and 1H 2016). Each dot represents a country.

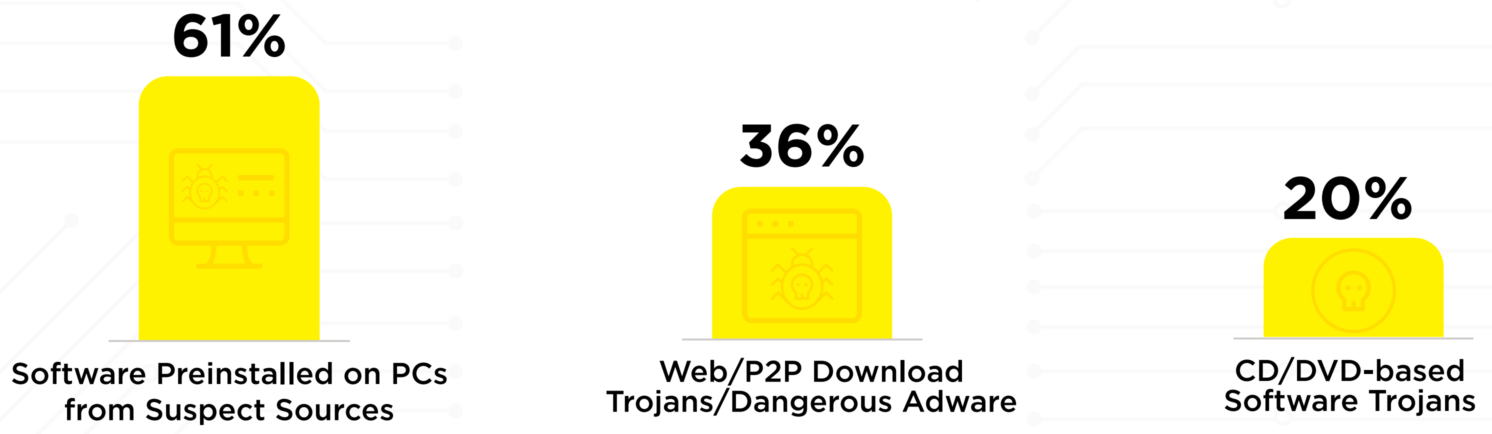
References:

BSA report "Unlicensed Software and Cybersecurity Threats," January 2015
(http://globalstudy.bsa.org/2013/malware/study_malware_en.pdf)

The New York Times, "China, Addicted to Bootleg Software, Reels from Ransomware Attack", May 15, 2017
(https://www.nytimes.com/2017/05/15/business/china-ransomware-wannacry-hacking.html?_r=0)

Cause of the Correlation: Malware Infection Rates of Pirated Software

Infection Rate by Pirated Software Source



- Malware can be transmitted by the sites from which pirated software is obtained, in the downloaded software, or in non-legitimate activation keys
- Malware may include dangerous adware, keystroke loggers, password and credential stealers, backdoors for hackers, and software that enables remote control of a PC

Based on IDC longitudinal study of infections on web/P2P sites offering pirate software and activation keys; supported by analysis of laptops obtained with pirated software on them conducted by the National University of Singapore.

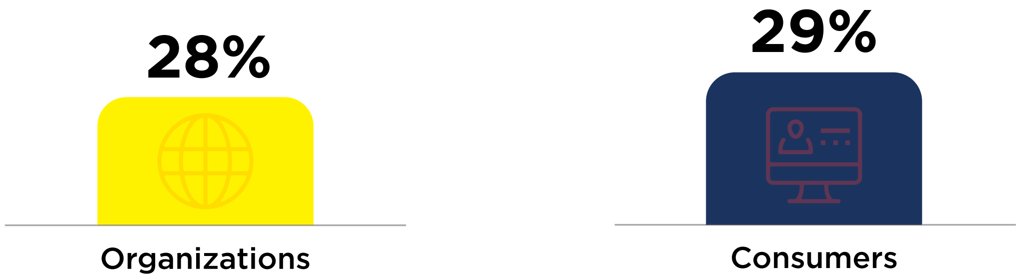
References:

IDC White Paper "The Link between Pirated Software and Cybersecurity Breaches," March 2014
(http://download.softwareculicenta.ro/raport-idc-2014-03.pdf)

Symantec report, "Underground Black Market: Thriving Trade in Stolen Data, Malware, and Attack Services," November 2015
(https://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services)

Chance of Infections from Pirated Software from All Sources?

