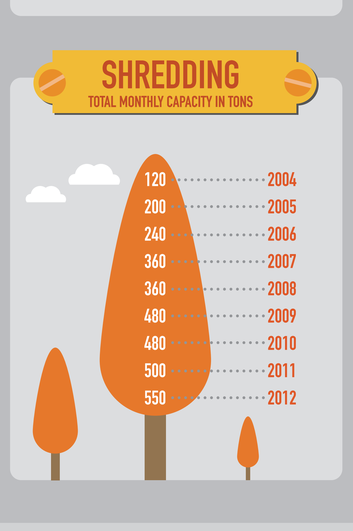
WHY CHOOSE KATANA AS AN ON-SITE SHREDDING SOLUTION

FLEET IN 2013

- 4X PAPER MOBILE SHREDDING TRUCKS
- 2X PAPER MOBILE SHREDDING TRUCKS – DIN 66399 – 2 LEVEL P4
- 1X PAPER MOBILE SHREDDING TRUCKS – RESERVE
- 1X HARD DRIVE MOBILE SHREDDING TRUCKS

SHREDDING

TOTAL MONTHLY CAPACITY IN TONS



WHO IS KATANA

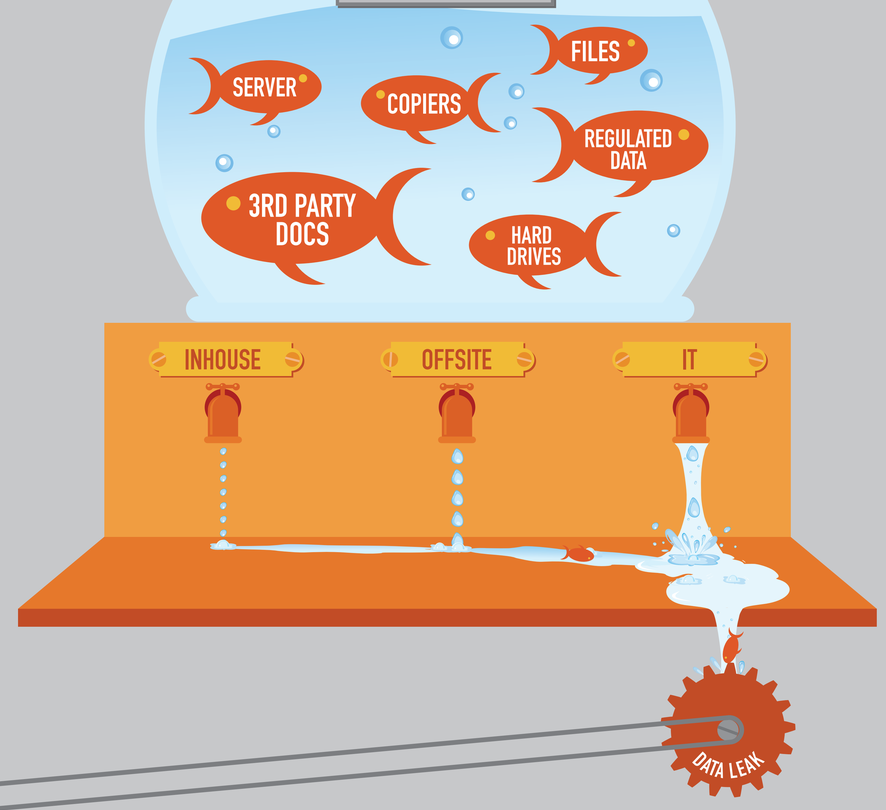
EMPLOYEES

- MANAGEMENT
- ADMINISTRATION
- SALES
- DRIVERS

KEY NUMBERS

- 8 MOBILE SHREDDING TRUCKS
- DIN (DIN 66399-2 LEVEL P4) SGS CERTIFIED SHRED SIZE (HIGH SECURITY)
- > 550 MONTHLY SHREDDING CAPACITY IN TONS
- > 2000 CLIENTS IN SWITZERLAND
- > 80 BANKS
- > 150 MULTINATIONALS
- 2004 ESTABLISHEMENT OF THE COMPANY
- 500K CAPITAL OF THE COMPANY

CONFIDENTIAL DATA



WHO CAN BENEFIT?