Likelihood of Malware Infections in Europe from Pirated Software, 2017

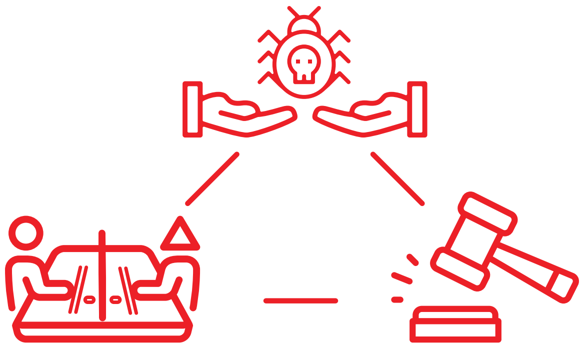


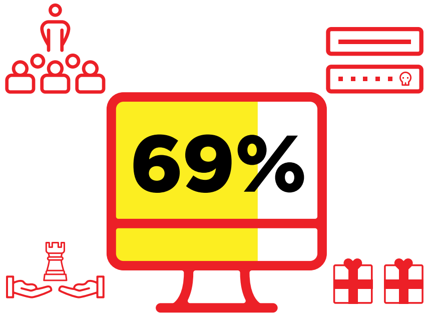
All sources of pirated software - comes with the PC, is downloaded from the internet (WEB or P2P), or is installed using media

- The likelihood of infection is about the same in all geographies and segments
- Infection rates are aggregated by source based on IDC research on software distribution

One in three unlicensed or pirated copies of PC software causes a malware infection!

The 1st Way Malware Invades: Software from Suspect Sources





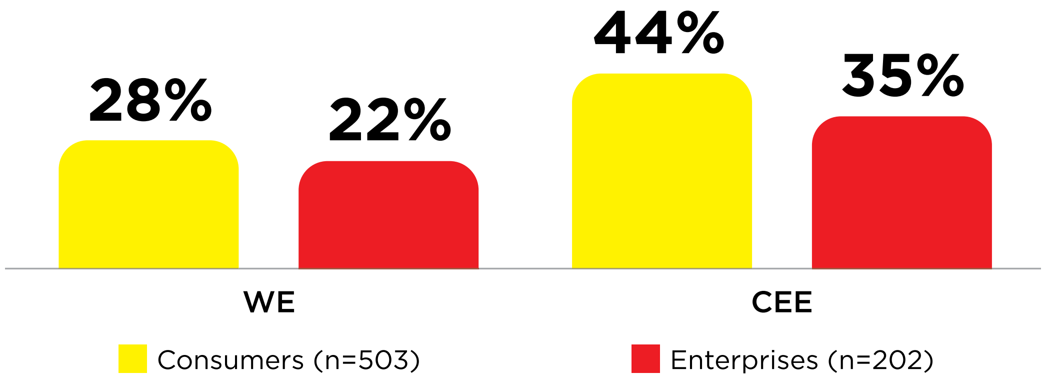
» 66% of European consumers had problems with software obtained from suspect sources—e.g., auction site or online supplier, borrowed from a friend, bought at a street market, etc.

» 69% of European consumer PCs bought in the last two years came from “risky” sources, too—e.g., consultants, online trading sites, gifts, PC assemblers, etc.

» 33% of organization PCs were obtained from suspect sources

The 2nd Way Malware Invades: Inattention to Security Updates

Chance of Malware Infections in Europe from Pirated Software, 2017



» Reasons for inattention to security updates range from **fear of being caught** with pirated software, to lack of processes and controls

» More than 2/3 of breaches take place after updates are available, but have not been applied

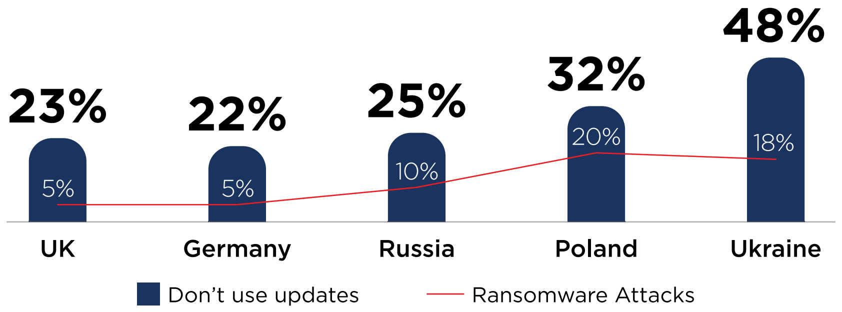
References:

Business Insider article, "The New Global Ransomware Attack Shows How Many People Still Don't Install Software Updates," June 28, 2017
(http://www.businessinsider.com/people-still-dont-install-software-updates-2017-6).

ZDNet article, "Seven Myths about Zero Day Exploits Debunked," August 3, 2010
(http://www.zdnet.com/article/seven-myths-about-zero-day-vulnerabilities-debunked/)

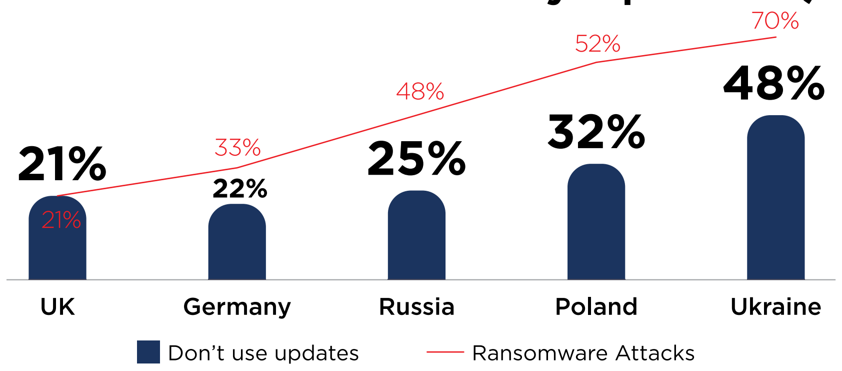
A Consequence of Security Update Negligence: Ransomware Attacks

Ransomware Attacks and Inattention to Security Updates (% Responding, n=202)



- The correlation between ransomware attacks and the inattention to security updates is high (0.79)
- Reasons users don't install updates vary from *"too much trouble,"* to fear of being discovered with pirated software
- The correlation between software problems is even higher (0.91)

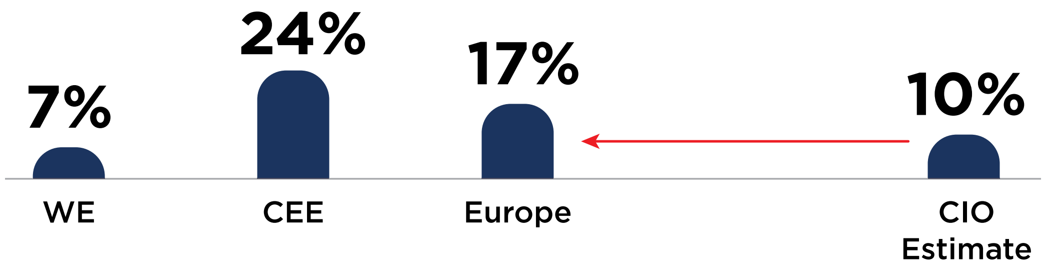
Problem Software* and Inattention to Security Updates (% Responding, n=202)



*Office pre-installed on PCs

The Trojan Horse of Malware Infections: Bring Your Own Software to Work

% of Employees Installing Software without Organization's Knowledge on Work PCs in the Last Two Years (n=369)