INSIDER

WHO: Disgruntled employees, contractors, whistleblowers.
OBJECTIVES: Score settling, leaks, money, "rights from wrongs"
TARGETS: Large companies, banking sector and service related companies.
SIGNATURE: Confidential ducuments support thefts (CD, Hard Drive, Paper)
CLASSIC CASE: Bradley Birkenfeld awarded 104 millions $ forwhistle blowing against UBS, Hervé Falciani / HSBC

ORGANIZED CRIME

WHO: Mafia groups (Eastern / Russian)
OBJECTIVES: Collecting data from any source such as paper, Hard Drive, Xerox machines to create data for virtual identity theft.
TARGETS: Banks and industry service related sectors, insurance, NGO.
SIGNATURE: Corruption of low / mid level employees, thefts of computers, hijacking of data
CLASSIC CASE: Purchase of old computers and Xerox machines to extract the data and create profiles.

GOVERNMENT

WHO: France, Germany, US, China
OBJECTIVES: Name and list of Tax payers, Intellectual Property
TARGETS: Banks and industry service related. Industrial espionage
SIGNATURE: Infiltration, press pressure, legitimization of illegal acts
CLASSIC CASE: France purchasing HSBC CD from Hervé Falciani. Germany openly offering $$$ rewards for any stolen information leading to tax recoveries.

HACKTIVIST

WHO: Anonymous, Antisec, ATAC, LulzSec
OBJECTIVES: Righting perceived wrongs, publicity, protecting internet freedoms
TARGETS: Corporations, governements
SIGNATURE: Leaking sensitive information, public shaming, creepy youtube videos.
CLASSIC CASE: Hacking Paypal website, Visa, Mastercard

OLD WAY VS NEW WAY OF VIEWING DATA THEFT

OLD WAY

"THIS WILL NEVER HAPPEN TO US."

DISORGANIZED, AMATEURISH HACKERS WORKING OUT OF THEIR HOMES, DOING IT FOR "FUN" RATHER THAN MONEY.

"THIS IS AN IT ISSUE."

NEGLIGIBLE IMPACT ON CUSTOMERS, EMPLOYEES, AND COMPANY COSTS.

"WE TRUST OUR EMPLOYEES TO SECURE OUR INFORMATION."

RISK EXPOSURES ARE SMALL AND MANAGEABLE.

"WE PASSED OUR AUDIT, SO WE'RE SAFE."

NEW WAY

COMPANIES OF ALL SIZES AND ACROSS ALL INDUSTRIES CONFRONT A REAL, GROWING, AND STRATEGIC RISK FROM DATA AND IDENTITY THEFT.

THEFT IS A LUCRATIVE BUSINESS FOR SOPHISTICATED, ORGANIZED CRIMINAL ENTERPRISES WORLDWIDE.

DATA LOSS COMMONLY OCCURS THROUGH PHYSICAL LOSS, DATA EXCHANGES, FRAUD, AND HUMAN ERROR, RATHER THAN JUST IT BREACHES.

LOSS OF PERSONAL DATA LEAVES CUSTOMERS AND EMPLOYEES AT RISK OF FRAUD AND PERSONAL IDENTITY THEFT.

EMPLOYEES AND COLLABORATION NETWORKS ARE THE MOST COMMON DATA LEAK SOURCES.

RISKS ARE SUBSTANTIAL, INCLUDING COMPROMISE OF COMPANY IT SYSTEMS, CUSTOMER LAWSUITS, EROSION OF BRAND REPUTATION, LOSS OF CUSTOMERS, GOVERNMENT FINES, AND NEW REGULATION.

DATA PROTECTION IS A CEO-LEVEL CONCERN.

SOME QUICK NUMBERS

THE MOST SENSITIVE TIME FOR INFORMATION THEFT IS WHEN AN EMPLOYEE LEAVES THE COMPANY.