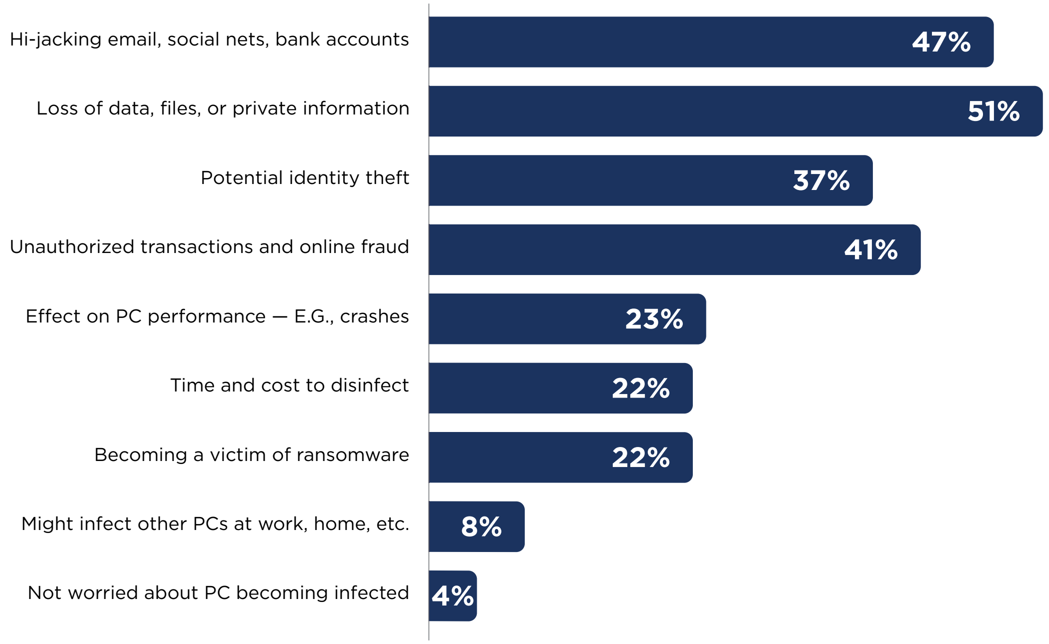


- CIO's underestimate the number of employees installing their own software.
- In Europe, nearly 50% of organizations don't monitor end-user software more than twice a year; less than half have a formal policy on end users installing software on work PCs
- BYO SW is costly: the 17% of European employees will add to the software installed on organizational PCs by 4%—but a good portion of that will be unlicensed and lack anti-malware vigilance. **Thus, BYOSW results in a 19% increase in infected software on organization PCs.**

Having processes to manage BYO software on enterprise PCs is a critical protection against malware effects

What European Consumers Fear Most from Infectious Pirated Software

Consumers’ Biggest Fears from Infectious Pirated Software Percent Responding % Responding (n=503)

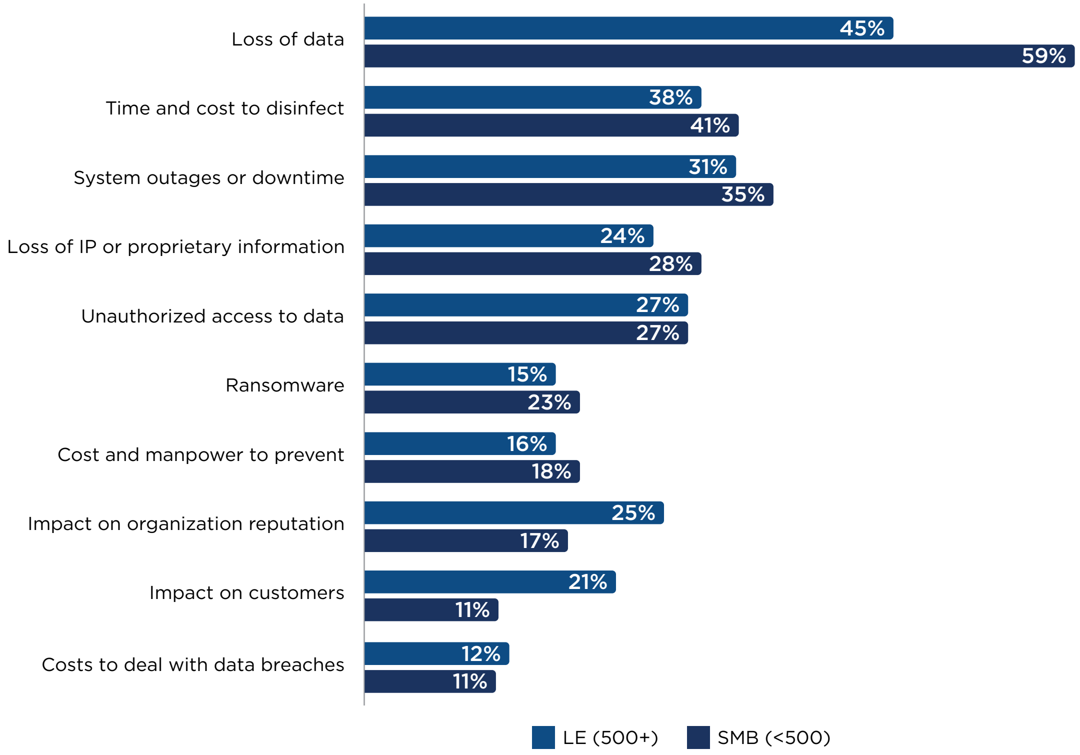


96% of consumers expressed worries about infected mis-licensed or pirated software