32% OF WORKERS SURVEYED **HAVE ADMITTED TO STEALING CONFIDENTIAL CORPORATE INFORMATION** ON AT LEAST ONE OCCASION.

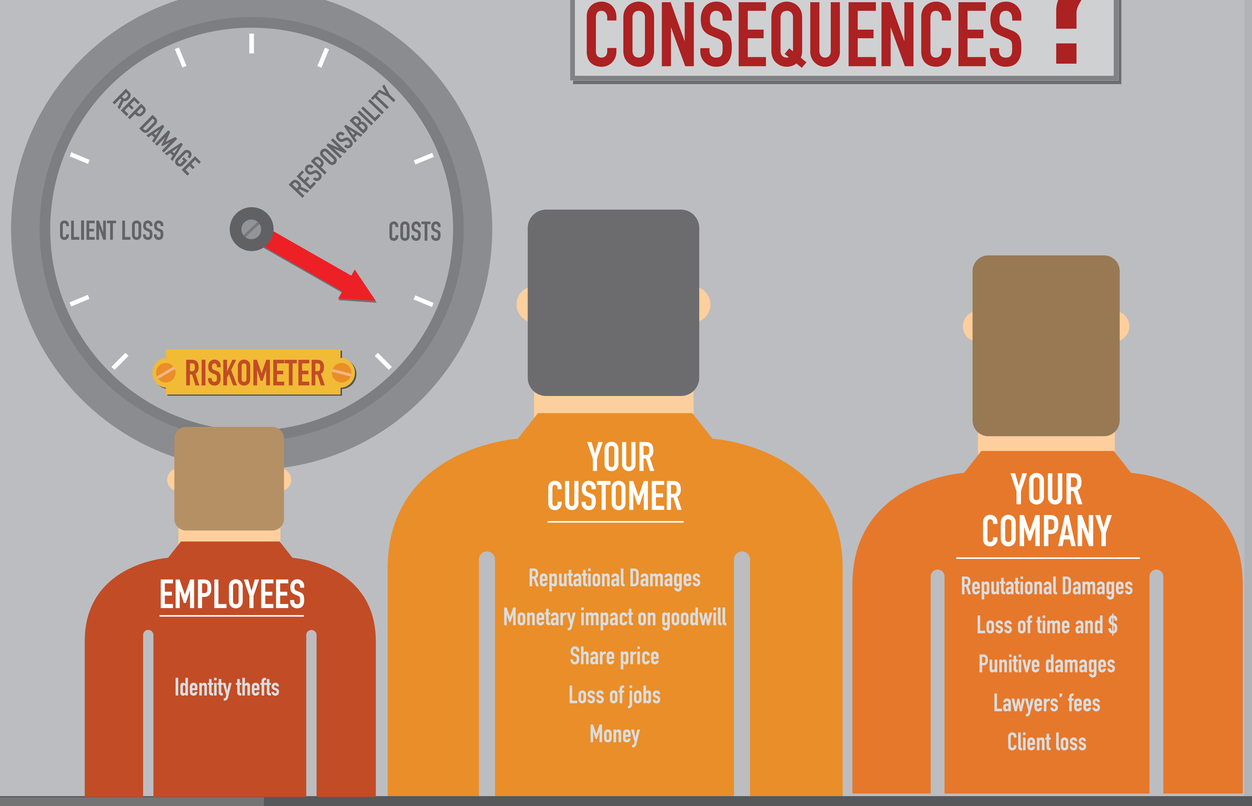
51% FOR EMPLOYEES WHO TAKE CUSTOMER DATA WITH THEM AFTER THEY LEAVE, **CUSTOMER DATA AND INTERNAL DATABASES ARE THE PRIMARY TARGETS** 51% OF THE TIME.

72% OF THOSE SURVEYED SAID THAT STOLEN INTERNAL CORPORATE DATA COULD BE HELPFUL IN THEIR FUTURE CAREERS.