(Being under-licensed means using legitimate software on more PCs than licensed to use)

What European Organizations Fear Most from Infectious Pirated Software

European Enterprises' Biggest Fears from Infectious Software % Responding (n=202)



» 16% experienced a data breach, with an average of 3.7 breaches; average breach was 2,900 records

» Data breaches were 2.5 times more common on CEE than WE. However, the number of records lost per beach was 5 x as big in WE

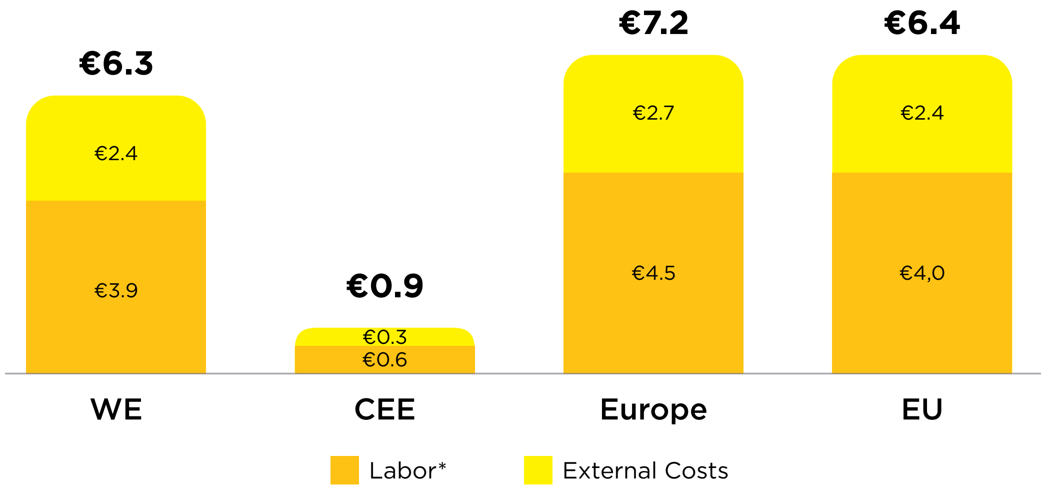
» 11% experienced a ransomware demand, with the average 4.1 demands in a year. The average ransomware demand was $1,395. However, only 18% of demands were paid

» Many users can avoid paying by reverting to back-up data or using tools to de-encrypt locked files. Microsoft, for instance, offers free tools, such as Windows Defender Online, that can help provide access to blocked files, as do other vendors

Data losses and breaches matter most

Cost to European Consumers from Infected Software: **€7.2 Billion, 319 Million Hours!**

European Consumers' Costs from Malware in Unlicensed PC Software (B Euro), 2017



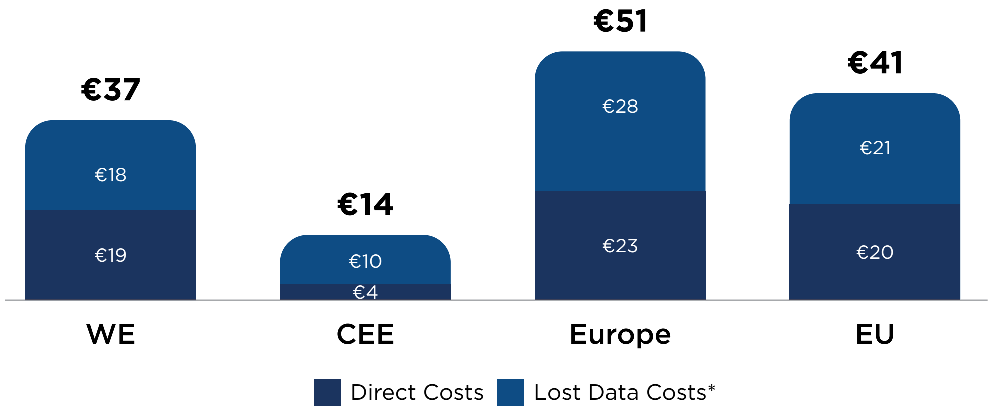
*labor costs at average 2017 salary for PC user

- Money and time are spent in identification, repair, recovering data, and dealing with Identity theft and ransomware
- Labor costs are valued at average worker hourly wages per country (2016 exchange rate)
- Total time lost is expected to be 319 million hours; losses equate to 10 hours per infected piece of software, or €231
- This analysis is built on averages, but per-costs may vary dramatically from the average. For example, according US statistics, half of identity theft victims deal with the associated problems in less than a day. But for 10% of them, it takes more than a month

The cost per infected unit can be many times the commercial price of legitimate software

Cost to European Organizations from Infected Software: **€51 Billion**

European Consumers' Costs from Malware in Unlicensed PC Software (B Euro), 2017



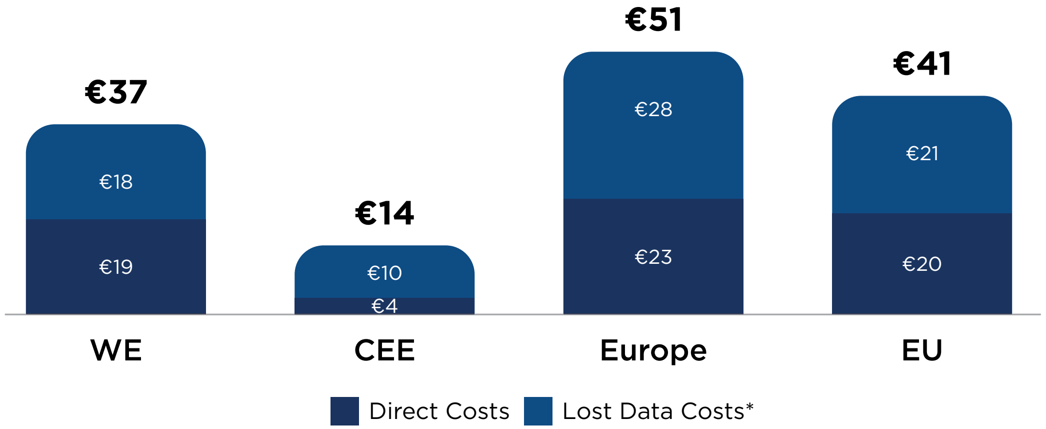
*assumes 1 in 1,000 infected SW units leads to a data breach

- Money and time are spent in identification, repair, recovering data, and dealing with ransomware; some is internal to the organization, some external
- Labor costs are valued at average IT hourly wages per country (2016 exchange rate)
- Total losses per infected unit is expected to be €6,220. This includes IT labor, external fees, a share of the IT budget for IT security, and fall-out from lost data
- Lost data costs assume that 1 in 1,000 infected unlicensed software programs leads to a data breach
- Lost data costs include remediation (finding and fixing the problems), customer outreach, fines, legal costs, and lost business. They do not include ransomware or catastrophic breaches of high value information (trade secrets, intellectual property, etc.)

The cost per infected unit can be many times the commercial price of legitimate software

Small and Midsize Organizations Incur the Highest Costs from Infected Software

European Consumers’ Costs from Malware in Unlicensed PC Software (Euro), 2017



*assumes 1 in 1,000 infected SW units leads to a data breach

- Small and medium organizations (SMOs) account for < 50% of deployed software to all organizations—but because of a higher piracy rate, more than 50% of pirated software
- Because of less attention to security updates, SMOs account for ~60% of infected pirated software in European organizations
- Small organizations account for 60% of total SMO costs

The smaller the organization, the greater the risk of economic damage from malware related to pirated software

IDC Recommends

» Acquire your PCs and software from trusted sources

» Beware of unlicensed or pirated software – make sure what you have is legitimate

» Install trusted security solutions

» Pay attention to security updates – don’t put them off

» Constantly monitor employee-installed software

» Back up data files in as real-time a fashion as possible

» Don’t pay ransomware – you can’t trust the perpetrators