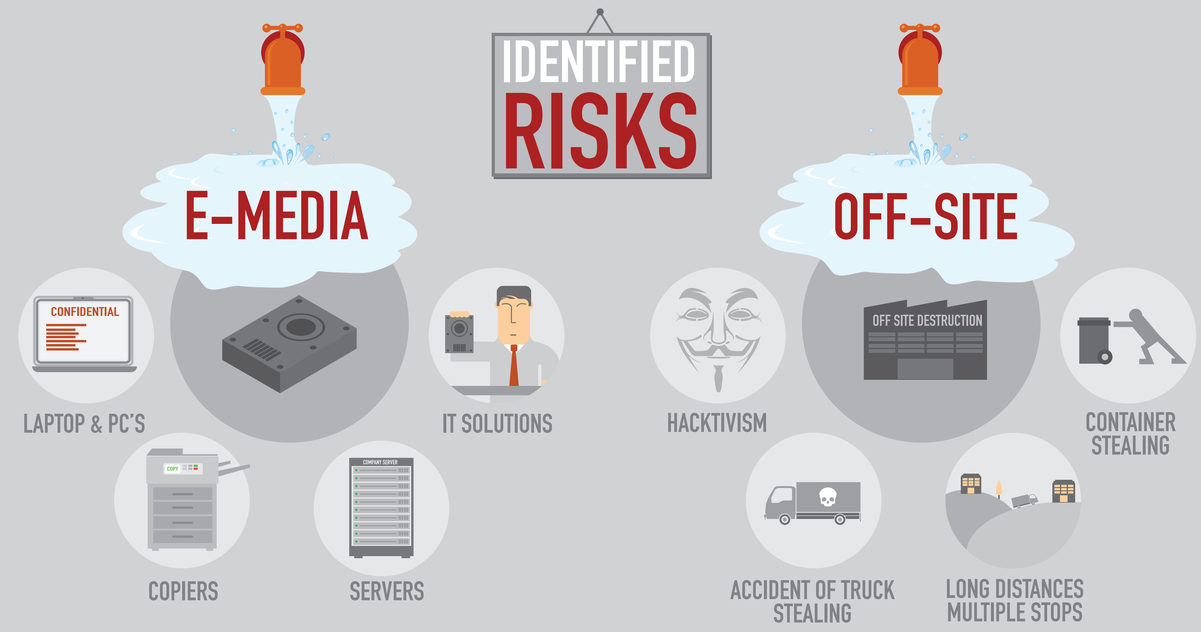
31% OF THOSE SURVEYED WOULD THAT **THEY WOULD RETALIATE TO A DISMISSAL BY DELIBERATELY STEALING** AND/OR SHARING SENSITIVE CORPORATE DATA

2500 TRUCK THEFT IN 2012.

WHAT ARE THE CONSEQUENCES?



IDENTIFIED RISKS



CONCLUSION

WHILE SEEKING AN OUTSOURCING SOLUTION FOR THE DESTRUCTION OF CONFIDENTIAL INFORMATION, WHETHER IN THE FORM OF IT SUPPORT SUCH AS HARD DRIVES OR PAPER SOURCES, THE WHOLE SYSTEM AND PROCESS SHOULD BE ANALYZED RATHER THAN ONLY THE FINAL OUTCOME.

AS WE CAN SEE FROM THE ABOVE INFOGRAPHICS, RISKS CAN OCCUR ALL ALONG THE PROCESS. THIS IS WHY IT IS CRUCIAL TO LIMIT TRANSPORT AND DESTRUCTION RELATED TASKS. PHYSICAL CONFIDENTIAL ON-SITE DESTRUCTION ALLOWS FOR ALL THE ADVANTAGES OF OUTSOURCING WITHOUT THE RISKS!

KATANA

SOURCES

PWC 10 minutes – Information for destruction theft
Fortune magazine – Who are the hackers
PWC – Key findings from the global state of information security, survey 2013
Ponemon institute
RTS documentaire sur vol de copieurs
Tribune de Genève du 23.2.2013
Admin.ch statistiques sur vol de véhicule